SAS Viya on the AWS Cloud

Quick Start Reference Deployment

May 2018  
Last update: October 2019 ([revisions](#_Document_Revisions))

*SAS Institute*

*AWS Quick Start Reference Team*

Contents

[Overview 3](#_Toc23401618)

[SAS Viya on AWS 3](#_Toc23401619)

[Costs and Licenses 3](#_Toc23401620)

[Architecture 5](#_Toc23401621)

[Prerequisites 8](#_Toc23401622)

[Specialized Knowledge 8](#_Toc23401623)

[Technical Requirements 8](#_Toc23401624)

[Authentication Provider Options 10](#_Toc23401625)

[Deployment Options 10](#_Toc23401626)

[Deployment Steps 11](#_Toc23401627)

[Step 1. Prepare Your AWS Account 11](#_Toc23401628)

[Step 2. Upload the SAS Software Order File to an Amazon S3 Location 11](#_Toc23401629)

[Step 3. Launch the Quick Start 12](#_Toc23401630)

[Step 4. Test the Deployment 18](#_Toc23401631)

[Step 5. Perform Further Configuration 20](#_Toc23401632)

[Step 6. (Optional) Enable Access to Existing Data Sources 20](#_Toc23401633)

[Step 7. (Optional) Deploy Data Agent, and Validate Communication 20](#_Toc23401634)

[Best Practices Using SAS Viya on AWS 23](#_Toc23401635)

[Utility Scripts for SAS Viya on AWS 23](#_Toc23401636)

[Troubleshooting 24](#_Toc23401637)

[View Log Files 24](#_Toc23401638)

[Restarting the SAS Services 25](#_Toc23401639)

[Recover from a Lost CAS Node VM 26](#_Toc23401640)

[FAQ 27](#_Toc23401641)

[Additional Resources 28](#_Toc23401642)

[GitHub Repository 29](#_Toc23401643)

[Addendum A: Resource Requirements 30](#_Toc23401644)

[Addendum B: Administrative Permission Requirements 30](#_Toc23401645)

[Addendum C: Set up a Mirror Repository 32](#_Toc23401646)

[Addendum D: Configuring the Identities Service 32](#_Toc23401647)

[Verify Port Settings 32](#_Toc23401648)

[Create Service Account 32](#_Toc23401649)

[Configure the Identities Service 32](#_Toc23401650)

[Verify the Configuration 33](#_Toc23401651)

[Configure PAM for SAS Studio 33](#_Toc23401652)

[Addendum E: Managing Users for the Provided OpenLDAP Server 34](#_Toc23401653)

[Document Revisions 36](#_Toc23401654)

This Quick Start deployment guide was created by Amazon Web Services (AWS) in collaboration with SAS Institute.

[Quick Starts](http://aws.amazon.com/quickstart/) are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

**Note**  For the current operational status of this Quick Start, visit the [SAS Viya repository](https://github.com/sassoftware/quickstart-sas-viya/tree/master).

## Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying the following SAS Viya products on the Amazon Web Services (AWS) Cloud:

* SAS Visual Analytics 8.3 on Linux
* SAS Visual Statistics 8.3 on Linux
* SAS Visual Data Mining and Machine Learning 8.3 on Linux
* SAS Data Preparation 2.3

This Quick Start is a reference architecture for users who want to deploy the SAS platform, using microservices and other cloud-friendly technologies. By deploying the SAS platform on AWS, you get SAS analytics, data visualization, and machine learning capabilities in an AWS-validated environment.

### SAS Viya on AWS

SAS Viya is a cloud-enabled, in-memory analytics engine. It uses elastic, scalable, and fault-tolerant processing to address complex analytical challenges. SAS Viya provides faster processing for analytics by using a standardized code base that supports programming in SAS, Python, R, Java, and Lua. It also supports cloud, on-premises, or hybrid environments and deploys seamlessly to any infrastructure or application ecosystem.

With SAS Viya, you can:

* Gather and share insights from embedded analytical services.
* Build centralized, governed analytics models for efficient deployment and maintenance.
* Use analytics to quickly deliver answers and results.

### Costs 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 will need a SAS license to launch this Quick Start. Your SAS account team and the SAS Enterprise Excellence Center can advise on the appropriate software licensing and sizing to meet workload and performance needs.

The AWS CloudFormation template for this Quick Start creates three EC2 instances:

* One compute virtual machine (VM)—the Cloud Analytic Services (CAS) controller
* One VM for administration—the Ansible controller
* One VM for the SAS Viya services

#### CAS Controller VM

We recommend that you configure your machine with twice the number of cores than the amount that you are licensed for in order to optimize thread utilization. For more information, see [Important Performance Considerations When Moving SAS to a Public Cloud](https://www.sas.com/content/dam/SAS/support/en/sas-global-forum-proceedings/2019/3363-2019.pdf).

**Note** Depending on the instance size, EBS volumes or ephemeral storage are used for your instance. For the CAS User Library, EBS volumes are created and attached to your instance for all instance types. For i3 instances, ephemeral storage is used for the CAS Cache. For non-i3 instances, EBS volumes are created and attached to your instance for the CAS Cache.

In MPP environments, this sizing is attached to the CAS worker and not the CAS controller.

|  |  |  |
| --- | --- | --- |
| Instance size | Size (GB)  CAS cache | Size (GB)  CAS user library |
| i3.large | 442 | 500 |
| i3.xlarge | 884 | 500 |
| i3.2xlarge | 1769 | 500 |
| i3.4xlarge | 3538 | 500 |
| i3.8xlarge | 7076 | 1000 |
| i3.16xlarge | 14156 | 1000 |
| i3.metal | 14156 | 1000 |
| r5.large | 180 | 500 |
| r5.xlarge | 180 | 500 |
| r5.2xlarge | 180 | 500 |
| r5.4xlarge | 360 | 500 |
| r5.12xlarge | 720 | 1000 |
| r5.24xlarge | 900 | 1000 |
| r5.metal | 900 | 1000 |
| r5a.large | 180 | 500 |
| r5a.xlarge | 180 | 500 |
| r5a.2xlarge | 180 | 500 |
| r5a.4xlarge | 360 | 500 |
| r5a.12xlarge | 720 | 1000 |
| r5a.24xlarge | 900 | 1000 |

#### SAS Viya Services VM

The Viya Services are deployed onto an r5.4xlarge EC2 instance by default. The instance has a 100-GB EBS volume attached for installation and user data.

**Note**  For the services VM, you can select a larger or smaller r4 or r5 instance by changing the **ServicesInstanceSize** configuration parameter during deployment, as shown in the following table.

|  |  |  |
| --- | --- | --- |
| Services instance size | Use | Storage (Amazon EBS) |
| r4.2xlarge | Demos and POCs | 32 GB+256 GB |
| r4.4xlarge | Robust sizing | 32 GB+256 GB |
| r4.8xlarge | Heavy concurrent loads/multiple users | 32 GB+256 GB |
| r5.2xlarge | Demos and POCs | 32 GB+256 GB |
| r5.4xlarge (default) | Robust sizing | 32 GB+256 GB |
| r5.12xlarge | Heavy concurrent loads/multiple users | 32 GB+256 GB |
| r5.24xlarge | Heavy concurrent loads/multiple users | 32 GB+256 GB |

For information about the number of resources in each type of deployment, see [Addendum A: Resource Requirements](#_Addendum_A:_Resource).

## Architecture

By default, Quick Start deployments enable Transport Layer Security (TLS) to help ensure that communication between external clients (on the internet) and the Elastic Load Balancing (ELB) load balancer is secure. Likewise, TLS is enabled between the ELB load balancer and the private subnet that contains the SAS Viya components.

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** in a symmetric multiprocessing (SMP) environment builds the following SAS Viya environment in the AWS Cloud, shown in Figure 1. In SMP environments, the **CASInstanceCount** parameter is set to one, indicating that only one CAS controller is configured.

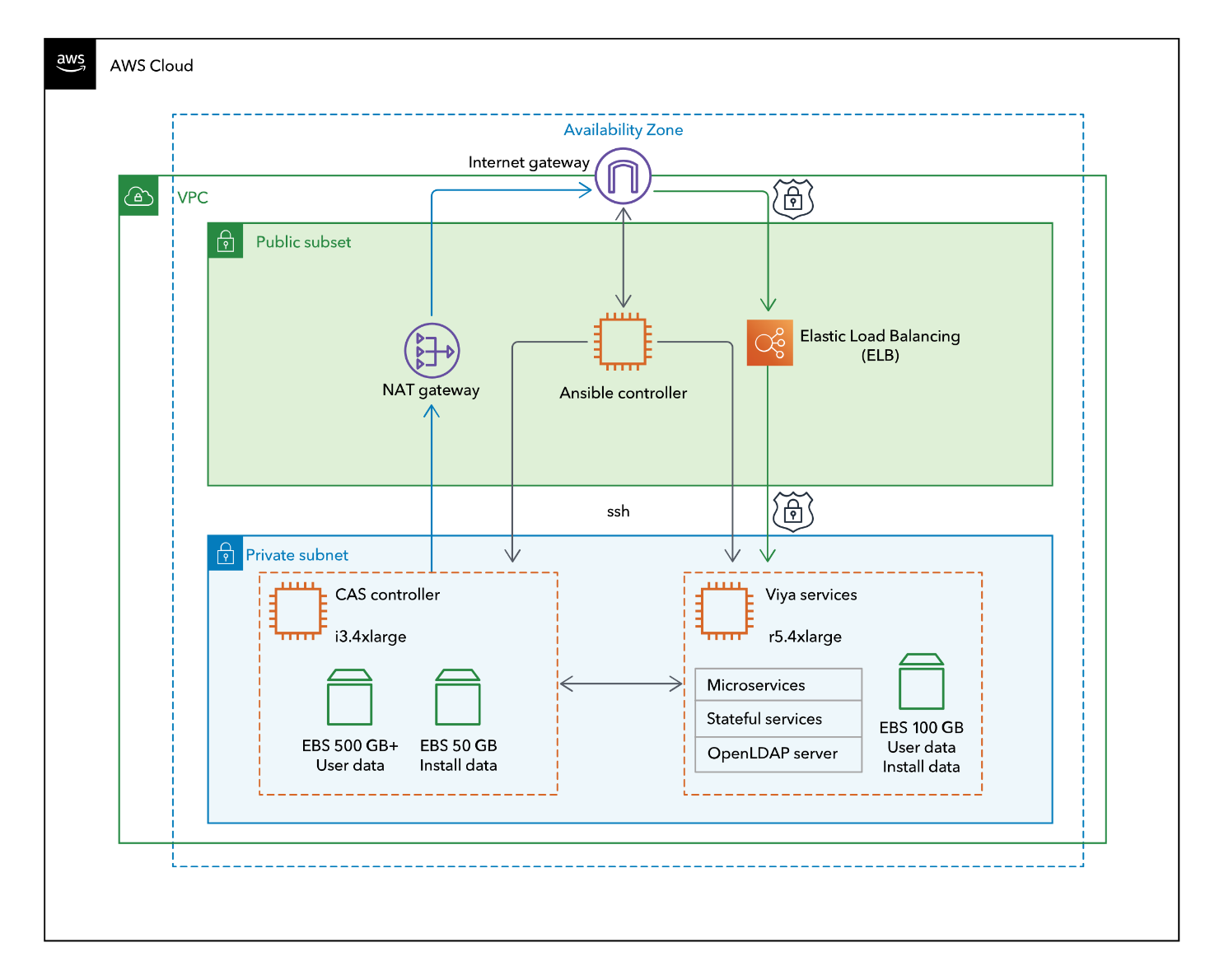


Figure 1: Quick Start architecture for SAS Viya on AWS in an SMP environment

Deploying this Quick Start for a new VPC in a massively parallel processing (MPP) environment builds the following SAS Viya environment in the AWS Cloud, shown in Figure 2. In MPP environments, the **CASInstanceCount** parameter is set to a number between two and ten, indicating the number of CAS workers that are configured in addition to the CAS controller.

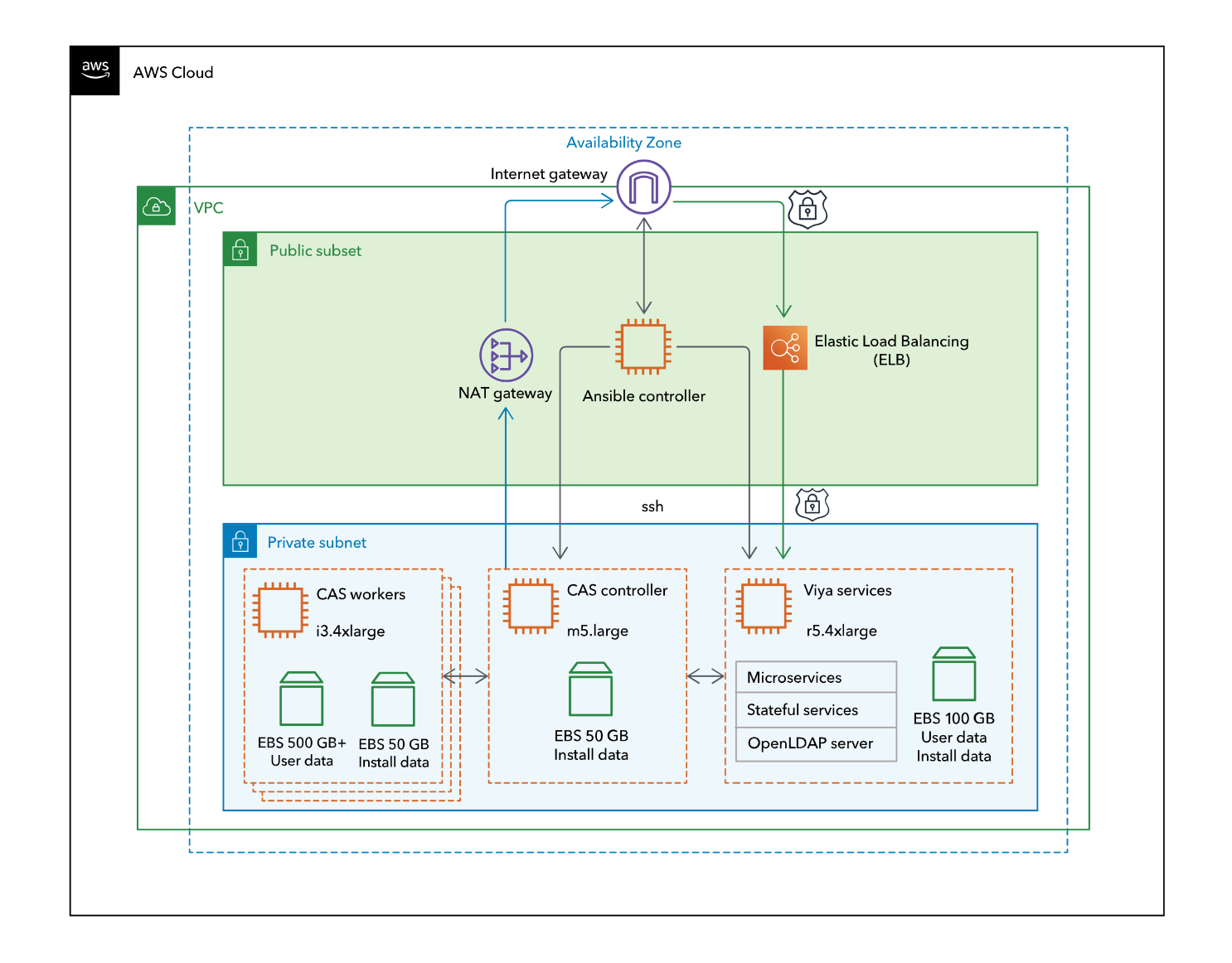


Figure 2: Quick Start architecture for SAS Viya on AWS in an MPP environment

The Quick Start sets up the following:

* A virtual private cloud (VPC) configured with public and private subnets according to AWS best practices. This provides the network infrastructure for your SAS Viya deployment.\*
* An ELB load balancer.
* An internet gateway to provide access to the internet.\*
* Managed NAT gateways to allow outbound internet access for resources in the private subnets.\*
* In the private subnet in an SMP environment, two EC2 instances with SAS Viya on Red Hat Enterprise Linux (RHEL) 7.4.
* In the private subnet in an MPP environment, two plus the number of worker nodes (defined in the **CASInstanceCoun**t parameter) EC2 instances with SAS Viya on Red Hat Enterprise Linux (RHEL) 7.4.
* In the public subnet, an EC2 instance running Amazon Linux. This instance is used as an Ansible controller that serves as an admin node, allowing access to the SAS Viya VMs in the private subnet.
* Security groups for the SAS Viya VMs and the Ansible controller.
* Optionally, a default identity provider with users “sasuser” and “sasadmin.”
* An Amazon CloudWatch Logs log group for deployment logs.
* Optionally, an Amazon Simple Notification Service (Amazon SNS) email notification when SAS Viya deployment starts and finishes.

\**The template that deploys the Quick Start into an existing VPC skips the components marked by asterisks above.*

## Prerequisites

### Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see [Getting Started with AWS](https://aws.amazon.com/getting-started/).)

* [Amazon Virtual Private Cloud (Amazon VPC)](https://aws.amazon.com/documentation/vpc/)
* [Amazon Elastic Compute Cloud (Amazon EC2)](https://aws.amazon.com/documentation/ec2/)
* [Amazon Elastic Block Store (Amazon EBS)](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html)
* [Amazon Simple Storage Service (Amazon S3)](https://aws.amazon.com/documentation/s3/)
* [AWS Identity and Access Management (IAM)](https://aws.amazon.com/documentation/iam/)
* [Amazon Route 53](https://aws.amazon.com/documentation/route53/)
* [AWS Certificate Manager](https://aws.amazon.com/documentation/acm/)

### Technical Requirements

Before deploying SAS Viya on AWS, you must have the following:

* An AWS account with appropriate creation privileges. The account that you use to create the AWS CloudFormation stack must have administrator privileges, including the ability to create IAM resources with custom names. For more information, see [Addendum B: Administrative Permission Requirements](#_Addendum_B:_Administrative_1).
* A SAS Software Order Confirmation e-mail that contains supported Quick Start products. Supported products include:
* SAS Visual Analytics 8.3 on Linux
* SAS Visual Statistics 8.3 on Linux
* SAS Visual Data Mining and Machine Learning 8.3 on Linux
* SAS Data Preparation 2.3
* SAS/ACCESS Interface to Amazon Redshift
* SAS/ACCESS Interface to MySQL
* SAS/ACCESS Interface to PostgreSQL
* You can create a mirror repository for your software order. For information, see [Addendum C: Set Up a Mirror Repository](#_Addendum_C:_Set).

#### DNS and SSL Certificate

To deploy with your own DNS name and SSL certificate:

1. Register a domain managed by Amazon Route 53 or have your own domain. For instructions on registering the domain, see the [Route 53 documentation](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/domain-register.html).
2. After you receive a confirmation email, navigate to **Hosted Zone** in the Route 53 console UI and make note of your hosted zone.
3. Register a certificate with AWS Certificate Manager. This certificate can be either of the following:

* An SSL certificate that AWS Certificate Manager generates and manages.
* Your own or third-party SSL certificate, which AWS Certificate Manager registers and manages in the region where you are deploying SAS Viya.

For instructions on creating a certificate, see [Request a Public Certificate](https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-request-public.html) in the AWS documentation. When you receive the email from the AWS Certificate Manager, follow the instructions and make note of the certificate Amazon Resource Name (ARN) ID.

1. When you launch this Quick Start, you are prompted for the following three parameters:

* **Domain Name (DomainName)**
* **Route 53 Hosted Zone (AWSHostedZoneID)**
* **SSL Certificate (SSLCertificateARN)**

If you specify these options, the deployment configures the Elastic Load Balancing (ELB) load balancer and the AWS hosted zone to use the DNS name and certificate.

Route 53 adjusts the DNS settings for the domain to point to the ELB load balancer. The final DNS names will be in the **Outputs** tab of your stack entry in the AWS CloudFormation console.

## Authentication Provider Options

This Quick Start provides two options for authentication:

* Use a default OpenLDAP server set up by the AWS Quick Start for SAS Viya deployment. When you deploy, set the **Password for Default User (SASUserPass)**. Two users are created:
* sasuser with **Password for Default User (SASUserPass)**
* sasadmin with **SAS Administrator Password (SASAdminPass)**

To add or remove users, see [Addendum E: Managing Users for the Provided OpenLDAP Server](#_Addendum_E:_Managing).

* Use your own identity management system. Ensure that the services VM can make outbound connections to your LDAP server.   To use your own authentication provider, when you deploy, do NOT set the value for the **Password for Default User (SASUserPass)**. The password for the initial administrator account (sasboot) is set to the value of **SAS Administrator Password (SASAdminPass)**. You can then use the sasboot account to configure your identity management system, once the deployment is completed. For details, see [Addendum D: Configuring the Identities Service](#_Addendum_D:_Configuring).

## Deployment Options

This Quick Start provides two deployment options:

* **Deploy SAS Viya 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, Ansible controllers, and other infrastructure components, and then deploys SAS Viyainto this new VPC.
* **Deploy SAS Viya into an existing VPC**. This option provisions SAS Viya in your existing AWS infrastructure.
* The Quick Start provides separate templates for these options. You can also configure CIDR blocks, instance sizes, and SAS Viya settings, 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 SAS Viya on AWS. The template is launched in the US East (Ohio) Region by default.
3. Create a [key pair](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html) in your preferred region.
4. If necessary, [request a service limit increase](https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-) for the 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 limit](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-resource-limits.html) with this reference deployment.
5. If desired, create a mirror repository.

### Step 2. Upload the SAS Software Order File to an Amazon S3 Location

For the Quick Start deployment, your SAS Software Order .zip file must be in an Amazon S3 location accessible from your account. To upload the .zip file that you received in your Software Order Confirmation email, [How Do I Upload Files and Folders to an S3 Bucket?](http://docs.aws.amazon.com/AmazonS3/latest/user-guide/upload-objects.html) in the AWS documentation.

**Note** Please ensure that the S3 bucket is not publicly accessible.

### Step 3. Launch the Quick Start

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

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see [deployment options](#_Deployment_Options_1) earlier in this guide.

|  |  |
| --- | --- |
| [Option 1](#_Scenario_1:_Deploy_1)  [**Launch**](https://fwd.aws/9y6nW)  Deploy SAS Viya into a  new VPC on AWS | [Option 2](#_Scenario_2:_Extending_1)  [**Launch**](https://fwd.aws/eRwdk)  Deploy SAS Viya into an existing VPC on AWS |

**Important** If you’re deploying SAS Viya into an existing VPC, make sure that your VPC has one public subnet and one private subnet in the same Availability Zones for the SAS Viya VM instances. These subnets require [NAT gateways or NAT instances](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat.html) in their route tables to allow the instances to download packages and software without exposing them to the internet. You also need the domain name option configured in the DHCP options as explained in the [Amazon VPC documentation](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html). You’ll be prompted for your VPC settings when you launch the Quick Start.

Each deployment takes about one hour to complete.

1. 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 SAS Viya will be built.
2. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
3. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. We recommend that you provide your email address for the **Operator Email** parameter.

**Note**  You will only receive emails about the SAS Viya deployment. You might not receive emails for all resource-creation failures during the AWS CloudFormation process.

For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

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

* [Parameters for deploying SAS Viya into a new VPC](#opt1)
* [Parameters for deploying SAS Viya into an existing VPC](#opt2)
* **Option 1: Parameters for deploying SAS Viya into a new VPC**

[View template](https://fwd.aws/wdjBr)

*SAS Viya License and Install Package:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| SAS Viya Software Order File (DeploymentDataLocation) | *Requires input* | The S3 location of the Software Order Confirmation e-mail attachment. Example: mysasbucket/viya\_deployment\_data/SAS\_Viya\_deployment\_data.zip |

*Administration:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| Key Name (KeyPairName) | *Requires input* | The name of an existing EC2 key pair. This will allow you to access the Ansible controller after it launches. |
| VPC Availability Zone (AvailabilityZone) | *Requires input* | The Availability Zone for the public and private subnet. |
| Permitted IP Range for Application Access (WebIngressLocation) | *Requires input* | Allow inbound HTTP traffic to the SAS Viya environment from this CIDR block (IP address range). Must be a valid IP CIDR range of the form x.x.x.x/x. |
| Permitted IP Range for Deployment Administrator (AdminIngressLocation) | *Requires input* | Allow inbound SSH traffic to the Ansible controller from this CIDR block (IP address range). Must be a valid IP CIDR range of the form x.x.x.x/x. |
| SAS Administrator Password (SASAdminPass) | *Requires input* | The password of the SAS Admin users (sasboot, optionally sasadmin). Must have at least 6 and no more than 255 characters. |
| Password for Default User (SASUserPass) | *Requires input* | The password of the default SAS user (sasuser). If left empty, no default users are being created.  **WARNING:** If not set, deployment will require additional setup steps before being usable. |
| EC2 Instance Size for the CAS compute VM (CASInstanceSize) | i3.4xlarge | The type and size of EC2 instance for the Viya compute nodes. Choose i3 for performance or r5 for auto-recovery. |
| Viya Compute Node Count (CASInstanceCount) | 1 | The number of Viya compute nodes to create. Note: Selecting 1 will install an SMP CAS deployment, but selecting 2 or more will create an MPP CAS deployment (controller + n workers deployment; max number of workers is 10). |
| EC2 Instance Size for the Viya Services VM (ServicesInstanceSize) | r5.4xlarge | Determines the type and size of the EC2 instance used for the Viya Services VM. |
| Mirror of SAS Viya Deployment Data (DeploymentMirror) | — | (Optional) The location of the SAS Viya Deployment Repository Mirror. |
| Operator Email (OperatorEmail) | — | (Optional) The email address to send a notification about deployment success or failure. |

*Server DNS Configuration (only required for custom DNS name and SSL):*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| Domain Name (DomainName) | — | The SAS Viya Server portal will be reachable at this DNS name (blank = generated ELB name will be used as application DNS name). |
| Route 53 Hosted Zone (AWSHostedZoneID) | — | The existing DNS Zone ID for the DomainName (blank = generated ELB name will be used as application DNS name). |
| SSL Certificate (SSLCertificateARN) | — | The AWS Certificate Manager Amazon Resource Name (ARN) for the SSL certificate to use to enable HTTPS. The certificate needs to match the DomainName. Syntax: arn:aws:acm:region:account-id:certificate/certificate-id  Example: arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012 |

*AWS Quick Start Source Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| Quick Start S3 Bucket Name (QSS3BucketName) | aws-quickstart | The S3 bucket name for the Quick Start assets. Only change this value if you customize or extend the Quick Start for your own use. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen. |
| Quick Start S3 Key Prefix (QSS3KeyPrefix) | quickstart-sas-viya/ | The S3 key prefix for the Quick Start assets. Only change this value if you customize or extend the Quick Start for your own use. The Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/) and must end in a forward slash. |

**Option 2: Parameters for deploying SAS Viya into an existing VPC**

[View template](https://fwd.aws/a5pzn)

*SAS Viya License and Install Package:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| SAS Viya Software Order File (DeploymentDataLocation) | *Requires input* | The S3 location of the Software Order Confirmation e-mail attachment. Example: mysasbucket/viya\_deployment\_data/SAS\_Viya\_deployment\_data.zip |

*Administration:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| Key Name (KeyPairName) | *Requires input* | The name of an existing EC2 key pair. This will allow you to access the Ansible controller after it launches. |
| Permitted IP Range for Application Access (WebIngressLocation) | *Requires input* | Allow inbound HTTP traffic to the SAS Viya environment from this CIDR block (IP address range). Must be a valid IP CIDR range of the form x.x.x.x/x. |
| Permitted IP Range for Deployment Administrator (AdminIngressLocation) | *Requires input* | Allow inbound SSH traffic to the Ansible controller from this CIDR block (IP address range). Must be a valid IP CIDR range of the form x.x.x.x/x. |
| SAS Administrator Password (SASAdminPass) | *Requires input* | The password of the SAS Admin users (sasboot, optionally sasadmin). Must have at least 6 and no more than 255 characters. |
| Password for Default User (SASUserPass) | *Requires input* | The password of the default SAS user (sasuser). If left empty, no default users are being created.  **WARNING:** If not set, deployment will require additional setup steps before being usable. |
| EC2 Instance Size for the CAS compute VM (CASInstanceSize) | i3.4xlarge | The type of EC2 instance for the Viya compute nodes. Choose i3 for performance or r5 for auto-recovery. |
| Viya Compute Node Count (CASInstanceCount) | 1 | The number of Viya compute nodes to create. Note: Selecting 1 will install an SMP CAS deployment, but selecting 2 or more will create an MPP CAS deployment (controller + n workers deployment; max number of workers is 10). |
| EC2 Instance Size for the Viya Services VM (ServicesInstanceSize) | r5.4xlarge | Determines the size of the EC2 instance used for the Viya Services VM. |
| Mirror of SAS Viya Deployment Data (DeploymentMirror) | — | (Optional) The location of the SAS Viya Deployment Repository Mirror. |
| Operator Email (OperatorEmail) | — | (Optional) The email address to send a notification about deployment success or failure. |

*Network Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| VPC ID (VPCID) | *Requires input* | The ID of an existing VPC with a public and a private subnet in the same Availability Zone. |
| Public Subnet ID (PublicSubnetID) | *Requires input* | The ID of the public subnet for the Elastic Load Balancer and Ansible controller (e.g. subnet-1234567890abcdef0). Must be in the same Availability Zone as PrivateSubnetID. |
| Private Subnet ID (PrivateSubnetID) | *Requires input* | The ID of the private subnet for the SAS Viya Application VMs (e.g. subnet-1234567890abcdef0). Must be in the same Availability Zone as PublicSubnetID. |

*Server DNS Configuration (only required for custom DNS name and SSL):*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| Domain Name (DomainName) | — | The SAS Viya Server portal will be reachable at this DNS name (blank = generated ELB name will be used as application DNS name). |
| Route 53 Hosted Zone (AWSHostedZoneID) | — | The existing DNS Zone ID for the DomainName (blank = generated ELB name will be used as application DNS name). |
| SSL Certificate (SSLCertificateARN) | — | The AWS Certificate Manager Amazon Resource Name (ARN) for the SSL certificate to use to enable HTTPS. The certificate needs to match the DomainName. Syntax: arn:aws:acm:region:account-id:certificate/certificate-id Example: arn:aws:acm:us-east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012 |

*AWS Quick Start Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label  (name) | Default | Description |
| Quick Start S3 Bucket Name (QSS3BucketName) | aws-quickstart | The S3 bucket name for the Quick Start assets. Only change this value if you customize or extend the Quick Start for your own use. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen. |
| Quick Start S3 Key Prefix (QSS3KeyPrefix) | quickstart-sas-viya/ | The S3 key prefix for the Quick Start assets. Only change this value if you customize or extend the Quick Start for your own use. The Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/) and must end in a forward slash. |

1. On the **Options** page, you can [specify tags](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-resource-tags.html) (key-value pairs) for resources in your stack and [set advanced options](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-add-tags.html). When you’re done, choose **Next**.
2. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
3. Choose **Create** to deploy the stack.
4. Monitor the status of the stack. When the status is **CREATE\_COMPLETE**, the SAS Viya cluster is ready.
5. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created, as shown in Figure 3.



Figure 3: Outputs tab

**Note** You might receive a security warning specific to your browser. Take the appropriate actions to accept the security certificate and proceed.

We highly recommend that you deploy your own SSL certificates. For detailed information, see [Technical Requirements](#_Technical_Requirements).

### Step 4. Test the Deployment

To test the deployment, log on to the SAS Viya launch page (SAS Drive) and then log on to SAS Studio, as shown in Figures 4 and 5.



Figure 4: Accessing your applications



Figure 5: Accessing SAS Studio

### Step 5. Perform Further Configuration

If you are connecting the environment to your own identity provider, see [Addendum D: Configuring the Identities Service](#_Addendum_D:_Configuring).

If you specified a value for the **Password for default user (SASUserPass)** parameter, the environment is set up with a default identity provider instance (OpenLDAP), and the following users were created:

|  |  |  |
| --- | --- | --- |
| Description | User ID | Password |
| Default SAS user | sasuser | Value of the **SASUserPass** parameter |
| Default admin user of the SAS Administrators group | sasadmin | Value of the **SASAdminPass** parameter |
| Default OpenLDAP administrator | admin | Value of the **SASAdminPass** parameter |

For guidelines on how to add and remove users and manage passwords in this OpenLDAP instance, see [Addendum E: Managing Users for the Provided OpenLDAP Server](#_Addendum_E:_Managing).

### Step 6. (Optional) Enable Access to Existing Data Sources

If you have existing database clusters that you want to access from your SAS Viya deployment, add the following inbound rule to the security group for each cluster, depending on where the cluster resides:

* If the cluster resides in the same VPC as the SAS Viya deployment, add an inbound rule for the CIDR of the CAS controller subnet.
* If the cluster resides in a different VPC from the SAS Viya deployment, add an inbound rule that allows access from the public IP address of the NAT Gateway used by the CAS controller subnet.

To verify the connection to your database, see the appropriate section on SAS/Access Interface in the [Validating your Deployment](https://go.documentation.sas.com/?docsetId=dplyml0phy0lax&docsetTarget=n18cthgsfyxndyn1imqkbfjisxsv.htm&docsetVersion=3.4&locale=en) section of the SAS Viya 3.4 for Linux: Deployment Guide.

### Step 7. (Optional) Deploy Data Agent, and Validate Communication

To deploy SAS Data Agent:

1. Perform the pre-installation and installation steps in the [SAS Data Agent for Linux Deployment Guide](http://go.documentation.sas.com/?docsetId=dplydagent0phy0lax&docsetTarget=p06vsqpjpj2motn1qhi5t40u8xf4.htm&docsetVersion=2.3&locale=en). For post-installation, you can either:

* (Recommended) Use the post-install playbooks as specified in this section.
* Perform the manual steps in the SAS Data Agent Deployment Guide.

1. **In the SAS Viya plus SAS Data Preparation environment**, open the firewall to allow access on port 443 as follows:
2. Obtain the public IP of the SAS Data agent firewall. The SAS Data Agent firewall address is either the public IP of the machine where the HTTPS service is running or the public IP of the NAT that routes outgoing traffic in the SAS Data Agent’s network.
3. Modify the security group of the Elastic Load Balancer. To locate the security group for the Elastic Load Balancer, in AWS CloudFormation, choose the **Resources** tab and locate the “ELBSecurityGroup”. You will then have the Physical ID of the security group.
4. For the ELBSecurityGroup, add an inbound rule for port 443 for the public IP.
5. To verify that the connection works, on the machine assigned to the [httpproxy] host group in the Ansible inventory file in your SAS Data Agent environment, run the following:

sudo yum install -y nc  
nc -v -z <DNS of SAS Viya endpoint> 443

**Note** The DNS of the SAS Viya endpoint should be the same value as the value that will be assigned to data\_prep\_host in step 6c.

1. Open the firewall of the SAS Data Agent environment to allow access on port 443 from the public IP of the NAT Gateway in the VPC of the SAS Viya deployment.

To verify that the connection works, on one of the machines in the [DataServices] host  
group in the Ansible inventory file in your SAS Data Preparation environment, run the following:

sudo yum install -y nc  
nc -v -z <IP or DNS of the Data Agent host> 443

**Note** The IP or DNS of the Data Agent host should be the same value that will be assigned to the data\_agent\_host in step 5c.

1. **On the Ansible controller machine in the SAS Data Preparation environment,** to register the Data Agent with the SAS Viya and SAS Data Preparation environment:
2. Log in to the Ansible controller VM as the deployment user ec2-user.
3. Change to the **/**sas/install/ansible/sas\_viya\_playbook directory.
4. Run the following commands:

cp /sas/install/ansible/playbooks/dataprep2dataagent.yml .

ansible-playbook dataprep2dataagent.yml \  
     -e "adminuser=sasadmin adminpw=<SASAdminPass>" \  
     -e "data\_agent\_host=<fqdn (dns) of data agent machine>" \  
     -e "secret=<handshake string>"

**Note** SASAdminPass is thevalue you used for the **SASAdminPass** parameter in the SAS on AWS Quick Start CloudFormation template.

1. **In the SAS Data Agent environment:** To register the SAS Viya plus SAS Data Preparation environment with the SAS Data Agent.
2. Copy the file **/**sas/install/ansible/playbooks/dataagent2dataprep.yml from the Ansible controller in your SAS Viya deployment into the playbook directory (sas\_viya\_playbook) on your Data Agent deployment.
3. Change to the playbook (sas\_viya\_playbook) directory for the SAS Data Agent.
4. Run the following command:

ansible-playbook dataagent2dataprep.yml \  
 -e "data\_prep\_host=<dns of SAS Viya endpoint>" \  
 -e "secret=<handshake string>"

**Note** The <dns of the SAS Viya endpoint> is the value of the **SASDrive** output parameter after removing the "https://" prefix and the "/SASDrive" suffix.

1. Perform validation, including validating the round-trip communication. For details, see the Validation chapter of the [[SAS Data Agent for Linux Deployment Guide](http://go.documentation.sas.com/?docsetId=dplydagent0phy0lax&docsetTarget=p06vsqpjpj2motn1qhi5t40u8xf4.htm&docsetVersion=2.3&locale=en).](http://go.documentation.sas.com/?docsetId=dplydagent0phy0lax&docsetTarget=n1v7mc6ox8omgfn1qzjjjektc7te.htm&docsetVersion=2.3&locale=en)

## Best Practices Using SAS Viya on AWS

We recommend the following as best practices:

* We recommend that you stop the SAS Viya environment when it isn’t in use. SAS provides utility scripts to shut down and start up the SAS Viya services and VMs in the correct order, so that the environment will come back up. For details about the scripts, see [Utility Scripts for SAS Viya on AWS](#_Utility_Scripts_for).
* To make changes to the configuration beyond what this Quick Start supports, start the Ansible controller instance.

**Note**  The SAS Viya playbook is located in the /sas/install/ansible/sas\_viya\_playbook directory.

* Perform any software updates. For task instructions, see [SAS Viya 3.4 for Linux: Deployment Guide](http://go.documentation.sas.com/?docsetId=dplyml0phy0lax&docsetTarget=titlepage.htm&docsetVersion=3.4&locale=en).   
  Note: When you initiate the update and the documentation specifies to run the same command and options as the initial deployment, use the following command:

ansible-playbook site.yml

* Follow best practices for backup and restore. See [SAS Viya 3.4 Administration](http://go.documentation.sas.com/?docsetId=calchkcfg&docsetTarget=n00004saschecklist0000config.htm&docsetVersion=3.4&locale=en).
* Apply new licenses. For task instructions, see “Apply New Licenses Using Ansible” in [SAS Viya 3.4 Administration](http://go.documentation.sas.com/?docsetId=callicense&docsetTarget=titlepage.htm&docsetVersion=3.4&locale=en).
* If you have requirements for other networks or home offices to access the deployment or Ansible controller, open the environment's firewall to allow access from additional IP ranges. For details, refer to the utility scripts in [Utility Scripts for SAS Viya on AWS](#_Utility_Scripts_for).

## Utility Scripts for SAS Viya on AWS

SAS Viya on AWS provides some utility scripts in the /sas/install/scripts directory of the Ansible controller:

**Note**  Run these scripts as the ec2-user.

* + Scripts to start and stop the SAS Viya services in the correct order.

On the Ansible controller, to stop the individual SAS Viya services in the correct order, and then stop the VMs:

/sas/install/scripts/stop\_viya\_vms.sh

On the Ansible controller, to start the VMs and then start the SAS Viya services in the proper order:

/sas/install/scripts/start\_viya\_vms.sh

* Script to open the environment's firewall to allow access to additional CIDR ranges. You must specify a valid IP CIDR range of the form x.x.x.x/x.

You can grant application access for an additional IP address range beyond what was specified with the **WebIngressLocation** parameter during deployment. On the Ansible controller, use the –-webaccess parameter and specify a CIDR range:

|  |
| --- |
| /sas/install/scripts/addaccess.sh --webaccess <CIDR-range> |

For example, to grant application access to 55.55.55.55:

|  |
| --- |
| /sas/install/scripts/addaccess.sh --webaccess 55.55.55.55/32 |

You can grant administrative access to log into the Ansible controller for an additional IP range. On the Ansible controller, use the --adminaccess parameter and specify a CIDR range:

|  |
| --- |
| /sas/install/scripts/addaccess.sh --adminaccess <CIDR-range> |

For example, to grant administrative access to 55.55.55.55:

|  |
| --- |
| /sas/install/scripts/addaccess.sh --adminaccess 55.55.55.55/32 |

## Troubleshooting

### View Log Files

**Note**  The log file retention is set to 1 week for the log group.

Logs are available in Amazon CloudWatch.

#### Deployment Logs

The deployment logs are located in the /var/log/sas/install directory:

* prepare\_nodes.log - Ansible logs for VM preparation
* openldap.log - Ansible logs for the OpenLDAP installation and configuration (if chosen)
* prepare\_deployment.log - Ansible logs for SAS Viya deployment preparation steps
* virk.log - Ansible logs for the Viya-ark pre-deployment node preparation playbook
* viya\_deployment.log- Ansible log for SAS Viya main deployment
* post\_deployment.log - Ansible logs for additional steps after the main deployment

#### SAS Viya Microservice Logs

The logs for SAS Viya microservices are on the SAS Viya EC2 instances in the /var/log/sas/viya directory.

#### Additional Ansible Log

You might also have the ansible-controller-commands.log file, which lists any commands executed by the "ec2-user" on the Ansible controller. The log is on the Ansible controller at /var/log/sas/bastion/bastion.log.

### Restarting the SAS Services

With some older licenses, some services might not be fully started after a full deployment. If you receive a connection error when connecting to SASHome or SASDrive, then you must restart the services.

*Checking the Status of the SAS Services through Viya-Ark*

Viya-Ark can check the status of the services by issuing the following commands as the ec2-user on the Ansible controller:

cd /sas/install/ansible/sas\_viya\_playbook

ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-status.yml

*Restarting the SAS Services through Viya-Ark*

Viya-Ark can restart all of the services by issuing the following commands as the ec2-user on the Ansible controller:

cd /sas/install/ansible/sas\_viya\_playbook

ansible-playbook viya-ark/playbooks/viya-mmsu/viya-services-restart.yml -e enable\_stray\_cleanup=true

### Recover from a Lost CAS Node VM

**Note:** The script to recover the CAS Controller works only on i3 instance sizes. In MPP environments, the CAS Controller size is automatically set to m5.large. Therefore, in MPP environments the CAS Controller cannot be recovered.

1. Use ssh to access the Ansible controller instance:
2. Sign in to the AWS Management Console.
3. In the EC2 Instance list, select the check box next to the "<Stack> Ansible Controller" instance. Ensure that the check box next to the CAS controller instance is no longer selected.
4. Make a note of the IPv4 Public IP address for the Ansible controller.
5. As the “ec2-user”, ssh to that IP address as the user by using the private key specified in the "Key pair name" property for the Ansible controller.
6. From the ssh session, run the recover\_cascontroller.sh bash script as follows:

To recover the CAS Controller in an SMP environment, run this command:

/sas/install/scripts/recover\_cascontroller.sh

To recover the CAS Worker in an MPP environment, run this command and specify which worker to recover:

/sas/install/scripts/recover\_cascontroller.sh worker01

**Note:** The CAS Controller in an MPP environment cannot be recovered.

It may take 30 minutes (or longer) for the script to complete. When the script has completed, a new CAS controller EC2 instance should be up and running.

**Note:** The script to recover the CAS controller creates an out-of-process resource that is not managed by the CloudFormation stack. Therefore, when you delete the CloudFormation Stack, the new CAS controller will not be terminated.

To delete the stack, terminate the CAS controller VM. Otherwise, the stack deletion will not complete because the following resources are held by the CAS Controller: AnsibleControllerSecurityGroup, CASLibVolume, CASViyaVolume, ViyaPlacementGroup, and ViyaSecurityGroup.

## FAQ

**Q.** I encountered a CREATE\_FAILED error when I launched the Quick Start. What should I do?

**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. (You'll want to look at the log files in /var/log/cfn-\*.log.)

If the /var/log directory is missing all "cfn-\*.log" files on one of the VMs, it is an indication that initialization code on that VM has failed.

**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.

Check the event log for the cause of failure. Some reasons this might occur are:

* The region is out of the particular resource that was requested. For details, see [Error: InsufficientInstanceCapacity](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-capacity.html).
* Initialization code of a VM has failed.

Delete and re-create the stack.

For more information, see [Troubleshooting AWS CloudFormation](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html) 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 location we’ve provided 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](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-limits.html).

**Q.** I encountered the following error: CREATE\_FAILED Reason- Failed to create resource. DeploymentDataLocation invalid.zip is not accessible. What should I do?

**A.** Ensure that the s3 location and file for the DeploymentDataLocation are accessible.

**Q.** I encountered the following error: CREATE\_FAILED AWS::EC2::NatGateway NATGateway =0">Nat Gateway is not available in this availability zone. What should I do?

**A.** Use a different availability zone to re-create the stack.

**Q.** When deleting a stack, I encountered a DELETE\_FAILED error. What should I do?

**A.** For troubleshooting, see [Delete Stack Fails](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html#troubleshooting-errors-delete-stack-fails) in the AWS documentation.

**Q.** Is interacting with CAS via TCP port 5570 from a locally running SAS Foundation client + Lua client + Java client supported in this AWS Quick Start?

**A.** Connecting to CAS in a SAS Viya stack via TCP port 5570 is not supported in the AWS Quick Start environment.

**Q.** Is interacting with CAS via TCP port 5570 from a locally running SAS Scripting Wrapper for Analytics Transfer (SWAT) Python client supported in this AWS Quick Start?

**A.** Connecting to CAS using the SWAT Python client via TCP port 5570 is not supported in the AWS Quick Start environment.

**Q.** Is interacting with CAS from a locally running SAS Foundation client + Lua client + Java client through the REST interface supported in this AWS Quick Start?

**A.** Yes, but it is only supported through the REST interface on the /cas-shared-default-http route on port 80.

## Additional Resources

**AWS services**

* [Amazon EC2](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/)
* [AWS CloudFormation](https://aws.amazon.com/documentation/cloudformation/)
* [Amazon VPC](https://aws.amazon.com/documentation/vpc/)
* [AWS Cloud Security](https://aws.amazon.com/security/)

**SAS Viya documentation**

* [SAS Viya 3.4 for Linux: Deployment Guide](http://go.documentation.sas.com/?docsetId=dplyml0phy0lax&docsetTarget=titlepage.htm&docsetVersion=3.4&locale=en)
* [SAS Viya 3.4 Administration](http://go.documentation.sas.com/?docsetId=calchkcfg&docsetTarget=n00004saschecklist0000config.htm&docsetVersion=3.4&locale=en)

**Quick Start reference deployments**

* [AWS Quick Start home page](https://aws.amazon.com/quickstart/)

## GitHub Repository

You can visit our [GitHub repository](https://fwd.aws/rG7nM) to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

## Addendum A: Resource Requirements

The following tables lists the total number of resources in each deployment.

If you are deploying into a new VPC, one deployment creates the following number of each resource:

|  |  |
| --- | --- |
| Resource | Total number |
| VPC | 1 |
| Subnets | 2 |
| EC2-VPC Elastic IPs | 2 |
| Route tables | 2 |
| EC2 instances | 3 |
| Classic Load Balancer | 1 |
| Security groups | 4 |

If you are deploying into an existing VPC, one deployment creates the following number of each resource:

|  |  |
| --- | --- |
| Resource | Total number |
| Classic Load Balancer | 1 |
| EC2-VPC Elastic IP | 1 |
| EC2 instances | 3 |
| Classic Load Balancer | 1 |
| Security groups | 4 |

## 

## Addendum B: Administrative Permission Requirements

The administrative user needs permissions to create the required resources. For details, see [Prerequisites: Granting Permissions for Stack Set Operations](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-prereqs.html) in the AWS documentation.

If you are deploying into an existing VPC, you need the Create permission to create the following resources:

* CloudFormation::Stack
* CloudWatch::Alarm
* EC2::EIP
* EC2::Instance
* EC2::PlacementGroup
* EC2::SecurityGroup
* EC2::SecurityGroupIngress
* EC2::Volume
* EC2::VolumeAttachment
* ElasticLoadBalancing::LoadBalancer
* IAM::InstanceProfile
* IAM::Role
* Lambda::Function
* Logs::LogGroup
* Route53::RecordSet
* SNS::Topic
* SSM::Parameter

If you are deploying into a new VPC, you also need the Create permission to create the following resources:

* CloudFormation::Stack
* EC2::DHCPOptions
* EC2::EIP
* EC2::InternetGateway
* EC2::NatGateway
* EC2::Route
* EC2::RouteTable
* EC2::Subnet
* EC2::SubnetRouteTableAssociation
* EC2::VPC
* EC2::VPCDHCPOptionsAssociation
* EC2::VPCGatewayAttachment

## Addendum C: Set up a Mirror Repository

1. To set up a mirror repository, refer to the instructions in the ["Create a Mirror Repository" in the SAS Viya 3.4 for Linux: Deployment Guide](https://go.documentation.sas.com/?docsetId=dplyml0phy0lax&docsetTarget=p1ilrw734naazfn119i2rqik91r0.htm&docsetVersion=3.4&locale=en).
2. Set up an S3 bucket that is accessible by the account where you deployed the SAS Viya Quick Start.
3. Move the file structure of your mirror repository to Amazon S3.
4. Upload the mirror repository into your S3 bucket.

To upload the mirror using the AWS command line interface (CLI), run the following command:

aws s3 sync /path/to/your/local/mirror/sas\_repos s3://your-bucket/your/mirror/

During your AWS Quick Start installation, specify the value for the **DeploymentMirror** parameter as follows:

s3://your-bucket/your/mirror/

## Addendum D: Configuring the Identities Service

### Verify Port Settings

Ensure that port 389 on your Lightweight Directory Access Protocol (LDAP) machine is accessible by the SAS Viya machines. To enable a higher level of security, use port 636 for LDAPS.

### Create Service Account

Create a service account in your LDAP system. The service account must have permission to read the users and groups that will log into the system.

### Configure the Identities Service

In the SAS Environment Manager, on the **Configuration** tab, select the Identities service. There are three sections to configure: connection, user, and group.

#### Connection

* host - the DNS address or IP address of your LDAP machine
* password - the password of the service account that SAS Viya will use to connect to your LDAP machine.
* port - the port your LDAP server uses
* userDN - the DN of the LDAP service account

#### User

* accountID - the parameter used for the user name. This may be uid, samAccountName or name depending on your system
* baseDN - DN to search for users under

#### Group

* accountID - the parameter used for the name of the group
* baseDN - DN to search for groups under

Set the default values to work with a standard Microsoft Active Directory system.

**Note**  OpenLDAP systems and customized AD setups may require additional configuration that is beyond the scope of this guide.

For further details about configuring the identities service, see ["Configure Your Environment with SAS Environment Manager" in the SAS Viya 3.4 for Linux: Deployment Guide.](https://go.documentation.sas.com/?docsetId=dplyml0phy0lax&docsetTarget=p0dt267jhkqh3un178jzupyyetsa.htm&docsetVersion=3.4&locale=en#n12f8m501xzcf6n12vdvervbz6gw)

### Verify the Configuration

**To verify:**

1. Log in to SAS Viya with your LDAP accounts. You may need to restart SAS Viya for the LDAP changes to take effect.
2. Run the ldapsearch command from one of the SAS Viya machines.
3. ldapsearch -x -h <YOUR LDAP HOST> -b <YOUR DN> -D <YOUR LDAP SERVICE ACCOUNT> -W
4. Enter the password to your LDAP service account.

If verification is successful, the list of your users and groups is displayed.

### Configure PAM for SAS Studio

SAS Studio does not use the SAS Logon Manager, and thus has different requirements for integration with an LDAP system. SAS Studio manages authentication through a pluggable authentication module (PAM). You can use System Security Services Daemon (SSSD) to integrate the PAM configuration of the services VM with your LDAP system.

To access SAS Studio the following conditions must be met:

* The user must exist locally on the system.
* The user must have an accessible home directory.

For a step by step guide for configuring SSSD against your LDAP setup, see the [Red Hat documentation](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system-level_authentication_guide/configuring_domains). In many cases SSSD is configured to automatically create home directories when a user logs into the system either via SSH or locally. SAS Studio does not do this; therefore, you must manually create home directories for each remote user.

After SSSD has been configured, you may need to restart the services VM.

## Addendum E: Managing Users for the Provided OpenLDAP Server

**To log in and list all users and groups:**

1. From the Ansible controller VM, log into the Services VM with ssh services.viya.sas
2. To list all users and groups, run this command

ldapsearch -x -h localhost -b "dc=sasviya,dc=com"

**To add a user:**

1. Create a user file that contains all the user info.

**Note**  You must increment the UID from the last one displayed by the ldapsearch command.

# newuser, sasviya.com

dn: uid=newuser,ou=users,dc=sasviya,dc=com

cn: newuser

givenName: New

sn: User

objectClass: top

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: posixAccount

loginShell: /bin/bash

uidNumber: 100011

gidNumber: 100001

homeDirectory: /home/newuser

mail: newuser@services.viya.sas

displayName: New User

1. Run the following command.

ldapadd -x -h localhost -D "cn=admin,dc=sasviya,dc=com" -W -f /path/to/user/file

**Note** You will be prompted for the admin password (the same one you set when you created the stack).

1. To allow the new user to access Viya products, add the user as a member of the sasusers group by creating an ldif file with the following data:

dn: cn=sasusers,ou=groups,dc=sasviya,dc=com

changetype: modify

add: memberUid

memberUid: newuser

-

add: member

member: uid=newuser,ou=users,dc=sasviya,dc=com

ldapadd -x -h localhost -D "cn=admin,dc=sasviya,dc=com" -W -f /path/to/user/file

1. Add the home directories for your new user on the services machine (services.viya.sas) and the CAS controller (controller.viya.sas). From the Ansible controller VM:

ssh services.viya.sas

sudo mkdir -p /home/newuser

sudo chown newuser:sasusers /home/newuser

exit

ssh controller.viya.sas

sudo mkdir -p /home/newuser/casuser

sudo chown newuser:sasusers /home/newuser

sudo chown newuser:sasusers /home/newuser/casuser

exit

**To change a password or set the password for a new user:**

ldappasswd -h localhost -s USERPASSWORD -W -D cn=admin,dc=sasviya,dc=com -x "uid=newuser,ou=users,dc=sasviya,dc=com"

**Note** To prevent the command from being saved to the bash history, preface this command with a space. The string following the -x should match the dn: attribute of the user.

**To delete a user:**

ldapdelete -h localhost -W -D "cn=admin,dc=sasviya,dc=com" "uid=newuser,ou=users,dc=sasviya,dc=com"

## Document Revisions

|  |  |  |
| --- | --- | --- |
| Date | Change | In sections |
| October 2019 | Added documentation for massively parallel processing (MPP), including new graphic. | [Overview](#_Overview);  [Architecture](#_Architecture);  additional MPP graphic  original graphic now an SVG file |
| July 2019 | Add note with link to SAS repository.  Correct code en dashes and curvy quotation  marks in ldap code samples. | Before Overview.  Addendum E |
| May 2019 | Add references to r5.  Changed graphic to show only size defaults.  Licensing updates to support unlimited licensing  Add troubleshooting topic for problem with old  licenses. | Throughout doc; graphic also  [Costs and Licenses](#_Costs_and_Licenses) |
| April 2019 | Change of sizes and topology  Changes in log files | Throughout document  [View Log Files](#_View_Log_Files) |
| November 2018 | Added support for utility scripts for stop/start and additional user access; Added support for access to PostgreSQL; Added support for SAS Data Agent communication. | [Utility Scripts for SAS Viya on AWS](#_Utility_Scripts_for) [(Optional) Enable Access to Existing Data Sources](#_(Optional)_Enable_Access) [(Optional) Deploy Data Agent, and Validate Communication](#_(Optional)_Deploy_Data_1) |
| September 2018 | Update from SAS version 8.2 to 8.3;  Updates to support licenses for latest release Added support for i3 instances for the CAS controller;  New addendums for resource requirements, administrative permission requirements, and setting up a mirror repository | Throughout doc;  [Costs and Licenses](#_Costs_and_Licenses); [Launch the Quick Start](#_Step_5._Launch) [Addendum A: Resource Requirements](#_Addendum_A:_Resource);  [Addendum B: Administrative Permission Requirements](#_Addendum_B:_Administrative);  [Addendum C: Set Up a Mirror Repository](#_Addendum_C:_Set) |
| August 2018 | Screen updates (Outputs tab) and log changes | [Launch the Quick Start](#_Step_5._Launch_1); [Troubleshooting](#_Troubleshooting) |
| May 2018 | Initial publication | — |

© 2019, Amazon Web Services, Inc. or its affiliates, and SAS Institute. 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.