Content Creation Workstation

AWS Implementation Guide

Jason Schliefer – Lead, Studio In the Cloud

John Bennett – Senior Consultant, M&E ProServe

Kevin Ashman – Senior Partner Solution Architect, Game Tech

Ben Moore – Principal GTM Specialist Sprinter

Sheikh Shuvo – Senior GTM Specialist Sprinter

October 2020

Contents

About this guide

This implementation guide describes architectural considerations and configuration steps for deploying Content Creation Workstation in the Amazon Web Services (AWS) Cloud. It includes links to a AWS CloudFormation template that launches and configures the AWS services required to deploy this solution using AWS best practices for security and availability.

The guide is intended for users that require virtual workstations that support graphics intensive workloads, such as visual effects studios, game development studios, and more.

Overview

Why did we build this solution?

This solution is designed to empower users to reduce the time it takes to create and evaluate a virtual workstation from hours and days to less than 30 minutes.

What problems does this solution solve?

The growth of popularity in virtual workstations has been accelerated recently with the rise of work from home and distributed teams. However, to enable virtual workstations, customers have had to either rely on consulting firms or self-educating on various AWS technologies, creating high barriers to entry for customers new to AWS or the concept of virtual workstations in general. Several customers have spent 2 – 3 weeks in building initial virtual workstations. Larger creative studios typically have entire departments and teams that focus on the intricacies of virtual workstation configurations. These are resources that smaller creative teams – typically less than 100 artists – do not have access to.

Not only does this solution democratize access to technology and shrinks a multi-week process into minutes, but it allows a customer to eliminate undifferentiated environment setup and focus on the things that gives them value – creating content. In addition, with the virtual workstation setup process accelerated, a customer is able to explore additional cloud-based services that add additional muscle to their creative process.

Who should use this solution?

This guide provides infrastructure and configuration information for planning and deploying the Content Creation Workstation, or VFX host, in the AWS Cloud.

This solution is targeted towards creative studios and teams that have less than 100 people, who are generally new to the virtual workstation concept and are new to AWS, as well.

Cost and licenses

While there is no cost for the use of this solution, you are responsible for the cost of AWS services used while running this solution.

The AWS CloudFormation templates for this solution includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of the deployment. For cost estimates, see the pricing pages of each AWS service you will be using. Prices are subject to change.

Architecture overview

Deploying this solution for a new virtual private cloud (VPC) with **default parameters** builds the following VFX workstation environment in the AWS Cloud.

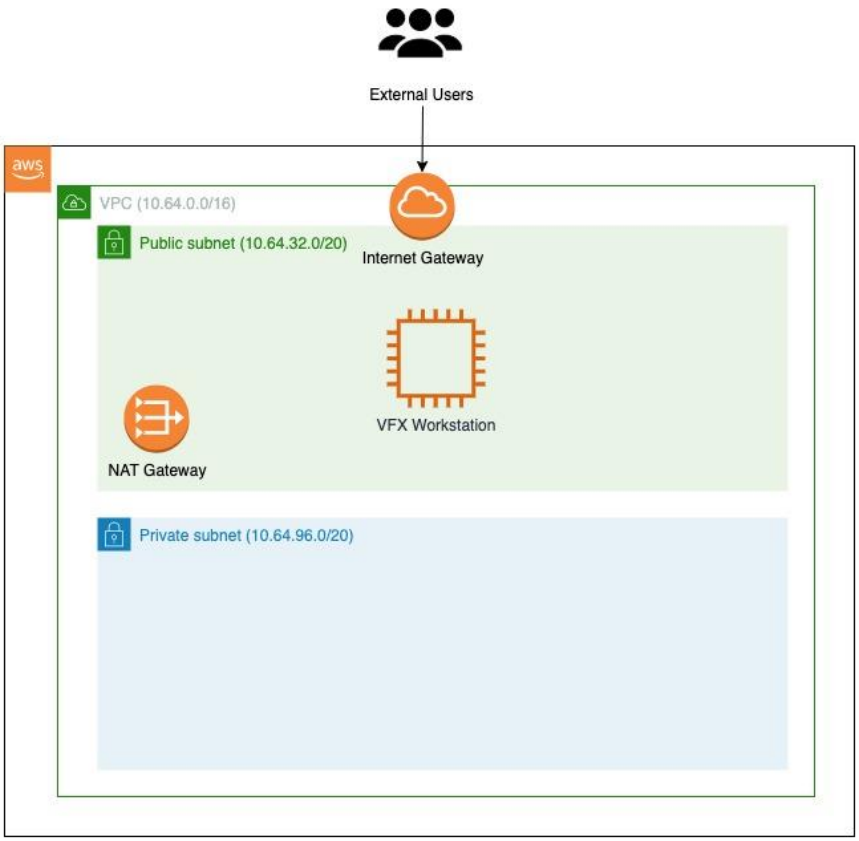


Figure 1: Solution architecture for Content Creation Workstations on AWS

The solution sets up the following:

- A virtual private cloud (VPC) configured with public and private subnet according to AWS best practices, to provide you with your own virtual network on AWS. 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.*
- An internet gateway to allow access to the internet.*

- In the public subnets, managed network address translation (NAT) gateways that allow outbound internet access to resources in the private subnets, but that prevent the internet from accessing those instances.*
- In the public subnet, one VFX host instance is provisioned. Users will install Autodesk Maya, Nuke, and other VFX software on these instances to do their daily work. Blender, an open source software, is already installed on the instance.
- Optionally, you can provision a Client VPN endpoint. This will allow to securely access VFX workstation through a VPN tunnel instead of traversing through the public internet. To provision client VPN endpoint, there are some prerequisite steps required to provision this successfully. (see Deployment Step 2b (Optional): Setup VPN Certificates).

***** The template that deploys the solution into an existing VPC skips the tasks marked by asterisks and prompts you for your existing VPC configuration.

AWS Sample GitHub Repository

This solution uses AWS CloudFormation to automate the deployment of the Content Creation Workstation in the AWS Cloud. The collection of files required for deployment can be found on the Content Creation Workstation AWS Sample GitHub Repository:

AWS Sample

Content Creation Workstation:
https://github.com/aws-samples/content-creation-workstation

Use this repository to launch the solution and all associated components. Clone the repository locally as the deployment is done via command line. You can also customize the template to meet your specific needs.

Automated deployment

Before you launch the solution, review the architecture, configuration, network security, and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Time to deploy: Approximately 20 minutes

Prerequisites

Specialized Knowledge

Before you deploy this Solution, we recommend that you become familiar with the following AWS services and components. (If you are new to AWS, see Getting Started with AWS.)

- Amazon EC2
- Amazon EC2 G4 instance
- Amazon S3
- Amazon VPC

We also recommend that you familiarize yourself with Cloud Access Software from Teradici.

Deployment Options

This Solution provides several deployment options:

VPC Options:

- **Deploy the VFX workstation environment into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, private and public

subnets, NAT gateways, security groups, and other infrastructure components, and then deploys the environment into this new VPC.

- **Deploy the VFX workstation environment into an existing VPC**. This option provisions the environment in your existing AWS infrastructure.
- **Enable VPC Flow Logs**. If creating a new VPC, this option allows you to capture traffic logs to an S3 bucket. The option captures ALL activity including both ACCEPTS and REJECTS.

  NOTE: If this CloudFormation template gets deleted, this S3 bucket and files inside it will not be deleted in the process. Therefore, to stop accruing costs for storage, manual deletion will have the be executed.

Host Options:

- **Enable Termination Protection**. If enabled, this option provides an additional layer of protection against accidental deletion of EC2 instance. By default, this option is disabled. For more information about EC2 termination protection, click here.

  NOTE: If this option is enabled, then the termination protection must be disabled before attempting to delete the instance. Otherwise, the delete will be unsuccessful.
- **Enable S3 Storage Option**. This option creates an S3 bucket where files can be stored and then later synced to the VFX Host. If enabled, the template will provision an S3 bucket and then generates code in the EC2 instance to sync from the S3 bucket to the local file system so the files can be accessed locally. The location of where these files are stored depends on the operating system chosen:

  CentOS: */home/centos/s3*

  Windows: *D:/s3*

  Note: If files are deleted either in S3 bucket or in the local file system, those changes will not be replicated in the other platform. Only new or modified files will be synced.

  Also, if the CloudFormation template gets deleted, this S3 bucket and files inside it will not be deleted in the process. Therefore, to stop accruing costs for S3 storage, manually delete files in S3 bucket.

  Sync occurs every 15 minutes.

Software Options:

- **Install Blender Software Option**. This option will download and install Blender software. Blender is an open-source 3D computer graphics software. By default, this option is enabled. However, it can be disabled if software is not going to be utilized.

Operating System Options:

- **Deploy the VFX workstation on CentOS 7 Operating System**. This option allows the Teradici Cloud Access Software to run on CentOS 7 operating system.
- **Deploy the VFX workstation on Windows Server 2019 Operating System**. This option allows the Teradici Cloud Access Software to run on Windows Server 2019 operating system.

Connectivity Options:

- **Enable Client VPN Endpoint (Optional)**. Client VPN endpoint allows to make VPN sessions and connect to VFX Workstation using private IP address instead of using a public connection.

This Solution has same AWS CloudFormation template for these options. These options are selected based on the parameter configuration for CIDR blocks, instance types, client VPN endpoint and other settings for the cloud VFX workstation environment, as discussed later in this guide.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy a VFX workstation environment on AWS.

> **Important** This Solution uses G4 instances, which aren't available in all AWS Regions. For more information, see the Amazon EC2 Pricing webpage, choose **Windows**, and check to make sure that the AWS Region you want to use for the deployment supports G4 instances.

3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase for the Amazon EC2 G4 instance type. You might need to do this if you already have an existing deployment that uses this instance type, and you think you might exceed the default limit with this reference deployment.

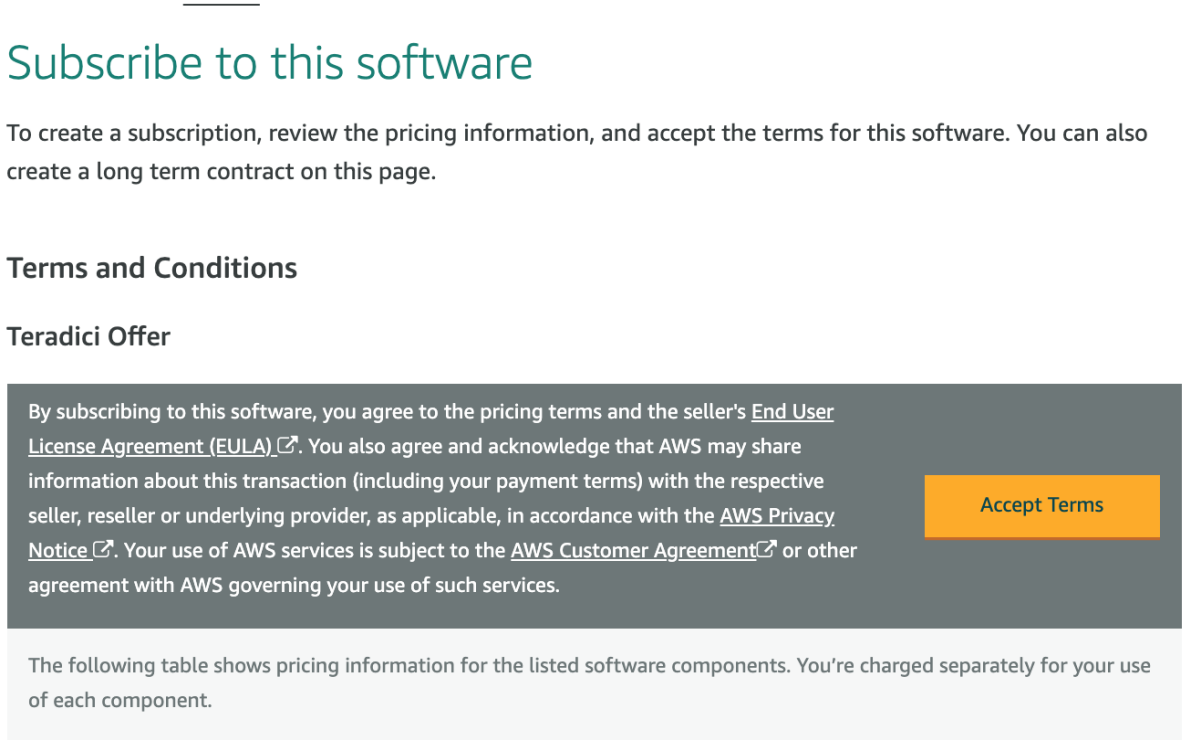
Step 2. Subscribe and accept terms in AWS Marketplace.

In order to be able to use the EC2 instances with Teradici Cloud Access Software installed, the terms and conditions have to be accepted through an AWS Marketplace subscription.

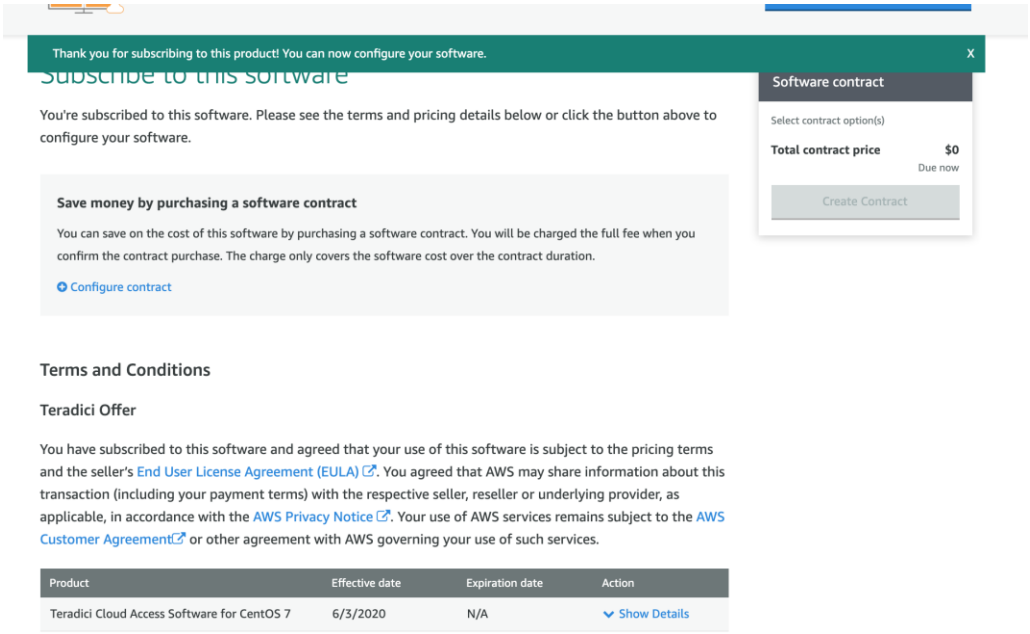
1. Select the correct link based on the preferred operating system. Teradici Cloud Access Software can run on CentOS 7 or Windows Server 2019. If you are going to provision both operating system, you will have to subscribe to both products.
    a. Teradici Cloud Access Software for Windows Server 2019
    b. Teradici Cloud Access Software for CentOS 7

2. On the AWS Marketplace product page, select “Continue to Subscribe” button on the top right of the webpage.

3. Select “Accept Terms” on the following page.



4. This completes the subscription process. Teradici Cloud Access Software can now be utilized.



Step 2b. (Optional): Create and upload VPN Certificates.

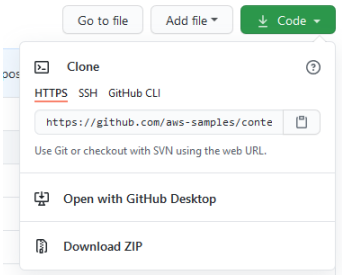
In order to provision a client VPN endpoint on AWS, user must generate a client/server SSL certs and upload them to Amazon Certification Manager (AWS ACM). The following link

provides detailed instructions on how to complete this. Once certificates are in ACM, then take note of the server and client certificate ARNs. These ARN values will be required as the CloudFormation will ask you to specify the ARNs in the VPN configuration center.
This step is optional and is only needed if provisioning client VPN endpoint as part of the deployment solution.

Step 3. Clone the Repository

You can download the repository contents or clone the repository locally from GitHub.

- To download the repository, go to the GitHub repository and click on the green “Code” button and “Download ZIP”. Unzip those files to a new directory to work from.



- To clone the repository, open a command line session from a folder you want the repository to be cloned to. Use the following command to clone the AWS Sample GitHub repository locally:

```
git clone https://github.com/aws-samples/content-creation-workstation.git
```

Step 4. Setup AWS Command Line Interface

1. Install the AWS Command Line Interface (CLI) following the AWS Command Line Interface User Guide installation steps.
2. Configure the AWS CLI with your AWS account details following the AWS Command Line Configuration steps. It is a best practice to setup a new role and generate credentials for this sample to use, with only the permissions required to launch this sample.

Step 5. Launch the Solution

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

1. Modify existing parameters file from the repository (deployment/parameters/test-param.json) or create your own. In the following table, parameters are listed by category. Some parameters require input and others have defaults as shown.

CloudFormation Template Parameters:

Amazon EC2 Configuration:

Parameter label (name)	Default	Description
VFX Host Operating System (OSType)	*linux*	Specify whether you want to run Teradici on Linux(CentOS 7) or Windows(Windows Server 2019) OS. Valid values are “linux” or “windows”
EBS Volume size for EC2 instance (EBSVolumeSize)	100	Volume size for the VFX Host, in GiB
Key Pair Name (KeyPairName)	*Requires input*	Name of AWS EC2 Key Pair.
VFX Host Instance Type (VFXHostInstanceType)	g4dn.xlarge	Amazon EC2 instance type for the VFX workstations. Teradici Cloud Access Software only allows the product to be provisioned on g4dn.xlarge – g4dn.16xlarge instances.
VFX Host Access CIDR (VFXHostAccessCIDR)	10.64.0.0/16	CIDR Range that will access the VFX Host. Input your network's current public or private IP depending if the VFX is being placed in a public or private subnet
VFX Host subnet placement. (VFXHostSubnetPlacement)	Public	Specify if VFX host should be placed in "Public" or "Private" subnet.
Enable Termination Protection (EnableDeleteProtection)	false	Specify if VFX host should have delete protection enabled.
Install Blender Software (InstallBlenderSoftware)	true	Specify if VFX host should download and install Blender software.
Creates S3 bucket to store files and then sync with workstation. (CreateS3StorageBucket)	true	Specify if template should create an AWS S3 Bucket and connect the host to sync files between local system and S3 bucket.

Existing VPC Configuration:

Parameter label (name)	Default	Description
Existing VPC ID (ExistingVPCID)	N/A	If solution should deploy into an existing VPC, Specify existing VPC ID. If solution is deployed into a new VPC, leave default value.

Parameter label (name)	Default	Description
Existing Subnet ID (ExistingSubnetID)	N/A	If solution should deploy into an existing VPN, specify subnet id in which the VFX Host should be placed in. If solution is deployed into a new VPC, leave default value.

New VPC Configuration:

Parameter label (name)	Default	Description
VPC CIDR Range (VPCCIDR)	10.64.0.0/16	If solution should create a new VPC, specify CIDR Block for the VPC. If solution is deployed into existing VPC, leave default value.
CIDR Range for Public Subnet in new VPC (PublicSubnet1CIDR)	10.64.32.0/20	If solution should create a new VPC, specify CIDR Block for the VPC. If solution is deployed into existing VPC, leave default value.
CIDR Range for Private Subnet in new VPC (PrivateSubnet1CIDR)	10.64.96.0/20	If solution should create a new VPC, specify CIDR Block for the VPC. If solution is deployed into existing VPC, leave default value.
VFX Host subnet placement. (EnableVPCFlowLogs)	false	Specify if newly created VPC should have VPC flow logs enabled. The CloudFormation template will create a new S3 bucket to store the logs. It will also capture ALL logs including ACCEPTS and REJECTS.

VPN Endpoint Configuration:

Parameter label (name)	Default	Description
Create VPN Endpoint. (CreateVPNEndpoint)	false	Should the CloudFormation create a Client VPN Endpoint. It is recommended if VFX Host is placed in private subnet and there is no other provisions created to connect to the private subnet. (Specify 'true' or 'false')
Client CIDR for VPN Endpoint. (ClientCidrBlock)	10.50.0.0/20	If creating Client VPN endpoint in the solution, specify the IPv4 address range. It should be in CIDR notation from which to assign client IP addresses. The address range cannot overlap with the local CIDR of the VPC in which the associated subnet. Otherwise, leave default value.
Server Cert Arn for VPN endpoint. (ServerCertArn)	N/A	If creating Client VPN endpoint in the solution, specify Server Cert Arn for VPN endpoint. Otherwise, leave default value.
Client Cert Arn for VPN endpoint. (ClientCertificateArn)	N/A	If creating Client VPN endpoint in the solution, specify Client Cert Arn for VPN endpoint. Otherwise, leave default value.
Target Network CIDR for VPN Endpoint. (TargetNetworkCidr)	10.64.0.0/16	If creating Client VPN endpoint in the solution, specify the IPv4 address range, in CIDR notation, of the network for which access is being authorized. Otherwise, leave default value.

2. Due to the use of Nested Templates in this solution, the parent template must be packaged in order to properly reference the child template(s). More information regarding CloudFormation packaging can be found here. Open a command line session at the location you cloned the repository, and use the following command to package the template (items in [] need to be changed to for your deployment):

```
aws cloudformation package --template-file ./deployment/content-creation-workstation.template --s3-bucket [desired s3 bucket for CF artifacts] --output-template-file ./deployment/outputs/vfx_packaged.yaml --region [AWS deployment region, should be the same region where S3 bucket is located.]
```

3. Use the following command to create the CloudFormation Stack (items in [] need to be changed to for your deployment):

```
aws cloudformation create-stack --template-body file://deployment/outputs/vfx_packaged.yaml --parameters file://deployment/parameters/test-param.json --stack-name [desired stack name] --region [AWS Deployment Region] --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_IAM
```

Each deployment will depend on several factors such workstation OS, VPN and VPC option. In general, CloudFormation takes about 15-45 minutes to complete. You can open the AWS Console in your browser and go to the CloudFormation service to see your stack being built and the status.

> **Important** If you're deploying the environment into an existing VPC, make sure that your VPC has the domain name option configured in the DHCP options as explained in the Amazon VPC documentation. You will be prompted for your VPC settings when you launch the Solution.

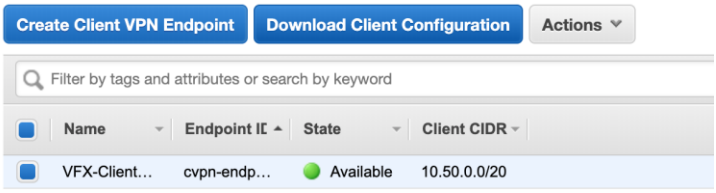
Step 6a. Install Tunnelblick and configure VPN (Optional).

This step is only required if you have chosen to create a client VPN endpoint. This step will guide you through how to connect to the VPN for your workstation.

1. Download and Install Tunnelblick or any other compatible OpenVPN client.

> **Important** This guide will show steps on how to configure VPN with the Tunnelblick client. Steps may vary for other OpenVPN clients.

2. Download the OpenVPN Configuration file by conducting the following steps.
    a. Sign in to the AWS Management Console and open the Amazon VPC console at https://console.aws.amazon.com/vpc.
    b. In the left navigation pane, chose **Client VPN Endpoints**.
    c. Select the Client VPN endpoint with name **VFX-ClientVPN**, and the select **Download Client Configuration** button.

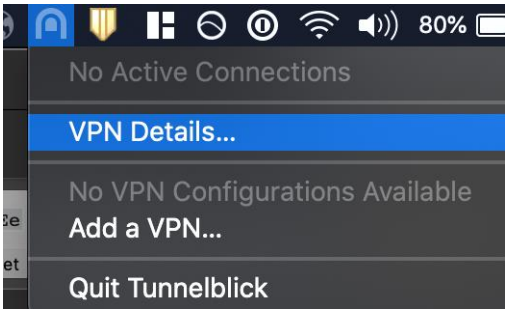


3. Open the downloaded file in an editor and add the following lines to the end of the file. Insert path value of where certificate and key files on your computer. These files would have been generated in Step 2b. Then save the file.

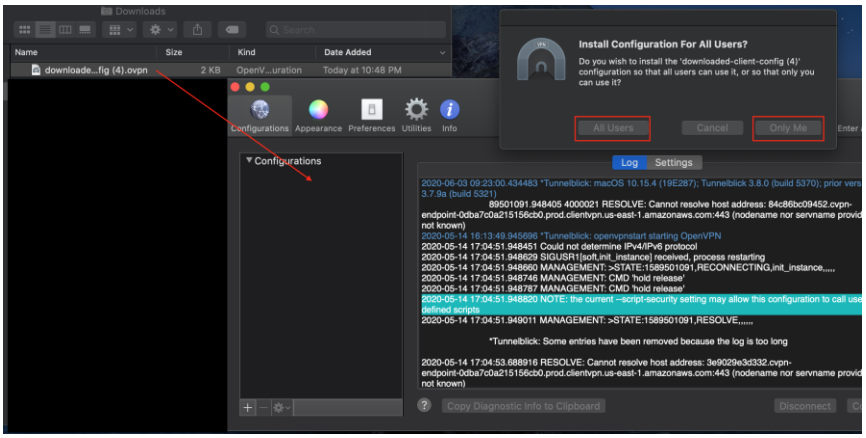
    cert <path to client.vfx.vpn.crt>

    key <path to client.vfx.vpn.key>

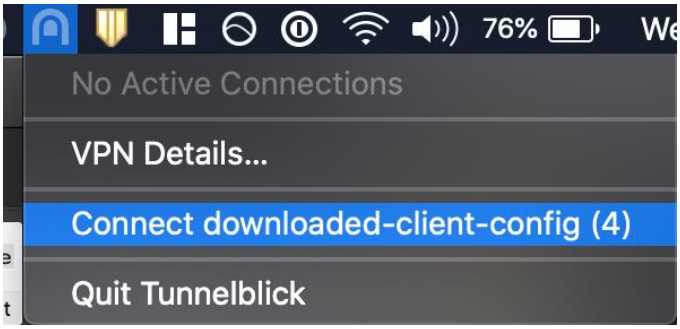
4. Open Tunnelblick application and then select **VPN Details**.



5. Drag updated openvpn file to the VPN Configuration window. Then select appropriate user level permissions.



6. To connect to VPN simply click on the Tunnelblick icon and selecting the imported openvpn file.



Step 6b. Install the Teradici PCoIPClient and Connect to VFX workstation.

After you deploy the VFX host environment on AWS, it is time to connect to your VFX workstation instance.

Install the Teradici PCoIP software

- Install the Teradici PCoIP Software Client by using the following link.

1. Sign in to the AWS Management Console and open the Amazon EC2 console at https://console.aws.amazon.com/ec2.
2. In the left navigation pane, choose **Instances**.
3. Choose the **VFX Host** instance. Note the IPv4 public IP address, which you will enter in the next steps. If the **VFX Host** was deployed to a private subnet and you are using VPN or Direct Connection to connect to the instance. Then, you will use the IPv4 private address instead.
4. Retrieving the password for the VFX Host instance will depend on the OS provisioned.

Windows Server 2019:

- Choose the **VFX Host** instance. Click the **Actions** button and the select **Get Windows Password**. In the popup window, upload your key file that was generated when creating the AWS EC2 Keypair. Click **Decrypt Password** button. Note the password, which you will enter in next steps.

CentOS 7:

- Choose the **VFX Host** instance. In the **Description** section, note the Instance ID as this will be the password for this instance that you will enter in the next steps.

Connect to the VFX from your computer

5. On your computer, open the Teradici PCoIP Software Client, and choose **New Connection.**
6. Enter the IPv4 public address from the EC2 VFX host instance and choose **Next**.
7. A message appears saying that Teradici cannot verify your connection. Choose **Connect Insecurely**.

> **Note** The PCoIP client generates this warning because it uses a default, self-signed Teradici certificate and can't validate the identity of the workstation. To avoid the warning, you can create and install your own certificate. For more information about Teradici connection security modes, see Connection Security Modes.

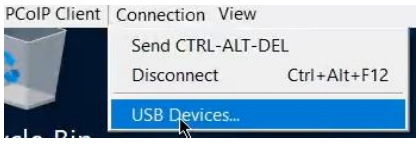
8. For the user name, enter **Administrator**.
9. Use the get the password you decrypted earlier for the VFX host instance and choose **Login**. You're now connected to your remote G4 GPU instance running on AWS.
10. Install the necessary VFX software tools to do your work.

Setup WACOM Device via Host Redirection (Optional)

11. Verify WACOM device compatibility by reviewing the supported models here.

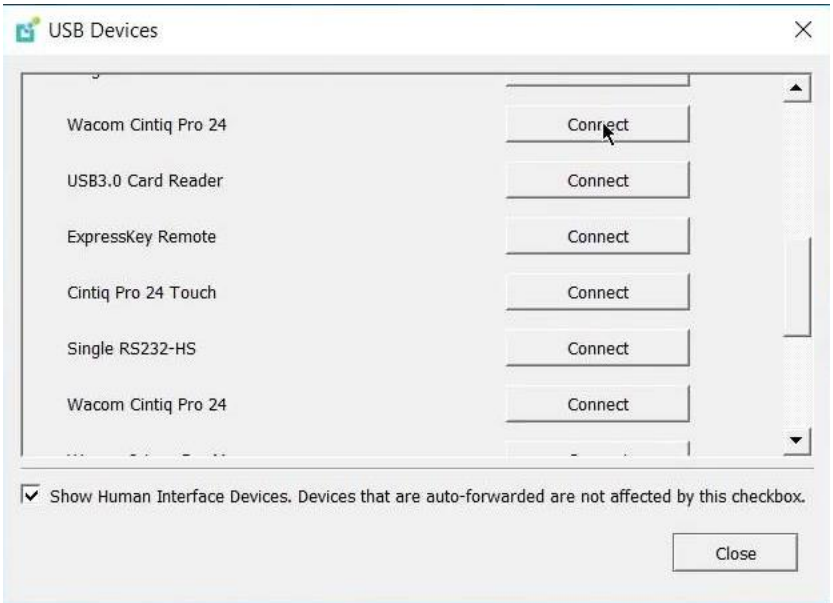
> **Note** Assumption that the PCoIP host has WACOM drivers already installed. Otherwise you will receive a warning that "No Wacom device in connected to your computer".

12. In the PCoIP Client menu select Connection > USB Devices

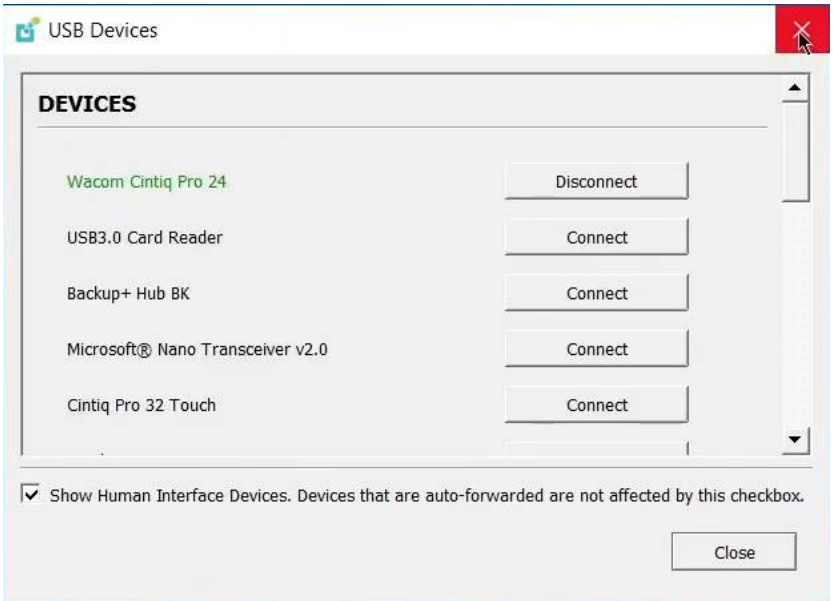


13. In the USB Devices Menu, check the “Show Human Interface Devices” check box. When the Warning Screen appears, select “ok” to acknowledge transfer of functionality to the Host system.

14. Select the desired WACOM device that shows up in the USB devices menu.



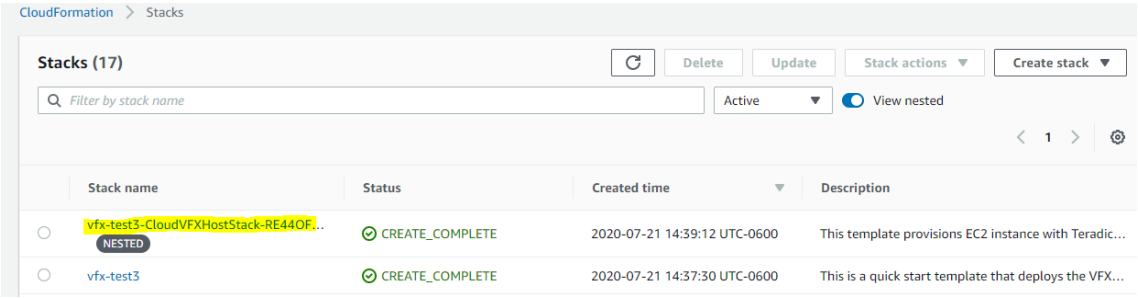
15. Press the “Connect” button to attach the device to the Host system.



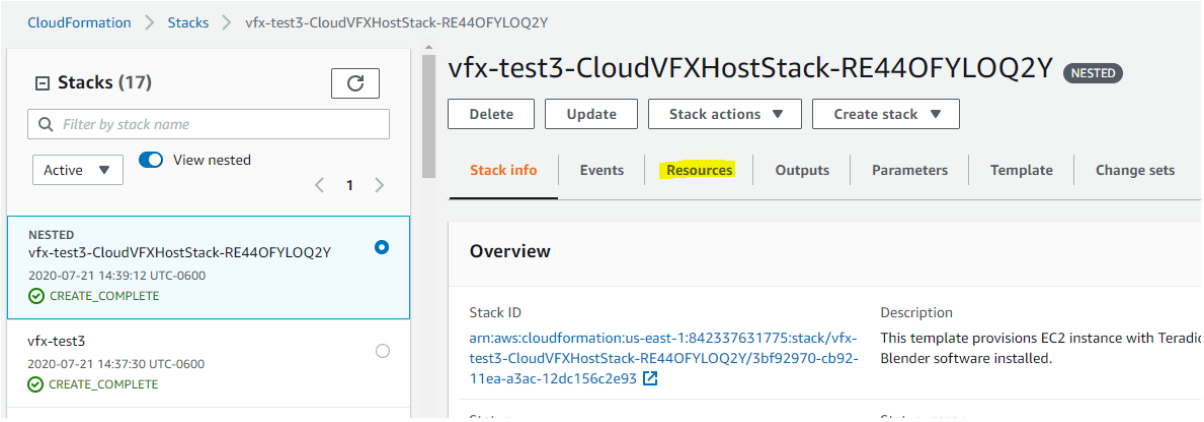
Step 6c. Transfer files to S3.

If the CreateS3StorageBucket option was selected, then you can transfer files to the instance from your computer through S3.

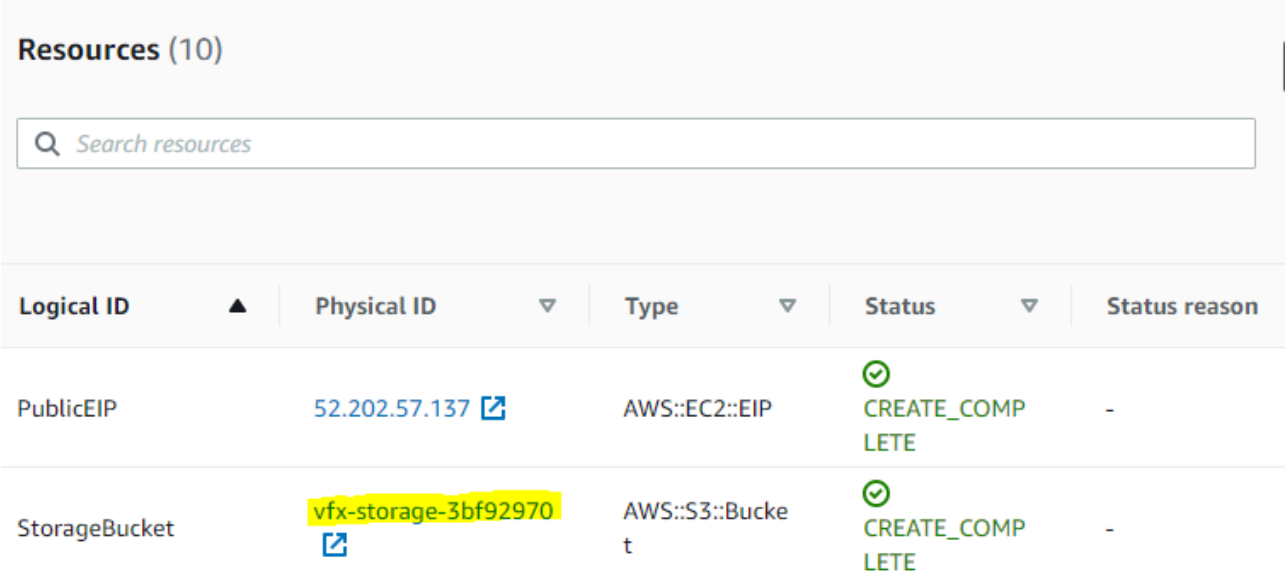
1. Sign in to the AWS Management Console and open the AWS CloudFormation at https://console.aws.amazon.com/cloudformation.
2. Select the nested template of your stack with the “CloudVFXHostStack” name in it.



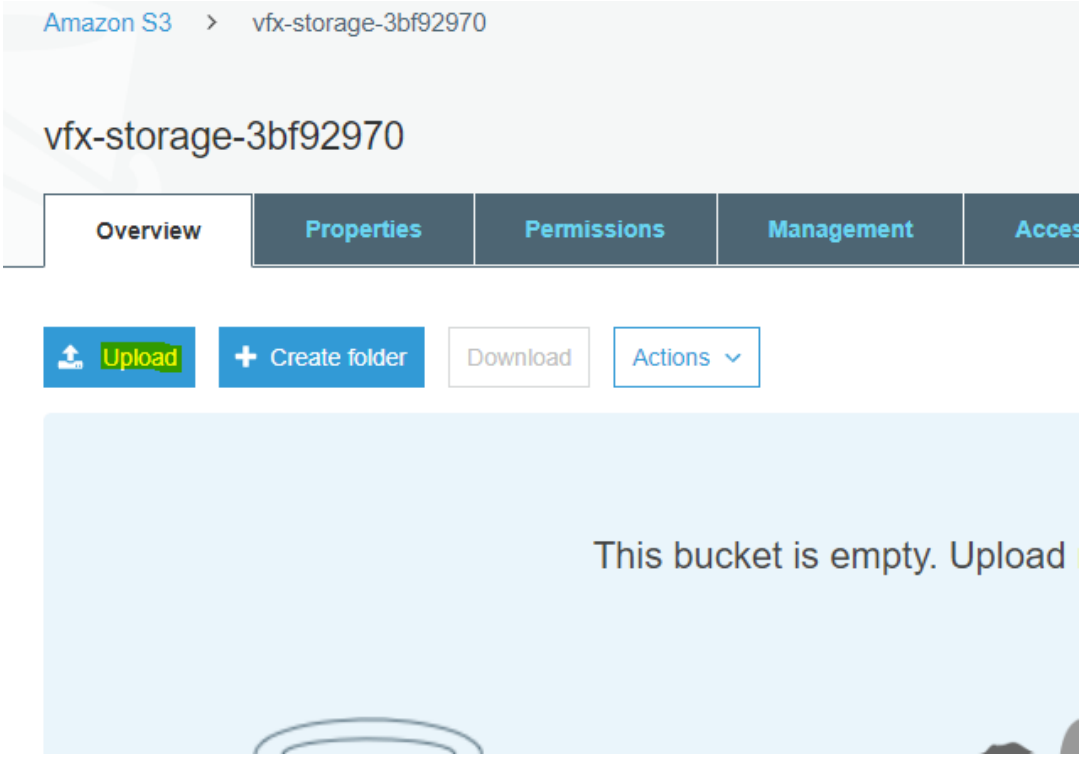
3. Click on the **Resources** tab.



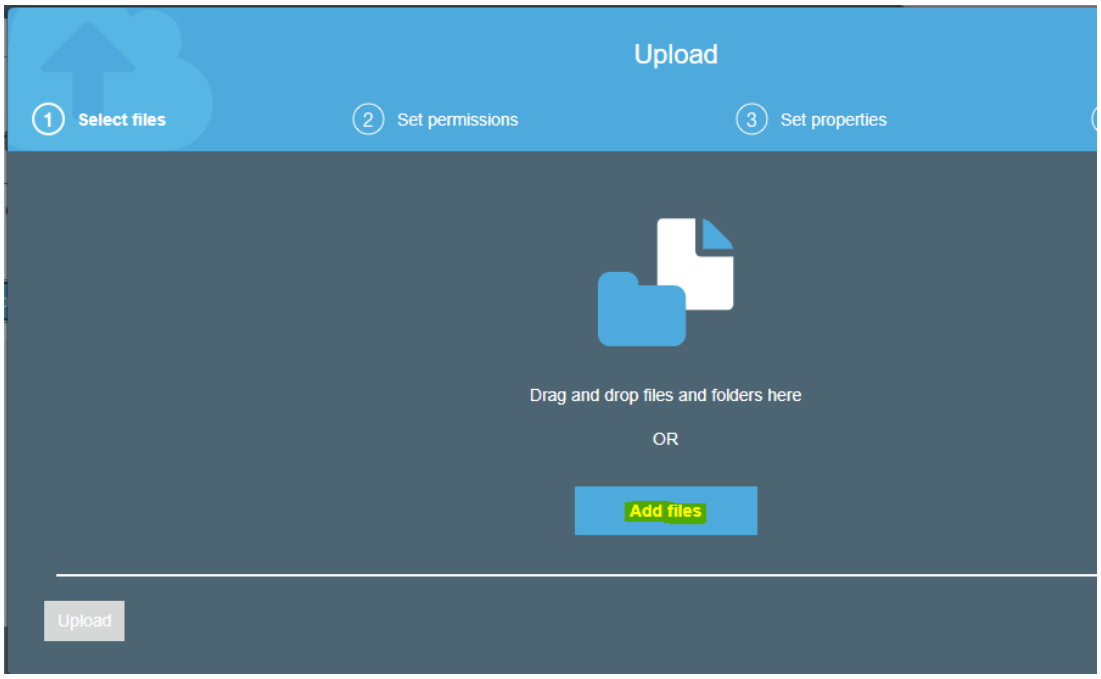
4. In the table, find resource that has a logical ID of **"Storage Bucket**". Click on the link in the **Physical ID** column.



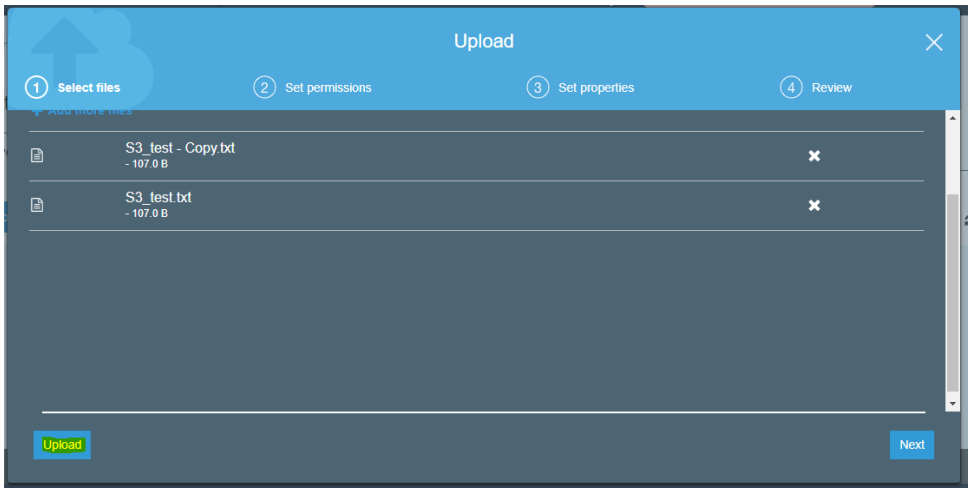
5. Once at the S3 Bucket page, select the **Upload Button.**



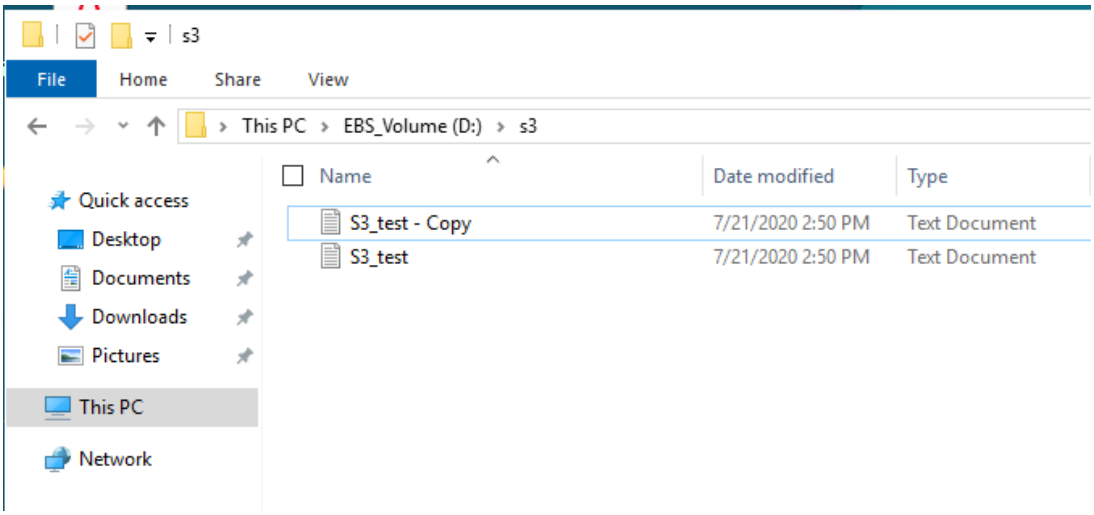
6. Click on the **Add Files** button and select the files that you want to upload to S3 Bucket.



7. Once the files have been selected, click **Upload** button.



8. Once the files have been uploaded to S3, they will sync with the EC2 instance within several minutes depending on file size.



Security

There are several security-related aspects of the architecture in this Solution. The VPC provides security using security groups and network access control lists (ACLs). This allows fine-grained control of traffic in and out of the VPC and to the host.

You should only allow access to IP addresses that use the VFX host (see the **VFXHostAccessCIDR** parameter in Amazon EC2 Configuration, earlier in this guide). This

helps keep the host protected from malicious attacks and helps protect the data (VFX assets, in this case).

Additional Resources

Troubleshooting

Q. I encountered a CREATE_FAILED error with the following status reason; "In order to use this AWS marketplace product you need to accept terms and subscribe…"

A. This means that Step 2: Subscribe and accept terms in AWS Marketplace was missed or you subscribed to the incorrect product.

Q. I encountered a CREATE_FAILED error when I launched the Solution.

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. (Look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log`.)

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.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

GitHub Repository

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

Additional Resources

AWS services

- Amazon EC2
  https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/

- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/
- AWS Command Line Interface (CLI)
  https://aws.amazon.com/cli/
- NAT Gateway managed service
  https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html

Teradici software

- Teradici Cloud Access Software
  https://www.teradici.com/products/cloud-access/cloud-access-software

Solution reference deployments

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

Document Revisions

Date	Change	In sections
October 2020	Modified for release as AWS Sample	Deployment Steps
August 2020	Initial submission	—