SAS Viya on the AWS Cloud

Quick Start Reference Deployment

May 2018
Last update: September 2018 (revisions)

SAS Institute
AWS Quick Start Reference Team

Contents

Overview........................................................................................................................................2
  SAS Viya on AWS ..........................................................................................................................3
  Costs and Licenses..........................................................................................................................3
Architecture......................................................................................................................................5
Prerequisites ......................................................................................................................................7
  Specialized Knowledge..................................................................................................................7
  Technical Requirements..................................................................................................................8
Authentication Provider Options......................................................................................................9
Deployment Options........................................................................................................................9
Deployment Steps ..........................................................................................................................10
  Step 1. Prepare Your AWS Account..............................................................................................10
  Step 2. Upload the SAS Software Order File to an Amazon S3 Location.................................10
  Step 3. Register the Domain, and Note the Hosted Zone.............................................................10
  Step 4. Create a Certificate, and Note the Certificate ARN ID....................................................10
  Step 5. Launch the Quick Start....................................................................................................11
  Step 6. (Optional) Enable Access to Existing Amazon Redshift Clusters....................................16
  Step 7. Test the Deployment .......................................................................................................17
  Step 8. Further Configuration.......................................................................................................18
This Quick Start deployment guide was created by Amazon Web Services (AWS) in collaboration with SAS Institute.

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

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying 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

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 five EC2 instances, including

• One compute virtual machine (VM)—the Cloud Analytic Services (CAS) controller
• One VM for administration—the Ansible controller
• Three VMs for the SAS Viya services—Viya visual interfaces, Viya stateful services, and Viya programming interfaces
Note With this Quick Start, the CAS controller of SAS Viya is limited to 4, 8, or 16 cores. If you do not have a license that is 4, 8, or 16 cores for the CAS controller, you cannot deploy the AWS Quick Start for SAS Viya. Please check your license to ensure that your CAS controller is licensed for 4, 8, or 16 cores.

For information about the machine size and other machine specifications of a 4-, 8-, or 16-core symmetric multiprocessing (SMP) CAS controller, see the following table:

<table>
<thead>
<tr>
<th>CPU</th>
<th>Machine size</th>
<th>Maximum users</th>
<th>Memory (RAM)</th>
<th>Maximum dataset size</th>
<th>Storage (Amazon EBS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-core SMP</td>
<td>2xlarge</td>
<td>1</td>
<td>61 GB</td>
<td>20-40 GB</td>
<td>500 GB</td>
</tr>
<tr>
<td>8-core SMP</td>
<td>4xlarge</td>
<td>2</td>
<td>122 GB</td>
<td>40-60 GB</td>
<td>500 GB</td>
</tr>
<tr>
<td>16-core SMP</td>
<td>8xlarge</td>
<td>4</td>
<td>244 GB</td>
<td>90-170 GB</td>
<td>1000 GB</td>
</tr>
</tbody>
</table>

Note For the CAS controller VM, the machine type can be customized by the CASInstanceType configuration parameter. The valid types are r4 and i3.

For the other VMs, the machine type and size, and EBS storage are shown in the following table:

<table>
<thead>
<tr>
<th>EC2 instance purpose</th>
<th>Machine type and size</th>
<th>Storage (Amazon EBS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viya visual interfaces</td>
<td>r4.4xlarge</td>
<td>20 GB+50 GB</td>
</tr>
<tr>
<td>Viya stateful services</td>
<td>r4.2xlarge</td>
<td>20 GB+50 GB</td>
</tr>
<tr>
<td>Viya programming interfaces</td>
<td>r4.2xlarge</td>
<td>20 GB+50 GB</td>
</tr>
</tbody>
</table>

For information about the number of resources in each type of deployment, see Addendum A: Resource Requirements.
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.

By default, a self-signed certificate is deployed on the ELB load balancer. We recommend that you specify your own DNS name and certificate.

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the following SAS Viya environment in the AWS Cloud, shown in Figure 1.

---

**Figure 1: Quick Start architecture for SAS Viya on AWS**
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, four EC2 instances for deploying 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 and application logs.
- Optionally, an SNS email notification when SAS Viya deployment starts and finishes.
- A generated self-signed certificate on the ELB load balancer, unless you bring your own Amazon Route 53 DNS name and SSL certificate registered with AWS Certificate Manager (ACM).

*The template that deploys the Quick Start into an existing VPC skips the components marked by asterisks above.
Figure 2 shows more details about the SAS Viya components:

**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](#).)

- Amazon VPC
- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon Identity and Access Management
- Amazon Route 53
• Amazon Certificate Manager
• Operational Checklists for AWS

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.

• A SAS Software Order Confirmation e-mail that contains supported Quick Start products:
  • 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

• You can create a mirror repository for your software order. For information, see Addendum C: Set Up a Mirror Repository.

To deploy with your own DNS name and SSL certificate:
1. Register a domain managed by Amazon Route 53 or have your own domain.
2. 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.
3. 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. By default, the ELB load balancer will be configured with a self-signed 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.

- Use your own identity management system. 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.

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 Viya into 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 in your preferred region.

4. If necessary, request a service limit increase for the Amazon EC2 r4.2xlarge 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.

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? in the AWS documentation.

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

Step 3. Register the Domain, and Note the Hosted Zone

For instructions on registering the domain, see the Route 53 documentation.

After you register the domain and receive the confirmation email, navigate to Hosted Zone in the Route 53 console UI and make note of your hosted zone.

Step 4. Create a Certificate, and Note the Certificate ARN ID

For instructions on creating a certificate, see Request a Public Certificate 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.
Step 5. 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 earlier in this guide.

   ![Option 1](Launch.png)
   ![Option 2](Launch.png)

   **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 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. You’ll be prompted for your VPC settings when you launch the Quick Start.

   Each deployment takes about one hour 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 SAS Viya will be built.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. 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.
Amazon Web Services – SAS Viya on the AWS Cloud

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
- Parameters for deploying SAS Viya into an existing VPC

• Option 1: Parameters for deploying SAS Viya into a new VPC

SAS Viya License and Install Package:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Viya Software Order File</td>
<td>Requires input</td>
<td>S3 location of the Software Order Confirmation e-mail attachment. Example: mysasbucket/viya_deployment_data/SAS_Viya_deployment_data.zip</td>
</tr>
<tr>
<td>(DeploymentDataLocation)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Administration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key name (KeyPairName)</td>
<td>Requires input</td>
<td>Name of an existing EC2 key pair. This will allow you to access the Ansible Controller after it launches.</td>
</tr>
<tr>
<td>VPC Availability Zone (AvailabilityZone)</td>
<td>Requires input</td>
<td>The Availability Zone for the public and private subnet.</td>
</tr>
<tr>
<td>Permitted IP Range for Application Access (WebIngressLocation)</td>
<td>Requires input</td>
<td>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.</td>
</tr>
<tr>
<td>Permitted IP Range for Deployment Admin (AdminIngressLocation)</td>
<td>Requires input</td>
<td>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.</td>
</tr>
<tr>
<td>SAS Administrator Password (SASAdminPass)</td>
<td>Requires input</td>
<td>Password of the SAS Admin Users (sasboot, optionally sasadmin). Must have at least 6 and no more than 255 characters.</td>
</tr>
</tbody>
</table>
Parameter label (name) | Default | Description
--- | --- | ---
Password for Default User (SASUserPass) | Requires input | 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 Type for the CAS compute VM (CASInstanceType) | i3 | Type of EC2 instance for the Viya Compute Nodes (i3 for performance, r4 for auto-recovery)

Mirror of SAS Viya Deployment Data (DeploymentMirror) | — | (Optional) Location of SAS Viya Deployment Repository Mirror

Operator Email (OperatorEmail) | — | (Optional) 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) | — | Existing DNS Zone ID for the DomainName (blank = generated ELB name will be used as application DNS name).


AWS Quick Start Source Location:

Parameter label (name) | Default | Description
--- | --- | ---
Quick Start S3 Bucket Name (QSS3BucketName) | aws-quickstart | 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/ | S3 key prefix for the Quick Start assets. Only change this value if you customize or extend the Quick Start for your own use. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/) and must terminate in a forward slash.
- **Option 2: Parameters for deploying SAS Viya into an existing VPC**
  
  **View template**

**SAS Viya License and Install Package:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Viya Software Order File (DeploymentDataLocation)</td>
<td>Requires input</td>
<td>S3 location of the Software Order Confirmation e-mail attachment. Example: myasbucket/viya_deployment_data/SAS_Viya_deployment_data.zip</td>
</tr>
</tbody>
</table>

**Administration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key name (KeyPairName)</td>
<td>Requires input</td>
<td>Name of an existing EC2 key pair. This will allow you to access the Ansible Controller after it launches.</td>
</tr>
<tr>
<td>Permitted IP Range for Application Access (WebIngressLocation)</td>
<td>Requires input</td>
<td>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.</td>
</tr>
<tr>
<td>Permitted IP Range for Deployment Admin (AdminIngressLocation)</td>
<td>Requires input</td>
<td>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.</td>
</tr>
<tr>
<td>SAS Administrator Password (SASAdminPass)</td>
<td>Requires input</td>
<td>Password of the SAS Admin Users (sasboot, optionally sasadmin). Must have at least 6 and no more than 255 characters.</td>
</tr>
<tr>
<td>Password for Default User (SASUserPass)</td>
<td>Requires input</td>
<td>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).</td>
</tr>
<tr>
<td>EC2 Instance Type for the CAS compute VM (CASInstanceType)</td>
<td>i3</td>
<td>Type of EC2 instance for the Viya Compute Nodes (i3 for performance, r4 for auto-recovery)</td>
</tr>
<tr>
<td>Mirror of SAS Viya Deployment Data (DeploymentMirror)</td>
<td>—</td>
<td>(Optional) Location of SAS Viya Deployment Repository Mirror</td>
</tr>
<tr>
<td>Operator Email (OperatorEmail)</td>
<td>—</td>
<td>(Optional) Email address to send a notification about deployment success or failure.</td>
</tr>
</tbody>
</table>
### Network Configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC ID (VPCID)</td>
<td>Requires input</td>
<td>ID of an existing VPC with a public and a private subnet in the same Availability Zone.</td>
</tr>
<tr>
<td>Public Subnet ID (PublicSubnetID)</td>
<td>Requires input</td>
<td>ID of public subnet for the Elastic Load Balancer and Ansible Controller (e.g. subnet-1234567890abcdef0) (must be in the same AZ as PrivateSubnetID).</td>
</tr>
<tr>
<td>Private Subnet ID (PrivateSubnetID)</td>
<td>Requires input</td>
<td>ID of private subnet for the SAS Viya Application VMs (e.g. subnet-1234567890abcdef0) (must be in the same AZ as PublicSubnetID).</td>
</tr>
</tbody>
</table>

### Server DNS configuration (only required for custom DNS name and SSL):

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name (DomainName)</td>
<td>—</td>
<td>The SAS Viya Server portal will be reachable at this DNS name (blank = generated ELB name will be used as application DNS name).</td>
</tr>
<tr>
<td>Route 53 Hosted Zone (AWSHostedZoneID)</td>
<td>—</td>
<td>Existing DNS Zone ID for the DomainName (blank = generated ELB name will be used as application DNS name).</td>
</tr>
</tbody>
</table>

### AWS Quick Start Source Location:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 Bucket Name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>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 (-).</td>
</tr>
<tr>
<td>Quick Start S3 Key Prefix (QSS3KeyPrefix)</td>
<td>quickstart-sas-viya/</td>
<td>S3 key prefix for the Quick Start assets. Only change this value if you customize or extend the Quick Start for your own use. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/) and must terminate in a forward slash.</td>
</tr>
</tbody>
</table>
5. On the **Options** page, you can **specify tags** (key-value pairs) for resources in your stack and **set advanced options**. When you’re done, choose **Next**.

6. 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.

7. Choose **Create** to deploy the stack.

8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the SAS Viya cluster is ready.

9. 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](image)

**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 **Step 4. Create a Certificate and Note the Certificate ARN ID**.

**Step 6. (Optional) Enable Access to Existing Amazon Redshift Clusters**

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

- If the Amazon Redshift 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 Amazon Redshift 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 Amazon Redshift, see “Verify SAS/ACCESS Interface to Amazon Redshift” in the **SAS Viya 3.4 for Linux: Deployment Guide**.
Step 7. Test the Deployment
To test the deployment, log on to the SAS Viya launch page (SAS Home) and then log on to SAS Studio, as shown in Figures 4 and 5:

Figure 4: Accessing your applications

Figure 5: Accessing files and folders
Step 8. Further Configuration

If you are connecting the environment to your own identity provider, see Addendum D: Configuring the Identities Service.

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

<table>
<thead>
<tr>
<th>Description</th>
<th>User ID</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default SAS user</td>
<td>sasuser</td>
<td>Value of the SASUserPass parameter</td>
</tr>
<tr>
<td>Default admin user of the SAS</td>
<td>sasadmin</td>
<td>Value of the SASAdminPass parameter</td>
</tr>
<tr>
<td>Administrators group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default openLDAP administrator</td>
<td>admin</td>
<td>Value of the SASAdminPass parameter</td>
</tr>
</tbody>
</table>

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.

Best Practices Using SAS Viya on AWS

We recommend the following as best practices:

- After you complete the Quick Start deployment, stop the Ansible controller instance. It’s only used for administrative tasks. For details, see [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html).
- To make changes to the configuration beyond what is supported by this Quick Start, start the Ansible controller instance.

  **Note**  The playbook is located in the /home/ec2-user/sas_viya_playbook directory.

- Perform any software updates. For task instructions, see SAS Viya 3.4 for Linux: Deployment Guide. 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.
- Apply new licenses. For task instructions, see “Apply New Licenses Using Ansible” in SAS Viya 3.4 Administration.
Troubleshooting

View Log Files
The following logs are available in Amazon CloudWatch and on the EC2 instances.

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

- Deployment logs in CloudWatch and on the Ansible controller in the /home/ec2-user/deployment-logs directory:
  - deployment-commands.log – lists the main deployment steps
  - deployment-pre.log – Ansible logs for VM preparation
  - deployment-post.log – Ansible logs for post-deployment steps
  - deployment-openldap.log – Ansible log for the openLDAP installation and configuration
  - deployment-main.log – Ansible log for main Viya deployment
- The logs for SAS Viya microservices are on the SAS Viya EC2 instances in the /var/log/sas/viya directory and mirrored in Amazon CloudWatch with the following naming convention:
  viya-<microservice name>-<viya host alias>.log
  where "viya host alias" can be "visual", "stateful", "prog", or "controller".

Recover from a Lost CAS controller VM
1. Use ssh to access the Ansible controller instance:
   a. Sign in to the AWS Management Console.
   b. 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.
   c. Make a note of the IPv4 Public IP address for the Ansible controller.
   d. As the “ec2-user”, ssh to that IP address as the user by using the public key specified in the "Key pair name" property for the Ansible controller.
2. From the ssh session, run the recover_cascontroller.sh bash script:

   cd deployment-scripts
   ./recover_cascontroller.sh
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.

**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-*`.)

If the `/var/log` directory is missing all "cfn-*" 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](#).
- Initialization code of a VM has failed.

Delete and re-create the stack.

For more 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 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](#).

**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 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
- AWS CloudFormation
- Amazon VPC
- AWS Cloud Security

SAS Viya documentation
- SAS Viya 3.4 for Linux: Deployment Guide
- SAS Viya 3.4 Administration
- SAS Viya 3.4 SAS Data Connector to Amazon RedShift section of SAS 9.4 and SAS Viya 3.4 Programming Documentation
Quick Start reference deployments

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

GitHub Repository

You can visit our GitHub repository 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:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Total number</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td>1</td>
</tr>
<tr>
<td>Subnets</td>
<td>2</td>
</tr>
<tr>
<td>EC2-VPC Elastic IPs</td>
<td>2</td>
</tr>
<tr>
<td>Route tables</td>
<td>2</td>
</tr>
<tr>
<td>EC2 instances</td>
<td>5</td>
</tr>
<tr>
<td>Classic Load Balancer</td>
<td>1</td>
</tr>
<tr>
<td>Security groups</td>
<td>4</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Resource</th>
<th>Total number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classic Load Balancer</td>
<td>1</td>
</tr>
<tr>
<td>EC2-VPC Elastic IP</td>
<td>1</td>
</tr>
<tr>
<td>Security groups</td>
<td>4</td>
</tr>
<tr>
<td>EC2 instances</td>
<td>5</td>
</tr>
<tr>
<td>Classic Load Balancer</td>
<td>1</td>
</tr>
<tr>
<td>Security groups</td>
<td>4</td>
</tr>
</tbody>
</table>
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 Prerequisites: Granting Permissions for Stack Set Operations.

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 SAS Viya 3.4 for Linux: Deployment Guide.

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 Security Settings

Ensure that port 389 on your Lightweight Directory Access Protocol (LDAP) machine is accessible by the SAS Viya machines.

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 SAS Viya 3.4 for Linux: Deployment Guide.
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 programming machine's (Prog) PAM configuration 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 RedHat documentation. 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 Prog machine.
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 'Stateful' VM with `ssh stateful.viya.sas`
2. To list all users and groups, run this command

   ```bash
   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@stateful.viya.sas
   displayName: New User
   ```

2. Run the following command.

   ```bash
   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).

3. 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:
4. Add the home directories for your new user on the programming machine (prog.viya.sas) and the CAS controller (controller.viya.sas). From the Ansible controller VM:

```bash
ssh prog.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:

```bash
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:

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2018</td>
<td>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</td>
<td>Throughout doc: Costs and Licenses; Launch the Quick Start Addendum A: Resource Requirements; Addendum B: Administrative Permission Requirements; Addendum C: Set Up a Mirror Repository</td>
</tr>
<tr>
<td>August 2018</td>
<td>Screen updates (Outputs tab) and log changes</td>
<td>Launch the Quick Start Troubleshooting</td>
</tr>
<tr>
<td>May 2018</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>

© 2018, 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.