AWS Compliance

Standardized Architecture for CJIS-based Assurance Frameworks in the AWS Cloud

Quick Start Reference Deployment

AWS Professional Services
AWS Envision Engineering
AWS Quick Start Reference Team

December 2017

This Quick Start supports the following requirements:

- CJIS Security Policy Version 5.6

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 standardized environment that helps organizations with workloads that fall in scope for the Criminal Justice Information Services (CJIS) Security Policy version 5.6. This Quick Start will help organizations get started, but additional effort will be needed for full alignment to the CJIS Security Policy.

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, standardized architecture solutions to help Managed Service Providers (MSPs), cloud provisioning teams, developers, integrators, and information security teams adhere to strict security, compliance, and risk management controls.

Quick Links

If you have an AWS account in the AWS GovCloud (US) Region that already meets the technical requirements for the deployment, you can launch the Quick Start to build the architecture shown in Figure 2. To comply with CJIS standards, this Quick Start **must** be deployed in the AWS GovCloud (US) Region.

Launch Quick Start

The deployment takes approximately 30 minutes. If you're new to AWS or to CJIS-compliant architectures 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

You can also view the security controls matrix (Microsoft Excel spreadsheet), which maps the architecture decisions, components, and configuration in this Quick Start to security requirements within the CJIS Security Policy 5.6 publication; indicates which AWS CloudFormation templates and stacks affect the controls implementation; and specifies the associated AWS resources within the templates and stacks. The excerpt in Figure 1 provides a sample of the available information.

View security controls matrix

Seq	CJIS 5.6 Controls			Quick Start Architecture Comments for Controls			
	Section	Heading	Description	Addressed By This Quick Start	Category: Influence	Category: Responsibility	AWS Quick Start Control Implementation
241	5.4.4	Time Stamps	The time stamps shall include the date and time values generated by the internal system clocks in the audit records.	Yes	Information Systems	Shared	Establishes baseline AWS CloudTrail service enablement for data collection related to account usage, events and actions performed by personnel within the customer environment. Log information provided via S3 data logs and CloudTrail native logs include this information. Logging provided outside AWS infrastructure will require the customer to ensure this information is included.
242	5.4.4	Time Stamps	The agency shall synchronize internal information system clocks on an annual basis.	Yes	Information Systems	Shared	AWS Infrastructure system clocks are synchronized. Any EC2 instances launched will be synchronized at the time of launch but must be configured for periodic synchronization to fully meet this control. AWS-provided Amazon Linux AMIs are pre-configured for continuous synchronization, however, the customer is responsible for maintenance of the daemon (restricting access to turn off the daemon/monitoring the daemon to ensure it continues to operate).
243	5.4.5	Protection of Audit Information	The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.	Yes	Information Systems	Shared	AWS CloudTrail logs are protected via bucket policy, IAM and Config Rules. Customer is responsible to configure the policies applied to logs created by customer furnished systems or applications
244	5.4.6	Audit Record Retention	The agency shall retain audit records for at least one (1) year.	Yes	Information Systems	Shared	CloudTrail and S3 logs are retained indefinately. Customer is responsible to configure the policies applied to logs created by customer furnished systems or applications
245	5.4.6	Audit Record Retention	Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.	Yes	Information Systems	Shared	CloudTrail and S3 logs are retained indefinately. Customer is responsible to configure the policies applied to logs created by customer furnished systems or applications
246	5.4.7	Logging NCIC and III Transactions	A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions.	No	Information Systems	Customer	
247	5.4.7	Logging NCIC and III Transactions	The III portion of the log shall clearly identify both the operator and the authorized receiving agency.	No	Information Systems	Customer	
248	5.4.7	Logging NCIC and III Transactions	III logs shall also clearly identify the requester and the secondary recipient.	No	Information Systems	Customer	
249	5.4.7	Logging NCIC and III Transactions	The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the	No	Information Systems	Customer	

Figure 1: Excerpt from the security controls matrix

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 AWS compliance 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 Quick Starts help streamline, automate, and implement secure baselines in AWS—from initial design to operational security readiness. They incorporate the expertise of AWS solutions architects, and security and compliance personnel to help you build a secure and reliable architecture easily through automation. This Quick Start will help organizations get started, but additional effort will be needed for full alignment to the CJIS Security Policy.

This Quick Start includes AWS CloudFormation templates, which can be integrated with AWS Service Catalog, to automate building a standardized baseline architecture that aligns with the requirements within the CJIS Security Policy 5.6. It also includes a security controls matrix, which maps the security controls and requirements to architecture decisions, features, and configuration of the baseline to enhance your organization's ability to understand and assess the system security configuration.

CJIS-based Assurance Framework

This Quick Start supports the requirements for the Criminal Justice Information Services (CJIS) Security Policy 5.6**.** These security controls apply "to all entities with access to, or who operate in support of, FBI CJIS Division's services and information" (CJIS Security Policy, version 5.6, June 2017, https://www.fbi.gov/file-repository/cjis-security-policy-v5_6_20170605.pdf). These entities are typically systems that must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems, based on the security category and impact level of the system (low, moderate, or high), and a risk determination.

Architecture for Compliance 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.

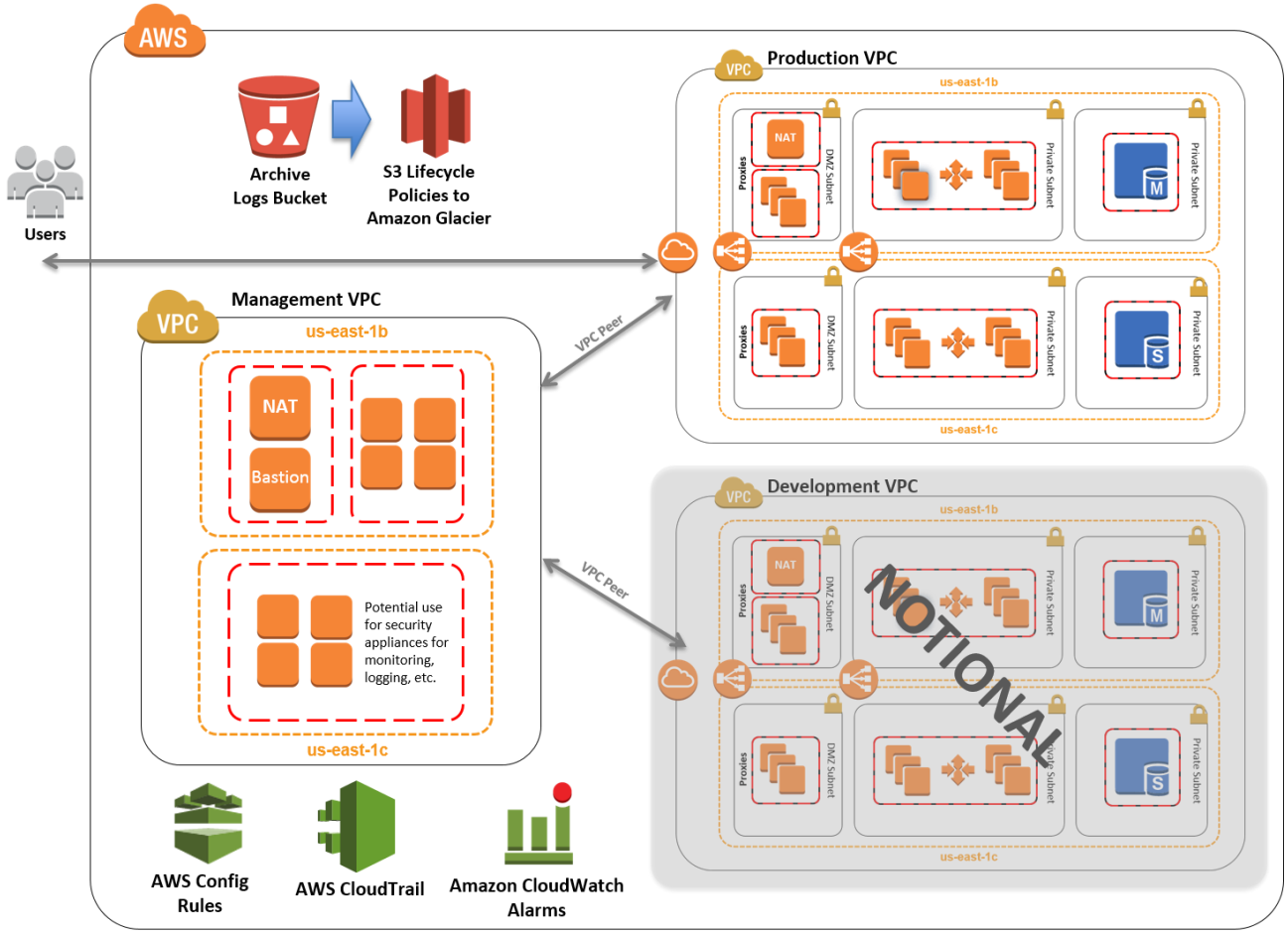

Figure 2: Standard three-tier web architecture depicting integration with multiple VPCs (notional development VPC shown)

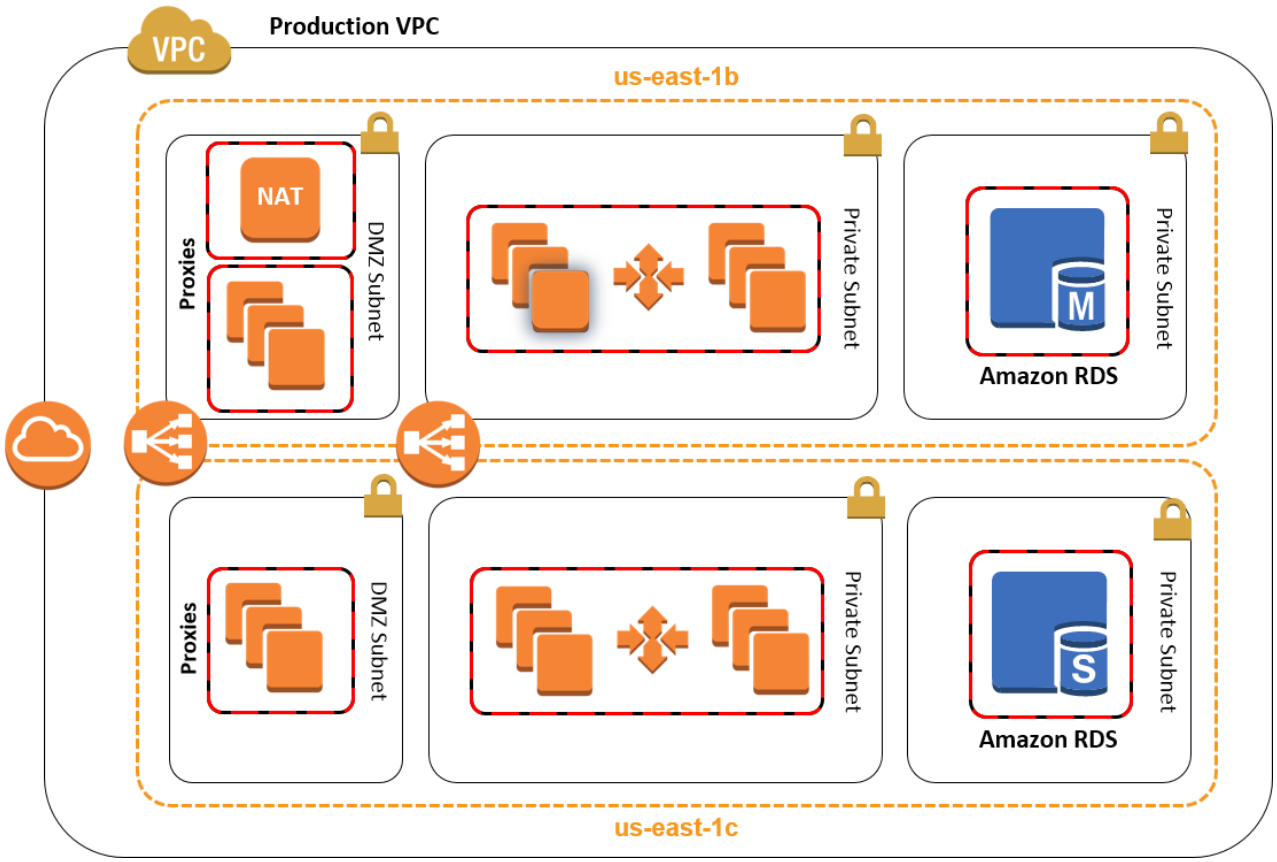

Figure 3: Production VPC design

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 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

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 Resource Center.)

- 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.
- 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 EBS – Amazon Elastic Block Store (Amazon EBS) provides persistent block-level storage volumes for use with EC2 instances in the AWS Cloud. Each EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. EBS volumes provide the consistent and low-latency performance needed to run your workloads.
- 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.

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 that limit 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

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 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.

AWS CloudFormation Templates

An AWS CloudFormation template is a JSON (JavaScript Object Notation)-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 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)	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 or NAT gateways, route tables, and custom 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 ACL rules, and a restricted, public-facing bastion host to support a secured login path for administrator access.	Production VPC stack

Stack and template	Description	Dependencies
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. The AWS GovCloud (US) Region does not currently have NAT gateway capability, so the Quick Start uses NAT instances.	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 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 https://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

Specialized Knowledge

This Quick Start requires a moderate to high level of understanding of the process to achieve and manage control requirements and compliance processes within a traditional hosting environment.

Additionally, this solution is targeted at Information Technology (IT) assessors 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.

This Quick Start 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.

For a production environment, you will also need to sign up for AWS GovCloud (US). During the signup process, customers are vetted to ensure they are a U.S. entity (such as a government body, contracting company, or educational organization) and that they cannot be prohibited or restricted by the U.S. government from exporting or providing services. The sign-up process differs for direct customers and resellers. For instructions, see the AWS GovCloud (US) documentation.

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	**5**
	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	For information about service support in the AWS GovCloud (US) Region, see Supported Services in the AWS GovCloud documentation.		
AWS Config and AWS Config rules	**Deployment will fail** if you have not previously manually set up AWS Config in the AWS GovCloud (US) Region. Before you deploy the Quick Start, navigate to the AWS Config console, and choose the **Get Started Now** button.		
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, 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 templates included with this Quick Start, 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 GovCloud (US) Region, 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.

Review AWS Service Limits

To review and (if necessary) increase service limits for the resources you need for the 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. Sign in to the AWS Management Console for the AWS GovCloud (US) Region, and then navigate to the Trusted Advisor console.
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 GovCloud (US) Region:
    - 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.

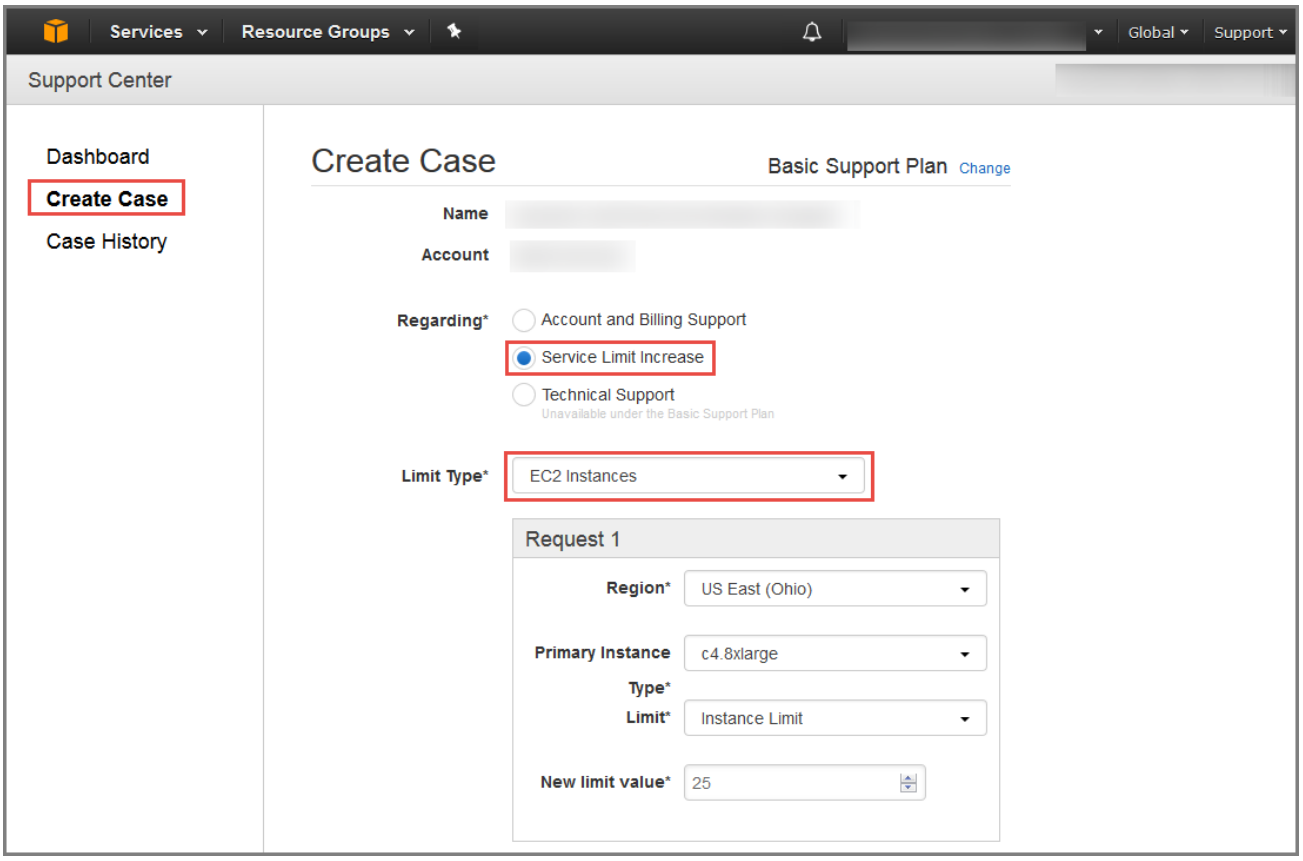

Figure 4: Requesting a service limit increase

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

1. Sign in to the AWS Management Console for the AWS GovCloud (US) Region, and then navigate to the Amazon EC2 console.
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 five (5) 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 AWS GovCloud (US) Region.

1. Sign in to the AWS Management Console for the AWS GovCloud (US) Region, and then navigate to the Amazon EC2 console.
2. In the navigation pane, under **Network & Security**, choose **Key Pairs**.
3. 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.

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

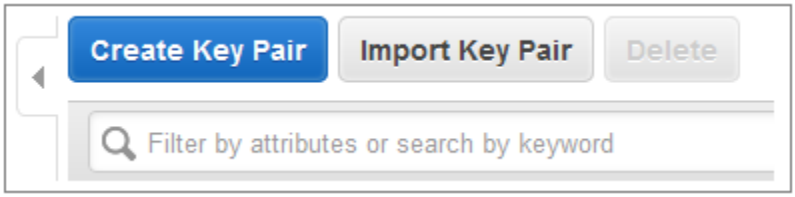

Figure 5: Creating a key pair

> **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 your AWS GovCloud account, follow these steps.

1. Sign in to the AWS Management Console for the AWS GovCloud (US) Region, and then navigate to the AWS Config console.

2. In the AWS Config console, choose **Get Started** (or **Get Started Now**).

Figure 6: AWS Config console

3. On the **AWS Config Settings** screen, you may leave all default values in place, or make modifications as necessary, and then choose **Next**.

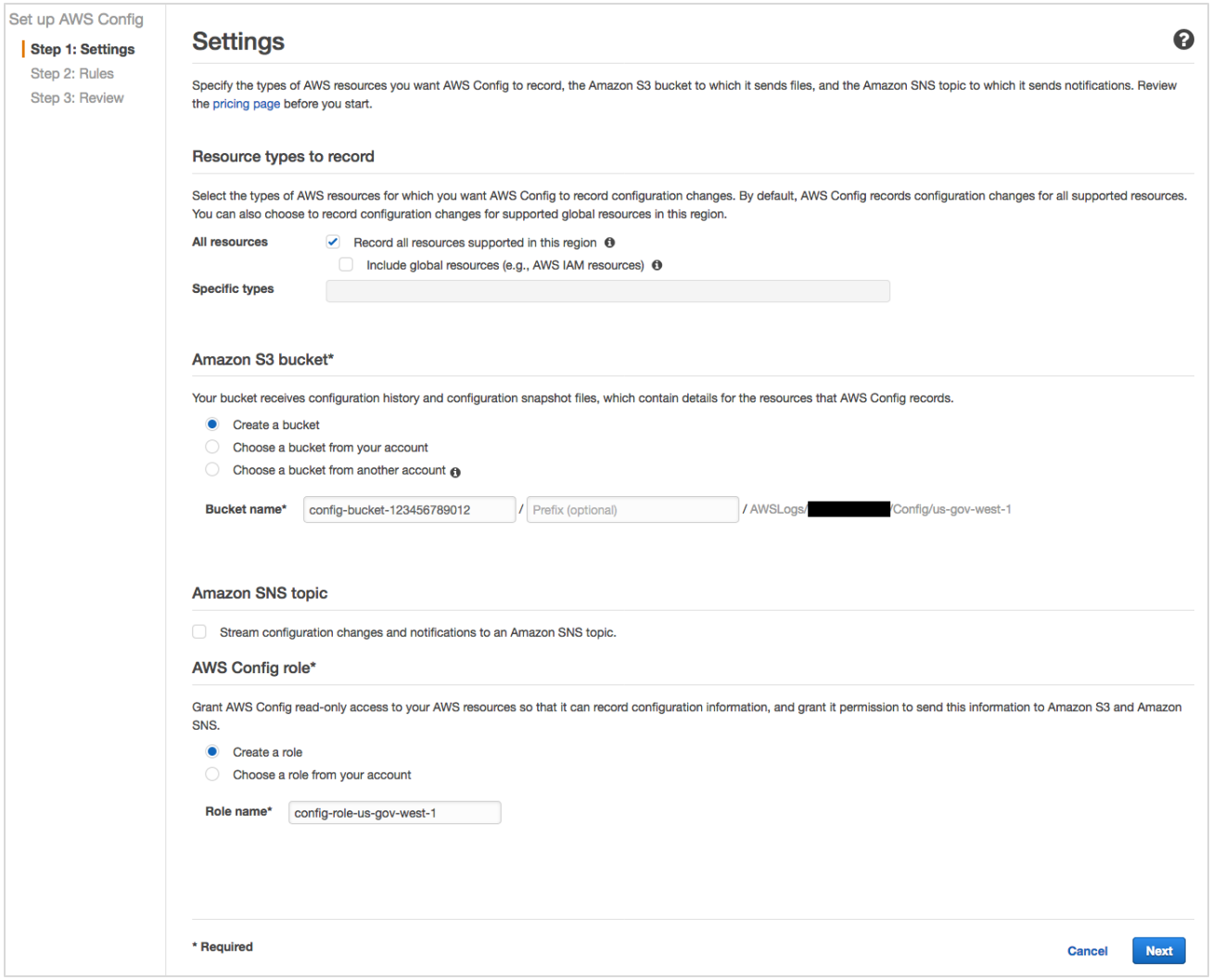

Figure 7: AWS Config settings screen

4. On the **Rules** screen, you can simply choose **Skip**.

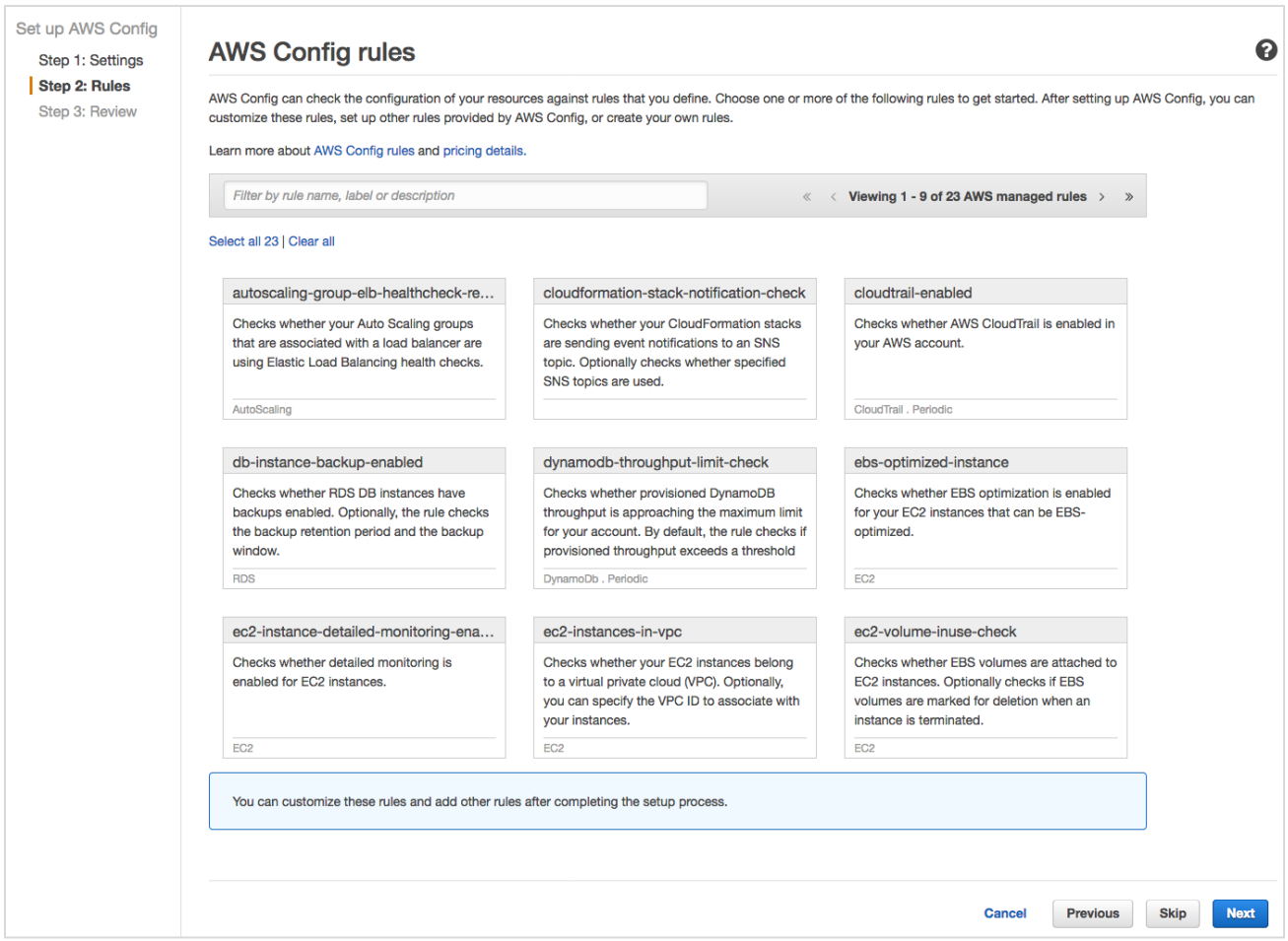

Figure 8: AWS Config Rules screen

5. On the **Review** screen, review and confirm your choices. AWS Config is now active.

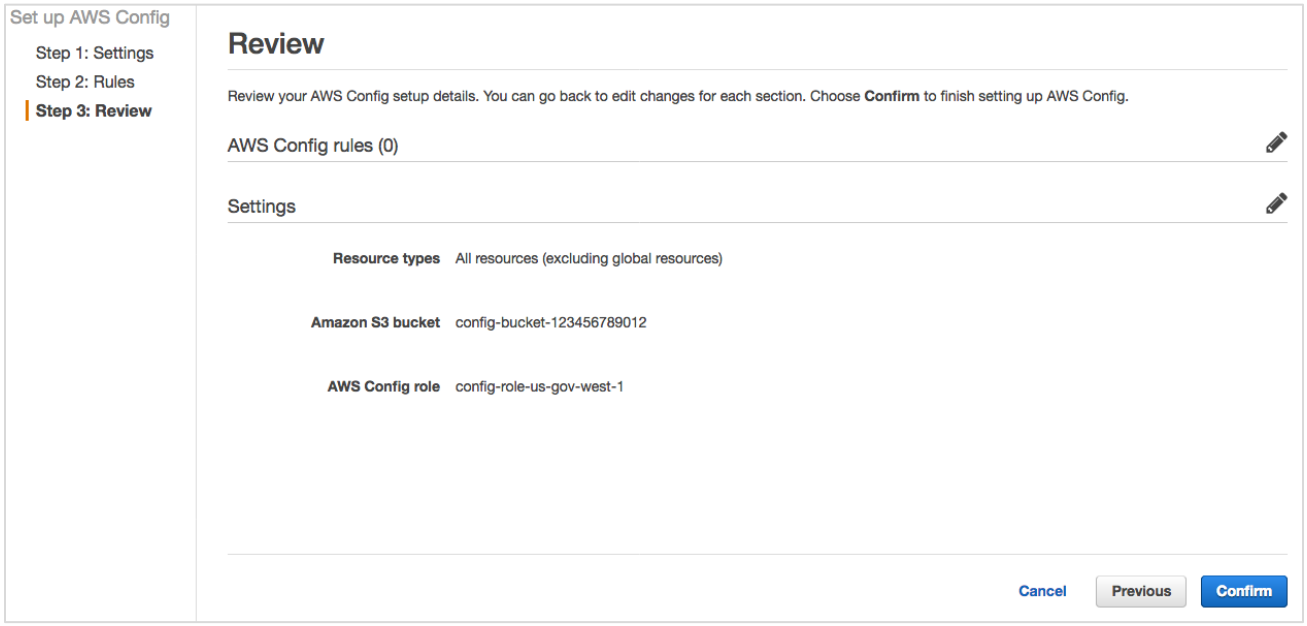

Figure 9: AWS Review screen

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 the AWS Management Console for the AWS GovCloud (US) Region 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 for information. Note that if you plan to use AWS Config, you must first set up the AWS Config service manually by following the instructions in the previous section.
3. 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 GovCloud (US) Region, which is the only region that allows full compliance with the CJIS standard.

   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).
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)	No	Select **Yes** if 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-cjis/	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.

Other Parameters:

Parameter	Default	Description
Instance Tenancy (pVPCTenancy)	default	Select **dedicated** to enforce the use of Amazon EC2 dedicated tenancy within the VPC.

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

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.

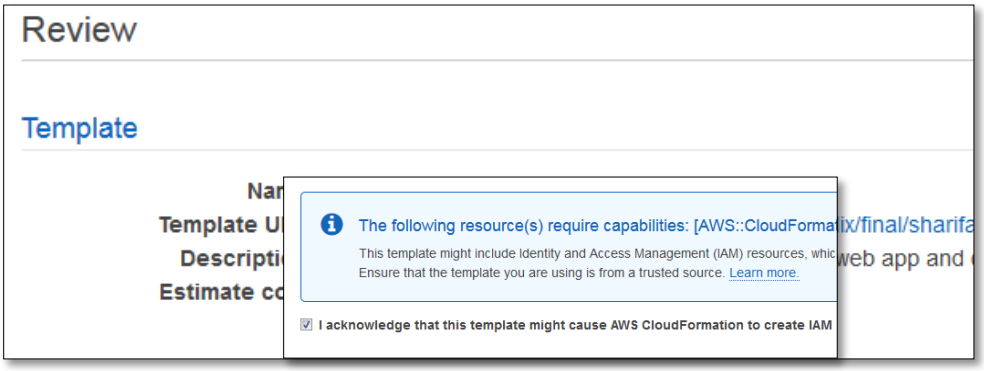

Figure 10: IAM resource acknowledgement

6. Choose **Create** to deploy the stack.
7. Monitor the status of the stack being deployed. When the status field shown in Figure 11 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).

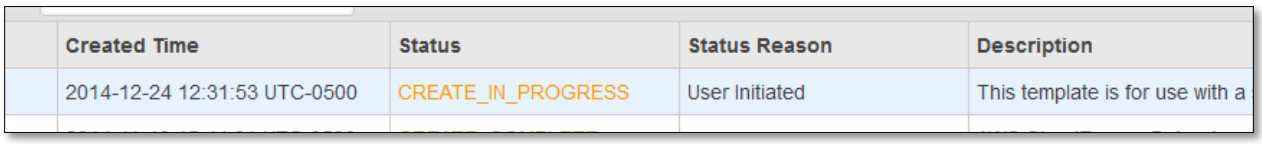

Figure 11: Status message for deployment

Step 3. Test Your Deployment

To test your deployment, choose the link for **LandingPageURL**, as shown in Figure 12. This URL is available from the **Outputs** tab for the main stack:

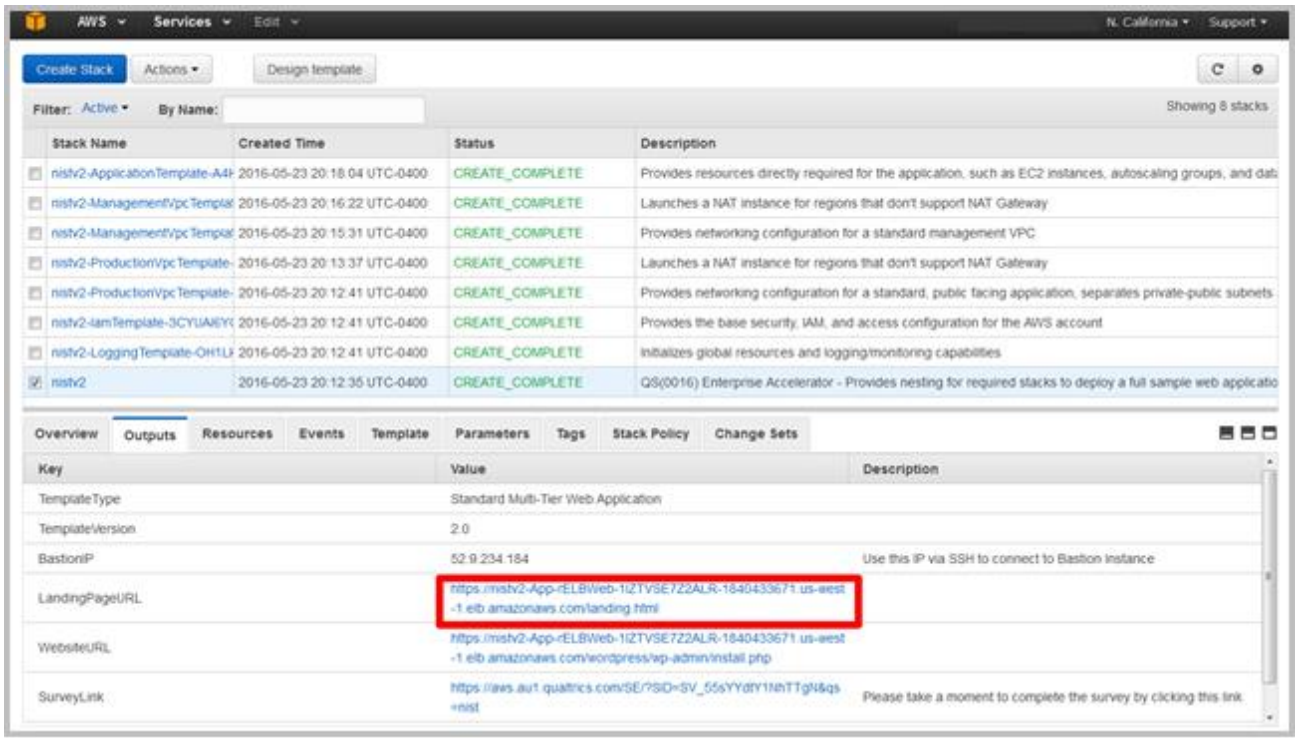

Figure 12: Opening the landing page

The link should launch a new page in your browser that looks similar to Figure 13.

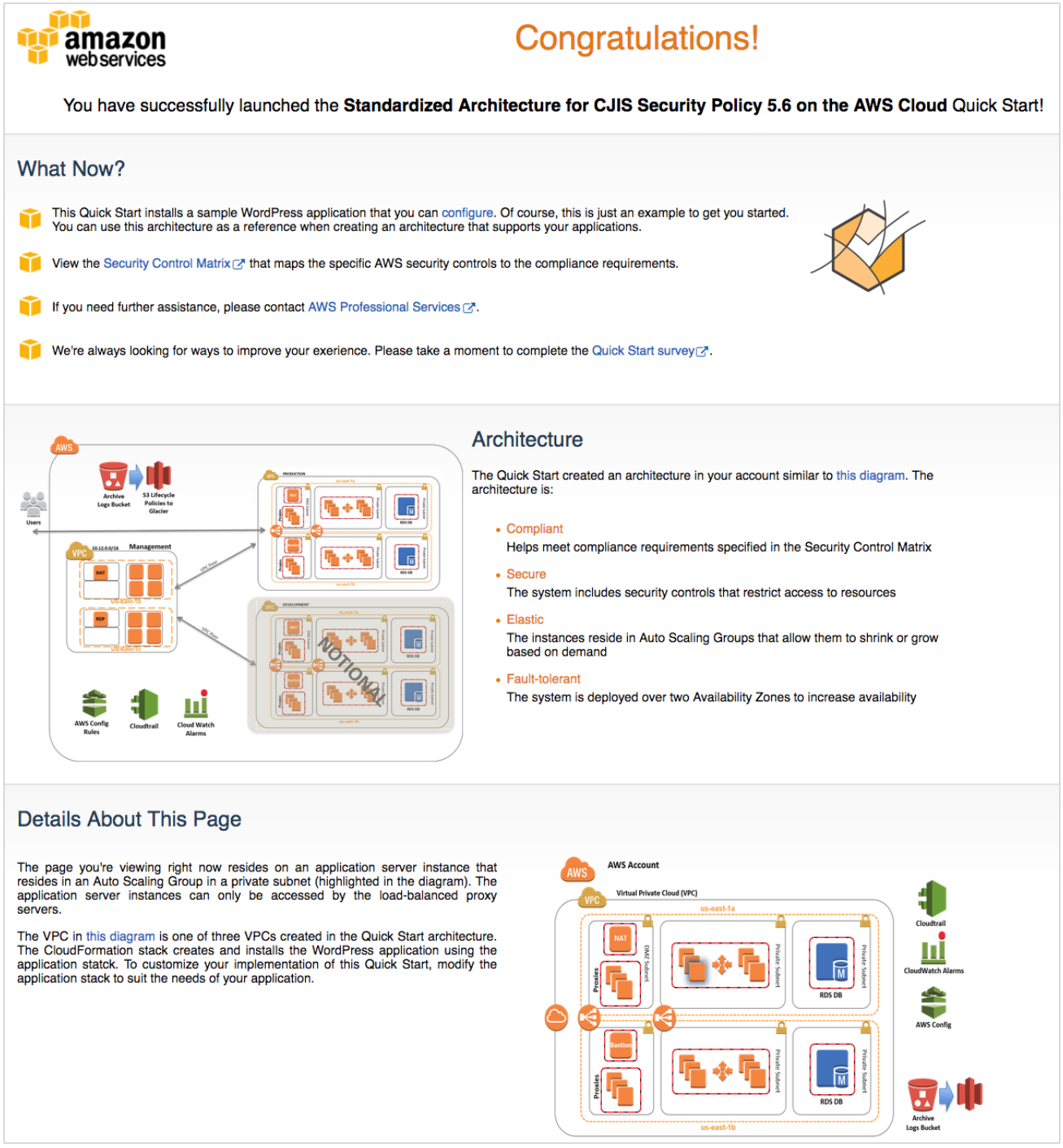

Figure 13: Landing page for compliance architecture on AWS

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 13. 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 14. You can install and test the WordPress deployment from here.

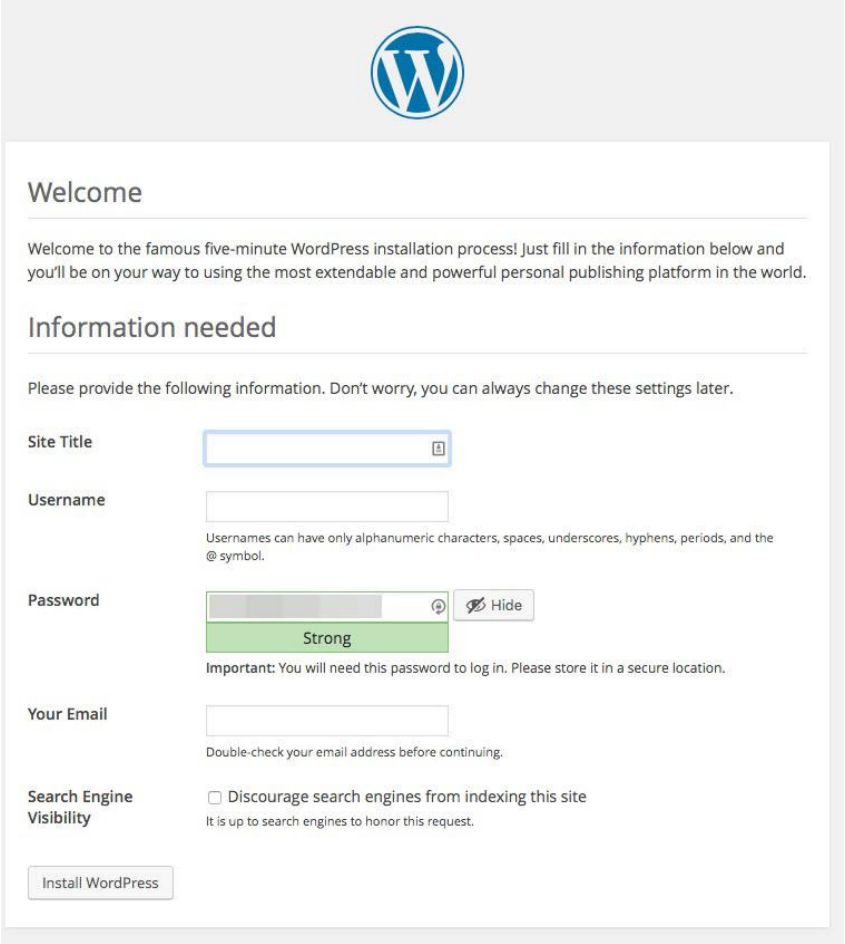

Figure 14: Installing WordPress

> **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 to avoid being charged for these resources.**

Now that you've deployed and tested the 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 AWS compliance 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 has not been initialized.	Set the **Support Config** parameter to **No**, or 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/
- AWS GovCloud (US) User Guide
  http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/

CJIS

- CJIS Security Policy 5.6
  https://www.fbi.gov/file-repository/cjis-security-policy-v5_6_20170605.pdf
- AWS Criminal Justice Information Services (CJIS) Workbook
  https://d0.awsstatic.com/whitepapers/compliance/AWS_CJIS_Workbook.pdf

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 Quick Start and other AWS compliance 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 help you customize and tailor the templates for your specific use cases. Please contact your AWS account manager for further information, or send an inquiry to compliance-accelerator@amazon.com.

Document Revisions

Date	Change	In sections
December 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.

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/ 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.