AWS Compliance
CIS AWS Foundations Benchmark

Quick Start Reference Deployment

December 2017
Last updated: August 2018 (see revisions)

Accenture
Amazon Web Services (AWS)

Contents

Overview..................................................................................................................................................2
CIS Security Software Certification........................................................................................................3
Costs and Licenses......................................................................................................................................3
Architecture..............................................................................................................................................3
AWS Components......................................................................................................................................3
Design ......................................................................................................................................................4
Prerequisites .............................................................................................................................................6
Specialized Knowledge ............................................................................................................................6
CloudTrail and AWS Config Options .......................................................................................................6
Deployment Steps .....................................................................................................................................7
  Step 1. Prepare Your AWS Account.........................................................................................................7
  Step 2. Launch the Quick Start ..............................................................................................................8
  Step 3. Test the Deployment ................................................................................................................10
Deleting the Stack ....................................................................................................................................14
This Quick Start deployment guide was created by Accenture, an AWS Premier Consulting Partner, in collaboration with Amazon Web Services (AWS).

**Quick Starts** are automated reference deployments that use AWS CloudFormation templates to launch, configure, and run the AWS services required to deploy workloads on AWS, following AWS best practices.

**Overview**

This Quick Start reference deployment guide provides step-by-step instructions for deploying the Center for Internet Security (CIS) Benchmark for AWS Foundations on the AWS Cloud.

**CIS Benchmarks** are consensus-based configuration guidelines developed by experts in US government, business, industry, and academic institutions to help organizations assess and improve their security.

This Quick Start implements the CIS AWS Foundations Benchmark, which is a set of security configuration best practices for hardening AWS accounts, and provides continuous monitoring capabilities for these security configurations. These industry-accepted best practices provide AWS users with clear, step-by-step implementation and assessment procedures. The goal of this Quick Start is to make the implementation of core AWS security measures straightforward for security teams and AWS account owners.

The Quick Start creates security configurations within your AWS account by creating AWS Config rules, Amazon CloudWatch alarms, and CloudWatch Events rules. It also configures AWS CloudTrail and AWS Config, if you customize parameter settings when you launch the Quick Start.

If you’re new to AWS, you can use the Quick Start to easily build foundational security into your AWS account. If you’re already familiar with the AWS Cloud and services, you can use the Quick Start to deploy an environment to serve as the starting point for your customizations.
To see how CIS controls map to Quick Start components and configuration, view the security controls matrix (Microsoft Excel spreadsheet) provided with this Quick Start.

For more information about the recommendations implemented by this Quick Start, see the CIS AWS Foundations Benchmark specification.

CIS Security Software Certification

AWS is a CIS Security Benchmarks Member company. This Quick Start has been awarded CIS Security Software Certification for the following CIS Benchmarks:

- CIS Benchmark for Amazon Web Services Foundations Benchmark v1.2.0 Level 1
- CIS Benchmark for Amazon Web Services Foundations Benchmark v1.2.0 Level 2

For more information, see the AWS certifications page on the CIS website.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Architecture

AWS Components

The core AWS components used by this Quick Start include the following AWS services.

Infrastructure

- **Amazon Cloudwatch** – CloudWatch is a monitoring service for AWS Cloud resources and the applications you run on AWS. CloudWatch lets you to collect and track metrics, log files, and automatically react to changes in your AWS resources.

- **AWS CloudTrail** – CloudTrail enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain events related to API calls across your AWS infrastructure.
- **AWS Config** – AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. AWS Config provides you with the ability to define rules for provisioning and configuring AWS resources.

- **AWS Lambda** – Lambda is used to run code without provisioning or managing servers. You can set up your code to automatically trigger from other AWS services or call Lambda directly from your apps.

- **IAM** – AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. With IAM, you can manage users, security credentials such as access keys, and permissions that control which AWS resources users can access, from a central location.

**Storage**

- **Amazon S3** – Amazon Simple Storage Service (Amazon S3) provides a secure and scalable repository for your data, and is closely integrated with other AWS services for post-processing and analytics. This Quick Start uses Amazon S3 to store data in its original format.

**Messaging**

- **Amazon SNS** – Amazon Simple Notification Service (Amazon SNS) is a publish/subscribe (pub/sub) messaging service for coordinating the delivery of messages to subscribing endpoints and clients.

**Design**

Deploying this Quick Start by choosing to configure AWS CloudTrail and AWS Config builds the environment shown in Figure 1 in your AWS account. You are responsible for further securing the EC2 instances and applications you deploy into the foundational environment built by the Quick Start. Amazon Inspector provides several CIS Certified rules packages to help establish secure configuration postures for various operating systems. CIS also publishes hardened Amazon Machine Images (AMIs) in AWS Marketplace.
The Quick Start sets up the following:

- **AWS Config rules** – A few CIS Benchmark controls are implemented as custom AWS Config rules, which are backed by a Lambda function, and AWS managed rules. To review these controls and their implementations, see the security controls matrix.

- **CloudWatch alarms** – Continuous monitoring for some of the CIS controls is implemented using a combination of CloudWatch alarms and custom log metric filters. To review these controls and their implementations, see the security controls matrix.

- **CloudWatch Events** – Continuous monitoring for some of the CIS controls is implemented using CloudWatch Events rules. To review these controls and their implementations, see the security controls matrix.
• **Lambda functions** – All custom AWS Config and CloudWatch Events rules are backed by Lambda functions that implement the relevant CIS security control, and either report compliance status or notify the end user of a security configuration change.

• **CloudTrail** – The CloudWatch Events rules and alarms depend on CloudTrail for change tracking and reporting continuous compliance. The Quick Start provides an option for configuring CloudTrail. The Quick Start also includes a pre-condition check to verify if CloudTrail is configured in your AWS account before it implements the security configurations for all the CIS controls.

• **AWS Config** – Both the custom AWS Config rules and AWS managed rules depend on the AWS Config service to be configured. The Quick Start provides an option for configuring AWS Config. The Quick Start also includes a pre-condition check to verify if AWS Config is configured in your AWS account before it implements the security configurations for all the CIS controls.

**Prerequisites**

**Specialized Knowledge**

Before you deploy this Quick Start, we recommend that you become familiar with the AWS services listed in the previous section by following the provided links. (If you are new to AWS, see the [Getting Started Resource Center](#).)

**CloudTrail and AWS Config Options**

When you launch the Quick Start, you will be able to set two parameters to specify how you want to handle CloudTrail and AWS Config. The following table explains how these parameter settings affect the configuration of these services in your account.

<table>
<thead>
<tr>
<th>To Use your existing CloudTrail and AWS Config settings</th>
<th>Set the ConfigureCloudTrail parameter to</th>
<th>Set the ConfigureConfig parameter to</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use your existing CloudTrail and AWS Config settings</td>
<td>No (default)</td>
<td>No (default)</td>
<td>Deployment fails if these parameters are set to No, but CloudTrail and AWS Config haven’t been configured correctly in your account.</td>
</tr>
<tr>
<td>Create or reconfigure your CloudTrail and AWS Config settings</td>
<td>Yes</td>
<td>Yes</td>
<td>Use these settings for new AWS accounts, or if you want to reconfigure your existing settings. If you have CloudTrail and AWS Config already set up, the Quick Start will create a new trail, and will delete and recreate the AWS Config delivery channel and the configuration recorder.</td>
</tr>
</tbody>
</table>

|
If you’re planning to keep the default settings for the CloudTrail and AWS Config parameters, you must make sure that these two services are configured correctly in the AWS Region you’ve selected for the deployment:

1. Turn on and set up AWS Config. Open the AWS Config console at https://console.aws.amazon.com/config/, and choose Get Started Now. For more information about configuring AWS Config, follow steps 1 through 8 in the AWS documentation.

2. Turn on and set up CloudTrail. Open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/home/, and configure your trail to deliver events to CloudWatch Logs by following the instructions in the AWS documentation.

Note The CIS AWS Foundations Benchmark requires AWS CloudTrail and AWS Config to be enabled in all AWS Regions. The Quick Start supports only one region per deployment, so we recommend that you launch the Quick Start multiple times, changing the deployment region for each launch. Make sure to turn on and set up AWS Config and CloudTrail for each region, and use the configuration parameters to use your existing settings or reconfigure settings, as described earlier in this section.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don’t already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.

2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy CIS AWS Foundations Benchmark on AWS.

Note The CIS AWS Foundations Benchmark requires AWS CloudTrail and AWS Config to be enabled in all AWS Regions. The Quick Start supports only one region per deployment, so we recommend that you launch the Quick Start multiple times, changing the deployment region for each launch. Make sure to turn on and set up AWS Config and CloudTrail for each region, and use the configuration parameters to use your existing settings or reconfigure settings, as described in the Prerequisites section.
Step 2. Launch the Quick Start

**Note**  You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. **Launch the AWS CloudFormation template** into your AWS account.

   The template will be deployed into the AWS Region that appears in the navigation bar at the upper-right corner of the AWS Management Console. You can change the region by using the region selector in the navigation bar. The template is launched in the US East (Ohio) Region by default.

   If you have an AWS GovCloud (US) account, you can launch the template in the AWS GovCloud (US) Region.

   The stacks take approximately 10 minutes to create.

2. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

3. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. These are described in the following table. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

   **Note**  You can also **download the main template** and edit it to create your own parameters based on your specific deployment scenario.

   ---

   **CIS Benchmark Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Level</strong> (ProfileLevel)</td>
<td>Level 2</td>
<td>Configuration profile to use for the deployment. The Level 1 profile represent baseline governance controls, whereas the Level 2 profile (recommended) represents redundant or stricter governance controls. For guidance, see the control list in the [CIS AWS Foundations Benchmark specification](<a href="https://docs.aws.amazon.com/cis/latest/guidance/cis">https://docs.aws.amazon.com/cis/latest/guidance/cis</a> AWS Foundations Benchmark specification).</td>
</tr>
<tr>
<td><strong>Notification Address</strong></td>
<td>Requires input</td>
<td>Email address that will be subscribed to the Amazon SNS topic for CloudWatch alarms and rules. A subscription confirmation message will be sent to this email address.</td>
</tr>
</tbody>
</table>
**Configure AWS CloudTrail and AWS Config (Optional):**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure CloudTrail?</td>
<td>No</td>
<td>Select <strong>Yes</strong> if you want the Quick Start to configure CloudTrail in your AWS account. For more information, see the <a href="#">CloudTrail and AWS Config Options</a> section.</td>
</tr>
<tr>
<td>Configure AWS Config?</td>
<td>No</td>
<td>Select <strong>Yes</strong> if you want the Quick Start to configure AWS Config. For more information, see the <a href="#">CloudTrail and AWS Config Options</a> section.</td>
</tr>
</tbody>
</table>

**AWS Quick Start Configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 Bucket Name</td>
<td>aws-quickstart</td>
<td>S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you’ve created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.</td>
</tr>
<tr>
<td>Quick Start S3 Key Prefix</td>
<td>quickstart-compliance-cis-benchmark/</td>
<td>The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.</td>
</tr>
</tbody>
</table>

4. On the **Options** page, you can [specify tags](#) (key-value pairs) for resources in your stack and [set advanced options](#). When you’re done, choose **Next**.

5. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.

6. Choose **Create** to deploy the stack.

7. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, as shown in Figure 2, the CIS benchmark security configuration is ready.

---

**Figure 2: Deployment status**
Step 3. Test the Deployment

1. When the Quick Start deployment has completed successfully, you’ll receive an email at the notification address you provided in step 2 to confirm a subscription to the Amazon SNS topic created by the Quick Start. Choose the **Confirm subscription** link in the message to subscribe to email that is sent whenever a security configuration change occurs within your AWS account.

![AWS Notification - Subscription Confirmation](image)

**Figure 3: Subscription confirmation**

2. Navigate to the CloudWatch console at [https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/) and choose **Alarms**. You should see the following alarms listed.

![CloudWatch alarms](image)

**Figure 4: CloudWatch alarms**

When the alarm metric condition breaches the threshold defined, you will be sent email. For example, you will receive an email whenever either a root user or an IAM user logs in to the console without a multi-factor authentication (MFA) token.

3. Navigate to the CloudWatch console and choose **Logs**. Choose the filter that lists “5 filters.” You should see CloudWatch Logs filters that match the five CloudWatch alarms.
4. Navigate to the CloudWatch console. Under **Events**, choose **Rules**. You should see the following rules listed.

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CIS-DetectCloudTrailChanges</td>
<td>Publishes formatted CloudTrail change events to an SNS topic</td>
</tr>
<tr>
<td></td>
<td>CIS-DetectConfigChanges</td>
<td>Publishes formatted Config change events to an SNS topic</td>
</tr>
<tr>
<td></td>
<td>CIS-DetectIAMPolicyChanges</td>
<td>Publishes formatted IAM policy change events to an SNS topic</td>
</tr>
<tr>
<td></td>
<td>CIS-DetectNetworkAclChanges</td>
<td>Publishes formatted network ACL change events to an SNS topic</td>
</tr>
<tr>
<td></td>
<td>CIS-DetectNetworkChangeEvents</td>
<td>Publishes formatted network change events to an SNS topic</td>
</tr>
<tr>
<td></td>
<td>CIS-DetectS3BucketPolicyChanges</td>
<td>Publishes formatted S3 bucket policy change events to an SNS topic</td>
</tr>
<tr>
<td></td>
<td>CIS-DetectSecurityGroupChanges</td>
<td>Publishes formatted security group change events to an SNS topic</td>
</tr>
</tbody>
</table>

5. Navigate to AWS Config console at [https://console.aws.amazon.com/config/](https://console.aws.amazon.com/config/) and choose **Rules**. You should see AWS Config rules listed, as shown in Figure 7 (not all rules are shown).
You will notice that the AWS Config rules have started to report the compliance status of each CIS control. For guidance on resolving non-compliance issues, see the security controls matrix.

6. Navigate to the AWS Lambda console at https://console.aws.amazon.com/lambda and choose Functions. You should see a list of functions, as shown in Figure 8.
Now that you’ve deployed and tested the CIS AWS Foundations Benchmark on AWS, please take a few minutes to complete our survey for this Quick Start. Your response is anonymous and will help us improve AWS compliance reference deployments.

If you have further questions or need assistance regarding this Quick Start, please email compliance-accelerator@amazon.com.

Deleting the Stack

When you have finished using the resources created by this Quick Start, you can delete the stack. Deleting a stack, either by using the command line interface (CLI) or through the AWS CloudFormation console, will remove all the resources created by the template for the stack. The only exceptions are S3 buckets and customer master keys (CMKs).

- **S3 buckets**: Remember to delete any S3 buckets created by the AWS CloudFormation deployment as they are not deleted upon stack deletion. If you do not delete the buckets, you will incur Amazon S3 storage costs.

- **AWS Key Management Service (AWS KMS) keys**: When you delete the stack, AWS KMS enforces a waiting period before it deletes the CMKs. It puts these keys in a pending deletion status, and you can schedule a waiting period of 7-30 days, after which the keys will be deleted. The maximum waiting period is 30 days. For more information about deleting CMKs, see the AWS documentation.

Troubleshooting

**Q.** I encountered a CREATE_FAILED error when I launched the Quick Start.

**A.** If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with Rollback on failure set to No. (This setting is under Advanced in the AWS CloudFormation console, Options page.) With this setting, the stack’s state will be retained, so you can troubleshoot the issue.

**Important** When you set Rollback on failure to No, you’ll continue to incur AWS charges for this stack. Please make sure to delete the stack when you’ve finished troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.
The most common reasons for stack creation to fail are CloudTrail and AWS Config configuration issues. In order to help you troubleshoot this issue, the Quick Start template logs errors into CloudWatch Logs, as shown in Figure 9.

![Figure 9: Stack creation errors](image)

Navigate to the CloudWatch console at [https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/), choose Logs, and search for the log group `/aws/lambda/CIS-EvaluateCISBenchmarkPreconditions`. Under this log group, you can find errors associated with the configuration of CloudTrail or AWS Config.

Figure 10 shows possible error messages. These configuration issues need to be fixed for the stack creation to be successful.

![Figure 10: Error messages associated with pre-condition checks](image)
Q. I encountered a size limitation error when I deployed the AWS Cloudformation templates.

A. We recommend that you launch the Quick Start templates from the location we’ve provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Additional Resources

AWS services

- Amazon CloudWatch
  - Using Amazon CloudWatch Metrics

- Amazon EC2
  - Amazon EC2 Security Groups for Linux Instances

- Amazon S3

- Amazon SNS
  https://aws.amazon.com/documentation/sns/

- Amazon VPC
  - VPC Flow Logs

- AWS Billing and Cost Management
  - What is AWS Billing and Cost Management?
    https://docs.aws.amazon.com/awssaccountbilling/latest/aboutv2/billing-what-is.html
  - Managing an AWS Account: Editing Contact Information
    https://docs.aws.amazon.com/awssaccountbilling/latest/aboutv2/manage-account-payment.html#contact-info
Billing and Cost Management Policy Examples
https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-permissions-ref.html#billing-example-policies

AWS CloudFormation
https://aws.amazon.com/documentation/cloudformation/

AWS CloudTrail
- Encrypting CloudTrail Log Files with AWS KMS-Managed Keys (SSE-KMS)
- Enabling Log File Integrity Validation for CloudTrail

AWS Config
https://aws.amazon.com/documentation/config/

AWS security credentials
- Managing Access Keys for Your AWS Account
  http://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html
- Best Practices for Managing AWS Access Keys

IAM
- IAM Best Practices
- Managed Policies and Inline Policies
- IAM Roles for Amazon EC2
- Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances
- Actions and Condition Context Keys for IAM

- Using MFA in AWS

- Configuring MFA-Protected API Access

- Enabling a Virtual MFA Device

- AWS CLI command reference for iam
  http://docs.aws.amazon.com/cli/latest/reference/iam/index.html#cli-aws-iam

- AWS CLI command reference for list-policies
  http://docs.aws.amazon.com/cli/latest/reference/iam/list-policies.html

- AWS CLI command reference for attach-role-policy

- AWS CLI command reference for list-entities-for-policy
  http://docs.aws.amazon.com/cli/latest/reference/iam/list-entities-for-policy.html

- AWS KMS
  - Creating Keys
    http://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html

- AWS Lambda
  https://aws.amazon.com/documentation/lambda/

CIS Benchmarks and CIS AWS Foundations Benchmark

- CIS Benchmarks
  https://www.cisecurity.org/partner/amazon-web-services/

- CIS AWS Foundations Benchmark
  https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/
GitHub Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

The GitHub repository for this Quick Start includes the following directories:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assets</td>
<td>Security controls matrix, architecture diagrams</td>
</tr>
<tr>
<td>templates</td>
<td>AWS CloudFormation template files for deployment</td>
</tr>
<tr>
<td>submodules</td>
<td>Scripts and sub-templates used by the Quick Start templates</td>
</tr>
</tbody>
</table>

Document Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2018</td>
<td>Added information about CIS Security Software Certification awarded to this Quick Start</td>
<td>CIS Security Software Certification</td>
</tr>
<tr>
<td>July 2018</td>
<td>Updated for CIS Benchmark version 1.2</td>
<td>Changes in templates, matrix, and Figures 7 and 8</td>
</tr>
<tr>
<td>December 2017</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>
© 2018, Amazon Web Services, Inc. or its affiliates, and Accenture. All rights reserved.

**Notices**

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS 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.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at [http://aws.amazon.com/apache2.0/](http://aws.amazon.com/apache2.0/) or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.