

# Standardised Architecture for UK-OFFICIAL in the AWS Cloud

## Quick Start Reference Deployment

*April 2020*

*AWS WWPS Team*

*Charlie Llewellyn, Chris King, Matt Johnson AWS Quick Start team*

Visit our [GitHub repository](#) for source files and to post feedback, report bugs, or submit feature ideas for this Quick Start.

### Contents

Overview.....	3
Quick Links .....	3
AWS Enterprise Accelerator – Compliance Architectures .....	5
UK Government Private Networks Connectivity .....	5
Architecture for Compliance on AWS .....	6
AWS Services.....	9
Best Practices .....	12
How You Can Use This Quick Start .....	12
Cost and licenses .....	13
AWS CloudFormation Templates.....	13
AWS CloudFormation Stacks .....	14
Templates Used in this Quick Start .....	14
Managing the Quick Start Source Files .....	15
Uploading the Templates to Amazon S3 .....	16
Using the Console.....	16

Using the AWS CLI.....	16
Updating the Amazon S3 URLs .....	16
Planning the deployment.....	16
Specialized knowledge .....	16
AWS account .....	17
Additional Considerations for production workloads .....	17
User Authentication and Privileges .....	18
Technical requirements .....	18
Deployment options.....	20
Pre-Deployment Steps .....	20
Review AWS Service Limits .....	20
Create Amazon EC2 Key Pairs.....	22
Deployment steps.....	23
Step 1. Sign in to your AWS account.....	23
Step 2. Launch the stacks.....	23
Step 3. Test your deployment .....	23
Step 1. Sign in to your AWS Account.....	24
Step 2. Launch the Stacks .....	25
Step 3. Test Your Deployment .....	27
Deleting the Stacks.....	30
Troubleshooting .....	31
Integrating with AWS Service Catalog .....	32
FAQ.....	32
Send us feedback.....	33
Additional resources .....	33
Document revisions .....	34

This Quick Start was created by AWS WWPS Team in collaboration with Amazon Web Services (AWS).

[Quick Starts](#) are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

## Overview

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 standardised environment that helps organisations adhere to guidelines set out by the UK National Cyber Security Centre (NCSC) for the Cloud Security Principles implementation.

The deployment guide includes links for viewing and launching AWS CloudFormation templates that automate the deployment, a control mapping matrix and additional recommendations and references for extending the approach to incorporate additional requirements.

The purpose of the AWS CloudFormation template is to provide an easily deployable reference architecture for evaluation and testing. Although the template covers many aspects of configuration to support OFFICIAL workloads, it is not intended for production workloads without appropriate review and validation.

Furthermore, organisations will have to consider their own risk, tolerance and internal/external requirements before they can define and implement an [AWS multi-account strategy](#), connectivity with other systems and networks, user authentication workflows, encryption methodologies, logging and auditing requirements and similar components of the architecture. We recommend that you customize the AWS CloudFormation template to meet your own needs in order to obtain a repeatable and auditable reference architecture.

This Quick Start is part of a set of [AWS Enterprise Accelerator – 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 that already meets the [technical requirements](#) for the UK-OFFICIAL deployment, you can [launch the Quick Start](#) to build the architecture shown in [Figure 2](#). The template is launched in the London (EU-WEST-2) region by default.

The deployment takes approximately 45 minutes. If you are new to AWS or to UK-OFFICIAL 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 NCSC publication; indicates which AWS CloudFormation templates and stacks affect the controls implementation; and specifies the associated AWS resources within the templates and stacks.

[View security  
controls  
matrix](#)

Furthermore, the template implements a number of controls to align with the Center for Internet Security (CIS) [Critical Security Controls \(CSC\)](#), and additional recommendations and links to other AWS documents are provided in the spreadsheet in order to assist with the design and deployment of environments in alignment with security best practices.

The excerpt in Figure 1 provides a sample of the available information.



AWS has worked with the UK Government Private Networks providers to develop a set of best practices integrated with architecture pattern defined below for public sector organizations to easily connect to these networks; please contact AWS for guidance.

## Architecture for Compliance on AWS

Deploying this Quick Start builds a multi-VPC network topology, a sample LAMP application and a scalable containerised outbound proxy solution in the AWS Cloud, as illustrated in Figures 2, 3 and 4.

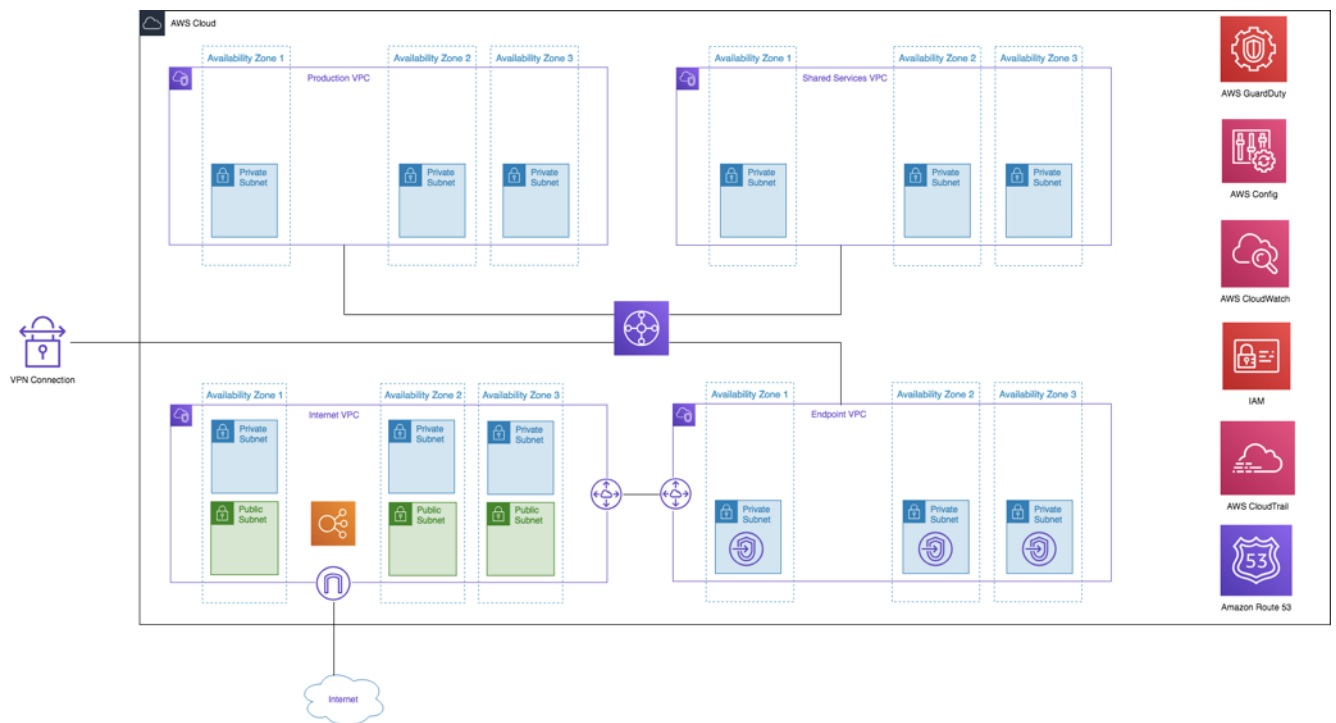


Figure 2: AWS VPC design depicting integration of a production VPC to host application services, an internet VPC to provide both inbound and outbound connectivity (This could also be replaced or enhanced to feature connectivity to a private government network), a shared services VPC to support common tooling e.g. active directory, an Endpoint VPC to provide consolidated access to AWS services and outbound access to the internet.

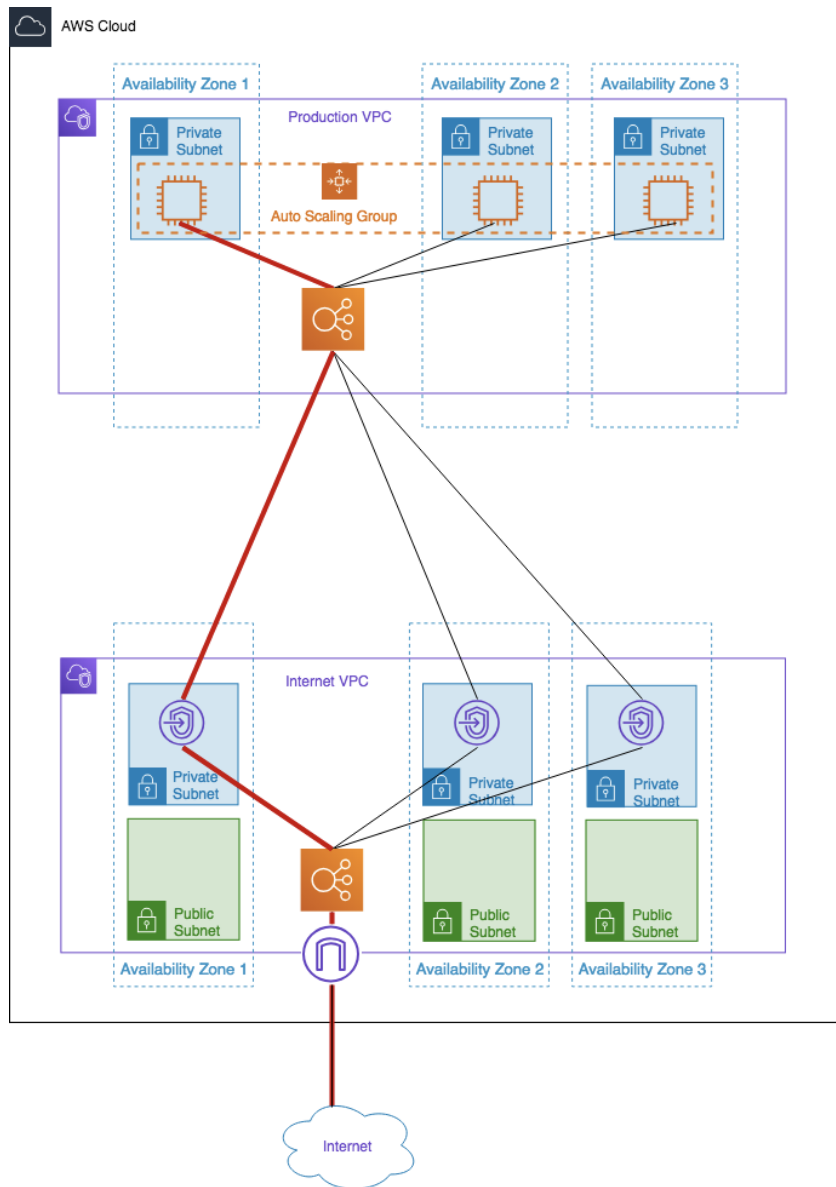


Figure 3: Production VPC depicting integration with Internet VPC for inbound communication to the sample application via AWS PrivateLink.

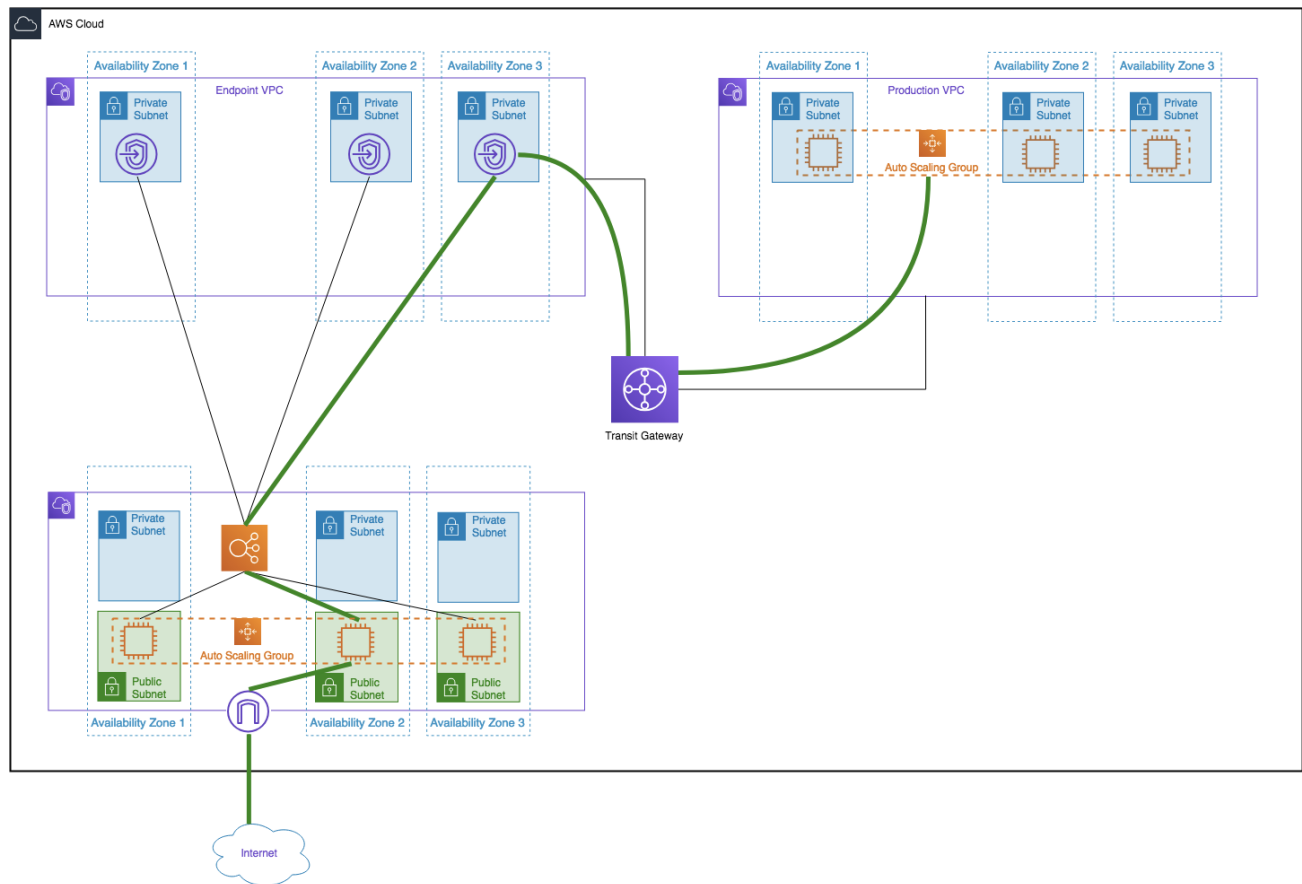


Figure 4: Production VPC depicting outbound access to the internet via the endpoint VPC which passes requests to an autoscaling proxy service.

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
- An external-facing Amazon Virtual Private Cloud (Amazon VPC) for controlled internet access with multi-AZ architecture and separate public and private communication
- An Internal-facing Amazon Virtual Private Cloud (Amazon VPC) for shared services (for example active directory) with multi-AZ architecture and private subnets to support shared services
- An Internal-facing Amazon Virtual Private Cloud (Amazon VPC) for PrivateLink endpoints to allow direct access to AWS services over the AWS backbone with multi-AZ architecture and private subnets to support shared services



- An Internal-facing Amazon Virtual Private Cloud (Amazon VPC) for application workloads with multi-AZ architecture and private subnets to support shared services
- AWS Transit Gateway for inter VPC communication and VPN termination
- Standard Amazon VPC security groups for Amazon Elastic Compute Cloud (Amazon EC2) instances, load balancers and endpoints used in the sample application stack
- LAMP application using Auto Scaling and Elastic Load Balancing, which can be modified and/or bootstrapped with customer application
- AWS Systems manager - sessions manager for administrative access to instances
- Logging, monitoring, and alerts using AWS CloudTrail, Amazon CloudWatch and AWS Config rules
- Route 53 resolver to manage shared private DNS for shared services and endpoints across VPC's
- AWS Certificate manager to store and deploy SSL certificates to endpoints to enable encryption in transit.
- Capture and analysis of security events and compliance status using AWS GuardDuty
- Audit compliance state across AWS with AWS Security Hub.

## 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 section](#) of the AWS documentation.)

- [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 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.
- [AWS Transit Gateway](#) - AWS Transit Gateway is a service that enables customers to connect their Amazon Virtual Private Clouds (VPCs) and their on-premises networks to a single gateway.

- [AWS Systems Manager](#) – AWS Systems Manager is a collection of capabilities for configuring and managing your Amazon EC2 instances, on-premises servers and virtual machines, and other AWS resources at scale. Systems Manager includes a unified interface that allows you to easily centralize operational data and automate tasks across your AWS resources.
- [AWS Resource Manager](#) - AWS Resource Access Manager (AWS RAM) enables you to share your resources with any AWS account or through AWS Organizations. If you have multiple AWS accounts, you can create resources centrally and use AWS RAM to share those resources with other accounts.
- [AWS Organizations](#) - AWS Organizations is an account management service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. AWS Organizations includes account management and consolidated billing capabilities that enable you to better meet the budgetary, security, and compliance needs of your business.
- [Amazon GuardDuty](#) - Amazon GuardDuty is a threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.
- [Route 53 Resolver](#) - Route 53 Resolver makes hybrid cloud easier for enterprise customers by enabling seamless DNS query resolution across your entire hybrid cloud. Create DNS endpoints and conditional forwarding rules to allow resolution of DNS namespaces between your on-premises data center and Amazon Virtual Private Cloud (VPC).
- [AWS Certificate Manager](#) - AWS Certificate Manager is a service that lets you easily provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.
- [AWS Security Hub](#) - AWS Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status across AWS accounts. There are a range of powerful security tools at your disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. But oftentimes this leaves your team switching back-and-forth between these tools to deal with hundreds, and sometimes thousands, of security alerts every day. With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or

findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. Your findings are visually summarized on integrated dashboards with actionable graphs and tables. You can also continuously monitor your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows. Get started with AWS Security Hub in just a few clicks in the Management Console and once enabled, Security Hub will begin aggregating and prioritizing findings.

## 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 and ports
- Network access control list (ACL) rules to filter traffic into subnets as an additional layer of network security
- Management of instances through managed services to facilitate restricted login access for system administrator actions
- NAT gateways, PrivateLink and proxies to manage internet access
- Serverless containers to provide explicit outbound proxy functionality
- Standard IAM policies with associated groups and roles, exercising least privilege
- Monitoring and logging; alerts and notifications for critical events such as logging of root activity, IAM changes, and changes to logging policies
- S3 buckets (with security features enabled) for logging and archive
- Implementation of proper load balancing and Auto Scaling capabilities
- HTTPS-enabled Application Load Balancing (ALB) load balancers with hardened security policy (please note that a self-signed certificate is auto-generated for testing purposes)
- Amazon RDS database with backup and encryption

## How You Can Use This Quick Start

You can 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.

As mentioned in the ‘About this Guide’ section, this template is not intended to be used for production workloads without thorough review, validation, and inclusion of your own business and technical requirements.

We’d highly recommend that following on from the learnings enabled by this template that the concepts are applied in line with concepts from [AWS Landing Zones](#).

## Cost and licenses

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

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, 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.

**Tip** After you deploy the Quick Start, we recommend that you enable the [AWS Cost and Usage Report](#) to track costs associated with the Quick Start. This report delivers billing metrics to an S3 bucket in your account. It provides cost estimates based on usage throughout each month, and finalizes the data at the end of the month. For more information about the report, see the [AWS documentation](#).

## AWS CloudFormation Templates

The CloudFormation templates included in this Quick Start are a YAML-formatted text file that describes the AWS infrastructure needed to run an application or service along with any interconnections among infrastructure components. YAML (YAML Ain’t Markup Language) is a human-friendly data serialization standard for all programming languages. 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.

Stack and template	Description	Dependencies
<b>Main stack</b> ( <a href="#">master_template.yaml</a> )	Primary template file that deploys the rest of the stacks and passes parameters between nested templates automatically.	None
<b>VPC stack</b> ( <a href="#">vpc.yaml</a> )	Customisable template to deploy secure VPCs.	None
<b>Networking stack</b> ( <a href="#">tgw.yaml</a> )	Sets up the transit gateway and VPC endpoints that provides network connectivity between the VPC's and between VPC's and AWS services.	VPC Stack
<b>Outbound proxy stack</b> ( <a href="#">outboundProxy.yaml</a> )	Configures a scalable outbound containerized proxy service on Fargate to allow applications to securely connect to the internet.	Networking Stack



Stack and template	Description	Dependencies
<b>Compliance Controls stack</b> <a href="#">(compliance-controls.yaml)</a>	Configures a number of good practices to adhere to the CIS benchmarks measured by AWS Security Hub.	VPC Stack
<b>Clean-up of the default VPC stack</b> <a href="#">(compliance-controls.yaml)</a>	Configures VPC best practices for OFFICIAL data in any pre-existing defaults VPC that may already be created	VPC Stack
<b>Application stack</b> <a href="#">(sampleApplication.yaml)</a>	Sets up EC2, instances, web application, an Amazon RDS database, HTTPS Application Load Balancing, Amazon CloudWatch alarms, and Auto Scaling groups.	Outbound Proxy Stack

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

To deploy the entire architecture (including IAM and Amazon VPC), use **master\_template.yaml** 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 **master\_template.yaml** 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.

## Uploading the Templates to Amazon S3

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/>.
6. Use the following AWS CLI command to upload each template file:

```
aws s3 cp <template file>.yaml 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 **master\_template.yaml** file.

## Planning the deployment

### 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 associated with UK-OFFICIAL 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 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

This deployment guide also requires a moderate level of familiarity with AWS services. If you're new to AWS, visit the [Getting Started Resource Center](#) and the [AWS Training and Certification website](#) for materials and programs that can help you develop the skills to design, deploy, and operate your infrastructure and applications on the AWS Cloud.

## 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.

Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

## ADDITIONAL CONSIDERATIONS FOR PRODUCTION WORKLOADS

A very important aspect of any AWS-based solution relates to the AWS accounts strategy. The section above describes the simple process for creating a single AWS account you can use to deploy the template for testing purposes. However, for production environments, we recommend that you adopt a [multi-account strategy](#) in order to maximize operational efficiency, finance management and reporting, security, auditability, and an effective implementation of security best practices.

For instance, your AWS accounts setup could include:

- Billing account (containing an Amazon S3 bucket to hold financial reporting only)
- Development account
- Production account
- Logging account (containing Amazon S3 bucket(s) to hold logs only)

And, as necessary:

- Auditing account (to provide read access to everything for auditors/accreditors)

- User account (used to manage user identities)

Additionally, regardless of which setup you choose, you should configure each AWS account by following the recommendations in the [CIS Foundation Benchmark for AWS](#), as appropriate.

## USER AUTHENTICATION AND PRIVILEGES

Whenever possible, users should be authenticated via federation (e.g. SAML) with a customer existing identity provider (IdP), as described in the [AWS IAM documentation](#), in order to avoid the proliferation of multiple IdPs – unless AWS identity services are used as your authoritative IdP. Furthermore, you should use [temporary user credentials](#) to control access to AWS resources, and granting users one default permission only, which is the [AssumeRole](#) permission. AWS IAM can then be used to manage users-to-roles mapping.

In this way, user identities will be managed in a consistent manner, and the credentials used to access AWS resources will be dynamically generated and limited in time, reducing the attack surface and improving the overall security posture. This is in line with the recommendations included in the [CIS Foundation Benchmark for AWS](#) and security best practices.

## Technical requirements

Before you launch the Quick Start, your account must be configured as specified in the following table. Otherwise, deployment might fail.

---

### [Resources](#)

If necessary, request [service limit increases](#) for the following resources. You might need to do this if you already have an existing deployment that uses these resources, and you think you might exceed the default limits with this deployment. For default limits, see the [AWS documentation](#).

[AWS Trusted Advisor](#) offers a service limits check that displays your usage and limits for some aspects of some services.

Resource	This deployment uses
VPCs	4
Elastic IP addresses	1
IAM security groups	10
IAM roles	14
Auto Scaling groups	1
Application Load Balancers	1
Network Load Balancers	2
t3.micro instances	7
db.t3.micro	2

---

### [Regions](#)

This deployment is built for UK Official Compliance and has only been tested in the London and Ireland Regions. In regions outside London and Ireland the required services may not exist, you can check the [AWS region table](#) to confirm.

---

### [Key pair](#)

Make sure that at least one Amazon EC2 key pair exists in your AWS account in the region where you are planning to deploy the Quick Start. Make note of the key pair name. You'll be prompted for this information during deployment. To create a key pair, follow the [instructions in the AWS documentation](#).

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

---

### [IAM permissions](#)

To deploy the Quick Start, you must log 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 S3 buckets that were created during the previous deployment; **otherwise, the re-deployment will fail**.

---

### [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 **master\_template.yaml** file. **Otherwise, deployment will fail**.

---

## Deployment options

This Quick Start provides two deployment options, both of which deploy new VPCs and resources:

- **Deploy using AWS CLI commands or AWS Management Console.** We've provided step-by-step instructions for the AWS Management Console deployment option in the following sections.
- **Deploy using AWS Service Catalog.** This option 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.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and <software> settings, as discussed later in this guide.

## 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 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.

## 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:

2. Open the Trusted Advisor console at <https://console.aws.amazon.com/trustedadvisor/>.

3. In the navigation pane, choose **Service Limits**.
4. Scroll through the service limit names and compare the **Limit Amount** column to the **Current Usage** column, to ensure that you have available capacity to support the deployment, as stated in [Technical Requirements table](#).

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

The screenshot shows the AWS Support Center 'Create case' interface. At the top, there's a navigation bar with 'aws', 'Services', 'Resource Groups', and a search bar. Below this, the 'Create case' section is active. It features three tabs: 'Account and billing support', 'Service limit increase' (which is selected), and 'Technical support'. The 'Service limit increase' tab shows a description: 'Requests to increase the service limit of your AWS resources'. Below the tabs is the 'Case classification' section, which includes a 'Limit type' dropdown set to 'EC2 Instances' and a 'Severity' dropdown set to 'General question'. The 'Requests' section contains a blue informational box stating: 'To request additional limit increases for the same limit type, choose Add another request. To request an increase for a different limit type, create a separate limit increase request.' Below this, there's a 'Request 1' section with a 'Region' dropdown set to 'EU (London)' and a 'Remove' button.

**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:

5. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
7. In the navigation pane, under **Network & Security**, choose **Elastic IPs**.
8. 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).
9. In the navigation pane, under **Load Balancing**, choose **Load Balancers**.

10. 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).
11. In the navigation pane, under **Auto Scaling**, choose **Auto Scaling Groups**.
12. 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 you are planning to deploy the Quick Start in**.

6. Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
7. Use the region selector in the navigation bar to choose the AWS Region where you plan to deploy.
8. In the navigation pane, under **Network & Security**, choose **Key Pairs**.
9. 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](#).

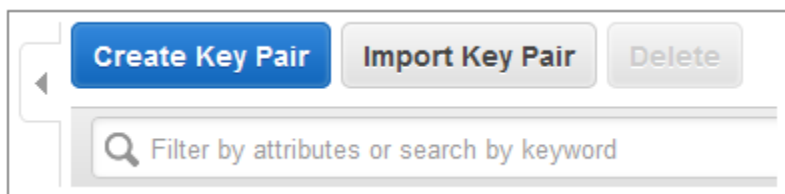


Figure 5: Creating a key pair

**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.

## Deployment steps

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

### Step 1. Sign in to your AWS account

- Sign in to your AWS account at <https://aws.amazon.com> with an IAM user role that has the necessary permissions. For details, see [Planning the deployment](#) earlier in this guide.
- Make sure that your AWS account is configured correctly, as discussed in the [Technical requirements](#) section.

### Step 2. Launch the stacks

- Sign in to your AWS account.
- 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.

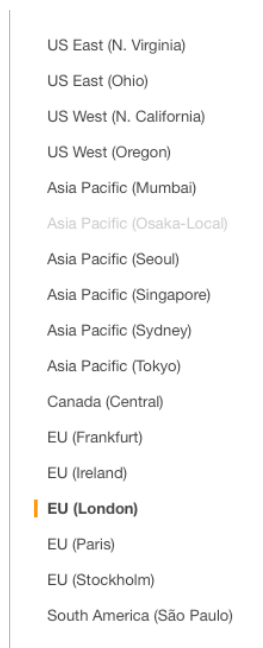
### Step 3. Test your deployment

- Use the URL provided in the **Outputs** tab for the main stack to test the deployment.

## Step 1. Sign in to your AWS Account

10. Sign in to your AWS account at <http://aws.amazon.com> with an IAM user role that has the appropriate privileges (see [IAM Permissions](#) earlier in this document).
11. 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](#).
12. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy the Quick Start 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 **t3.micro** instance type for the WordPress portion of the deployment.



**Figure 10: Choosing an AWS Region**

13. 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.

13. [Launch the AWS CloudFormation template](#) into your AWS account.

[Launch](#)

The template will be deployed into the UK (London) Region. 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.

The stacks take approximately 40 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. As of the date of publication, the cost for using the Quick Start with default settings is approximately \$0.96 an hour, and you can complete the initial deployment for about \$3.00. Prices are subject to change. See the pricing pages for each AWS service you will be using in this Quick Start for full details.

You can also [download the template](#) to use it as a starting point for your customization.

14. On the **Select Template** page, keep the default settings for the template URL, and then choose **Next**.
15. 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
<b>Project Name</b> (ProjectName)	official-quickstart	Project Name used to tag resources for cost attribution.
<b>Internet VPC Cidr</b> (InternetVPCCidr)	10.0.0.0/16	CIDR used for the internet VPC.
<b>Shared services VPC Cidr</b> (SharedVPCCidr)	10.10.0.0/16	CIDR used for the shared services VPC.
<b>Production VPC Cidr</b> (ProductionVPCCidr)	172.16.0.0/16	CIDR used for the production VPC used to host the sample application.
<b>Endpoint VPC Cidr</b> (EndpointVPCCidr)	192.168.0.0/16	CIDR used for the endpoint VPC.

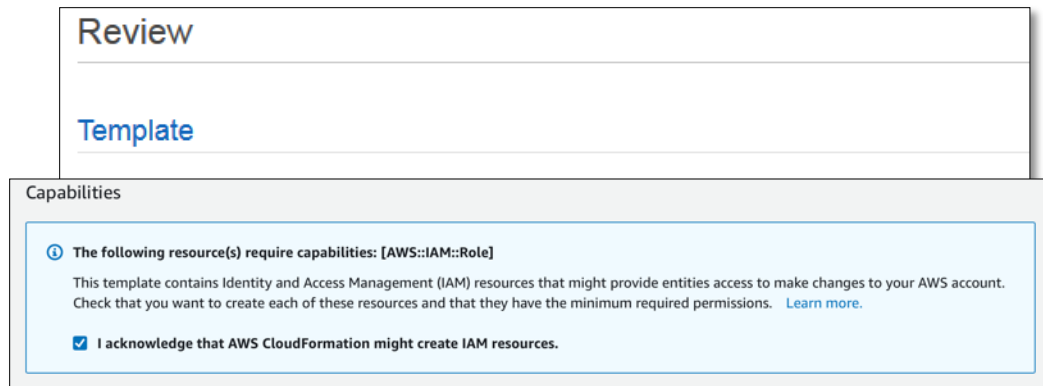
Parameter label (name)	Default	Description
<b>Database Password</b> (DBPassword)	<b><i>Requires input</i></b>	Password for the database administrator account. This must be a <a href="#">complex password</a> that's between 8 and 28 mixed, alphanumeric characters.
<b>CIS alerting emails</b> (CisAlertingEmail)	<b><i>Requires input</i></b>	Email address that will be subscribed to alerting emails for CIS compliance controls.

### *AWS Quick Start Configuration:*

Parameter label (name)	Default	Description
<b>Quick Start S3 Bucket Name</b> (QSS3BucketName)	quickstart-reference	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.
<b>Quick Start S3 Bucket Name</b> (QSS3BucketName)	quickstart-reference	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.
<b>Quick Start S3 Key Prefix</b> (QSS3KeyPrefix)	enterprise-accelerator/uk/official/latest	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.

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

- 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**.
- 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

Capabilities

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

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more.](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources.

Figure 11: IAM resource acknowledgement

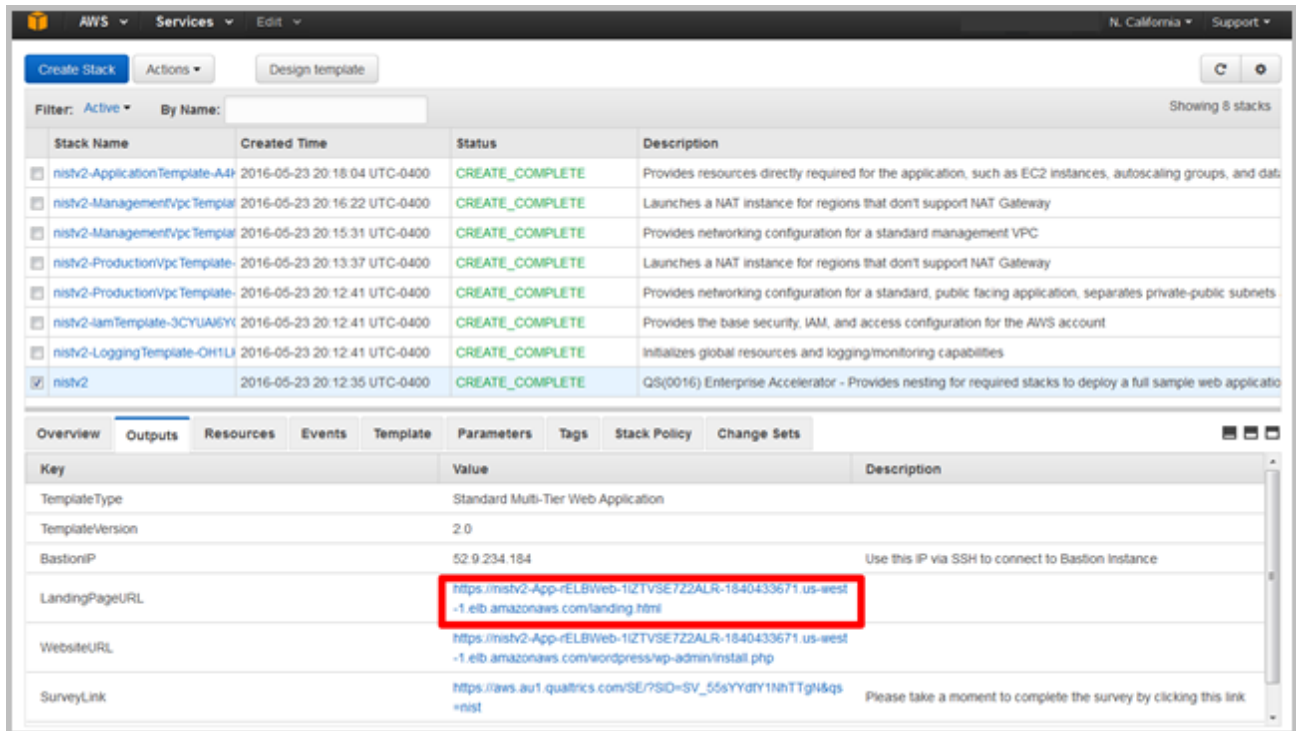
18. Choose **Create** to deploy the stack.
19. Monitor the status of the stack being deployed. When the status field shown in Figure 12 displays **CREATE\_COMPLETE for all the stacks deployed**, the cluster for this reference architecture is ready. Since you're deploying the full architecture, you'll see eight stacks listed (for the main template and seven nested templates).

	Stack name	Status	Created time
<input type="radio"/>	private-network-tgw	⌚ CREATE_IN_PROGRESS	Thu, 21 Feb 2019 13:22:17 GMT

Figure 12: Status message for deployment

### Step 3. Test Your Deployment

To test your deployment, choose the link for **LandingPageURL**, as shown in Figure 13. This URL is available from the **Outputs** tab for the main stack:




The screenshot shows the AWS CloudFormation console. At the top, there's a navigation bar with 'AWS', 'Services', and 'Edit'. Below that, there are buttons for 'Create Stack', 'Actions', and 'Design template'. A filter is set to 'Active' and 'By Name'. A table lists 8 stacks, all with a status of 'CREATE\_COMPLETE'. The 'nistv2' stack is selected. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', and 'Change Sets'. The 'Outputs' tab is active, showing a table with columns 'Key', 'Value', and 'Description'. The 'LandingPageURL' output is highlighted with a red box, showing the URL 'https://nistv2-App-ELBWeb-1iZTVSE7Z2ALR-1840433671-us-west-1.elb.amazonaws.com/landing.html'.

Stack Name	Created Time	Status	Description
nistv2-ApplicationTemplate-A4	2016-05-23 20:18:04 UTC-0400	CREATE_COMPLETE	Provides resources directly required for the application, such as EC2 instances, autoscaling groups, and data
nistv2-ManagementVpcTempla	2016-05-23 20:16:22 UTC-0400	CREATE_COMPLETE	Launches a NAT instance for regions that don't support NAT Gateway
nistv2-ManagementVpcTempla	2016-05-23 20:15:31 UTC-0400	CREATE_COMPLETE	Provides networking configuration for a standard management VPC
nistv2-ProductionVpcTempla	2016-05-23 20:13:37 UTC-0400	CREATE_COMPLETE	Launches a NAT instance for regions that don't support NAT Gateway
nistv2-ProductionVpcTempla	2016-05-23 20:12:41 UTC-0400	CREATE_COMPLETE	Provides networking configuration for a standard, public facing application, separates private-public subnets
nistv2-iamTemplate-3CYUA6YK	2016-05-23 20:12:41 UTC-0400	CREATE_COMPLETE	Provides the base security, IAM, and access configuration for the AWS account
nistv2-LoggingTemplate-OH1LJ	2016-05-23 20:12:41 UTC-0400	CREATE_COMPLETE	Initializes global resources and logging/monitoring capabilities
nistv2	2016-05-23 20:12:35 UTC-0400	CREATE_COMPLETE	QS(0016) Enterprise Accelerator - Provides nesting for required stacks to deploy a full sample web applicatio

Key	Value	Description
TemplateType	Standard Multi-Tier Web Application	
TemplateVersion	2.0	
BastionIP	52.9.234.184	Use this IP via SSH to connect to Bastion Instance
LandingPageURL	<a href="https://nistv2-App-ELBWeb-1iZTVSE7Z2ALR-1840433671-us-west-1.elb.amazonaws.com/landing.html">https://nistv2-App-ELBWeb-1iZTVSE7Z2ALR-1840433671-us-west-1.elb.amazonaws.com/landing.html</a>	
WebsiteURL	<a href="https://nistv2-App-ELBWeb-1iZTVSE7Z2ALR-1840433671-us-west-1.elb.amazonaws.com/wordpress/wp-admin/install.php">https://nistv2-App-ELBWeb-1iZTVSE7Z2ALR-1840433671-us-west-1.elb.amazonaws.com/wordpress/wp-admin/install.php</a>	
SurveyLink	<a href="https://aws.au1.qualtrics.com/SE?SID=SV_55sYYdY1NHTTgH&amp;qsr=nist">https://aws.au1.qualtrics.com/SE?SID=SV_55sYYdY1NHTTgH&amp;qsr=nist</a>	Please take a moment to complete the survey by clicking this link

Figure 13: Opening the landing page





The link should launch a new page in your browser that looks similar to Figure 14.



Congratulations!

You have successfully launched the **Standardized Architecture for (compliance-body)** on the AWS Cloud Quick Start!

---

### 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 experience. 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 stack. To customize your implementation of this Quick Start, modify the application stack to suit the needs of your application.



**Figure 14: 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 14. 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 15. You can install and test the WordPress deployment from here.

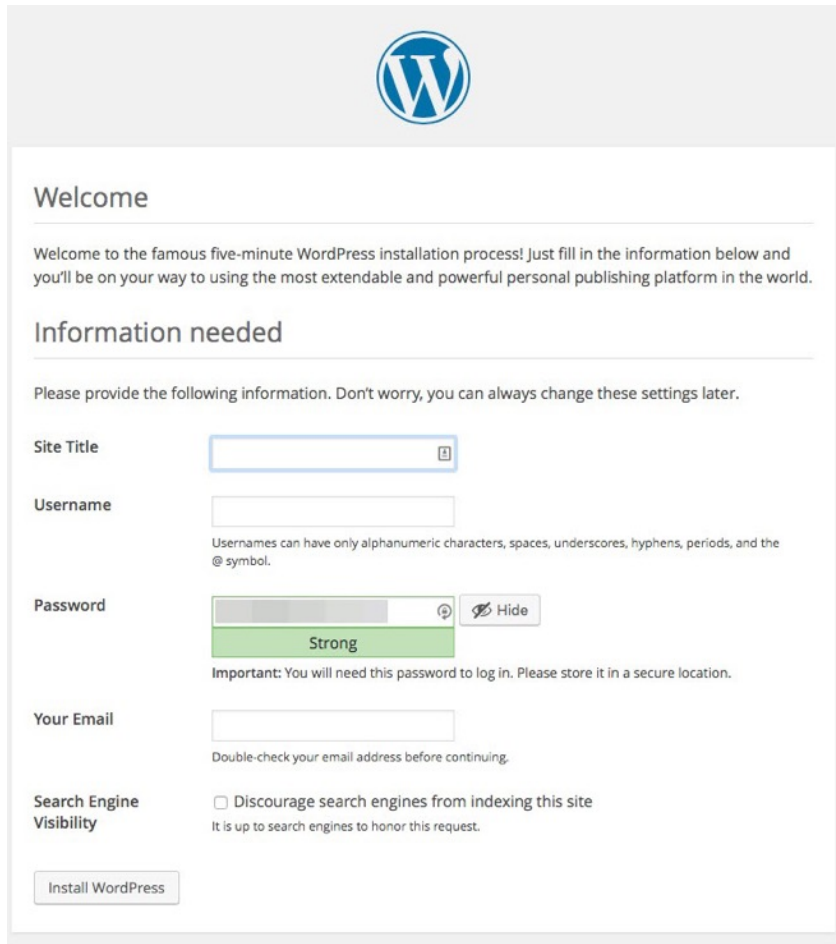
The image shows the WordPress installation 'Welcome' screen. At the top is the WordPress logo. Below it, the heading 'Welcome' is followed by a paragraph: 'Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.' The next section is 'Information needed', with a subtext: 'Please provide the following information. Don't worry, you can always change these settings later.' The form includes: 'Site Title' with a text input field; 'Username' with a text input field and a note: 'Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.'; 'Password' with a masked input field, a 'Hide' button, and a green bar indicating 'Strong' password strength, followed by the note: 'Important: You will need this password to log in. Please store it in a secure location.'; 'Your Email' with a text input field and a note: 'Double-check your email address before continuing.'; and 'Search Engine Visibility' with a checkbox 'Discourage search engines from indexing this site' and a note: 'It is up to search engines to honor this request.' At the bottom is an 'Install WordPress' button.

Figure 15: 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 NIST 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 Enterprise Accelerator – 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
<b>The following resource(s) failed to create:</b> <b>[rConfigRuleForRequiredTags, rConfigRuleForUnrestrictedPorts, rConfigRuleForSSH, rConfigRulesLambdaRole]</b>	The <b>Support Config</b> parameter was set to <b>Yes</b> , but AWS Config isn't available in the region you selected, or AWS Config has not been initialized.	Set the <b>Support Config</b> parameter to <b>No</b> , or select another region. Also make sure that AWS Config is set up properly, as described in the <a href="#">pre-deployment steps</a> .
<b>Maximum VPCs limit reached</b>	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 <a href="#">technical requirements</a> .
<b>Maximum EIPs limit reached</b>	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 <a href="#">technical requirements</a> .
<b>Other limits exceeded</b>	You've exceeded the use of resources in your AWS account.	See <a href="#">technical requirements</a> , and <a href="#">request service limit increases</a> 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	<a href="#">Creating and Deleting Portfolios</a>
Create a new product	<a href="#">Adding and Removing Products</a>
Give users access	<a href="#">Granting Access to Users</a>
Assign IAM roles for deploying stacks	<a href="#">Applying Launch Constraints</a> 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	<a href="#">Tagging Portfolios</a>
Perform other administrative tasks	<a href="#">AWS Service Catalog Administrator Guide</a>
Launch products from AWS Service Catalog	<a href="#">AWS Service Catalog User Guide</a>

## FAQ

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

**A.** If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. (For Windows, look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)



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

For additional information, see [Troubleshooting AWS CloudFormation](#) on the AWS website.

**Q.** I encountered a size limitation error when I deployed the AWS CloudFormation templates.

**A.** We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the [AWS documentation](#).

## Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the [GitHub repository](#) for this Quick Start. If you'd like to submit code, please review the [Quick Start Contributor's Guide](#).

## Additional resources

### AWS resources

- [Getting Started Resource Center](#)
- [AWS General Reference](#)
- [AWS Glossary](#)

### AWS services

- [AWS CloudFormation](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [IAM](#)
- [Amazon VPC](#)

### Other Quick Start reference deployments

- [AWS Quick Start home page](#)

## Document revisions

Date	Change	In sections
<b>October 2019</b>	Initial review	—
<b>April 27, 2020</b>	Updated to use new services available with AWS	All

### 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

