

# VFX Burst Rendering Framework on the AWS Cloud

## Using ISE Content Security Recommendations

### Quick Start Reference Deployment

*April 2019*

*John Bennett – AWS UK Proserve*

*Franco Rezabek, Stefano Vozza – AWS UK Builders*

*Shivansh Singh – 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 .....	2
VFX Burst Render Framework on AWS .....	3
Cost and licenses .....	3
Architecture .....	4
Planning the deployment .....	8
Specialized knowledge .....	8
AWS account .....	8
Technical requirements .....	8
Deployment steps .....	9
Step 1. Sign in to your AWS account.....	9
Step 2. Launch the Quick Start .....	10
Parameters for deploying VFX burst rendering framework.....	11
Step 3. Test the deployment .....	15

Deleting the stacks .....	15
Security .....	16
Customizing the environment after deployment.....	17
Troubleshooting .....	20
Send us feedback .....	21
Additional resources .....	21
Document revisions.....	21

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

## Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying an example Linux framework architecture for visual effects (VFX) burst rendering on the AWS Cloud by using the best practices and recommendations for content security adopted by the VFX industry.

VFX studios can use this Quick Start to build an initial framework to elastically burst their render capacity on the AWS Cloud, and automate the implementation of best practices and recommended content security controls required by major studio content owners. The Quick Start can be used by VFX studios that are new to burst rendering on AWS, or by VFX studios that are already using burst rendering on AWS and require further guidance on securing their VFX burst rendering environment.

The Quick Start deployment is automated by AWS CloudFormation templates. You can launch the Quick Start in the AWS CloudFormation console to create a framework AWS Cloud burst rendering environment in about 10 minutes within your AWS account.

**Important** This Quick Start deploys the framework architecture and infrastructure for VFX burst rendering, but it does not deploy VFX applications onto the infrastructure or integrate the framework with your on-premises systems. After you deploy the Quick Start, you can install your custom applications into the provisioned framework architecture and integrate the architecture with your on-premises environment, as explained in the [Customizing the environment](#) section.

## VFX Burst Render Framework on AWS

The framework architecture for VFX burst rendering set up by this Quick Start follows the guidelines and best practice recommendations developed by Independent Security Evaluators (ISE). The ISE recommendations are documented in *Studio Security Controls for VFX/Rendering*, which is available on the [AWS Artifact website](#) (access requires an AWS account). Your VFX studio can use this framework to deploy a VFX burst rendering environment that meets content security best practices, and can then customize this environment with their custom applications and integrate it with their on-premises environment.

This Quick Start also provides a [security control mapping document](#) (PDF format): *VFX Burst Rendering on AWS Using ISE Content Security Recommendations and Best Practices – Security Control Mapping*. This document has been validated by the AWS Security team and by ISE. It describes how the deployed and customized VFX burst rendering environment on the AWS Cloud should be implemented to meet ISE best practices and recommended security controls. This mapping provides your VFX studio with the guidance needed to demonstrate, document, and prepare the VFX burst rendering environment for an ISE security audit.

## 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.

You are responsible for the cost of the physical private networking connection between your on-premises environment and the AWS Cloud. This network connection can be provided by an AWS Partner. See the [AWS Partner Solutions Finder](#) for a list of networking partners.

You are responsible for the license cost of any VFX rendering application, render scheduler application, and license server application you decide to use on the Amazon Elastic Compute Cloud (Amazon EC2) instances.

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](#).

## Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the Linux framework VFX burst rendering environment illustrated in Figures 1 and 2 in the AWS Cloud.

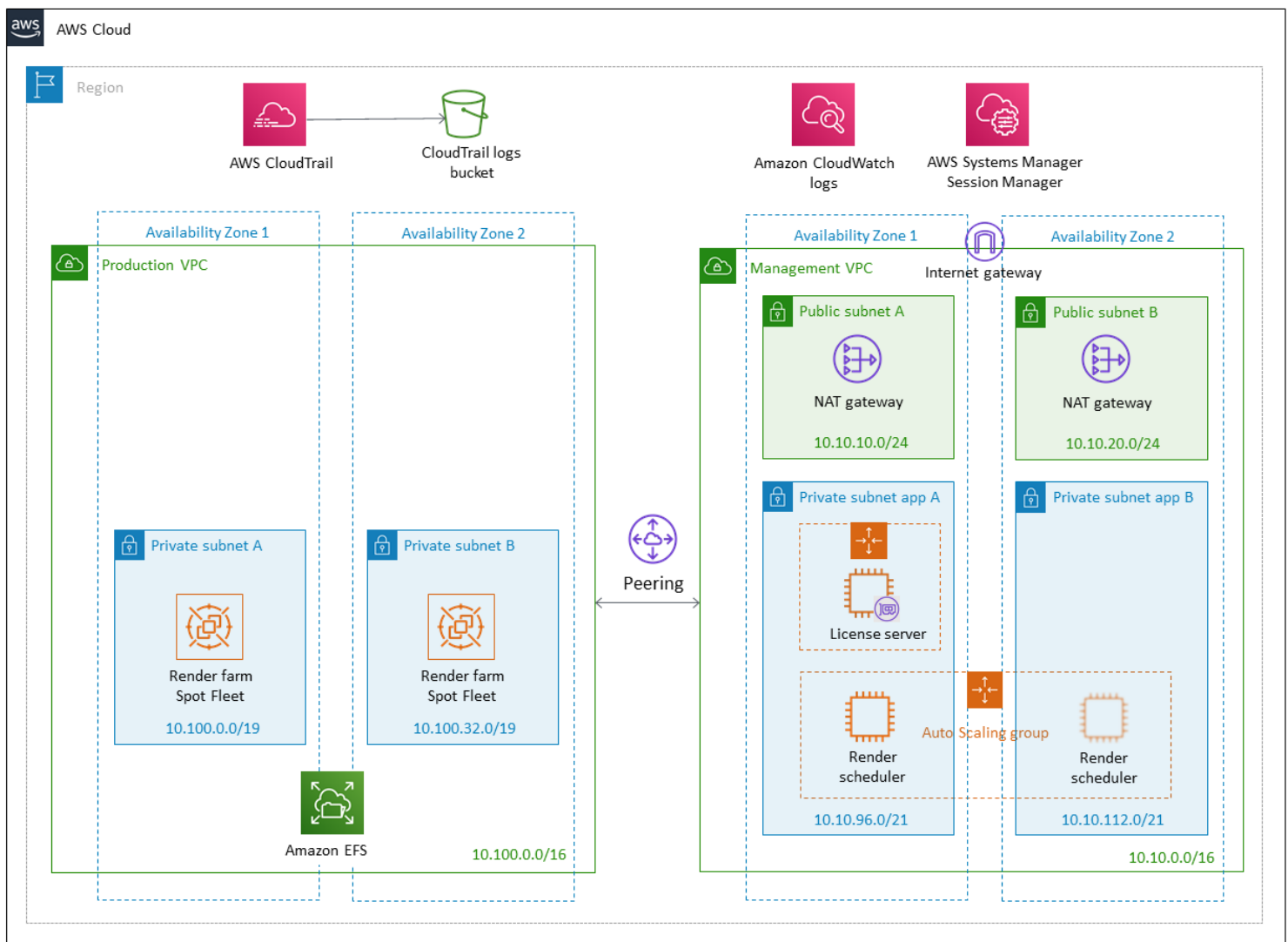


Figure 1: High-level framework architecture

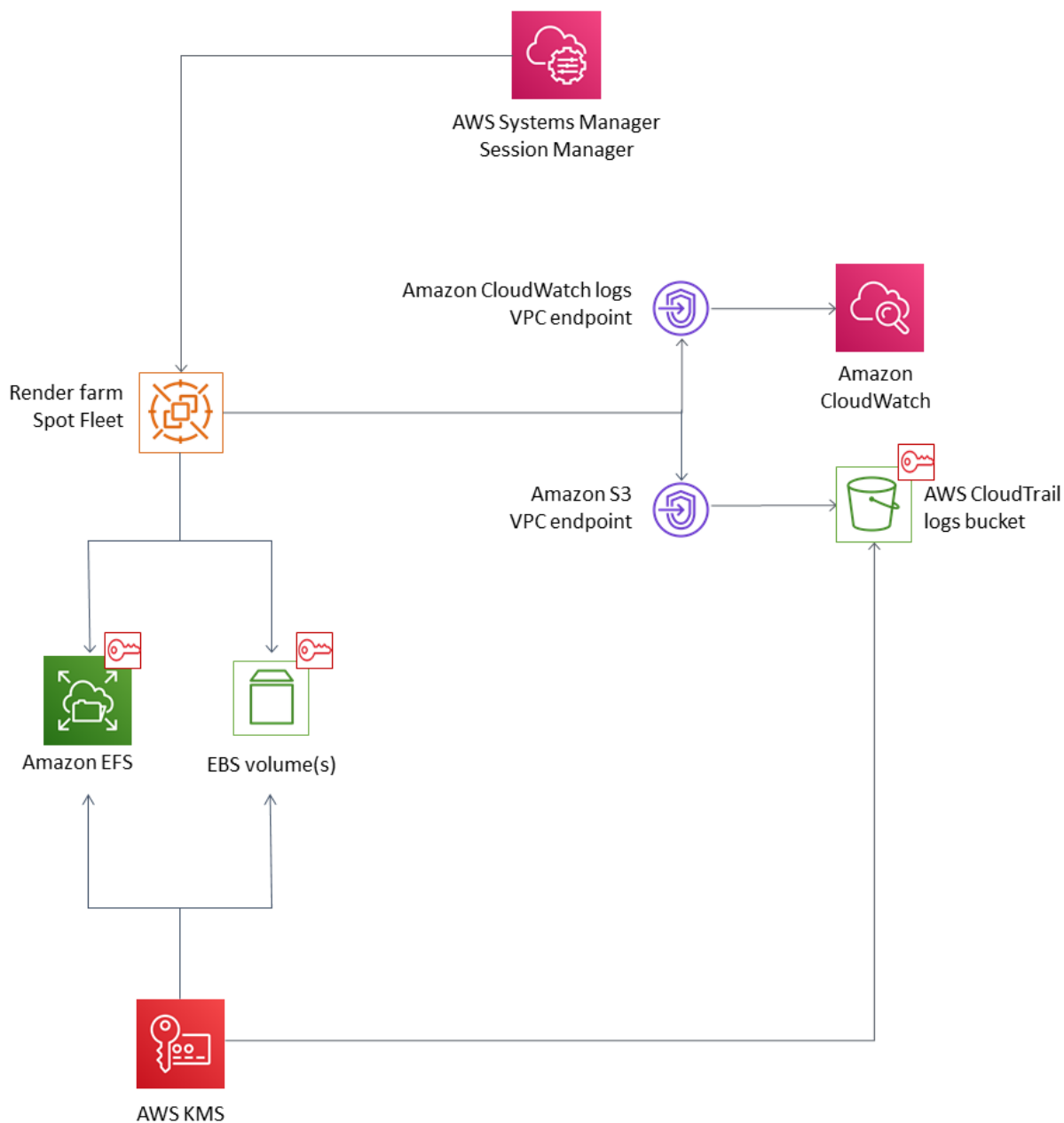
The Quick Start sets up the following:

- A highly available architecture that spans two Availability Zones.
- Two peered VPCs:
  - A **production VPC** that is configured only with private subnets for content-aware burst rendering instances and encrypted asset storage. This VPC is completely isolated from the internet, to provide you with your own virtual network for each project on AWS.
  - A **management VPC** that is configured with public and private subnets and internet connectivity, according to AWS best practices. This provides you with your own virtual network for common, core resources used by the production VPC. Some VFX studios might omit this management VPC and use their on-premises, shared-services equivalent for common, core resources instead. Alternatively, some VFX studios might eventually migrate their on-premises, shared-services resource into this management VPC.
- Amazon VPC security groups for limiting access between resources within the private and public subnets of each VPC, between VPCs, and to other resources and services.

### In the production VPC:

- In the private subnets, a Spot Fleet of EC2 burst rendering instances that can be scaled to meet render demand. After the initial deployment, you can modify the AWS CloudFormation template to select the instance type of the EC2 burst rendering instance to suit your vCPU and memory requirements. You can also customize the EC2 burst rendering instance image for your VFX studio to include applications such as the VFX rendering engine software, specific configurations for storage mount points, and communication with specific configurations of the render scheduler and license server applications in the management VPC.
- AWS Key Management Service (AWS KMS), to create and control the encryption keys used for the server-side encryption (SSE) of data at rest. The Quick Start creates the following three default, AWS managed keys for your use, as illustrated in Figure 2:
  - Amazon Elastic Block Store (Amazon EBS) for encrypted root volumes for EC2 instances.
  - Amazon Elastic File System (Amazon EFS) for encrypted production content assets.
  - Amazon Simple Storage Service (Amazon S3) for encrypted AWS CloudTrail logs.

- Encrypted, shared file storage for render assets used by all EC2 burst rendering instances, using Amazon EFS. Amazon EFS storage was chosen because the EC2 burst rendering instances and applications can access it easily as NFS mounts. After the initial deployment, you can replace this storage with an alternate, high-performance storage system such as a native Amazon FSx for Lustre file system or a third-party parallel file system that uses an underlying AWS instance and storage infrastructure.



**Figure 2: High-level encryption architecture**

**In the management VPC:**

- In the public subnets, managed NAT gateways to allow controlled, outbound internet access.
- An internet gateway to allow access to the internet via the NAT gateways.
- In one of the private subnets, a license server instance with a media access control (MAC) address in a Single-AZ Auto Scaling group.
- In the private subnets, a render scheduler instance in a Multi-AZ Auto Scaling group.

The license server and render scheduler instances are configured to access third-party licensing schemes via the NAT gateway and internet gateway. The license server and render scheduler are used by VFX rendering applications running on the EC2 burst rendering instances in the production VPC's private subnets. After the initial deployment, you can modify the EC2 instance types (`t2.micro` by default) for the license server and render scheduler to suit your specific vCPU and memory requirements. You can also customize or bootstrap the render scheduler instance AMI with a hardened instance image that contains your own render scheduler application. You can also customize or bootstrap the license server instance AMI with the license server application using the MAC address of the elastic network interface. After you customize the license server and render scheduler, you must configure the security groups between these and the VFX rendering applications running on the EC2 burst rendering instances in the production VPC.

In addition, the architecture includes:

- VPC endpoints to enable private connections from the production and management VPCs to resources outside the VPCs, such as Amazon S3 and AWS Systems Manager Sessions Manager.
- Systems Manager Session Manager to facilitate command-line access for administrative users who manage the EC2 instances for troubleshooting and systems administration activities. This replaces the need for SSH access through a bastion host instance.
- Basic AWS Identity and Access Management (IAM) configuration with custom IAM policies, with associated groups, roles, and instance profiles. These enable the AWS resources created through the Quick Start to access other AWS resources when required.
- Illustrative tagging of AWS resources with a project name you specify during deployment. Tagging all resources in the production VPC with the project name enables AWS Cost Explorer to isolate project-based resource costs.
- Amazon S3-encrypted bucket for logging data.

- Logging, monitoring, and alerts using AWS CloudTrail and Amazon CloudWatch rules and alarms.

Once the framework VFX burst rendering environment is deployed, you can customize it to meet your VFX studio's specific requirements for instance types, storage types, and applications. You will also need to customize the integration of your network connectivity between the deployed VFX burst rendering environment and your VFX studio's on-premises rendering environment. For details, see the [Customizing the environment](#) section later in this guide.

## Planning the deployment

### Specialized knowledge

This Quick Start assumes familiarity with the basic concepts in the areas of networking, compute instances and their operating system (OS) images, and data encryption. It also assumes familiarity with VFX rendering, licensing, and render scheduler applications.

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.

### 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	2
Elastic IP addresses	2
IAM security groups	4
IAM roles	8
Auto Scaling groups	2
t2.micro instances	3
t3.micro instances	1

---

### [Regions](#)

This deployment includes Amazon EFS and T3 Linux instances, which aren't currently supported in all AWS Regions. For a current list of supported regions, see [AWS Regions and Endpoints](#) and [Amazon EC2 Pricing](#) on the AWS website.

---

### [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. 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 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. For details, see [Planning the deployment](#) earlier in this guide.

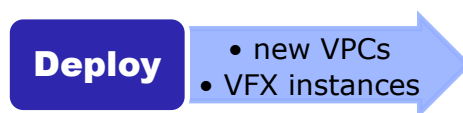
2. Make sure that your AWS account is configured correctly, as discussed in the [Technical requirements](#) section.

## Step 2. Launch the Quick Start

**Notes** The instructions in this section reflect the newer version of the AWS CloudFormation console. If you're using the older console, some of the user interface elements might be different.

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

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



[Deploy VFX Burst Render Framework  
into new VPCs on AWS](#)

The deployment takes about 10 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 the VFX burst rendering framework will be built. The template is launched in the US East (Ohio) Region by default.

**Note** This deployment includes Amazon EFS and T3 Linux instances, which aren't currently supported in all AWS Regions. For a current list of supported regions, see [AWS Regions and Endpoints](#) and [Amazon EC2 Pricing](#) on the AWS website.

3. On the **Specify template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify stack details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input, such

as the notification email address. For all other parameters, review the default settings and customize them as necessary.

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

## PARAMETERS FOR DEPLOYING VFX BURST RENDERING FRAMEWORK

[View template](#)

*Region configuration:*

Parameter label (name)	Default	Description
<b>Availability Zones</b> (pAvailabilityZones)	<i>Requires input</i>	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.

*Production VPC network configuration:*

Parameter label (name)	Default	Description
<b>Production VPC CIDR</b> (pProductionVpcCIDR)	10.100.0.0/16	The CIDR block for the production VPC.
<b>Production VPC private subnet 1 CIDR</b> (pProdAppPrivateSubnetACIDR)	10.100.0.0/19	The CIDR block for the private subnet located in Availability Zone 1 of the production VPC.
<b>Production VPC private subnet 2 CIDR</b> (pProdAppPrivateSubnetBCIDR)	10.100.32.0/19	The CIDR block for the private subnet located in Availability Zone 2 of the production VPC.

*Management VPC network configuration:*

Parameter label (name)	Default	Description
<b>Management VPC CIDR</b> (pManagementVpcCIDR)	10.10.0.0/16	The CIDR block for the management VPC.
<b>Management VPC public subnet 1 CIDR</b> (pManagementDMZSubnetACIDR)	10.10.10.0/24	The CIDR block for the public (internet-facing) subnet located in Availability Zone 1 of the management VPC.
<b>Management VPC public subnet 2 CIDR</b>	10.10.20.0/24	The CIDR block for the public (internet-facing) subnet located in Availability Zone 2 of the management VPC.

Parameter label (name)	Default	Description
(pManagementDMZSubnetBCIDR)		
<b>Management VPC private subnet 1 CIDR</b> (pMgmtAppPrivateSubnetACIDR)	10.10.96.0/21	The CIDR block for the private subnet located in Availability Zone 1 of the management VPC.
<b>Management VPC private subnet 2 CIDR</b> (pMgmtAppPrivateSubnetBCIDR)	10.10.112.0/21	The CIDR block for the private subnet located in Availability Zone 2 of the management VPC.

*Render farm instance configuration:*

Parameter label (name)	Default	Description
<b>Capacity of Spot Fleet instances</b> (pRenderFarmTargetCapacity)	2	The number of instances in the Spot Fleet.

*License server configuration:*

Parameter label (name)	Default	Description
<b>License server instance type</b> (pLicenseServerInstanceType)	t2.micro	The EC2 instance type for the license server.
<b>Desired capacity of license server</b> (pLicenseServerDesiredCapacity)	1	The number of license server instances that you want to run in the Auto Scaling group. This number must be less than or equal to the maximum capacity you specify in the following parameter.
<b>Maximum capacity of license server</b> (pLicenseServerMaxCapacity)	1	The maximum number of license server instances that you can run in the Auto Scaling group.

*Render scheduler configuration:*

Parameter label (name)	Default	Description
<b>Render scheduler instance type</b>	t2.micro	The EC2 instance type for the render scheduler.

Parameter label (name)	Default	Description
(pRenderSchedulerInstanceType)		
<b>Desired capacity of render scheduler</b> (pRenderSchedulerDesiredCapacity)	1	The number of render scheduler instances that you want to run in the Auto Scaling group. This number must be less than or equal to the maximum capacity you specify in the following parameter.
<b>Maximum capacity of render scheduler</b> (pRenderSchedulerMaxCapacity)	1	The maximum number of render scheduler instances that you can run in the Auto Scaling group.

### Email and environment configuration:

Parameter label (name)	Default	Description
<b>Notification email address</b> (pNotifyEmail)	<i>Requires input</i>	The email address that security event notifications should be sent to. You will receive a confirmation email at this address.
<b>Project name</b> (pProjectName)	MyProject	The project name to use for tagging render farm instances.
<b>VFX environment</b> (pEnvironment)	DEV	The type of VFX environment to set up. You can specify DEV (development), TEST (test), or PROD (production).  This value is used as a tag to identify the stack. You can deploy the Quick Start multiple times into different accounts and use this parameter to identify each environment.

### AWS Quick Start configuration:

**Note** We recommend that you keep the default settings for the following two parameters, unless you are customizing the Quick Start templates for your own deployment projects. Changing the settings of these parameters will automatically update code references to point to a new Quick Start location. For additional details, see the [AWS Quick Start Contributor's Guide](#).

Parameter label (name)	Default	Description
<b>Quick Start S3 bucket name</b> (QSS3BucketName)	aws-quickstart	The S3 bucket you created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.

Parameter label (name)	Default	Description
<b>Quick Start S3 key prefix</b> (QSS3KeyPrefix)	quickstart-vfx-ise/	The <a href="#">S3 key name prefix</a> used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.

- 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**.
- 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 capability to auto-expand macros.
- Choose **Create stack** to deploy the stack.
- Monitor the status of the stack. When the status is **CREATE\_COMPLETE**, the VFX burst rendering framework is ready, as shown in Figure 3.

CloudFormation > Stacks > vfx-dev: Stack details

**vfx-dev** Actions ▾

Stack info | Events | **Resources** | Outputs | Parameters | Template

**Resources (10)** 🔄 ⚙️

🔍 Search resources

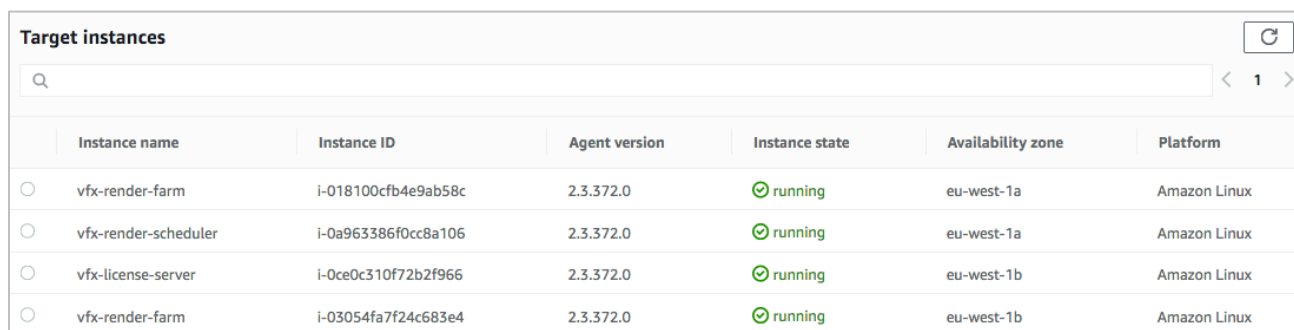
Logical ID ▾	Physical ID ▾	Type ▾	Status ▾	Status reason ▾
IamTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
LicenseServerTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
LoggingTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
ManagementVpcTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
PeeringConnectionTempl...	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
ProductionVpcTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
RenderFarmTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
RenderSchedulerTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
SecurityGroupsHelperTe...	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-
VpcEndpointsTemplate	arn:aws:cloudformation:e...	AWS::CloudFormation::St...	✔️ CREATE_COMPLETE	-

Figure 3: Stack resources

### Step 3. Test the deployment

When the deployment is complete, you can verify the environment by logging into the instances from the AWS Systems Manager Session Manager console. You can use this console to start a command-line session on an instance in your account.

1. Open the Systems Manager console at <https://console.aws.amazon.com/systems-manager/>.
2. In the navigation pane, choose **Session Manager**.
3. Choose **Start session**.
4. In the **Target instances** list, choose the option button to the left of the instance you want to connect to, as shown in Figure 4.



	Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
<input type="radio"/>	vfx-render-farm	i-018100cfb4e9ab58c	2.3.372.0	✔ running	eu-west-1a	Amazon Linux
<input type="radio"/>	vfx-render-scheduler	i-0a963386f0cc8a106	2.3.372.0	✔ running	eu-west-1a	Amazon Linux
<input type="radio"/>	vfx-license-server	i-0ce0c310f72b2f966	2.3.372.0	✔ running	eu-west-1b	Amazon Linux
<input type="radio"/>	vfx-render-farm	i-03054fa7f24c683e4	2.3.372.0	✔ running	eu-west-1b	Amazon Linux

**Figure 4: Selecting instances to connect to in Session Manager**

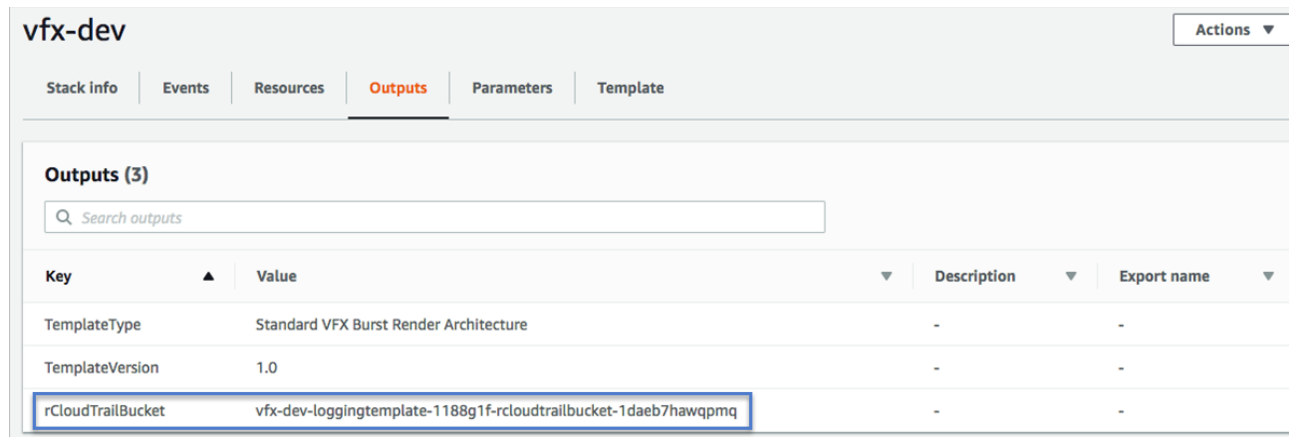
5. Choose **Start session**.

After the Session Manager connection is made, you can run Linux shell commands, as you would through any other connection type.

6. Test the deployment by enabling a Linux VFX rendering instance to be used by your render scheduler.

### Deleting the stacks

When you've finished using the VFX burst rendering framework on AWS, you can delete the stacks. Deleting a stack, either by using the [AWS Command Line Interface \(AWS CLI\) and APIs](#), or through the [AWS CloudFormation console](#), will remove all the resources created by the template for that stack. The only exception is the S3 bucket for logging. By default, the deletion policy for this bucket is set to "Retain," so you have to delete it manually. The bucket can be found in **Outputs** tab of the main stack, as shown in Figure 5.



Key	Value	Description	Export name
TemplateType	Standard VFX Burst Render Architecture	-	-
TemplateVersion	1.0	-	-
rCloudTrailBucket	vfx-dev-loggingtemplate-1188g1f-rcloudtrailbucket-1daeb7hawqpmq	-	-

Figure 5: S3 bucket for logging stack

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

## Security

This Quick Start uses AWS security best practices and ISE's content security best practices and recommendations, as required by major studio content owners. The framework architecture for VFX burst rendering on the AWS Cloud is deployed by using the information in the [security control mapping document](#) (PDF format): *VFX Burst Rendering on AWS Using ISE Content Security Recommendations and Best Practices – Security Control Mapping*. This document is derived from *Studio Security Controls for VFX/Rendering*, which is available on the [AWS Artifact website](#) (access requires an AWS account), and was approved by AWS Security and ISE. Here are some of the ISE implementation recommendations deployed by the Quick Start:

- The VPCs use security groups for fine-grained control of traffic in and out of the VPC, and between tiered subnets within the VPC.
- IAM is used with illustrative group, role, user and instance profiles for controlling and segregating access to resources and between resources.
- The VFX burst rendering instances are in a private subnet within a production VPC. There is no outbound or inbound internet connection to these instances. VPC endpoints are used to allow access to other AWS resources, such as S3 buckets and Systems Manager Session Manager.

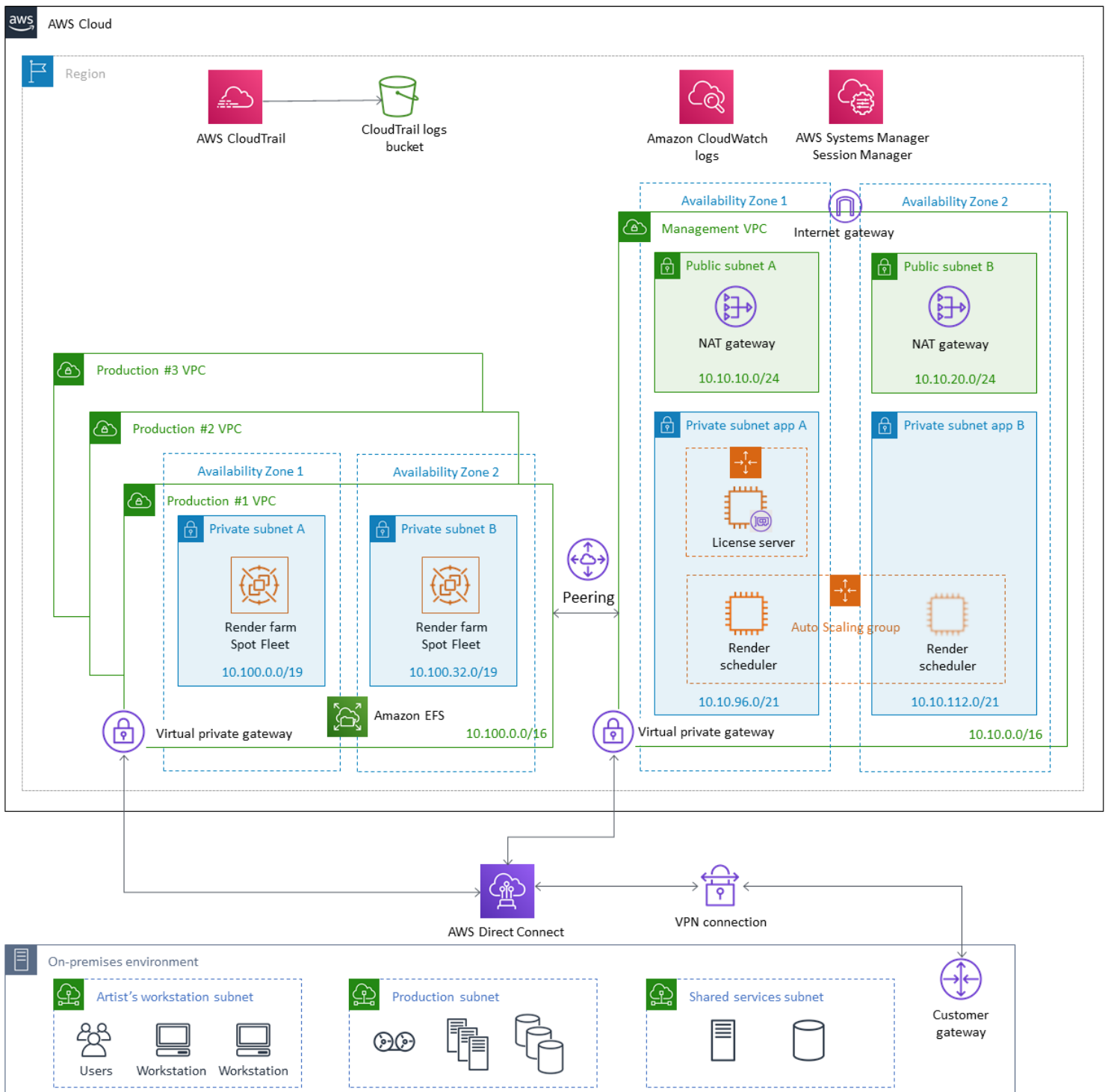


- The VFX license server and render scheduler instances are in a private subnet in the management VPC. The NAT Gateway managed service allows these instances from private subnets to access the internet or other AWS resources, but prevents the internet from initiating a connection with these instances.
- The Amazon EFS storage and EC2 instance EBS volumes are encrypted by using encryption keys managed by AWS KMS. The S3 bucket that contains CloudTrail logs uses an AWS KMS-managed encryption key to encrypt all data. This S3 bucket is also configured to prevent unauthorized users from deleting or tampering with log files.
- Systems Manager Session Manager is used to access instances via the Systems Manager Agent (SSM Agent) across an encrypted tunnel that originates on the instance. All Session Manager sessions are logged by the SSM service and are available for audit. SSM is used instead of opening up inbound SSH ports, configuring bastion host access, and setting up user accounts, passwords, or SSH keys on the instances. You can additionally enable the logging of all SSM session data to an S3 bucket or to a CloudWatch log stream; this is not configured as part of the Quick Start.

You can use the the [security control mapping document](#) as a recommendation checklist to ready your VFX studio for an ISE content security audit of the burst rendering environment. You can also use the document to provide your VFX studio with compliance-related information that validates the implementation and operating effectiveness of AWS security controls.

## Customizing the environment after deployment

The Quick Start does not provide the network connectivity between the deployed VFX burst rendering environment and your VFX studio's on-premises rendering environment. After you deploy the Quick Start, you can customize the VFX burst rendering environment to connect and integrate it with your VFX studio's on-premises rendering environment, as shown in Figure 6.



**Figure 6: Integration of framework architecture and on-premises environment**

For example, we recommend using a private, low-latency AWS Direct Connect (DX) network connection between the AWS Cloud VFX burst rendering environment and the on-premises rendering environment. The DX connection can be provided by an AWS Partner. See the [AWS Partner Solutions Finder](#) for a list of networking partners. We also recommend using a VPN for encrypted-in-transit network connectivity over the private DX. Once these connections are in place, you can make the following manual customizations:

- Adding virtual private gateway devices to the VPCs
- Adding a customer gateway device to the on-premises network
- Configuring the private DX network between the on-premises customer gateway and the virtual private gateway devices
- Configuring VPNs to run over the private network connection for encrypted-in-transit networking between the on-premises customer gateway and the virtual private gateway devices
- Configuring the deployed VFX burst rendering environment's VPN access over the DX network to on-premises resources such as shared-services application servers and production storage

The Quick Start does not deploy VFX applications onto the infrastructure or integrate the framework with your VFX studio's on-premises environment. You must further customize the VFX burst rendering environment to meet your VFX studio's specific requirements for instance types, storage types, and applications, and to integrate it with your on-premises environment. These customizations include:

- Choosing the EC2 instance type for render server, license server, and render scheduler.
- For each instance type, using customized and hardened AMIs that are bootstrapped with the applications and specific configurations for the storage mount points.
- Using the MAC address of the elastic network interface of the Single-AZ license server to establish the required rendering application licenses.
- Extending the automatic scaling of the license server from a Single-AZ, single instance, single MAC address to a Multi-AZ, multi-instance, multi-MAC address cluster.
- Choosing a high-performance asset storage type, such as another native AWS file system or a third-party parallel file system, to store the rendering assets.
- Further securing the deployed security groups between instances, once application specific ports are known.

- Using KMS customer managed keys instead of the automatically created KMS AWS managed keys to provide more flexibility to create, rotate, disable, and define access controls, so granular policies can be defined to control how each encryption key can be used.
- Integrating the deployed VFX burst rendering environment with your VFX studio's on-premises rendering environment via storage network mounts and security groups.
- Adding private subnets for additional segregation of content-aware resources (servers, storage, workstations) and content-unaware resources (corporate applications).

For further implementation guidance to meet ISE's content security best practices and recommendations for these items, see the [security control mapping document](#) (PDF format): *VFX Burst Rendering on AWS Using ISE Content Security Recommendations and Best Practices – Security Control Mapping*.

## Troubleshooting

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

**A.** If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained 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. 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](#)
- [Amazon EFS](#)
- [IAM](#)
- [Amazon S3](#)
- [Amazon FSx for Lustre](#)
- [AWS System Manager Session Manager](#)
- [Amazon VPC](#)
- [Amazon VPC Peering](#)

### Other Quick Start reference deployments

- [AWS Quick Start home page](#)

## Document revisions

Date	Change	In sections
April 2019	Initial publication	—

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved

### **Notices**

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at <http://aws.amazon.com/apache2.0/> 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.