Reference Architecture for HIPAA on the AWS Cloud

Quick Start Reference Deployment

AWS Envision Engineering
AWS Professional Services
AWS Quick Start Reference Team

February 2017
(last update: August 2017)

This guide is also available in HTML format at https://docs.aws.amazon.com/quickstart/latest/compliance-hipaa/.

Contents

About This Guide

This Quick Start reference deployment guide discusses architectural considerations and steps for deploying security-focused baseline environments on the Amazon Web Services (AWS) Cloud. Specifically, this Quick Start deploys a model environment that can help organizations with workloads that fall within the scope of the U.S. Health Insurance Portability and Accountability Act (HIPAA). The Quick Start addresses certain technical requirements in the Privacy, Security, and Breach Notification Rules under the HIPAA Administrative Simplification Regulations (45 C.F.R. Parts 160 and 164). The deployment guide includes links for viewing and launching AWS CloudFormation templates that automate the deployment.

This Quick Start is part of a set of AWS compliance offerings, which provide security-focused architecture solutions to help Managed Service Providers (MSPs), cloud provisioning teams, developers, integrators, and information security teams follow strict security, compliance, and risk management controls. For additional Quick Starts in this category, see the Quick Start catalog.

IMPORTANT: PLEASE READ

You must have an AWS Business Associate Addendum (BAA) in place, and follow its configuration requirements, before running protected health information (PHI) workloads on AWS. You should not use your AWS account in connection with PHI until you have accepted the AWS BAA and configured your AWS account(s) as required by the AWS BAA. Under HIPAA regulations, covered entities and business associates are responsible for putting in place a business associate agreement between themselves and each of their business associates. You are solely responsible for determining whether you and your organization need a business associate agreement with AWS. **If you determine you need a business associate agreement with AWS, you can accept the AWS BAA through a self-service portal in AWS Artifact.** It is your responsibility to obtain a BAA from AWS. For more information about the AWS BAA, please visit the AWS HIPAA Compliance webpage.

This Quick Start does not address state-specific laws that may apply to you. This Quick Start only addresses requirements set forth under HIPAA, a U.S. federal law. Many individual states have adopted rules that are different and in some cases, stricter than those that are federally mandated under HIPAA.

This Quick Start will not, by itself, make you HIPAA-compliant. The information contained in this Quick Start package is not exhaustive, and must be reviewed, evaluated, assessed, and approved by you in connection with your organization's particular security features, tools, and configurations. The security controls reference document included with this Quick Start explains how this Quick Start can be used to help support your compliance with certain requirements under the HIPAA Privacy and Security Rules. **However, it is the sole responsibility of you and your organization to determine which HIPAA regulatory requirements are applicable to you, and to ensure that you comply with those applicable requirements**. Importantly, most of the requirements under HIPAA are not technical but administrative (that is, people- and process-oriented). Although the security controls reference that is included with this Quick Start lists and discusses both the technical and administrative requirements, this Quick Start cannot help you comply with the non-technical HIPAA requirements.

Does HIPAA Apply to Your Organization?

Customers are solely responsible for determining whether HIPAA applies to them, and if so, for complying with their obligations under HIPAA, the AWS BAA, and all other applicable laws, rules, and regulations. AWS does not provide legal or compliance advice. Customers should consult with qualified legal counsel or consultants, as needed, to ensure that their use of AWS complies with HIPAA, the terms of the AWS BAA, and other applicable laws, rules, and regulations.

Quick Links

If you have an AWS account that already meets the technical requirements for this Quick Start deployment, you can launch the Quick Start to build the architecture shown in Figure 2. The template is launched in the US East (N. Virginia) Region by default. If you have an AWS GovCloud (US) account, you can launch the template in the AWS GovCloud (US) Region.

Launch Quick Start

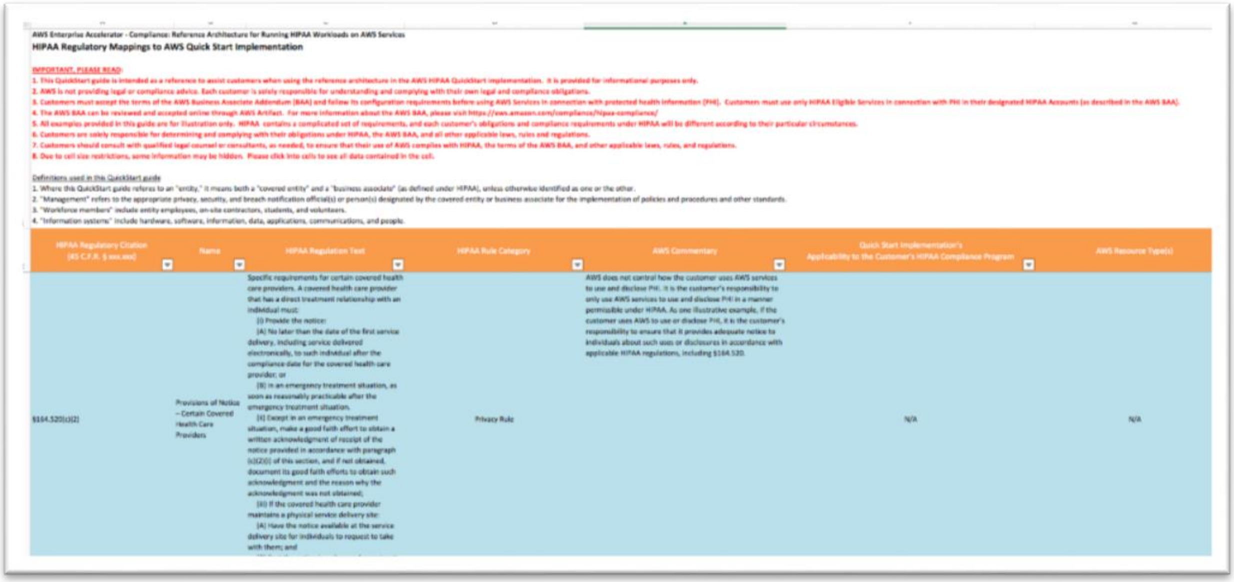
The deployment takes approximately 30 minutes. If you're new to AWS or to configuring architectures for HIPAA workloads on AWS, please read the overview and follow the detailed pre-deployment and deployment steps described in this guide.

If you want to take a look under the covers, you can view the main template that automates this deployment. The main template includes references to child templates, and provides default settings that you can customize by following the instructions in this guide. For descriptions of the templates and guidance for using the nested templates separately, see the Templates Used in this Quick Start section of this guide.

View main template

To see how HIPAA regulatory requirements map to Quick Start architecture decisions, components, and configurations, view the security controls reference (Microsoft Excel spreadsheet). The excerpt in Figure 1 provides a sample of the available information.

View security controls reference



AWS Enterprise Accelerator - Compliance: Reference Architecture for Running HIPAA Workloads on AWS Services

HIPAA Regulatory Mappings to AWS Quick Start Implementation

IMPORTANT, PLEASE READ:

1. This QuickStart guide is intended as a reference to assist customers when using the reference architecture in the AWS HIPAA QuickStart implementation. It is provided for informational purposes only.
2. AWS is not providing legal or compliance advice. Each customer is solely responsible for understanding and complying with their own legal and compliance obligations.
3. Customers must accept the terms of the AWS Business Associate Addendum (BAA) and follow its configuration requirements before using AWS Services in connection with protected health information (PHI). Customers must use only HIPAA Eligible Services in connection with PHI in their designated HIPAA Accounts (as described in the AWS BAA).
4. The AWS BAA can be reviewed and accepted online through AWS Artifact. For more information about the AWS BAA, please visit https://aws.amazon.com/compliance/hipaa-compliance/
5. All examples provided in this guide are for illustration only. HIPAA contains a complicated set of requirements, and each customer's obligations and compliance requirements under HIPAA will be different according to their particular circumstances.
6. Customers are solely responsible for determining and complying with their obligations under HIPAA, the AWS BAA, and all other applicable laws, rules and regulations.
7. Customers should consult with qualified legal counsel or consultants, as needed, to ensure that their use of AWS complies with HIPAA, the terms of the AWS BAA, and other applicable laws, rules, and regulations.
8. Due to cell size restrictions, some information may be hidden. Please click into cells to see all data contained in the cell.

Definitions used in this QuickStart guide

1. Where this QuickStart guide referes to an "entity," it means both a "covered entity" and a "business associate" (as defined under HIPAA), unless otherwise identified as one or the other.
2. "Management" refers to the appropriate privacy, security, and breach notification official(s) or person(s) designated by the covered entity or business associate for the implementation of policies and procedures and other standards.
3. "Workforce members" include entity employees, on-site contractors, students, and volunteers.
4. "Information systems" include hardware, software, information, data, applications, communications, and people.

HIPAA Regulatory Citation (45 C.F.R. § xxx.xxx)	Name	HIPAA Regulation Text	HIPAA Rule Category	AWS Commentary	Quick Start Implementation's Applicability to the Customer's HIPAA Compliance Program	AWS Resource Type(s)
§164.520(c)(2)	Provisions of Notice – Certain Covered Health Care Providers	Specific requirements for certain covered health care providers. A covered health care provider that has a direct treatment relationship with an individual must: (i) Provide the notice: (A) No later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the covered health care provider; or (B) In an emergency treatment situation, as soon as reasonably practicable after the emergency treatment situation. (ii) Except in an emergency treatment situation, make a good faith effort to obtain a written acknowledgment of receipt of the notice provided in accordance with paragraph (c)(2)(i) of this section, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained; (iii) If the covered health care provider maintains a physical service delivery site: (A) Have the notice available at the service delivery site for individuals to request to take with them; and	Privacy Rule	AWS does not control how the customer uses AWS services to use and disclose PHI. It is the customer's responsibility to only use AWS services to use and disclose PHI in a manner permissible under HIPAA. As one illustrative example, if the customer uses AWS to use or disclose PHI, it is the customer's responsibility to ensure that it provides adequate notice to individuals about such uses or disclosures in accordance with applicable HIPAA regulations, including §164.520.	N/A	N/A

Figure 1: Excerpt from the HIPAA security controls reference

We'd like your feedback After you deploy this Quick Start, please take a few minutes to fill out our survey. Your response is anonymous and will help us improve this and other compliance-related reference deployments.

About Quick Starts

Quick Starts are automated reference deployments for key workloads on the AWS Cloud. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

Overview

AWS Compliance Architectures

AWS compliance solutions help streamline, automate, and implement secure baselines in AWS—from initial design to operational security readiness. They incorporate the expertise of AWS solutions architects, security, and compliance personnel to help you build a secure and reliable architecture easily through automation.

This Quick Start includes AWS CloudFormation templates, which can be integrated with AWS Service Catalog, to automate building a baseline architecture that fits within your organization's larger HIPAA compliance program. It also includes a security controls reference, which maps HIPAA regulatory requirements to architecture decisions, features, and configuration of the baseline.

Architecture for HIPAA on AWS

Deploying this Quick Start builds a multi-tier, Linux-based web application in the AWS Cloud. Figures 2 and 3 illustrate the architecture.

Note You can also download these diagrams in Microsoft PowerPoint format, and edit the icons to reflect your specific workload.

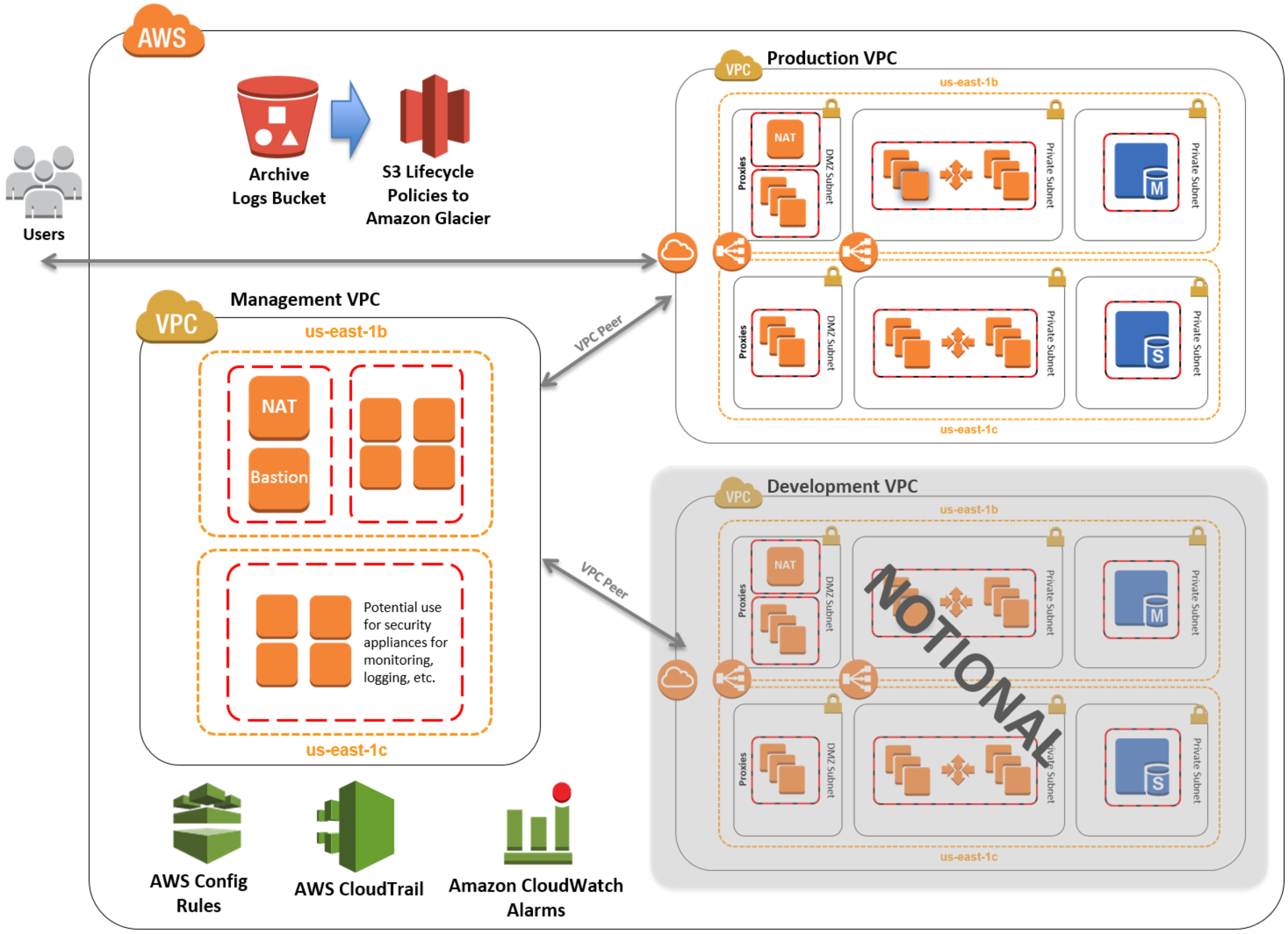


Figure 2: Standard three-tier web architecture for HIPAA on AWS depicting integration with multiple VPCs (notional development VPC shown)

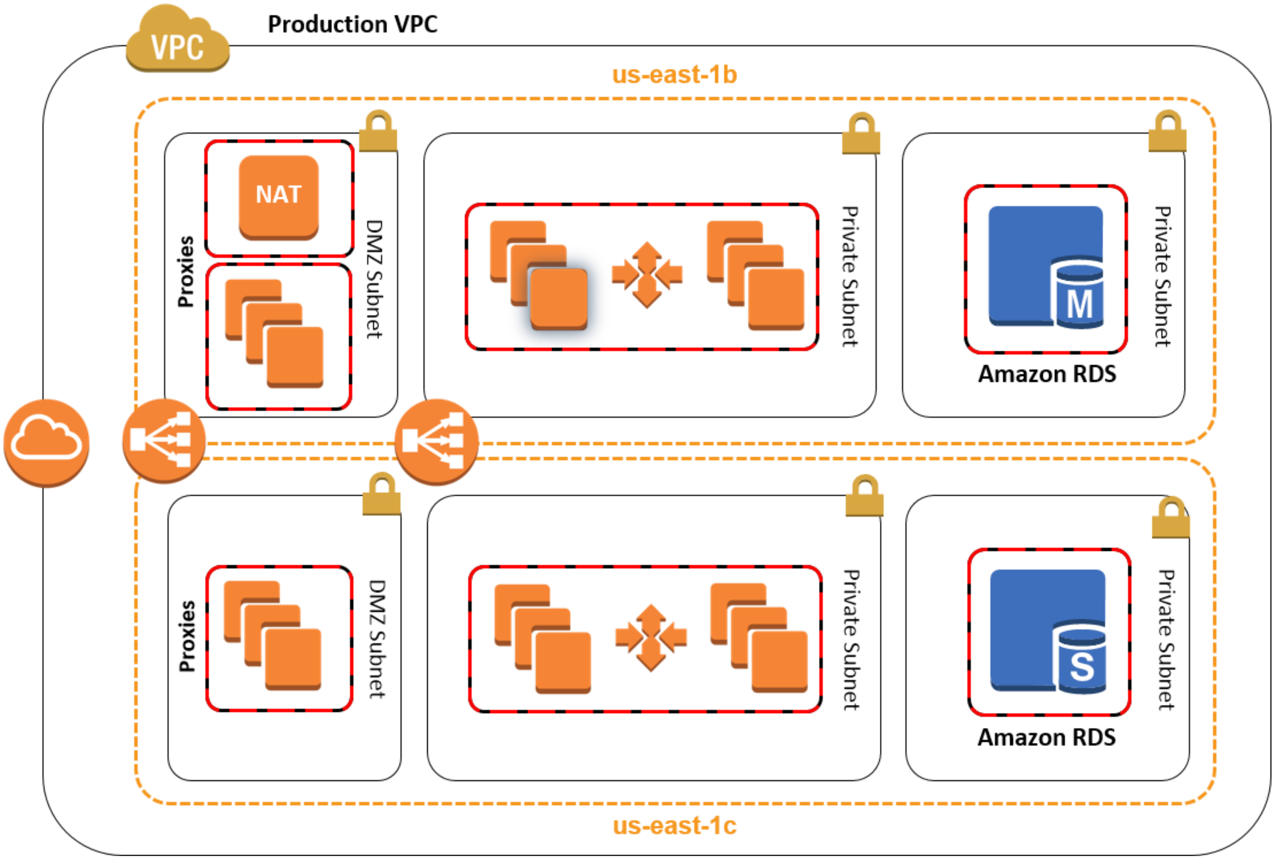


Figure 3: Production VPC design for HIPAA on AWS

The sample architecture includes the following components and features:

- Basic AWS Identity and Access Management (IAM) configuration with custom IAM policies, with associated groups, roles, and instance profiles
- Standard, external-facing Amazon Virtual Private Cloud (Amazon VPC) Multi-AZ architecture with separate subnets for different application tiers and private (back-end) subnets for application and database
- Amazon Simple Storage Service (Amazon S3) buckets for encrypted web content, logging, and backup data
- Standard Amazon VPC security groups for Amazon Elastic Compute Cloud (Amazon EC2) instances and load balancers used in the sample application stack
- Three-tier Linux web application using Auto Scaling and Elastic Load Balancing, which can be modified and/or bootstrapped with customer application
- A secured bastion login host to facilitate command-line Secure Shell (SSH) access to Amazon EC2 instances for troubleshooting and systems administration activities

- Encrypted, Multi-AZ Amazon Relational Database Service (Amazon RDS) MySQL database
- Logging, monitoring, and alerts using AWS CloudTrail, Amazon CloudWatch, and AWS Config rules
- Encrypted secondary EBS volumes on all EC2 instances

AWS Services

The core AWS components used by this Quick Start include the following AWS services. (If you are new to AWS, see the Getting Started with AWS.)

- AWS CloudTrail – AWS CloudTrail records AWS API calls and delivers log files that include caller identity, time, source IP address, request parameters, and response elements. The call history and details provided by CloudTrail enable security analysis, resource change tracking, and compliance auditing.
- Amazon CloudWatch – Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.
- AWS Config – AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config rules enable you to automatically check the configuration of AWS resources recorded by AWS Config.

> **Note** The AWS Config rules feature is currently available in the AWS Regions listed on the AWS Regions and Endpoints webpage.

- Amazon EBS – Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. Amazon EBS volumes provide the consistent and low-latency performance needed to run your workloads.
- Amazon EC2 – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.

- Elastic Load Balancing – Elastic Load Balancing automatically distributes traffic across multiple EC2 instances, to help achieve better fault tolerance and availability.
- Amazon Glacier – Amazon Glacier is a storage service for archiving and long-term backup of infrequently used data. It provides secure, durable, and extremely low-cost storage, supports data transfer over SSL, and automatically encrypts data at rest. With Amazon Glacier, you can store your data for months, years, or even decades at a very low cost.
- Amazon RDS – Amazon Relational Database Service (Amazon RDS) enables you to set up, operate, and scale a relational database in the AWS Cloud. It also handles many database management tasks, such as database backups, software patching, automatic failure detection, and recovery, for database products such as MySQL, MariaDB, PostgreSQL, Oracle, Microsoft SQL Server, and Amazon Aurora. This Quick Start includes a MySQL database by default.
- Amazon VPC – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, logically isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

HIPAA Eligible Services

You must process, store, and transmit protected health information (PHI) using only HIPAA Eligible Services, as defined in the AWS BAA. The most current list of HIPAA Eligible Services can be found at https://aws.amazon.com/compliance/hipaa-eligible-services-reference/. You may use the full range of AWS services with non-PHI data, even in a HIPAA Account under the AWS BAA.

Best Practices

The architecture built by this Quick Start supports AWS best practices for high availability and security:

- Multi-AZ architecture intended for high availability
- Isolation of instances between private/public subnets
- Security groups limiting access to only necessary services
- Network access control list (ACL) rules to filter traffic into subnets as an additional layer of network security
- A secured bastion host instance to facilitate restricted login access for system administrator actions
- Standard IAM policies with associated groups and roles, exercising least privilege
- Monitoring and logging; alerts and notifications for critical events
- S3 buckets (with security features enabled) for logging, archive, and application data
- Implementation of proper load balancing and Auto Scaling capabilities
- HTTPS-enabled Elastic Load Balancing (ELB) load balancers with hardened security policy
- Amazon RDS database backup and encryption
- HTTPS to the endpoint. Traffic is carried encrypted to the ELB load balancer, and then sent encrypted to the instance.

How You Can Use This Quick Start

You can use this Quick Start to build an environment that serves as an example for learning, as a prototyping environment, or as a baseline for customization.

Since AWS provides a very mature set of configuration options (and new services are being released all the time), this Quick Start provides security templates that you can use for your own environment. These security templates (in the form of AWS CloudFormation templates) provide a comprehensive rule set that can be systematically enforced. You can use these templates as a starting point and customize them to match your specific use cases.

Cost

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 templates for this Quick Start include 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.

AWS CloudFormation Templates

An AWS CloudFormation template is a JSON (JavaScript Object Notation) or YAML-formatted text file that describes the AWS infrastructure needed to run an application or service along with any interconnections among infrastructure components. You can deploy a template and its associated collection of resources (called a *stack*) by using the AWS Management Console, the AWS Command Line Interface (AWS CLI), or the AWS CloudFormation API. AWS CloudFormation is available at no additional charge, and you pay only for the AWS resources needed to run your applications. Resources can consist of any AWS resource you define within the template. For a complete list of resources that can be defined within an AWS CloudFormation template, see the AWS Resource Types Reference in the AWS documentation.

AWS CloudFormation Stacks

When you use AWS CloudFormation, you manage related resources as a single unit called a stack. In other words, you create, update, and delete a collection of resources by creating, updating, and deleting stacks. All the resources in a stack are defined by the stack's AWS CloudFormation template.

To update resources, you first modify the stack templates and then update the stack by submitting the modified template. You can work with stacks by using the AWS CloudFormation console, AWS CloudFormation API, or AWS CLI.

For more information about AWS CloudFormation and stacks, see Get Started in the AWS CloudFormation documentation.

Templates Used in this Quick Start

This Quick Start uses nested AWS CloudFormation templates to deploy the architecture for a multi-tier, Linux-based web application.

The Quick Start consists of a main template and seven child templates: IAM, logging, production VPC, management VPC, Config rules, NAT instance, and application. These templates are designed to deploy the architecture within stacks that align with AWS best practices and the security compliance framework. The following table describes each template and its dependencies. To view the child templates, see the GitHub repository.

Stack and template	Description	Dependencies
Main stack (main.template — or see GovCloud version)	Primary template file that deploys the rest of the stacks and passes parameters between nested templates automatically.	None
IAM stack (iam.template)	Creates a basic IAM configuration with custom policies, groups, and roles.	None
Logging stack (logging.template)	Sets up baseline AWS Config rules for monitoring. Enables AWS CloudTrail, S3 buckets, and bucket policies for logging and archive data. Creates standard Amazon CloudWatch alarms for security-related CloudTrail events.	None
Production VPC stack (vpc-production.template)	Configures a secure VPC for a public-facing application that includes subnets, NAT instances, route tables, and custom network access control list (network ACL) rules.	None
Management VPC stack (vpc-management.template)	Configures a secure VPC for management functions that support the production VPC, and includes subnets, NAT, route tables, custom network access control list (network ACL) rules, and a restricted, public-facing bastion host to support a secured login path for administrator access.	Production VPC stack
Config rules stack (config-rules.template)	Sets up baseline AWS Config rules for monitoring.	IAM, Production VPC, and Management VPC stacks
NAT instance stack (nat-instance.template)	Conditionally launched by the Management and Production VPC templates to set up EC2 instances for NAT.	None
Application stack (application.template)	Sets up EC2 instances for reverse proxy and web application, an Amazon RDS database, HTTPS Elastic Load Balancing, Amazon CloudWatch alarms, and Auto Scaling groups.	Production VPC stack

The AWS CloudFormation template **main.template** is the entry point for launching the entire architecture, and also allows parameters to be passed into each of the nested stacks. The JSON templates for those nested stacks deploy the resources for the architecture.

To deploy the entire architecture (including IAM and Amazon VPC), use **main.template** when launching the stacks. To deploy the full package, the IAM user must have permissions to deploy the resources each template creates, which includes IAM configuration for groups and roles.

You can also edit **main.template** to customize stacks or to omit stacks to be deployed. This can be useful for provisioning teams who must deploy the initial base architecture in accounts for application owners. For more information about deployment options and use cases, see Deployment Methods.

Additionally, you can deploy each stack independently. However, this requires that you pass individual parameters to each template upon launch, instead of relying on the main template to pass these values automatically.

Managing the Quick Start Source Files

We've provided a GitHub repository for the tools and templates for this Quick Start so you can modify, extend, and customize them to meet your needs. You can also use your own Git or Apache Subversion source code repository, or use AWS CodeCommit. This is recommended to ensure proper version control, developer collaboration, and documentation of updates.

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

assets	Security controls matrix, architecture diagrams, and landing page assets
templates	AWS CloudFormation template files for deployment
submodules	Scripts and sub-templates used by the Quick Start templates

Uploading the Templates to Amazon S3

The Quick Start templates are available in an Amazon S3 bucket for Quick Starts. If you're using your own S3 bucket, you can upload the AWS CloudFormation templates by using the AWS Management Console or the AWS CLI, by following these instructions.

Using the Console

1. Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.
2. Choose a bucket to store the templates in.
3. Choose **Upload** and specify the local location of the file to upload.
4. Upload all template files to the same S3 bucket.

5. Find the template URLs by selecting each template file, and then choosing **Properties**. Make a note of the URLs.

Using the AWS CLI

1. Download the AWS CLI tool from http://aws.amazon.com/cli/.
2. Use the following AWS CLI command to upload each template file:

```
aws s3 cp <template file>.template s3://<s3bucketname>/
```

Updating the Amazon S3 URLs

The template for the main stack lists the Amazon S3 URLs for the nested stacks. If you upload the templates to your own S3 bucket and would like to deploy the templates from there, you must modify the `Resources` section of the **main.template** file.

Planning the Deployment

Prerequisites

AWS Business Associate Addendum

Before you use AWS services with protected health information (PHI), you must accept the AWS Business Associate Addendum (BAA) and ensure that the AWS account(s) you use with PHI are configured as required by the BAA. You do not necessarily have to accept the AWS BAA before deploying this Quick Start (for example, if you deploy it for demo or testing purposes), as long as you do not use the Quick Start with PHI.

Specialized Knowledge

This Quick Start requires a moderate to high level of understanding of HIPAA legal requirements, and the processes needed to achieve and manage HIPAA compliance within a traditional hosting environment. Before you deploy the Quick Start, please review the important notes at the beginning of this guide about customer responsibilities under HIPAA and the AWS BAA.

This Quick Start is designed for Information Technology (IT) professionals and security personnel, and assumes familiarity with basic security concepts in the area of networking, operating systems, data encryption, operational controls, and cloud computing services. If you are new to AWS, visit https://aws.amazon.com/getting-started/ for more information about AWS.

This deployment guide also requires a moderate level of understanding of AWS services and requires the following, at a minimum:

- Access to a current AWS account with IAM administrator-level permissions
- Basic understanding of AWS services, AWS service limits, and AWS CloudFormation
- Knowledge of architecting applications on AWS
- Understanding of security and compliance requirements in the customer organization

AWS offers training and certification programs to help you develop skills to design, deploy, and operate your infrastructure and applications on the AWS Cloud. Whether you are just getting started or looking to deepen your technical expertise, AWS has a variety of resources to meet your needs. For more information, see the AWS Training and Certification website, or read the AWS Training and Certification Overview.

AWS Account

If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

Technical Requirements

Before you launch the Quick Start, your account must be configured as specified in the following table. Otherwise, deployment might fail. For step-by-step configuration instructions, see the Pre-Deployment Steps section.

Resources	**Resource**	**Default**	**Used in this deployment (by default)**
	VPCs	5 per region	**2**
	EIPs	5 per region	**3**
	IAM groups	100 per account	**6**
	IAM roles	250 per account	**5**
	Amazon EC2 Auto Scaling groups	20 per region	**2**
	ELB load balancers	20 per region	**2**

Regions	The AWS services used in this Quick Start exist in all commercial regions, but AWS Config rules, which are used for configuration enforcement, are currently available only in the regions listed in AWS Regions and Endpoints. If you require this capability, you must deploy in one of these regions until AWS Config rules become available more widely. It is important to be aware of what is available in the region you choose to deploy. To see the latest list of supported services per region, see AWS Regions and Endpoints in the AWS documentation. For information about service differences in the AWS GovCloud (US) Region, see Supported Services in the AWS GovCloud documentation.
AWS Config and AWS Config rules	If you deploy this Quick Start in an AWS Region where AWS Config and AWS Config rules are available, the AWS CloudFormation template `config-rules.template` will attempt to automatically use the service. However, **the deployment will fail** if you have not previously manually set up AWS Config in that region. Before you deploy the Quick Start, navigate to the AWS Config console, and choose the **Get Started Now** button. Note that this feature is currently available only in the AWS Regions listed in AWS Regions and Endpoints.
Amazon S3 URLs	If you're copying the templates to your own S3 bucket for deployment, make sure that you update the `Resources` section of the **main.template** file with a valid and accessible URL. **Otherwise**, **deployment will fail**.
IAM permissions	To deploy the Quick Start using the console, you must be logged in to the AWS Management Console with IAM permissions for the resources and actions the templates will deploy. The *AdministratorAccess* managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions.
S3 buckets	Unique S3 bucket names are automatically generated based on the account number and region. If you delete a stack, **the logging buckets are not deleted** (to support security review). If you plan to re-deploy this Quick Start in the same region, you must first manually delete the previously created S3 buckets; **otherwise, the re-deployment will fail**.

Deployment Methods

You can deploy the Quick Start templates by using AWS CLI commands or from the AWS Management Console. You can also deploy the template package as an AWS Service Catalog product. AWS Service Catalog enables a self-service model for deploying applications and architecture on AWS. You can create portfolios that include one or more products, which are defined by AWS CloudFormation templates. You can grant IAM users, groups, or roles access to specific portfolios, which they can then launch from a separate interface. We've provided step-by-step instructions for the AWS Management Console deployment option in the following sections.

Pre-Deployment Steps

Before you deploy the HIPAA Quick Start templates, follow the instructions in this section to confirm that your account is set up correctly:

- Review the service limits and service usage of your AWS account and request increases if required, to ensure that there is available capacity to launch resources in your account.
- Ensure that your AWS account is set up with at least one SSH key pair (but preferably two separate key pairs) **in the AWS Region where you plan to deploy**, for use with the bastion login host and other Amazon EC2 hosts.
- Ensure that you have manually set up AWS Config in the AWS Config console, if you are deploying into an AWS Region where AWS Config is available. AWS Config is currently available only in the regions listed in AWS Regions and Endpoints.

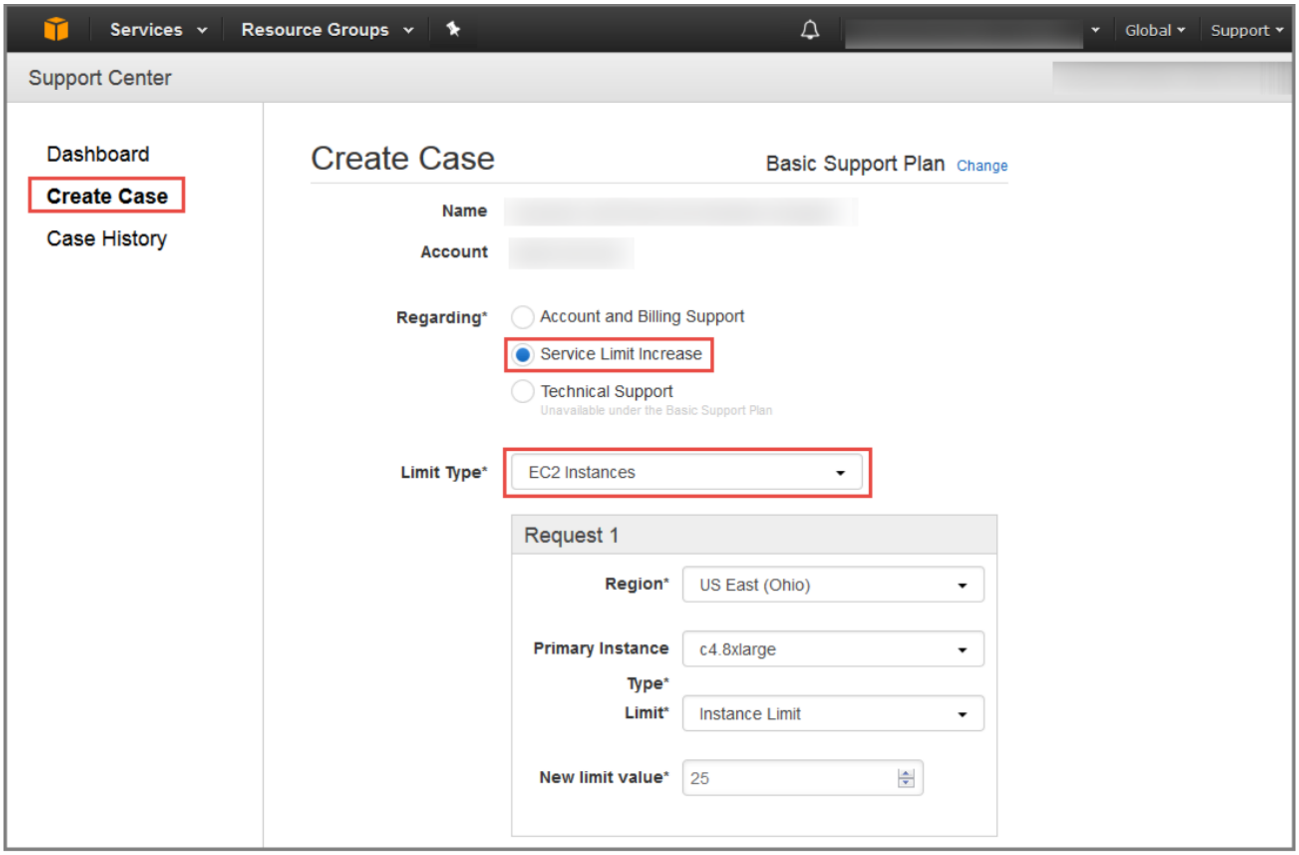
Review AWS Service Limits

To review and (if necessary) increase service limits for the resources you need for the HIPAA Quick Start deployment, you use the AWS Trusted Advisor console and the Amazon EC2 console. You'll need the resources specified in the Technical Requirements table.

Use Trusted Advisor to view the existing service limits for Amazon VPC, IAM groups, and IAM roles within your account, and ensure that there is availability to deploy additional resources:

1. Open the Trusted Advisor console at https://console.aws.amazon.com/trustedadvisor/.
2. In the navigation pane, choose **Performance**.
3. On the **Performance** page, scroll through the list of performance checks until you find **Service Limits**, and expand that section.
4. Scroll through the service limit names and compare the **Limit Amount** column to the **Current Usage** column, to ensure that you can allocate the following without exceeding the default limit in the AWS Region you will deploy this Quick Start into (US East [N. Virginia] is recommended):
   - Two (2) more VPCs
   - Six (6) more IAM groups
   - Five (5) more IAM roles

If an increase is needed, you can choose the limit name to open the limit increase request form shown in Figure 4.



Create Case

Basic Support Plan Change

Name [redacted]

Account [redacted]

Regarding*
○ Account and Billing Support
● Service Limit Increase
○ Technical Support
Unavailable under the Basic Support Plan

Limit Type* EC2 Instances

Request 1

Region* US East (Ohio)

Primary Instance Type* c4.8xlarge

Limit* Instance Limit

New limit value* 25

Figure 4: Requesting a service limit increase

Now use the Amazon EC2 console to check your limits for Elastic IP addresses, load balancers, and Auto Scaling groups:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **Network & Security**, choose **Elastic IPs**.
3. Count the number of allocated Elastic IPs (if any) displayed in the list, and ensure that you can allocate three (3) more without exceeding the default limit of 5 (or the limit increase you previously requested).
4. In the navigation pane, under **Load Balancing**, choose **Load Balancers**.
5. Count the number of existing load balancers (if any) displayed in the list and ensure that you can create two (2) more without exceeding the default limit of 20 (or the limit increase you previously requested).
6. In the navigation pane, under **Auto Scaling**, choose **Auto Scaling Groups**.

7. Count the number of existing Auto Scaling groups (if any) displayed in the list and ensure that you can create two (2) more without exceeding the default limit of 20 (or the limit increase you previously requested).

Create Amazon EC2 Key Pairs

Make sure that at least one Amazon EC2 key pair exists within your AWS account **in the region where you are planning to deploy the Quick Start**.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Use the region selector in the navigation bar to choose the AWS Region where you plan to deploy.
3. In the navigation pane, under **Network & Security**, choose **Key Pairs**.
4. In the key pair list, verify that at least one available key pair (but preferably two available key pairs) exist and make note of the key pair name(s). You'll need to provide a key pair name for the parameters **pEC2KeyPairBastion** (for bastion host login access) and **pEC2KeyPair** (for all other Amazon EC2 host login access) when you launch the Quick Start. Although you can use the same key pair for both parameters, we recommend that you use a different key pair for each. This recommendation is based on a hardened security concept. We publicly expose the bastion box but keep other instances as private, so if the bastion key pair becomes compromised, it will not affect your live data instances.

   If you want to create a new key pair, choose **Create Key Pair**. For additional information, see the Amazon EC2 documentation.

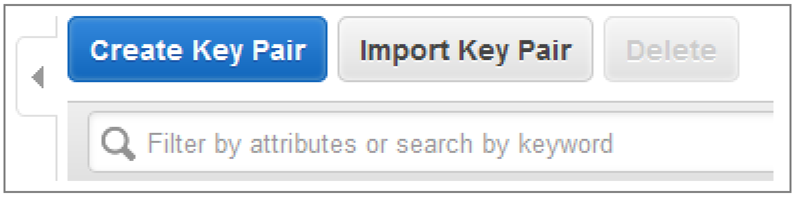


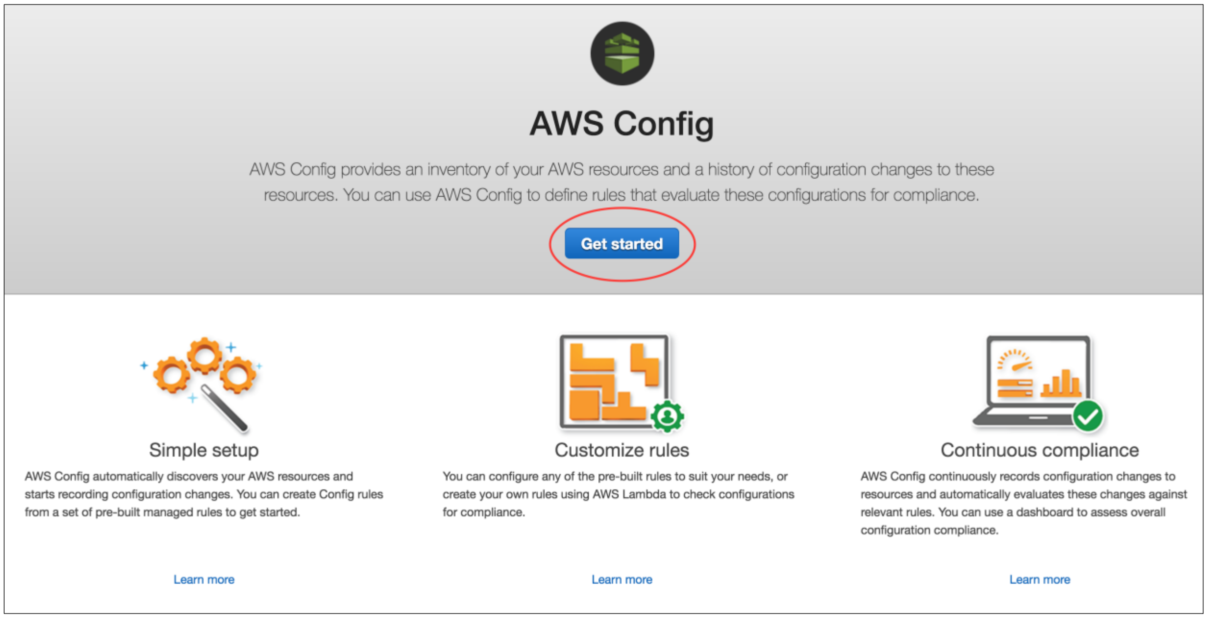
Figure 5: Creating a key pair

Note If you're deploying the Quick Start for testing or proof of concept, we recommend that you create a new key pair instead of specifying a key pair that's already being used by a production instance.

Set up AWS Config

If AWS Config has not yet been initialized in the region where you are deploying this Quick Start, follow the steps below **in the region where you are planning to deploy the Quick Start**.

1. Open the AWS Config console at https://console.aws.amazon.com/config/.
2. Use the region selector in the navigation bar to choose the AWS Region where you plan to deploy.
3. In the AWS Config console, choose **Get Started**.



AWS Config

AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance.

Simple setup

AWS Config automatically discovers your AWS resources and starts recording configuration changes. You can create Config rules from a set of pre-built managed rules to get started.

Customize rules

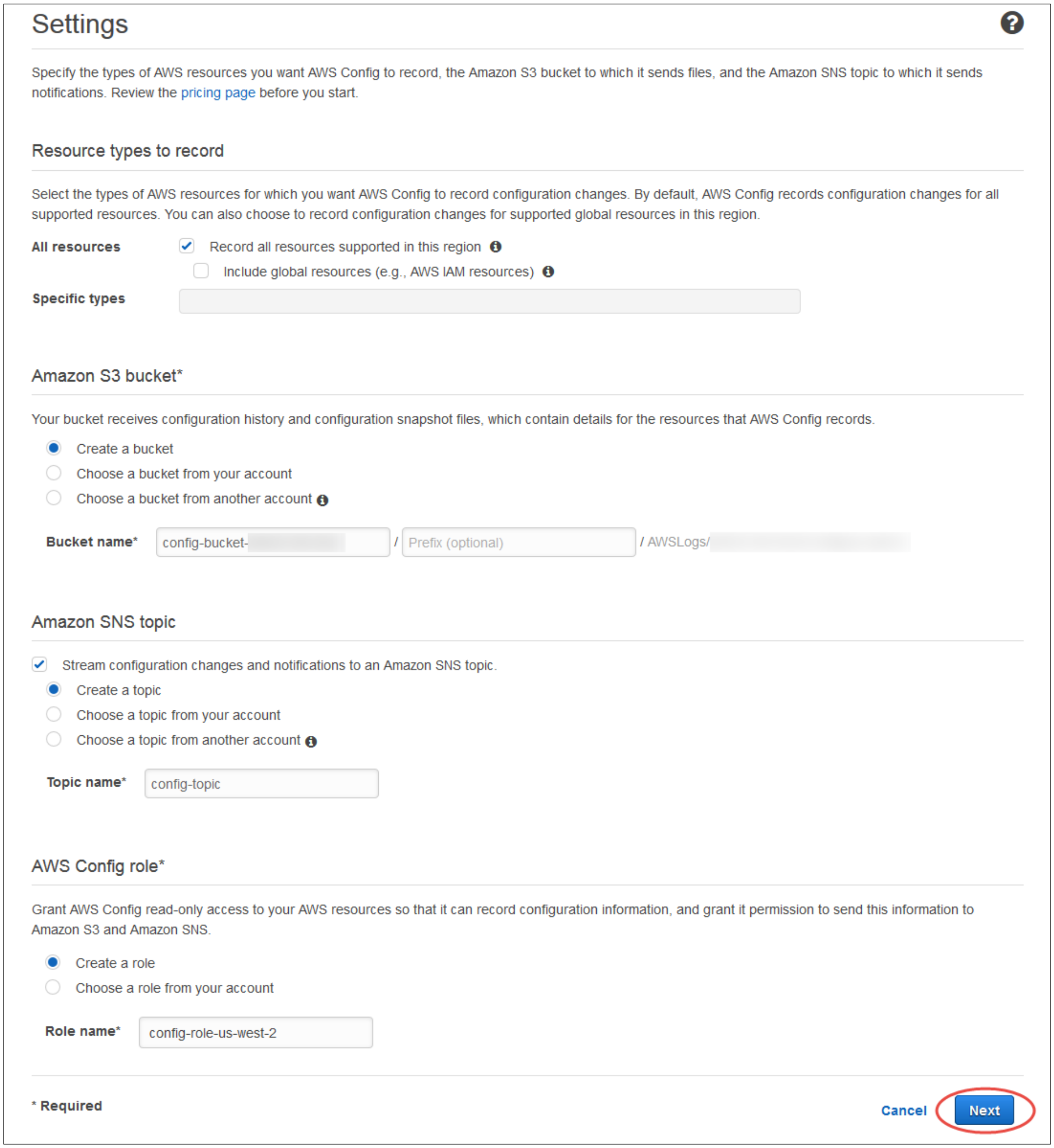
You can configure any of the pre-built rules to suit your needs, or create your own rules using AWS Lambda to check configurations for compliance.

Continuous compliance

AWS Config continuously records configuration changes to resources and automatically evaluates these changes against relevant rules. You can use a dashboard to assess overall configuration compliance.

Figure 6: AWS Config console

4. On the **Set up AWS Config** screen, you are prompted to select or create an IAM role for AWS Config. You may leave all default values in place, or make modifications as you see fit, and then choose **Next.**



Settings

Specify the types of AWS resources you want AWS Config to record, the Amazon S3 bucket to which it sends files, and the Amazon SNS topic to which it sends notifications. Review the pricing page before you start.

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all supported resources. You can also choose to record configuration changes for supported global resources in this region.

All resources ☑ Record all resources supported in this region
☐ Include global resources (e.g., AWS IAM resources)

Specific types

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources that AWS Config records.

● Create a bucket
○ Choose a bucket from your account
○ Choose a bucket from another account

Bucket name* config-bucket-[redacted] / Prefix (optional) / AWSLogs/[redacted]

Amazon SNS topic

☑ Stream configuration changes and notifications to an Amazon SNS topic.

● Create a topic
○ Choose a topic from your account
○ Choose a topic from another account

Topic name* config-topic

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and grant it permission to send this information to Amazon S3 and Amazon SNS.

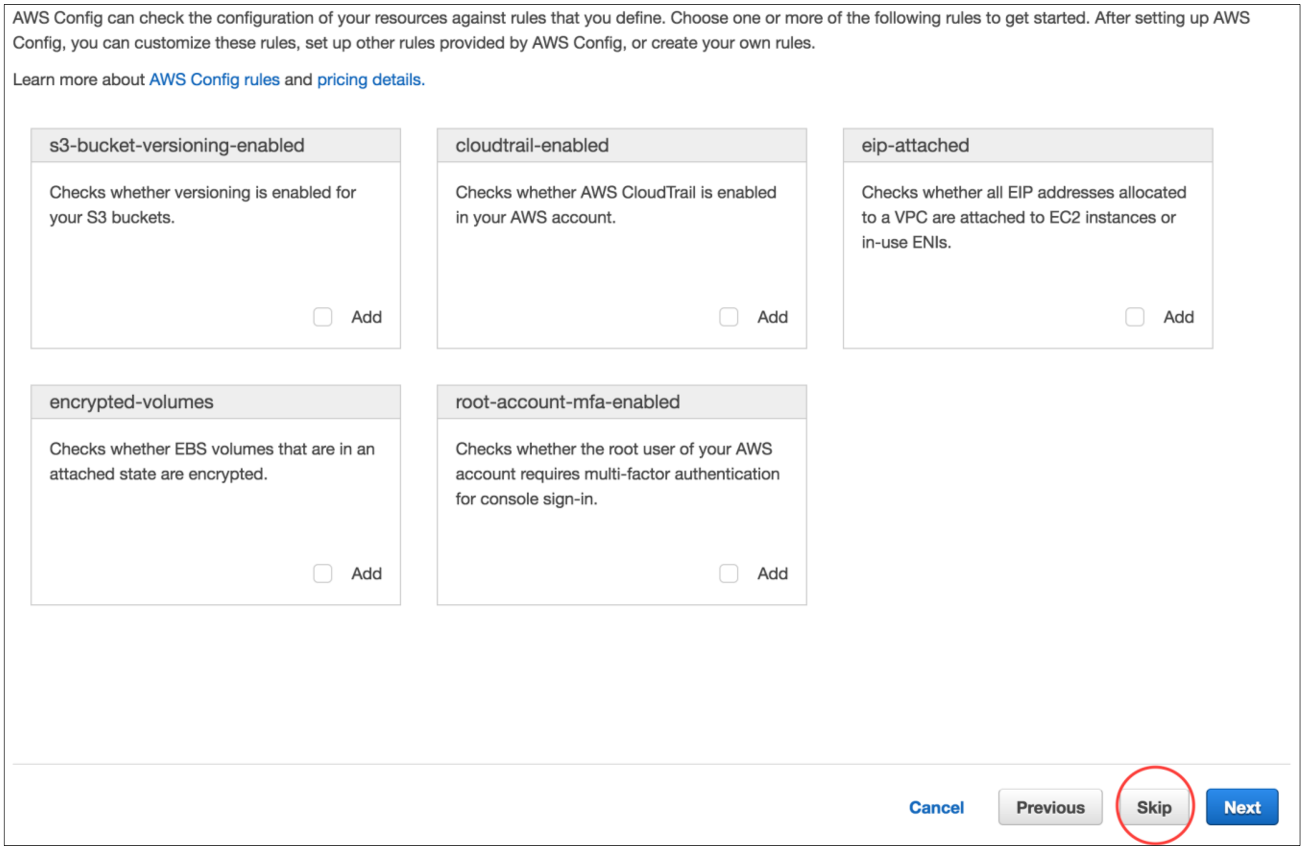
● Create a role
○ Choose a role from your account

Role name* config-role-us-west-2

* **Required**

Figure 7: AWS Config setup screen

5. You are now presented with a screen to add rules. Choose **Skip**.



AWS Config can check the configuration of your resources against rules that you define. Choose one or more of the following rules to get started. After setting up AWS Config, you can customize these rules, set up other rules provided by AWS Config, or create your own rules.

Learn more about AWS Config rules and pricing details.

s3-bucket-versioning-enabled

Checks whether versioning is enabled for your S3 buckets.

□ Add

cloudtrail-enabled

Checks whether AWS CloudTrail is enabled in your AWS account.

□ Add

eip-attached

Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.

□ Add

encrypted-volumes

Checks whether EBS volumes that are in an attached state are encrypted.

□ Add

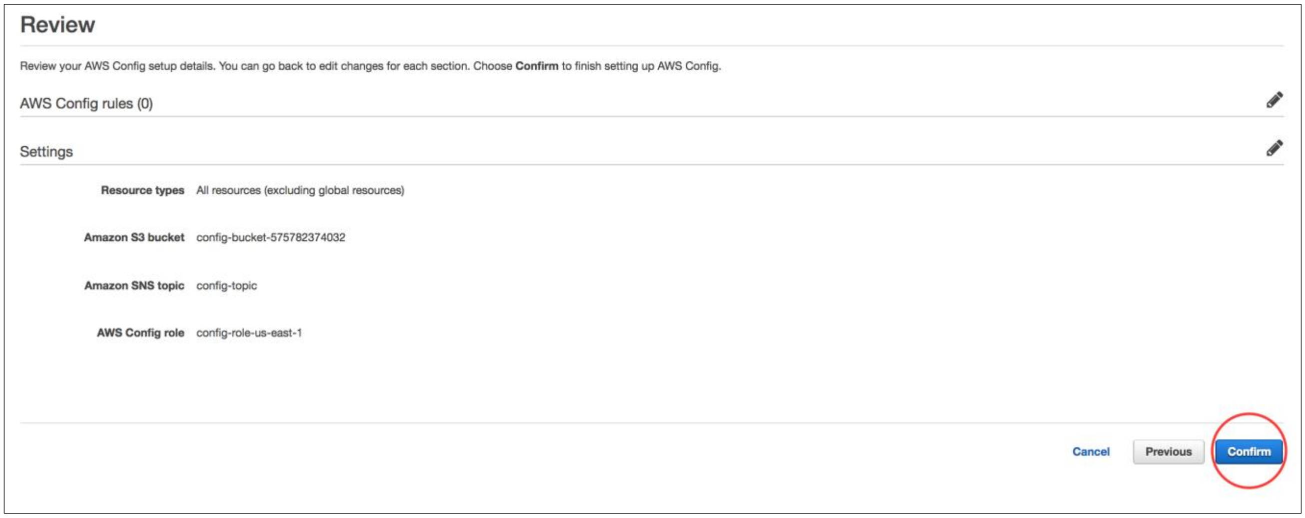
root-account-mfa-enabled

Checks whether the root user of your AWS account requires multi-factor authentication for console sign-in.

□ Add

Figure 8: Additional AWS Config screen for rules

6. On the next screen, you are prompted to review the information. Choose **Confirm**.



Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

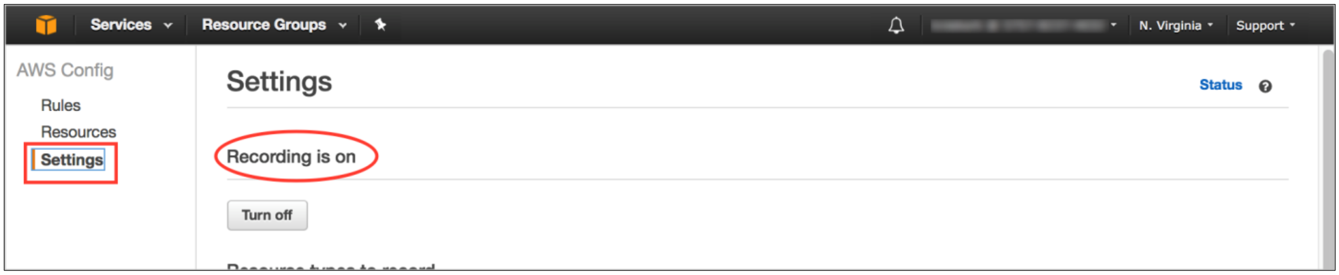
AWS Config rules (0)

Settings

Resource types	All resources (excluding global resources)
Amazon S3 bucket	config-bucket-575782374032
Amazon SNS topic	config-topic
AWS Config role	config-role-us-east-1

Figure 9: Confirm choices for AWS Config

7. Choose the **Settings** button. You should now see **Recording is on** in the window, indicating that AWS Config is now active in this AWS Region.



Recording is on

Figure 10: AWS Config activation verification

Deployment Steps

Follow the step-by-step instructions in this section to sign in to your AWS account, customize the Quick Start templates, and deploy the software into your account.

What We'll Cover

The procedure for deploying the Quick Start architecture on AWS consists of the following steps, which we'll cover in detail in the following sections.

Step 1. Sign in to your AWS account

- Sign in to your AWS account, and make sure that it's configured correctly.

Step 2. Launch the stacks

- Launch the main AWS CloudFormation template into your AWS account.
- Enter values for required parameters.
- Review the other template parameters, and customize their values if necessary.

Step 3. Test your deployment

- Use the URL provided in the **Outputs** tab for the main stack to test the deployment.
- Use the IP address for the bastion host provided by the **Outputs** tab for the main stack, and use your private key if you would like to connect to that host through SSH.

Step 1. Sign in to Your AWS Account

1. Sign in to your AWS account at https://aws.amazon.com with an IAM user role that has the appropriate privileges (see IAM Permissions earlier in this document).
2. Make sure that your AWS account is configured correctly. See the Technical Requirements and Pre-Deployment Steps sections for information. Note that if you plan to use an AWS Region with the AWS Config capability, you must first set up the AWS Config service manually by following the instructions in the previous section.
3. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy the HIPAA architecture on AWS.

   Amazon EC2 locations are composed of *Regions* and *Availability Zones*. Regions are dispersed and located in separate geographic areas. This Quick Start uses the **m3.large** instance type for the WordPress and Nginx portion of the deployment. m3.large instances are currently available in all AWS Regions except China (Beijing). The AWS Config Rules service is currently available only in the AWS Regions listed in AWS Regions and Endpoints.

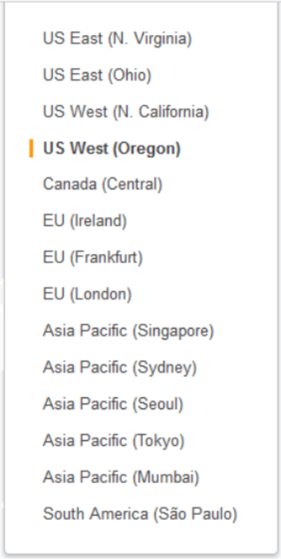


Figure 11: Choosing an AWS Region

Tip Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network. If you plan to use the optional AWS Config rules capability, you must choose one of the regions listed in AWS Regions and Endpoints.

4. Select the key pair that you created earlier. In the navigation pane of the Amazon EC2 console, choose **Key Pairs**, and then choose the key pair from the list.

Step 2. Launch the Stacks

This automated AWS CloudFormation template deploys the Quick Start architecture in multiple Availability Zones into Amazon VPCs. Please review the technical requirements and pre-deployment steps before launching the stacks.

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

   Launch

   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. Note that if you select a region where AWS Config is available, make sure to manually initialize the AWS Config service in that region.

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

   The stacks take approximately 30 minutes to create.

   > **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.

   You can also download the template to use it as a starting point for your customization.

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

3. On the **Specify Details** page, provide the seven required parameter values for the template. These are described in the following table.

Parameter label (name)	Default	Description
Database Password (pDBPassword)	***Requires input***	Password for the database administrator account. This must be a complex password that's between 8 and 28 mixed, alphanumeric characters.
Notification Email Address (pNotifyEmail)	distlist@example.org	Notification email address for security events (you will receive confirmation email).

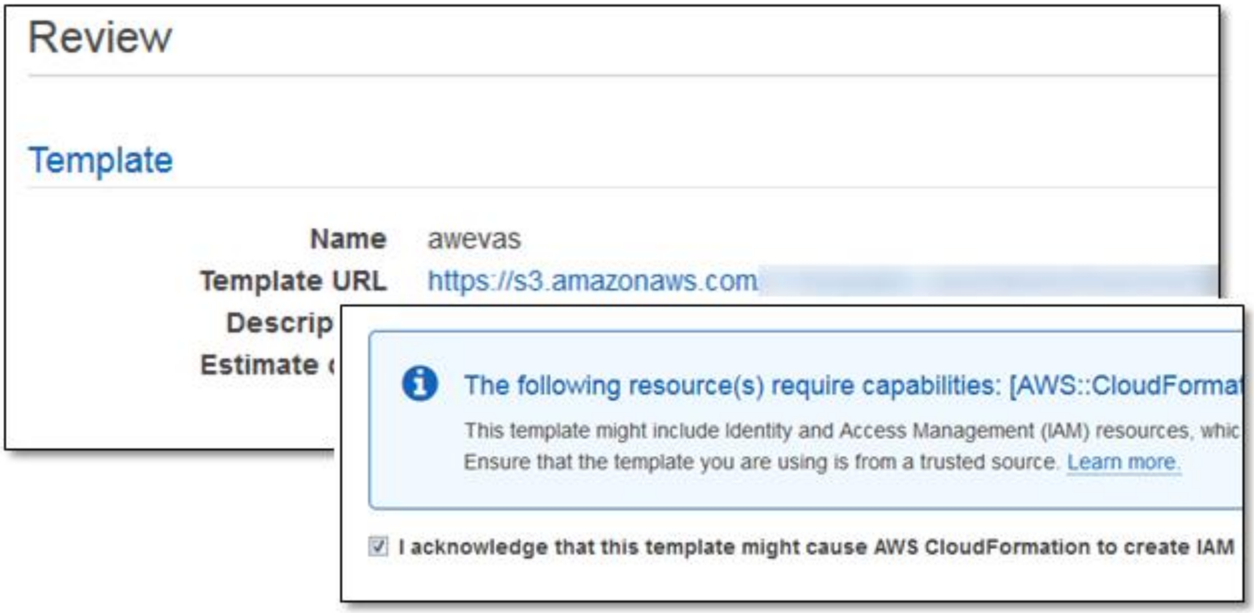
Parameter label (name)	Default	Description
Existing SSH Key for Bastion Instance (pEC2KeyPairBastion)	***Requires input***	The SSH key pair in your account to use for bastion host login (see pre-deployment steps).
Existing SSH Key for Other Instances (pEC2KeyPair)	***Requires input***	The SSH key pair in your account to use for all other host logins (see pre-deployment steps).
Support Config (pSupportsConfig)	***Requires input***	Select **Yes** if you are deploying in an AWS Region where AWS Config is available **and** you want to use AWS Config (see pre-deployment steps).
First Availability Zone (pAvailabilityZoneA)	***Requires input***	Select your desired first Availability Zone (Note: Some Availability Zones may be restricted. If the deployment fails, you may need to use a different Availability Zone.)
Second Availability Zone (pAvailabilityZoneB)	***Requires input***	Select your desired second Availability Zone (Note: Some Availability Zones may be restricted. If the deployment fails, you may need to use a different Availability Zone.)

AWS Quick Start Configuration:

Parameter	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	S3 bucket name for the Quick Start assets. This bucket name can include numbers, lowercase letters, uppercase letters, and hyphens (-), but should not start or end with a hyphen. You can specify your own bucket if you copy all of the assets and submodules into it, if you want to override the Quick Start behavior for your specific implementation.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	quickstart-compliance-hipaa/	S3 key prefix for the Quick Start assets. This prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slashes (/), but should not start or end with a forward slash (which is automatically added). This parameter enables you to override the Quick Start behavior for your specific implementation.

4. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set additional options. You can use the tags to organize and control access to resources in the stacks. When you're done, choose **Next**.

5. On the **Review** page, review the settings and select the acknowledgement check box. This simply states that the template will create IAM resources.



Review

Template

Name awevas

Template URL https://s3.amazonaws.com

Descrip

Estimate

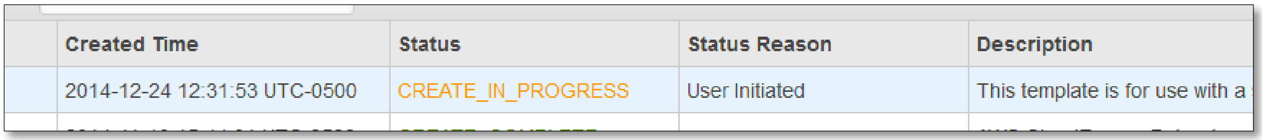
The following resource(s) require capabilities: [AWS::CloudForma

This template might include Identity and Access Management (IAM) resources, whic
Ensure that the template you are using is from a trusted source. Learn more.

☑ I acknowledge that this template might cause AWS CloudFormation to create IAM

Figure 12: IAM resource acknowledgement

6. Choose **Create** to deploy the stack.
7. Monitor the status of the stack being deployed. When the status field shown in Figure 13 displays **CREATE_COMPLETE for all the stacks deployed**, the cluster for this reference architecture is ready. Since you're deploying the full architecture, you'll see eight stacks listed (for the main template and seven nested templates).

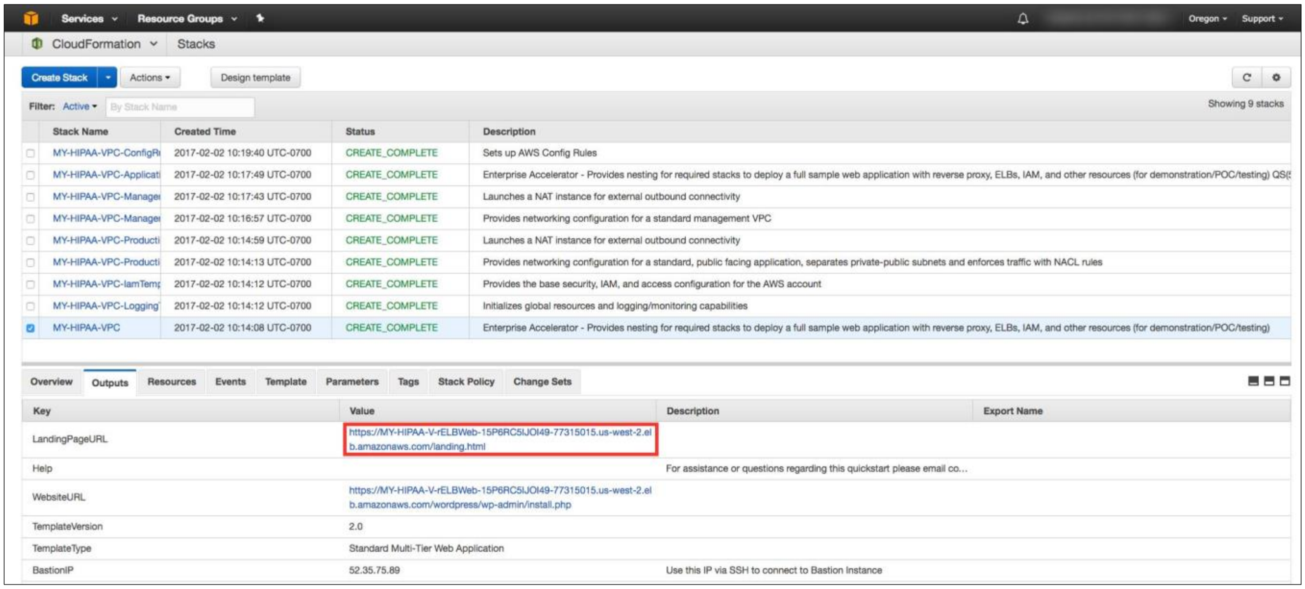


Created Time	Status	Status Reason	Description
2014-12-24 12:31:53 UTC-0500	CREATE_IN_PROGRESS	User Initiated	This template is for use with a

Figure 13: Status message for deployment

Step 3. Test Your Deployment

To test your deployment, choose the link for **LandingPageURL**, as shown in Figure 14. This URL is available from the **Outputs** tab for the main stack:

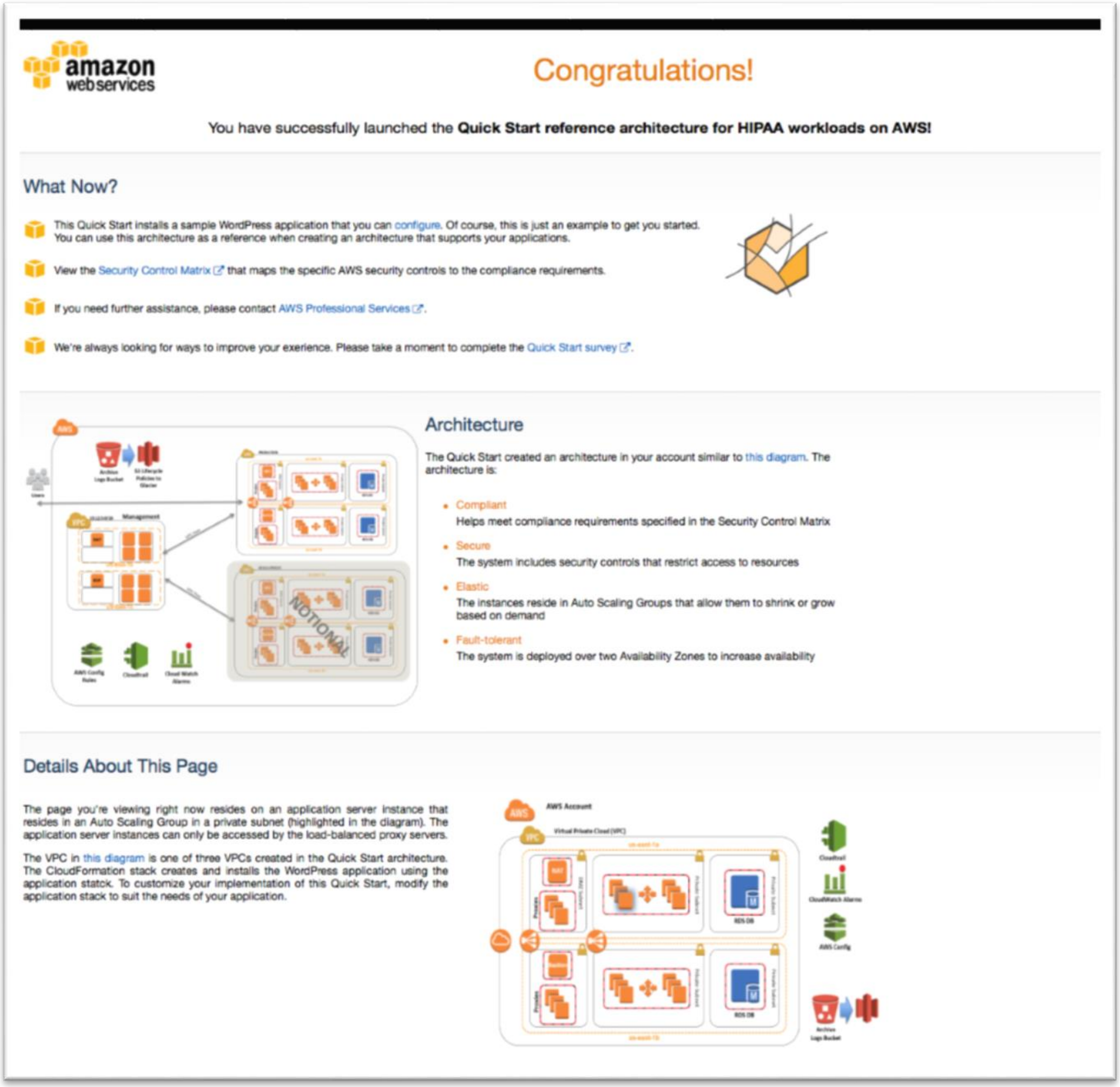


	Stack Name	Created Time	Status	Description
□	MY-HIPAA-VPC-ConfigRı	2017-02-02 10:19:40 UTC-0700	CREATE_COMPLETE	Sets up AWS Config Rules
□	MY-HIPAA-VPC-Applicati	2017-02-02 10:17:49 UTC-0700	CREATE_COMPLETE	Enterprise Accelerator - Provides nesting for required stacks to deploy a full sample web application with reverse proxy, ELBs, IAM, and other resources (for demonstration/POC/testing) QS(
□	MY-HIPAA-VPC-Manager	2017-02-02 10:17:43 UTC-0700	CREATE_COMPLETE	Launches a NAT instance for external outbound connectivity
□	MY-HIPAA-VPC-Manager	2017-02-02 10:16:57 UTC-0700	CREATE_COMPLETE	Provides networking configuration for a standard management VPC
□	MY-HIPAA-VPC-Producti	2017-02-02 10:14:59 UTC-0700	CREATE_COMPLETE	Launches a NAT instance for external outbound connectivity
□	MY-HIPAA-VPC-Producti	2017-02-02 10:14:13 UTC-0700	CREATE_COMPLETE	Provides networking configuration for a standard, public facing application, separates private-public subnets and enforces traffic with NACL rules
□	MY-HIPAA-VPC-IamTemp	2017-02-02 10:14:12 UTC-0700	CREATE_COMPLETE	Provides the base security, IAM, and access configuration for the AWS account
□	MY-HIPAA-VPC-Logging	2017-02-02 10:14:12 UTC-0700	CREATE_COMPLETE	Initializes global resources and logging/monitoring capabilities
☑	MY-HIPAA-VPC	2017-02-02 10:14:08 UTC-0700	CREATE_COMPLETE	Enterprise Accelerator - Provides nesting for required stacks to deploy a full sample web application with reverse proxy, ELBs, IAM, and other resources (for demonstration/POC/testing)

Key	Value	Description	Export Name
LandingPageURL	https://MY-HIPAA-V-rELBWeb-15P6RC5IJOI49-77315015.us-west-2.elb.amazonaws.com/landing.html		
Help		For assistance or questions regarding this quickstart please email co…	
WebsiteURL	https://MY-HIPAA-V-rELBWeb-15P6RC5IJOI49-77315015.us-west-2.elb.amazonaws.com/wordpress/wp-admin/install.php		
TemplateVersion	2.0		
TemplateType	Standard Multi-Tier Web Application		
BastionIP	52.35.75.89	Use this IP via SSH to connect to Bastion Instance	

Figure 14: Opening the landing page

The link should launch a new page in your browser that looks similar to Figure 15.



Congratulations!

You have successfully launched the **Quick Start reference architecture for HIPAA workloads on AWS!**

What Now?

- This Quick Start installs a sample WordPress application that you can configure. Of course, this is just an example to get you started. You can use this architecture as a reference when creating an architecture that supports your applications.
- View the Security Control Matrix that maps the specific AWS security controls to the compliance requirements.
- If you need further assistance, please contact AWS Professional Services.
- We're always looking for ways to improve your exerience. Please take a moment to complete the Quick Start survey.

Architecture

The Quick Start created an architecture in your account similar to this diagram. The architecture is:

- Compliant
  Helps meet compliance requirements specified in the Security Control Matrix
- Secure
  The system includes security controls that restrict access to resources
- Elastic
  The instances reside in Auto Scaling Groups that allow them to shrink or grow based on demand
- Fault-tolerant
  The system is deployed over two Availability Zones to increase availability

Details About This Page

The page you're viewing right now resides on an application server instance that resides in an Auto Scaling Group in a private subnet (highlighted in the diagram). The application server instances can only be accessed by the load-balanced proxy servers.

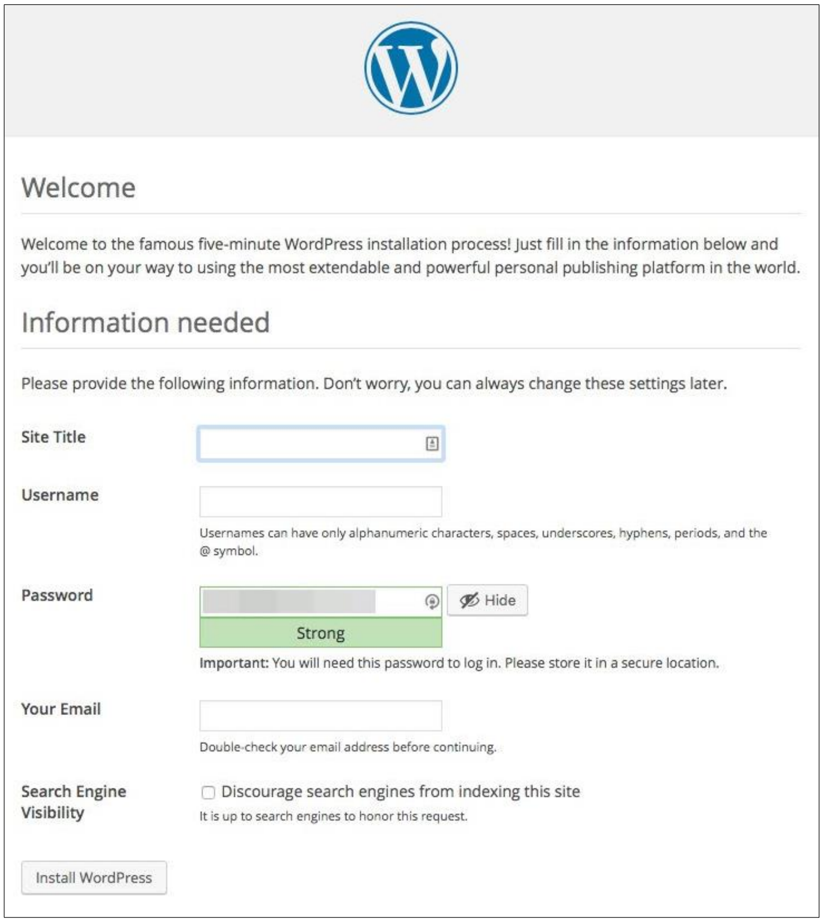
The VPC in this diagram is one of three VPCs created in the Quick Start architecture. The CloudFormation stack creates and installs the WordPress application using the application statck. To customize your implementation of this Quick Start, modify the application stack to suit the needs of your application.

Figure 15: Landing page for HIPAA architecture on AWS

This deployment builds a working demo of a Multi-AZ WordPress site. To connect to the WordPress site, choose the URL provided for the WordPress application on the landing page shown in Figure 15. This URL is also available from the **WebsiteURL** link on the **Outputs** tab for the main stack.

> **Note** WordPress is provided for testing and proof-of-concept purposes only; it is not intended for production use. You can replace it with another application of your choice.

This URL brings up the page shown in Figure 16. You can install and test the WordPress deployment from here.



Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

Username

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password

Important: You will need this password to log in. Please store it in a secure location.

Your Email

Double-check your email address before continuing.

Search Engine Visibility

□ Discourage search engines from indexing this site

It is up to search engines to honor this request.

Figure 16: Installing WordPress

> **Note** The WordPress application included in this Quick Start deployment is for demo purposes only. Application-level security, including patching, operating system updates, and addressing application vulnerabilities, is the customer's responsibility (see the [AWS Shared Responsibility Model)](). **For this Quick Start, we recommend that you delete the AWS CloudFormation stacks after your proof-of-concept demo or testing is complete.**

Now that you've deployed and tested the HIPAA reference architecture on AWS, please take a few minutes to complete our survey for this Quick Start. Your response is anonymous and will help us improve these reference deployments.

Deleting the Stacks

When you've finished using the baseline environment, you can delete the stacks. Deleting a stack, either via CLI and APIs or through the AWS CloudFormation console, will remove all the resources created by the template for that stack. **The only exceptions are the S3 buckets for logging and backup. By default, the deletion policy for those buckets is set to "Retain," so you have to delete them manually.**

> **Important** This Quick Start deployment uses nested AWS CloudFormation templates, so deleting the main stack will remove the nested stacks and all associated resources.

Troubleshooting

If you encounter a **CREATE_FAILED** error when you deploy the Quick Start, refer to the following table for known issues and solutions.

Error message	Possible cause	What to do
The following resource(s) failed to create: [rConfigRuleForRequiredTags, rConfigRuleForUnrestrictedPorts, rConfigRuleForSSH, rConfigRulesLambdaRole]	The **Support Config** parameter was set to **Yes**, but AWS Config isn't available in the region you selected, or AWS Config has not been initialized.	Set the **Support Config** parameter to **No**, or select another region. Also make sure that AWS Config is set up properly, as described in the pre-deployment steps.
Maximum VPCs limit reached	You've exceeded the number of VPCs allowed in your account.	Delete VPCs and/or request a limit increase. Try to create the stack again. For more information, see technical requirements.
Maximum EIPs limit reached	You've exceeded the limit of Elastic IP addresses in your account.	Disassociate Elastic IPs or request a Elastic IP limit increase, and try to create the stack again. For more information, see technical requirements.
Other limits exceeded	You've exceeded the use of resources in your AWS account.	See technical requirements, and request service limit increases as necessary.

If the problem you encounter isn't covered in this table, we recommend that you re-launch the template with **Rollback on failure** set to **No** (this setting is under **Advanced** in the AWS CloudFormation console, **Options** page) and open a support case in the AWS Support Center for further troubleshooting. When rollback is disabled, the stack's state will be retained and the instance will be left running, so the support team can help 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.

Integrating with AWS Service Catalog

You can add the AWS CloudFormation templates for this Quick Start to AWS Service Catalog as portfolios or products to manage them from a central location. This helps support consistent governance, security, and compliance requirements. It also enables users to quickly deploy only the approved IT services they need.

For complete information about using AWS Service Catalog, see the AWS documentation. The following table provides links for specific tasks.

To	See
Create a new portfolio	Creating and Deleting Portfolios
Create a new product	Adding and Removing Products
Give users access	Granting Access to Users
Assign IAM roles for deploying stacks	Applying Launch Constraints Make sure that the IAM role has a policy and trust relationship defined.
Assign tags to portfolios to track resource ownership, access, and cost allocations	Tagging Portfolios
Perform other administrative tasks	AWS Service Catalog Administrator Guide
Launch products from AWS Service Catalog	AWS Service Catalog User Guide

Additional Resources

AWS services

- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- Amazon EC2 User Guide for Linux:
  https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- AWS CloudTrail
  https://aws.amazon.com/documentation/cloudtrail/
- AWS Config
  https://aws.amazon.com/documentation/config/
- Amazon CloudWatch
  https://aws.amazon.com/documentation/cloudwatch/
- AWS Identity and Access Management
  https://aws.amazon.com/documentation/iam/
- Amazon RDS
  https://aws.amazon.com/documentation/rds/
- AWS CLI
  https://aws.amazon.com/documentation/cli/
- AWS Service Catalog
  https://aws.amazon.com/documentation/servicecatalog/

HIPAA

- HIPAA Compliance page on the AWS website
  https://aws.amazon.com/compliance/hipaa-compliance/
- Step-by-step guide to accepting the AWS Business Associate Addendum on AWS Artifact
  https://aws.amazon.com/artifact/getting-started/#BAA_Agreements
- AWS Whitepaper: *Architecting for HIPAA Security and Compliance on Amazon Web Services*
  https://d0.awsstatic.com/whitepapers/compliance/AWS_HIPAA_Compliance_Whitepaper.pdf

- U.S Department of Health & Human Services (HHS) HIPAA website https://www.hhs.gov/hipaa/for-professionals/index.html

Quick Start Reference Deployments

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

Send Us Feedback

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

If you haven't filled out our survey yet, please take a few minutes to do so. Your response is anonymous and will help us improve the quality of this HIPAA Quick Start and other AWS reference deployments.

For Further Assistance

If you need assistance with an enterprise implementation of the capabilities introduced through this Quick Start, AWS Professional Services can guide and assist with the related training, customization, and implementation of deployment and maintenance processes. Please contact your AWS Account Manager for further information, or send an inquiry to compliance-accelerator@amazon.com.

Document Revisions

Date	Change	In sections
August 2017	Removed references to dedicated VPC	Revisions throughout guide
February 2017	Initial publication	—

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.