Evidian SafeKit on the AWS Cloud

Quick Start Reference Deployment

July 2020

Thierry Leconte, Evidian

Troy Ameigh, 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

This Quick Start was created by Evidian in collaboration with Amazon Web Services (AWS). Evidian is a wholly owned subsidiary of Atos.

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 provides step-by-step instructions for deploying an Evidian SafeKit cluster automatically on the AWS Cloud.

This Quick Start is for people who want to try the Evidian SafeKit product for building high-availability clusters with synchronous real-time replication, network load balancing, and automatic failover. SafeKit addresses business continuity, disaster recovery, and scalability for Windows and Linux applications with redundancy and with active or passive backup servers.

Please know that we may share who uses an AWS Quick Start with the AWS Partner Network (APN) Partner that collaborated with AWS on its content.

SafeKit on AWS

Inside the Atos cybersecurity division, Evidian has developed SafeKit, a software-only high-availability product that helps companies secure 24/7 operation of critical applications. It does not require specific hardware, specific network configuration, or specific external storage. It lends itself to the AWS Cloud because it is hardware agnostic.

The unavailability of an application can be due to three types of problems that SafeKit addresses on AWS:

- **Hardware and environment (20%):** This problem includes the failure of a server, a rack, or an entire data center. This Quick Start addresses the problem by deploying across multiple AWS Availability Zones.
- **Software (40%):** Software failures can be triggered by faulty software updates, software bugs, or overloaded services. SafeKit on AWS addresses these with smooth server-by-server updating, process monitoring, custom application checkers, and load balancing of front-end applications.
- **Human errors (40%):** Problems related to human error include administration error and the inability to properly restart a critical service. The SafeKit interface enables users to control all their AWS clusters and servers from a single web console. They can access the console in a browser either on the servers or on an external workstation.

Mirror and farm modules

SafeKit works with various software clusters. Customers can configure clusters for a given application using one or more application modules: mirror modules, farm modules, or a combination. Mirror modules use primary and secondary servers with real-time file replication and failover. Farm modules use network load balancing with failover for up to four servers.

Customers configure each module with the following: the server IP addresses for heartbeats, the virtual IP address of the cluster, load-balancing rules (for farm modules), the file directories to replicate (for mirror modules), the hardware and software failure detectors, and the service to restart in case of failure.

Examples of preconfigured mirror modules delivered with SafeKit are Microsoft SQL Server, PostgreSQL, Oracle, MySQL, Firebird, Hyper-V, Milestone, and Hanwha for video surveillance. Customers can create a new module for a new application starting from the generic mirror module and configuring it to replicate any type of data and restart any services.

Examples of preconfigured farm modules delivered with SafeKit are Apache and Microsoft IIS. Customers can create a new module for a new application starting from the generic farm module and configuring it to load balance any port and restart any services.

Mirror modules work as follows:

- Users are connected to a primary/secondary virtual IP address, which is configured in the load balancer. SafeKit provides a generic health check for the load balancer. On the primary server, the health check returns **OK** to the load balancer and **NOK** on the secondary server.
- On each server, SafeKit monitors the critical application with process checkers and custom checkers.
- SafeKit automatically restarts the critical application via restart scripts when there is a software or hardware failure.
- SafeKit replicates files between the instance file systems that contain critical data synchronously in real time.
- A connector for the SafeKit web console is installed in each server, enabling you to manage the high-availability cluster from a browser.

Farm modules work as follows:

- Users are connected to a virtual IP address, which is configured in the load balancer.
- SafeKit provides a generic health check for the load balancer. When the farm module is stopped on a server or when the server terminates, the health check returns **NOK** to the load balancer, which stops load-balancing requests to the server.
- On each server, SafeKit monitors the critical application with process checkers and custom checkers.
- SafeKit automatically restarts the critical application via restart scripts in a server when there is a software failure.
- A connector for the SafeKit web console is installed in each server, enabling you to manage the high-availability cluster from a browser.

The generic mirror and farm modules can be automatically deployed with the AWS Quick Start. Customers can also manually install SafeKit on existing AWS servers. See the FAQ section of this deployment guide.

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 Amazon Simple Storage Service (Amazon 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.

Evidian SafeKit provides a free trial license that's good for three days of continuous uptime. For a full license, contact an Evidian sales representative or an Evidian partner.

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the following SafeKit environment in the AWS Cloud.

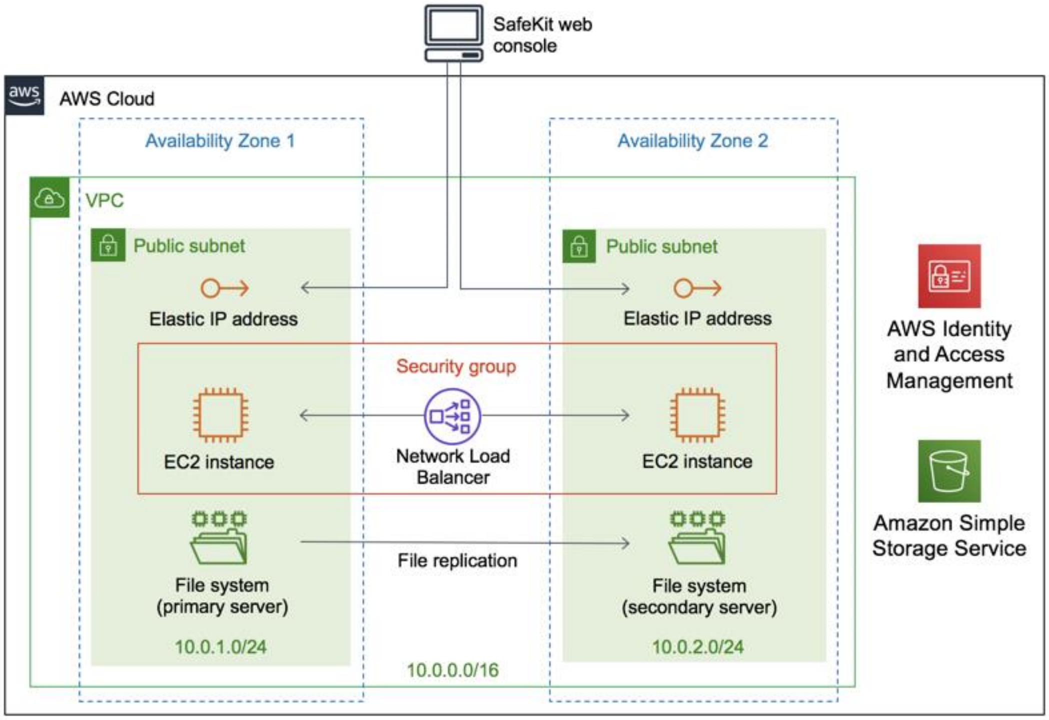


Figure 1: Quick Start architecture for SafeKit mirror on AWS

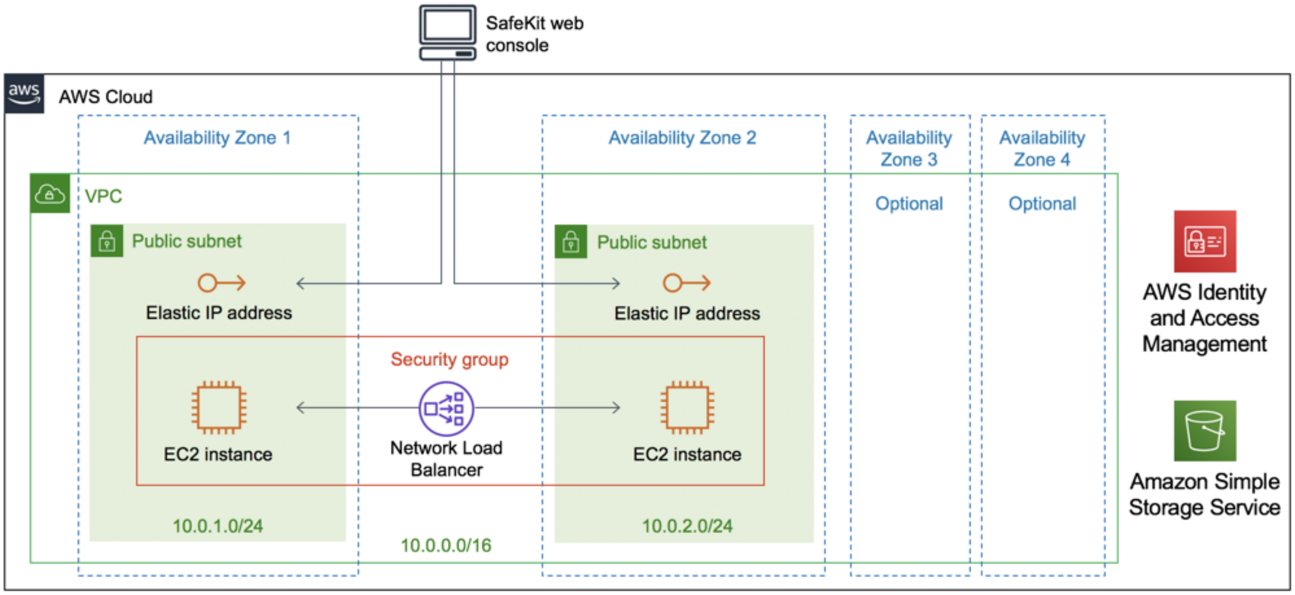


Figure 2: Quick Start architecture for SafeKit farm on AWS

As shown in Figures 1 and 2, the Quick Start sets up the following:

- A highly available architecture that spans two Availability Zones for the mirror module and up to four for the farm module.
- A VPC configured with public subnets, according to AWS best practices, providing you with your own virtual network on AWS.
- An AWS Identity and Access Management (IAM) role that accesses the SafeKit Quick Start S3 bucket.
- In the public subnets:
  - An Elastic IP address that gives access to the SafeKit web console.
  - One Amazon Elastic Compute Cloud (EC2) instance for either Linux or Windows.
  - A security group that allows inbound Secure Shell (SSH) or Windows Remote Desktop Protocol (RDP) access to the EC2 instances through the public IP addresses. The security group also allows access to the virtual IP port to the Elastic IP addresses.
  - A Network Load Balancer that balances traffic between the instances and checks the health of the SafeKit URL.

Figure 1 shows the mirror module:

- Two servers—one primary and one secondary—that run in separate Availability Zones. The critical application runs on the primary server.

Figure 2 shows the farm module:

- One to four servers that run in separate Availability Zones. The critical application runs in all servers in the farm.

Planning the deployment

Specialized knowledge

This deployment guide 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 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.

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 quota 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 quotas with this deployment. The Service Quotas console displays your usage and quotas for some aspects of some services. For more information, see the AWS documentation.

Resource	This deployment uses
VPC	1
IAM security group	1
IAM role	1
Elastic IP addresses	2–4
Network Load Balancer	1
EC2 instances	2–4

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're 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**.

Deployment options

This Quick Start provides two deployment options: mirror and farm.

- **Mirror:** Deploy Evidian SafeKit into a new VPC with a mirror module running. This option builds a new AWS environment consisting of the VPC, subnets, security groups, load balancer, instances, and other infrastructure components. It then deploys SafeKit into this new VPC, and then installs, configures, and launches a SafeKit generic mirror module.
- **Farm:** Deploy Evidian SafeKit into a new VPC with a farm module running. This option builds a new AWS environment consisting of the VPC, subnets, security groups, load balancer, instances, and other infrastructure components. It then deploys SafeKit into this new VPC, and then installs, configures, and launches a SafeKit generic farm module.

The Quick Start provides separate templates for these options. It also lets you configure Classless Inter-Domain Routing (CIDR) blocks, instance types, and SafeKit settings, as discussed later in this guide.

Deployment steps

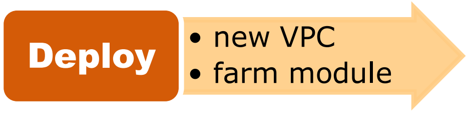
Step 1. Sign in to your AWS account

1. Sign in to your AWS account at https://aws.amazon.com with an IAM user role that has the necessary permissions. See Planning the deployment earlier in this guide.
2. Make sure that your AWS account is configured correctly, as discussed in the Technical requirements section.

Step 2. Launch the Quick Start

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

1. Sign in to your AWS account. Choose one of these options to launch the AWS CloudFormation template. For help, see Deployment options earlier in this guide.



Deploy SafeKit mirror into a new VPC on AWS

Deploy SafeKit farm into a new VPC on AWS

Each deployment takes about 30 minutes to complete.

2. Check the Region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for SafeKit will be built. The template is launched in the US East (N. Virginia) Region by default.

3. On the **Create stack** page, keep the default setting for the template URL, and then choose **Next,** two times.
4. On the **Specify stack details** page, set the stack name and review the parameters for the template.
5. Provide values for the parameters that require input (Availability Zones, key pair, and certificates password). For all other parameters, review the default settings and customize them as necessary.

In the following tables, parameters are listed by category and described separately for the two deployment options:

- Parameters for deploying SafeKit mirror into a new VPC
- Parameters for deploying SafeKit farm into a new VPC

When you finish reviewing and customizing the parameters, choose **Next**.

Option 1: Parameters for deploying SafeKit mirror into a new VPC

View template

Network configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	*Requires input*	Choose the Availability Zones to use. The Quick Start uses two Availability Zones from your list.
Public subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for the public DMZ subnet located in Availability Zone 1.
Public subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for the public DMZ subnet located in Availability Zone 2.
Allowed CIDR for SafeKit environment (RemoteAccessCIDR)	*Requires input*	Enter the CIDR IP range that is permitted to access SafeKit environment. Set this value to a trusted IP range. For example, you might grant access only to your corporate network.
Allowed CIDR for virtual IP access to SafeKit web console (VipCIDR)	*Requires input*	Enter the CIDR IP range that is permitted to access SafeKit web console. Set this value to a trusted IP range. For example, you might grant access only to your corporate network.

Amazon EC2 configuration:

Parameter label (name)	Default	Description
Key pair name (KeyPairName)	*Requires input*	Enter the public/private key pair you created in your preferred AWS Region; see the Technical requirements section of the deployment guide.
Instance type (InstanceType)	t2.small	Choose the Amazon EC2 instance type.
Operating system (OSType)	Linux	Choose Windows to change the operating system.

Evidian SafeKit – mirror cluster configuration:

Parameter label (name)	Default	Description
SafeKit module name (SafekitModuleName)	mirror	The name of the SafeKit module you're deploying. This is not editable.
Instance name prefix (InstanceNamePrefix)	server	The prefix in the SafeKit web console for each instance name. Enter a different name if required for your configuration.
Virtual IP port (VipPort)	9453	The port of the virtual IP that is used for failover of the SafeKit mirror. Enter a port 1–49151.
Password (CAservPwd)	*Requires input*	Password for SafeKit web console certificates. Must be at least 8 characters long and contain at least 1 uppercase letter, 1 lowercase letter, and 1 number. Do not use quotation marks, backslashes, forward slashes, or the @ symbol.

AWS Quick Start configuration:

Note: We recommend keeping these default settings for the “AWS Quick Start configuration” parameters unless you are customizing the Quick Start templates for your own deployment projects. Changing these parameter settings automatically updates code references to point to a new Quick Start location. For details, see the AWS Quick Start Contributor’s Guide.

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	aws-quickstart	The S3 bucket that you created for your copy of Quick Start assets. Use this if you decide to customize the Quick Start. This bucket name can include numbers, lowercase letters, uppercase letters, and hyphens but should not start or end with a hyphen.
Quick Start S3 bucket Region (QSS3BucketRegion)	us-east-1	The AWS Region where the Quick Start S3 bucket (QSSBucketName) is hosted. When using your own bucket, you must specify this value.
Quick Start S3 key prefix (QSS3KeyPrefix)	quickstart-atos-evidian-safekit/	The S3 key name prefix that is used to simulate a folder for your copy of Quick Start assets. Use this if you decide to customize the Quick Start. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes. See https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html.

OPTION 2: PARAMETERS FOR DEPLOYING SAFEKIT FARM INTO A NEW VPC

View template

Network configuration:

Parameter label (name)	**Default**	**Description**
Number of instances (NumberOfInstances)	2	Number of EC2 instances to create.
Availability Zones (AvailabilityZones)	*Requires input*	Set as many Availability Zones as there are instances.
Public subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	CIDR block for the public DMZ subnet 1 located in Availability Zone 1.
Public subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	CIDR block for the public DMZ subnet 2 located in Availability Zone 2.
Public subnet 3 CIDR (PublicSubnet1CIDR)	10.0.160.0/20	CIDR block for the public DMZ subnet 3 located in Availability Zone 3.
Public subnet 4 CIDR (PublicSubnet2CIDR)	10.0.176.0/20	CIDR block for the public DMZ subnet 4 located in Availability Zone 4.
Allowed CIDR for SafeKit environment (RemoteAccessCIDR)	*Requires input*	Enter the CIDR IP range that is permitted to access SafeKit environment. Set this value to a trusted IP range. For example, you might grant access only to your corporate network.
Allowed CIDR for virtual IP access to SafeKit web console (VipCIDR)	*Requires input*	Enter the CIDR IP range that is permitted to access SafeKit web console. Set this value to a trusted IP range. For example, you might grant access only to your corporate network.

Amazon EC2 configuration:

Parameter label (name)	**Default**	**Description**
Key pair name (KeyPairName)	*Requires input*	Enter the public/private key pair you created in your preferred AWS Region; see the Technical requirements section of the deployment guide.
Instance type (InstanceType)	t2.small	Choose the Amazon EC2 instance type.
Operating system (OSType)	Linux	Choose Windows to change the operating system.

Evidian SafeKit – farm cluster configuration:

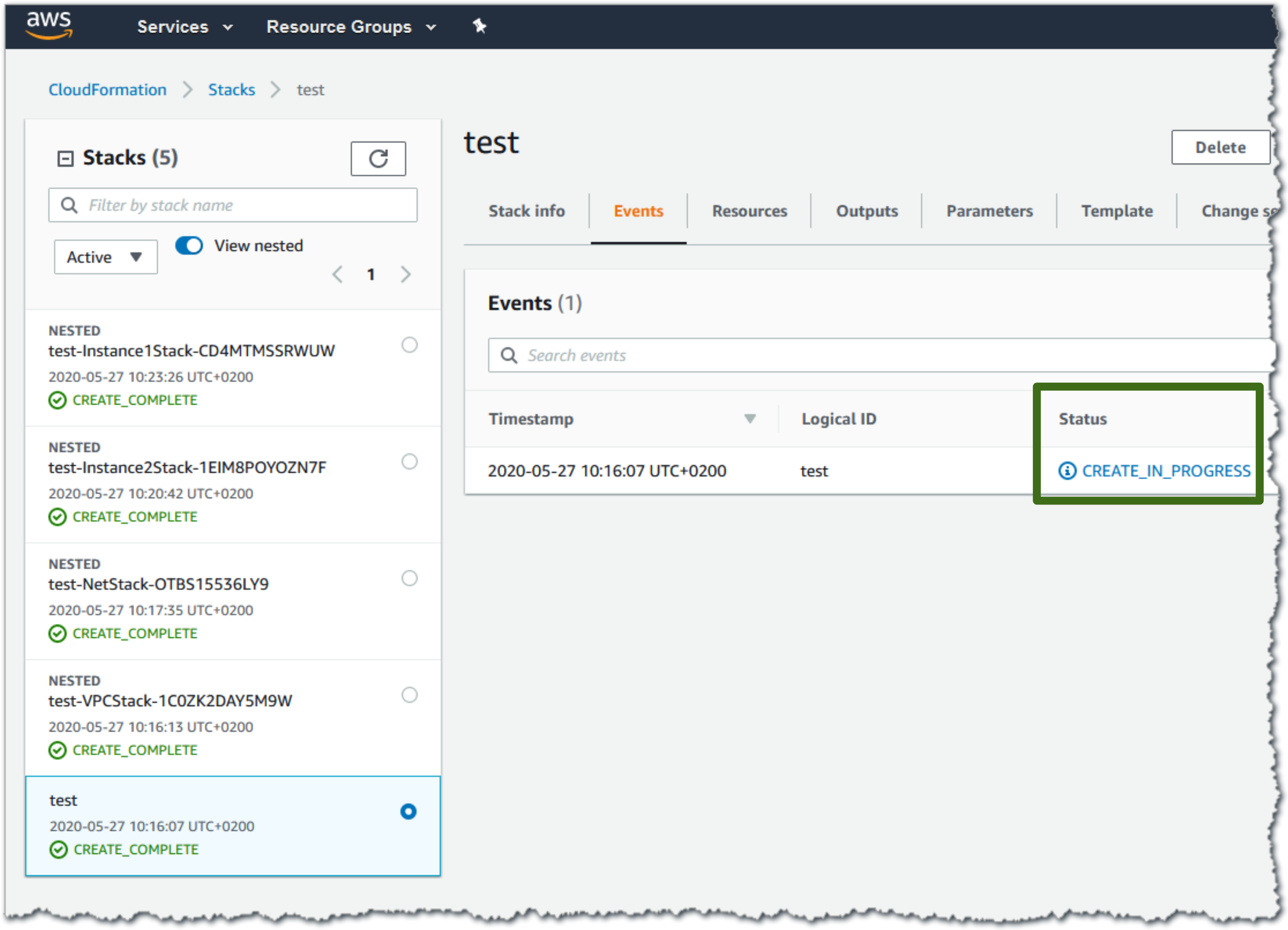
Parameter label (name)	Default	Description
SafeKit module name (SafekitModuleName)	farm	The name of the SafeKit module you're deploying. This is not editable.
Instance name prefix (InstanceNamePrefix)	server	The prefix in the SafeKit web console for each instance name. Enter a different name if required for your configuration.
Virtual IP port (VipPort)	9453	The port of the virtual IP that is used for failover of the SafeKit mirror. Enter a port 1–49151.
Password (CAservPwd)	*Requires input*	Password for SafeKit web console certificates. Must be at least 8 characters long and contain at least 1 uppercase letter, 1 lowercase letter, and 1 number. Do not use quotation marks, backslashes, forward slashes, or the @ symbol.

AWS Quick Start configuration:

Note: We recommend keeping these default settings for the “AWS Quick Start configuration” parameters unless you are customizing the Quick Start templates for your own deployment projects. Changing these parameter settings automatically updates code references to point to a new Quick Start location. For details, see the AWS Quick Start Contributor’s Guide.

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	aws-quickstart	The S3 bucket that you created for your copy of Quick Start assets. Use this if you decide to customize the Quick Start. This bucket name can include numbers, lowercase letters, uppercase letters, and hyphens but should not start or end with a hyphen.
Quick Start S3 bucket Region (QSS3BucketRegion)	us-east-1	The AWS Region where the Quick Start S3 bucket (QSSBucketName) is hosted. When using your own bucket, you must specify this value.
Quick Start S3 key prefix (QSS3KeyPrefix)	quickstart-atos-evidian-safekit/	The S3 key name prefix that is used to simulate a folder for your copy of Quick Start assets. Use this if you decide to customize the Quick Start. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes. See https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html.

6. On the **Configure stack options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
7. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the two check boxes to acknowledge that the template will create IAM resources and that it might require the ability to automatically expand macros.
8. Choose **Create stack** to deploy the stack.
9. Monitor the status of the stack. See the **Status** heading shown in Figure 3.



NESTED
test-Instance1Stack-CD4MTMSSRWUW
2020-05-27 10:23:26 UTC+0200
✓ CREATE_COMPLETE

NESTED
test-Instance2Stack-1EIM8POYOZN7F
2020-05-27 10:20:42 UTC+0200
✓ CREATE_COMPLETE

NESTED
test-NetStack-OTBS15536LY9
2020-05-27 10:17:35 UTC+0200
✓ CREATE_COMPLETE

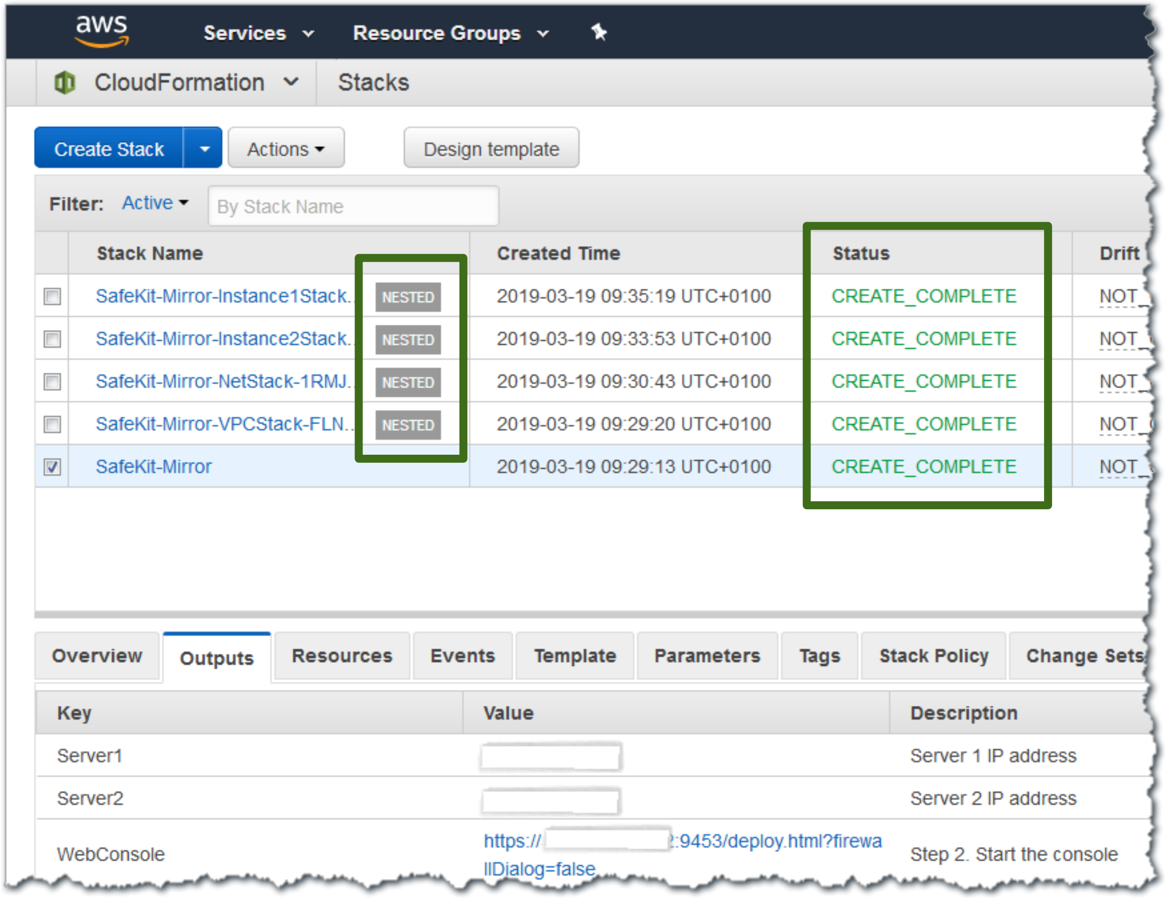
NESTED
test-VPCStack-1COZK2DAY5M9W
2020-05-27 10:16:13 UTC+0200
✓ CREATE_COMPLETE

test
2020-05-27 10:16:07 UTC+0200
✓ CREATE_COMPLETE

Timestamp	Logical ID	Status
2020-05-27 10:16:07 UTC+0200	test	ⓘ CREATE_IN_PROGRESS

Figure 3: Stack page after successful deployment

When the status is **CREATE_COMPLETE**, as shown in Figure 4, the SafeKit cluster is ready. Note that a few nested stacks are created too.



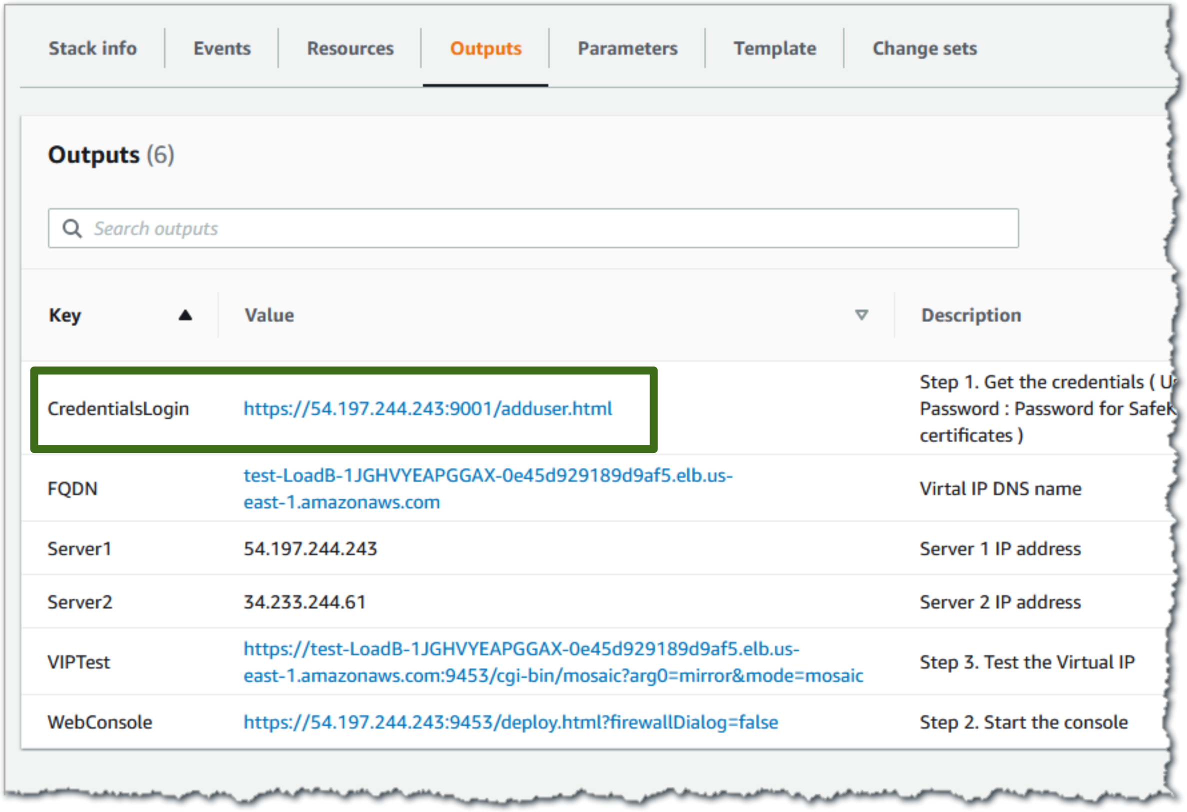
	Stack Name		Created Time	Status	Drift
□	SafeKit-Mirror-Instance1Stack...	NESTED	2019-03-19 09:35:19 UTC+0100	CREATE_COMPLETE	NOT
□	SafeKit-Mirror-Instance2Stack...	NESTED	2019-03-19 09:33:53 UTC+0100	CREATE_COMPLETE	NOT
□	SafeKit-Mirror-NetStack-1RMJ...	NESTED	2019-03-19 09:30:43 UTC+0100	CREATE_COMPLETE	NOT
□	SafeKit-Mirror-VPCStack-FLN...	NESTED	2019-03-19 09:29:20 UTC+0100	CREATE_COMPLETE	NOT
☑	SafeKit-Mirror		2019-03-19 09:29:13 UTC+0100	CREATE_COMPLETE	NOT

Key	Value	Description
Server1	[redacted]	Server 1 IP address
Server2	[redacted]	Server 2 IP address
WebConsole	https://[redacted]:9453/deploy.html?firewallDialog=false	Step 2. Start the console

Figure 4: SafeKit mirror outputs after successful deployment

Step 3. Test the deployment

1. After deployment, go to the **Outputs** tab, as shown in Figure 5.



Key	Value	Description
CredentialsLogin	https://54.197.244.243:9001/adduser.html	Step 1. Get the credentials (U Password : Password for Safek certificates)
FQDN	test-LoadB-1JGHVYEAPGGAX-0e45d929189d9af5.elb.us-east-1.amazonaws.com	Virtal IP DNS name
Server1	54.197.244.243	Server 1 IP address
Server2	34.233.244.61	Server 2 IP address
VIPTest	https://test-LoadB-1JGHVYEAPGGAX-0e45d929189d9af5.elb.us-east-1.amazonaws.com:9453/cgi-bin/mosaic?arg0=mirror&mode=mosaic	Step 3. Test the Virtual IP
WebConsole	https://54.197.244.243:9453/deploy.html?firewallDialog=false	Step 2. Start the console

Figure 5: SafeKit outputs after successful deployment

2. Visit the CredentialsLogin URL, and install the client and CA certificates in your web browser.

    a. When you access the CredentialsLogin URL, your browser displays a site-not-trusted warning. It does so because the SafeKit certificate hasn't been added to the "Trusted Root Certification Authority" store on your workstation. The warning message varies depending on which web browser you're using.

    b. If you click the not-secure message in the browser's URL bar, choose the option to view the certificate. Then, import it to your local certificate store.

    c. Save the certificate to the "Trusted Root Certification Authorities" store. See page 180 of the SafeKit User's Guide for step-by-step instructions.

3. Start the SafeKit web console.

4. Test your deployment.

- **For a mirror module**, test the primary/secondary virtual IP address with the test URL in the template output. A primary/secondary load-balancing rule has been set for external port 9453, internal port 9453. The URL returns the name of the primary server.
- **For a farm module**, test the load-balanced virtual IP address with the test URL in the template output. A load-balancing rule has been set for external port 9453, internal port 9453. A mosaic of server names is displayed according to the server answering to the TCP session.

Security

For security reasons, only users with the necessary permissions can manage SafeKit clusters. For that, SafeKit implements certificates that must be installed in the user's browser.

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.

> **Important**: When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. 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 location other than an S3 bucket, you might encounter template-size limitations when you create the stack. For more information about AWS CloudFormation quotas, see the AWS documentation.

Q. How can I install an Evidian SafeKit mirror cluster on existing AWS servers?

A. See the manual installation here: https://www.evidian.com/products/high-availability-software-for-application-clustering/aws-high-availability-cluster-synchronous-replication-failover/#trial

Q. How can I install an Evidian SafeKit farm cluster on existing AWS servers?

A. See the manual installation here: https://www.evidian.com/products/high-availability-software-for-application-clustering/aws-load-balancing-cluster-failover/#trial

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, 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

SafeKit documentation on the Evidian website

- Evidian SafeKit mirror cluster
- Evidian SafeKit farm cluster
- Evidian SafeKit with modules, demos, customers, training, differentiators
- Evidian SafeKit User's Guide

Other Quick Start reference deployments

- AWS Quick Start home page

Document revisions

Date	Change	In sections
July 2020	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.