SAS® Viya® 3.5 for Windows: Deployment Guide

SAS® Documentation
December 22, 2023

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2019. *SAS® Viya® 3.5 for Windows: Deployment Guide*. Cary, NC: SAS Institute Inc.

SAS® Viya® 3.5 for Windows: Deployment Guide

SAS Institute Inc., SAS Campus Drive, Cary, NC 27513-2414

December 2023

3.5-P1:dplyml0phy0win

Contents

1

Introduction

Steps for a Successful Deployment

Before You Begin

- If you are viewing a saved copy of a PDF of this guide, the content might be outdated because this guide is subject to continual updates. You can always view the latest SAS Viya deployment guides at the SAS Viya Install Center.
- To use this guide successfully, you should have a working knowledge of Microsoft Windows PowerShell and the Windows operating system. To learn about the deployment tools and the differences between a full deployment and a programming-only deployment, see “How Deployment Works” on page 3.

Step 1 — Prepare for the Deployment

1. Perform one of the following tasks:
   - To update or add software to an existing deployment, go directly to Chapter 8, “Managing Your Software,” on page 93.
   - To deploy a new instance of the software, continue with the following the steps.
2. Go to Chapter 2, “System Requirements,” on page 7 to learn about requirements for hardware, software, data sources and storage, user accounts, security, and clients.
3. Go to Chapter 3, “Pre-installation Tasks,” on page 29 to prepare your environment before you deploy the software.

Step 2 — Perform the Deployment

1. Go to Chapter 4, “Installing SAS Viya,” on page 43 to deploy the software.
2. Go to Chapter 5, “Post-installation Tasks,” on page 57 to configure your environment.

Step 3 — Validate and Complete the Deployment

1. Go to Chapter 6, “Validating the Deployment,” on page 79 to log on to SAS Studio and perform other validation tasks, such as that verifying that the servers were deployed correctly and that SAS can access your data.
2. Go to Chapter 7, “Completing the Deployment,” on page 89 to learn about post-deployment best practices and to find documentation about administrative tasks.

How Deployment Works

Using Deployment Scripts to Deploy SAS Viya

The Basics

Here is an overview of how the deployment works:

- To prepare for deployment, you must create the deployment scripts that are used to install and configure the software that you ordered. To do that, you download and run a tool provided by SAS called the SAS Orchestration Command Line Interface (CLI). You can run the SAS Orchestration CLI on a machine with a supported version of Windows, Linux, or Macintosh.

  The instructions for downloading the SAS Orchestration CLI and creating the deployment scripts are provided in this guide. Also, the Software Order Email (SOE) that SAS sends to your business or organization contains a file attachment which is required to create the deployment scripts. The file attachment in the SOE contains information that is specific to your order.

  Note: During deployment, the software to which you are entitled is downloaded from repositories that are maintained by SAS, or from mirror repositories at your own site. Creating mirror repositories is an optional task that you can perform before deployment. The instructions for using the SAS Mirror Manager utility to create mirror repositories are provided in this guide.

- To deploy the software, you run (as Administrator) a `setup.bat` command that executes the deployment scripts. Each time you run the command, the software is securely downloaded from repositories that are maintained by SAS, or from the mirror repositories that you have created.

Deployment Types

By default, you deploy the full suite of products and user interfaces that you ordered. In the SAS documentation, this type of deployment is referred to as a “full deployment.”

Although SAS recommends a full deployment, you can configure a deployment script to perform a “programming-only” deployment. A programming-only deployment limits support to data scientists and programmers who use SAS Studio, or direct programming interfaces such as Python or REST APIs. Understand that this type of deployment does not include SAS Drive, SAS Environment Manager, and the complete suite of services that are included with a full deployment.

Therefore, make sure that you are providing your users with the features that they require.

Your version of SAS Studio depends on which type of deployment that you perform. If you deploy a full environment, then your environment contains both SAS Studio (Enterprise) and SAS Studio (Basic). By default, users will log on to SAS Studio (Enterprise). If you deploy a programming-only environment, then your environment contains SAS Studio (Basic).

Note: To deploy SAS Data Science, perform a programming-only deployment. A full deployment does not support SAS Data Science.

Note: To deploy SAS Event Stream Manager, perform a full deployment. A programming-only deployment does not support SAS Event Stream Manager.

How a SAS Viya Deployment Differs from a SAS 9 Deployment

The SAS Viya deployment differs from a SAS 9 deployment in the following ways:

- The SAS Deployment Wizard and the SAS Deployment Manager that support SAS 9.4 are not used to install and configure SAS Viya.
- Because the MSI-based deployment model works with repositories that are native to your operating system, a SAS Software Depot is not required for your SAS Viya software.

SAS Products and Supporting Components

This guide provides information for deploying the following software:

SAS Cloud Analytic Services for Viya 3.5

SAS Data Science 8.3 (for more information about SAS Data Science, see the SAS Data Science product page)

SAS Event Stream Processing (SAS Viya Enabled) 6.2

SAS Job Flow Scheduler (on SAS Viya)

SAS Visual Analytics (on SAS Viya) 8.5

SAS Visual Data Mining and Machine Learning 8.5

SAS Visual Statistics (on SAS Viya) 8.5

SAS/ACCESS Interface to ODBC (on SAS Viya)

SAS/ACCESS Interface to PC Files (on SAS Viya)

SAS Studio 5.2 (Basic) SAS Studio 5.2 (Enterprise) SAS Text Analytics (for languages)	SAS/ACCESS Interface to PostgreSQL (on SAS Viya) SAS/ACCESS Interface to Salesforce (on SAS Viya) SAS/ACCESS Interface to Snowflake (on SAS Viya) SAS/CONNECT (on SAS Viya)

Note: Check your Software Order Email (SOE) for the list of software that you have licensed.

Contact SAS Technical Support

Technical support is available to all customers who license SAS software. However, you are encouraged to engage your designated on-site SAS support personnel as your first support contact. If your on-site SAS support personnel cannot resolve your issue, have them contact SAS Technical Support to report your problem.

Before you contact SAS Technical Support, explore the SAS Support website at support.sas.com/techsup/. This site offers access to the SAS Knowledge Base, as well as SAS communities, Technical Support contact options, and other support materials that might answer your questions.

When you contact SAS Technical Support, you are required to provide information, such as your SAS site number, company name, email address, and phone number, that identifies you as a licensed SAS software customer.

2

System Requirements

Hardware Requirements

General Hardware Considerations

A full deployment is the recommended configuration for most customer requirements. To deploy SAS Event Stream Manager, you must perform a full deployment. However, SAS Data Science is always deployed as programming-only. SAS Viya 3.5 for Microsoft Windows supports single-machine deployments only.

SAS strongly recommends consulting with a sizing expert to obtain an official hardware recommendation that is based on your deployment type, the estimated SAS workload, and the number of users. To request sizing expertise, contact your SAS account representative. If you need assistance in determining your SAS account representative, send an email to contactcenter@sas.com.

Host Requirements

Use a dedicated host for your SAS Viya deployment. Co-installation with SAS 9.4 is not supported.

The machine target for the deployment must have the following attributes:

- A static IP address.

  After the deployment has completed, changes to IP addresses are not supported.

- A static host name that conforms to internet standards.

  After the deployment has completed, changes to host names or domain names are not supported.

  Multiple internet standards include a restriction on special characters, with the exception of hyphens. Host names can consist of ‘a-z’, ‘A-Z’, ‘0-9,’ and ‘–’ only and cannot contain underscore characters (_).

- A fully qualified domain name that is 64 characters or fewer in length.

  This restriction is related to the implementation of transport layer security (TLS). One of the specifications for the certificate revocation list is a 64-character limit for the common name (CN=) attribute. For more information, see RFC 5280.

CPU and RAM Recommendations

SAS Viya has undergone rigorous performance testing with various hardware combinations. In addition to being tested on high-performing Intel Xeon E3-E7 series microprocessors, SAS Viya has also been tested with newer Intel chips, such as Intel Xeon Scalable Processors. SAS Viya also supports 64-bit AMD chipsets. Thirty-two-bit chipsets are not supported.

Consider the following as you prepare for the deployment process:

- The hardware guidelines in this guide apply to a production environment. For a test environment, CPU, RAM, and disk resources can be reduced slightly.
- Overall system performance will improve with the addition of both RAM and CPU cores. The start-up times for the various services in the environment and the level of performance that they deliver will also improve as resources are added.
- Test machines were equipped with RAM that had a minimum memory clock speed of 1600 MHz.

Architectural Considerations

SAS Viya 3.5 for Microsoft Windows is supported on single-machine deployments only.

The SAS Viya architecture consists of three categories of components that you should consider as you plan your deployment. These components should each be considered individually to determine the attributes of the server to host SAS Viya on Windows:

- SAS Cloud Analytic Services (CAS server)

  The CAS server is required for all deployments, regardless of type (full or programming-only). It is licensed by CPU core, with a minimum license size of 4 cores.

  The amount of RAM that is required for the CAS Server is determined by the amount of data that is processed, and by the level of user activity in the environment. However, out of the box, the amount of RAM that is required to start the CAS Server is less than 1 GB.

- Programming Runtime

  The Programming Runtime consists of multiple components that are required for all deployments. It includes the SAS compute server, SAS Foundation, SAS Studio, SAS Workspace Server, SAS/CONNECT Server, and any SAS/ACCESS engines that you have licensed.

  The number of CPU cores that are required for the Programming Runtime depends on your specific license. If your CAS license is for *N* cores, you are also entitled to run the Programming Runtime on the same number of cores. However, the minimum requirement is 2 cores. SAS recommends that you allocate at least 4 cores for optimal performance.

The minimum required amount of RAM for the Programming Runtime is 4 GB. SAS recommends that you allocate at least 16 GB of RAM or that you allocate 4 GB for each CPU core that you have licensed, whichever is greater.

- Service Layer

  This category consists of components that are required for a full deployment, as well as services that support specific SAS products. These components are not usage restricted. They include services that support SAS Viya analytics processing.

Disk Space Requirements

SAS Viya installs executables into `C:\Program Files\SAS` and creates configuration directories in `C:\ProgramData\SAS`.

The minimum available disk space that is required to install and start a full deployment of SAS Viya is less than 90 GB. However, logs and operational data will quickly grow to exceed that amount. Therefore, the actual disk space that is required will depend on the amount of data and the level of activity in your specific deployment.

Because installation is performed using the MSI deployment process, reserve some disk space for installation files. The `C:\Windows\Installer` directory will require 16.8 GB in order to store the MSI files, which will be reused for a few operations and, eventually, for uninstallation procedures.

Hardware Guidelines for a Programming-Only Deployment

A programming-only deployment consists of the CAS server, SAS Programming Runtime, and SAS Studio (Basic). Use the following formula to determine the minimum suggested core count to support the SAS processes that are running on your server:

```
2 + (number-of-licensed-CAS-cores * 2)
```

For example, for a 4-core CAS license, the minimum recommendation is 10 CPU cores. This level of resources supports the following execution environment:

- CAS (4 cores)
- SAS Programming Runtime processes (4 cores)
- SAS Studio and other system overhead (2 cores)

Note: These 10 cores are in addition to the resources that are required in order to execute the additional workload on your server.

The minimum recommended RAM calculation for a programming-only deployment is the sum of the following:

- 2 GB for SAS Studio

- Anticipated *maximum-number-of-concurrent-users* * 4 GB

  Note: These RAM resources support the SAS Programming Runtime sessions for each user.

- 1 GB + *total-size-of-data-to-be-loaded-into-CAS-memory*

  Note: This amount of RAM is specific to your anticipated usage.

Hardware Requirements for a Full Deployment

The following table lists products that can be separately licensed. It also specifies the RAM and the number of CPU cores that are needed to support individual components when they are installed on a single machine. These out-of-the-box requirements should be increased for larger deployments.

Table 2.1 *Minimum Hardware Requirements for Each Product*

Products	RAM (GB)	CPU Cores
SAS Visual Analytics	48	4
SAS Visual Analytics and SAS Visual Statistics	48	4
SAS Visual Analytics, SAS Visual Statistics, and SAS Visual Data Mining and Machine Learning	64	6

Taking your license into consideration, you can estimate the total number of CPU cores that are required for a full deployment by using the recommendations in the table. The Windows operating system itself requires at least 2 cores. You should also consider the number of cores that are included in your product license. Here are some examples of equations that can guide your resource decision-making process:

For SAS Visual Analytics, SAS Visual Statistics, and SAS Visual Data Mining and Machine Learning:

```
6 + (2 * number-of-licensed-CAS-cores)
```

For SAS Visual Analytics, or SAS Visual Analytics and SAS Visual Statistics:

```
4 + (2 * number-of-licensed-CAS-cores)
```

To estimate the RAM that is required for the same license, consider the following:

- RAM from the information in the table, based on your license
- (Number of concurrent SAS Studio users + Number of concurrent SAS Visual Data Mining and Machine Learning users) * 4

These resources are required to support the SAS Programming Runtime processes.

- 1 GB + Total size of data to be loaded into CAS memory

Consider the following hypothetical usage scenario:

- An order includes SAS Visual Analytics, SAS Statistics, and SAS Visual Data Mining and Machine Learning
- 10 concurrent users of SAS Studio
- 4 concurrent users of SAS Visual Data Mining and Machine Learning
- Maximum of 128 GB of data to be concurrently loaded into CAS memory

For this scenario, you can calculate the estimated RAM that would be required:

```
64 GB + (14 * 4 GB) + 128 GB = 248 GB of RAM
```

Therefore, a machine that is provisioned with 256 GB of RAM should be able to accommodate the SAS resource usage and operating system overhead.

> **IMPORTANT** These scenarios are hypothetical. SAS recommends that you obtain an official sizing from SAS, based on your specific requirements.

Deployment from a mirror repository is optional. For disk space requirements that apply to mirror repositories, see "Create a Mirror Repository" on page 29.

Hardware Requirements for Deep Learning

Deep learning capabilities are included with SAS Visual Data Mining and Machine Learning. Use the requirements for that product to prepare your target machines. The deep learning features are automatically installed.

A graphical processing unit (GPU) is not required on your computer in order to use deep learning features. However, a GPU provides additional functionality. To enable deep learning with GPU functionality, here are additional requirements:

- ☐ Only one NVIDIA GPU device is supported on a Microsoft Windows machine.
- ☐ The NVIDIA display driver, version 411.82 or later. SAS recommends using the latest version.

  SAS recommends following the instructions in the NVIDIA CUDA Installation Guide for Microsoft Windows.

  You can download the current drivers from http://www.nvidia.com/Download/index.aspx?lang=en-us.

At a command prompt, run the following command in order to verify the device type, the driver version, and the CUDA version:

```
nvidia-smi
```

Some post-deployment steps might be required to enable GPU functionality. For more information, see "(Optional) Enable GPU Functionality" on page 68.

Operating System Requirements

Supported Operating Systems

For the full list of supported operating systems, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-operating-systems.html.

SAS Support for Alternative Operating Systems

SAS provides support on a limited basis for alternative operating system distributions that customers might select. For more information, see the official support policy statement at https://support.sas.com/en/technical-support/services-policies/policies-for-sas-products.html#altos .

Server Software Requirements

Windows PowerShell Requirements

Microsoft Windows PowerShell version 5.1 or later is required in order to install SAS Viya on Windows. PowerShell is a framework that supports a scripting language and configuration management capabilities on Windows. Running the deployment scripts in Windows PowerShell Integrated Scripting Environment (ISE) is not supported.

Follow these steps to determine the current version of PowerShell if it is already installed:

1. Start PowerShell.
2. At the PowerShell command prompt, enter the following command to find out the PowerShell version:

   ```
   $PSVersionTable.PSVersion
   ```

   In the output, verify that the major version is 5 and that the minor version is 1 or later.

3 If required, install a newer version of PowerShell by installing Windows Management Framework 5.1.

Note: You can skip these steps if you are installing SAS Viya on Microsoft Windows Server 2016.

On Windows Server 2012 R2, follow these steps:

a Microsoft .NET 4.6.1 is a requirement for Windows Management Framework 5.1. Download it from https://www.microsoft.com/en-us/download/details.aspx?id=49981.

b Double-click the executable, and follow the prompts to install it.

c Download and install the Windows Server 2012 R2 update for Windows Management Framework 5.1. Navigate to the Install and Configure WMF 5.1 page to download the package.

d Double-click the executable, and follow the prompts to install it. A restart of your machine might be required.

4 SAS Viya will use PowerShell scripts to configure and run services. SAS supports all the PowerShell execution policies except Undefined and Restricted. Manually enable script execution in PowerShell by running the following command:

```
Set-ExecutionPolicy  -scope LocalMachine execution-policy
```

Note: For more information about the PowerShell execution policies, see About Execution Policies.

PowerShell does not require a graphical user interface. It can be run on a machine that lacks a monitor.

Additional Software Requirements

Microsoft Windows Defender Credential Guard is supported by SAS Viya. Windows Defender Credential Guard enforces constrained delegation for Kerberos protected services. However, constrained delegation is not supported for SAS/ACCESS Interface to PostgreSQL. If this product is included in your order, Windows Defender Credential Guard must be disabled.

If you are installing on Windows Server 2016 or later, you must disable Windows Defender Credential Guard before you start the deployment process. In addition, you must disable it on any client systems that are running Microsoft Windows 10.

If you are installing on Windows Server 2012 R2, the Microsoft .NET Framework 4.6.1 or later is required. It is also required for the Microsoft Windows Management Framework, which is typically installed in order to obtain PowerShell. Therefore, do not uninstall the .NET Framework after you install PowerShell.

The Microsoft Visual C++ Redistributable Packages for Visual Studio 2013 and 2015 (64-bit versions) are required for all supported platforms. In addition, the Microsoft Visual C++ 2010 Redistributable Package with Service Pack 1 is required.

You can download the packages from the following Microsoft websites:

- Package for Visual Studio 2013: https://www.microsoft.com/en-us/download/details.aspx?id=40784
- Package for Visual Studio 2015: https://www.microsoft.com/en-us/download/details.aspx?id=48145
- Package for Visual C++ 2010 with Service Pack 1: https://www.microsoft.com/en-us/download/details.aspx?id=26999

Support for Dynamic Data Exchange (DDE) with Microsoft Excel has been deprecated with SAS Viya 3.4 and later.

Java Requirements

A 64-bit version of the Java Runtime Environment (JRE) must be installed on the machine where you install SAS Viya components. For a list of supported JRE distributions, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-jre.html.

Third-party distributions of the JRE are supported as long as the version matches the one that is listed on the SAS Support website. However, IBM SDK, Java Technology Edition is not supported.

Determine the Version of Java on the Machine

To determine the version of Java that is installed on the local machine, follow these steps:

1. Open the Windows Control Panel.
2. Navigate to **Programs and Features**.

   If Java is installed on the computer, one or more Java versions are listed in the **Programs and Features** panel.

Additional Requirements for Oracle Java

If you have installed Oracle Java, a few required files might be missing. By default, earlier versions of the Oracle Java installation on Microsoft Windows lacked the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy files. However, more recent Java releases, version 1.8.0_161-b12 and later, contain the feature, which is enabled by default, and some earlier Java releases might include the feature without enabling it.

To determine whether your version of Oracle Java has the JCE files, see the Release Notes for your particular release.

If you have an earlier version of Oracle Java, follow these steps:

1. Navigate to the Oracle website at http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html.
2. Accept the license agreement.
3. Download the link for the ZIP file, jce_policy-8.zip.
4. Uncompress the files in the directory where Java is installed on your machine, such as `c:\Program Files\Java\jre1.8.0_131\lib\security\` .

Set the SAS_JAVA_HOME Environment Variable

If you want to specify a different JRE for SAS Viya to use, you can set the SAS_JAVA_HOME environment variable to the location of a supported JRE. By default, the deployment process sets the variable automatically when it locates a JRE on the machine.

1. Click the **Windows** key and open This PC.
2. Right-click **This PC** and select **Properties**.
3. In the Control Panel window, click **Advanced system settings**. When the System Properties dialog box appears, click **Environment Variables**.
4. When the Environment Variables dialog box appears, in the System Variables section, click **New**.
5. Enter SAS_JAVA_HOME for the **Variable name** parameter.

   For the **Variable value**, navigate to the location of an installed JRE that meets SAS requirements.
6. Click **OK** to save the new environment variable.

Disable Microsoft IIS Web Server

If Microsoft Internet Information Services (IIS) for Windows is installed on the machine where you plan to install SAS Viya, be sure to disable or uninstall it before you start the deployment process. Otherwise, port conflicts will occur. You must restart the machine after uninstalling IIS in order to complete the deployment process.

Data Source and Storage Requirements

Overview of Data Warehouse and Storage Requirements

You can install software to enable data retrieval from various data storage appliances. Depending on your data sources, you might also install one or more SAS/ACCESS products.

Refer to the section that corresponds to your SAS/ACCESS product for additional system requirements that might apply.

Supported Data Sources

SAS Viya supports the following data sources:

- PC files
- Data sources that are accessible with an ODBC driver
- PostgreSQL
- Salesforce
- Snowflake

Note: The ODBC and PostgreSQL data sources require a SAS/ACCESS interface product. Some SAS/ACCESS engines have individual system requirements.

SAS Viya also supports CSV files. Files of this type do not require a SAS/ACCESS product and can be accessed directly.

Requirements to Transfer Data from SAS 9.4

For SAS 9.4 deployments that are earlier than SAS 9.4 TS1M5 (SAS 9.4M5), SAS/CONNECT is required in the environment in order to transfer data to SAS Viya. SAS/CONNECT is not included with a standard SAS Viya order, and must be separately licensed.

By contrast, SAS 9.4M5 and later are integrated with SAS Viya directly. As a result, SAS/CONNECT is no longer required in order to transfer data from SAS 9.4M5 and later. All SAS programming clients in a 9.4M5 or later environment can call procedures that are enabled in SAS Viya and submit DATA step code, operating

directly on CAS data sources. Examples of SAS programming clients are SAS Studio, SAS Enterprise Guide, SAS Data Integration Studio, and SAS Data Management Studio.

SAS/CONNECT is still supported, but if you are running SAS 9.4M5 or later, it is no longer required in order to transfer data into SAS Viya.

Transport Layer Security (TLS) is supported for SAS/CONNECT, but it is not enabled by default. SAS provides a self-signed certificate to assist you in enabling TLS for SAS/CONNECT as a post-deployment task. For more information, see Configure SAS/CONNECT to Use TLS (Windows) in *Encryption in SAS Viya: Data in Motion*.

Requirements for SAS/ACCESS Interface to ODBC

SAS/ACCESS Interface to ODBC (on SAS Viya) includes SAS Data Connector to ODBC. SAS/ACCESS Interface to ODBC enables access to multiple data source types by means of a generic ODBC driver.

For information about ODBC support, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-databases.html.

Requirements for SAS/ACCESS Interface to PC Files

SAS/ACCESS Interface to PC Files (on SAS Viya) includes SAS Data Connector to PC Files.

SAS/ACCESS Interface to PC Files enables access to the following file formats:

- `.jmp`
- `.spss`
- `.stata`
- `.xlsx` or `.xls`

No additional software is required.

Requirements for SAS/ACCESS Interface to PostgreSQL

SAS/ACCESS Interface to PostgreSQL (on SAS Viya) includes SAS Data Connector to PostgreSQL.

For SAS Viya 3.5 on Microsoft Windows, PostgreSQL client 14.7 or later is required in order to bulk load and bulk unload files that are larger than 2 GB. Otherwise, the psql tool is limited to files that are smaller than 2 GB. You can download the latest

client from the following PostgreSQL site: https://www.enterprisedb.com/downloads/postgres-postgresql-downloads.

For information about supported PostgreSQL versions and requirements, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-databases.html.

Requirements for SAS/ACCESS Interface to Salesforce

SAS/ACCESS Interface to Salesforce (on SAS Viya) includes SAS Data Connector to Salesforce.

For information about Salesforce requirements, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-databases.html.

Requirements for SAS/ACCESS Interface to Snowflake

SAS/ACCESS Interface to Snowflake (on SAS Viya) includes SAS Data Connector to Snowflake.

For information about third-party requirements for SAS/ACCESS Interface to Snowflake, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-databases.html.

User Account Requirements

Installation User Account Requirements

The user account that initiates the deployment process requires Administrator privileges for the machine where the deployment is launched.

Additional Required User Accounts

The following tables describe SAS Viya user accounts. These accounts are required for installation, for running services during the product's normal operation, and for access to user interfaces. Account requirements depend on your deployment type.

Here are the user account requirements for a full deployment. You can grant account privileges using the Windows Local Security Policy editor:

Table 2.2 Required User Accounts for a Full Deployment

Account Name	Description	Purpose
cas	A domain administrator must create this user account as a domain account before you begin the deployment process. **Note:** You can use the same user account for both CAS and the HTTP server. Here are the requirements for this account: ■ Membership in the Local Administrators group ■ Trusted for delegation to any service ■ Log on as a Service privilege ■ Replace Process Level Token privilege ■ A unique user name with maximum length of 20 characters. The user name `cas` is recommended. This account requires a password. If the password expires, the CAS service no longer starts. When you create the user account: ■ Clear the check box labeled **User must change the password at the next logon**. ■ Select the check box labeled **User cannot change password**. If the security policies at your enterprise allow you to disable password expiration, disable it by selecting the check box labeled **Password never expires**. You can also periodically change the password for the service in the Windows Control Panel and restart the service. However, you must also	Owns the CAS service and is required for managing and enabling CAS and backup files. Also acts as the file owner of many of the files that are copied to the computer by the installation. Before you start the installation, you must save the user ID and password to an encrypted credentials file. For more information, see "Specify Credentials for the cas User Account" on page 43.

Account Name	Description	Purpose
	regenerate the credentials file each time the password changes. If you used the same user account for the HTTP server, the Kerberos administrator must re-create the keytab file with the new password.	
user for HTTP service account	A user account that can be used as a service account for the HTTP proxy server (the Apache HTTP Server). Here are the requirements for this account: ■ It must be a domain account that exists in LDAP. ■ It must be trusted for delegation to any service.	A requirement from Kerberos, this account serves as the owner of the HTTP proxy server.
PostgreSQL server user account	A domain administrator must create this user account as either a local account or a domain account before you begin the deployment process. It must be a standard user account that does not have administrator privileges. The user name `postgres` is recommended. This account requires the privilege to Log on as a Service. When you create the user account: ■ Clear the check box labeled **User must change the password at the next logon**. ■ Select the check box labeled **User cannot change password**. If the security policies at your enterprise allow you to disable password expiration, disable it by selecting the check box labeled **Password never expires**. If the password expires, the PostgreSQL service will no longer start.	Enables the SAS Infrastructure Data Server, which runs on PostgreSQL, to start automatically. Before you start the installation, you must save the user ID and password to an encrypted credentials file. For more information, see "Specify Credentials for the postgres User Account" on page 44.

Account Name	Description	Purpose
	You can also periodically change the password for the service in the Windows Control Panel and restart the service. However, you must also regenerate the credentials file each time the password changes. The following restrictions apply to the password: ■ Must contain alphanumeric characters only. Cannot contain any non-alphanumeric characters, such as hyphens or underscores. ■ Must be at least six characters long.	
sasboot	Administrative user account that is created automatically during the deployment process, with an expired password. The sasboot user is internal only to SAS. It does not exist on a machine or in LDAP.	Used for preliminary access to the visual administration interface after the deployment process has completed. Use this account to log on to the SAS Viya visual interface in order to configure the connection to your identity provider and to set up user accounts. The sasboot account is typically not used after you have completed configuration activities. However, it can be used as an indirect logon option in case your identity provider becomes unavailable.

Here are the user account requirements for a programming-only deployment. You can grant account privileges using the Windows Local Security Policy editor:

Table 2.3 *Required User Accounts for a Programming-Only Deployment*

Account Name	Description	Purpose
cas	A domain administrator must create this user account as a domain account before you begin the deployment process. Here are the requirements for this account:	Owns the CAS service and is required for managing and enabling CAS. Also, it acts as the owner of many of the files that are copied to the machine during installation. Before you start the installation process, you must save the

Account Name	Description	Purpose
	■ Membership in the Local Administrators group ■ Log on as a Service privilege ■ Replace Process Level Token privilege ■ A unique user name with maximum length of 20 characters. The user name `cas` is recommended. This account requires a password. If the password expires, the CAS service no longer starts. When you create the user account: ■ Clear the check box labeled **User must change the password at the next logon**. ■ Select the check box labeled **User cannot change password**. If the security policies at your enterprise allow you to disable password expiration, disable it by selecting the check box labeled **Password never expires**. You can also periodically change the password for the service in the Windows Control Panel and restart the service. However, you must also regenerate the credentials file each time the password changes.	user ID and password to an encrypted credentials file. For more information, see "Specify Credentials for the cas User Account" on page 43.
User accounts for SAS Studio access	Host accounts with access to the machine where SAS Viya has been deployed. These user accounts require the privilege to Log on as Batch Job.	SAS Studio (Basic) does not support Kerberos authentication. The privilege to Log on as Batch Job enables user access in a programming-only deployment.

TIP The Windows privilege to Log on as Batch Job is required for users in a programming-only deployment. However, it is also helpful in a full deployment, which includes Kerberos. Users of SAS Viya products who have this privilege can specify a user name and password for authentication of batch jobs from command-line interfaces if they are not using Kerberos. If a user's Kerberos ticket has expired, the privilege enables SAS Viya to check the credential store to authenticate that user.

Security Requirements

LDAP Requirements

LDAP is required for SAS Viya visual interfaces. It is not required in a programming-only deployment.

To support the visual interfaces, SAS Viya must have Read access to your LDAP provider. SAS Viya requires a userDN and password in order to bind to the LDAP server. Anonymous binding is supported for clients that are authenticating to the LDAP server.

If the mail attribute is specified for LDAP accounts, it must have a non-null value that is unique for each user.

LDAPS is supported, but the required certificates are not configured automatically by the deployment process.

Configuring your LDAP provider is a required post-installation task. For more information, see "Configure the Connection to Your Identity Provider" on page 58.

Authentication Requirements

Kerberos is the required network authentication protocol for SAS Viya deployments on Windows. By default, Kerberos 5 is implemented on Windows Server operating systems.

Note: Kerberos is not supported for a programming-only deployment of SAS Viya. For a programming-only deployment, users must have local Windows accounts that are authorized to log on to SAS Studio (Basic).

For a full deployment, Windows security integrates with the Kerberos Key Distribution Center, which uses the Active Directory database for user accounts. Therefore, Kerberos support requires Active Directory Domain Services.

SAS provides a utility, SAS Viya Deployment Assistant for Windows, to validate Kerberos configuration on your system. You can obtain the package when you

download the SAS Orchestration CLI package. Running this utility is optional, but recommended. For more information, see "Evaluate the Kerberos Configuration and Windows Tuning" on page 48.

Note: SAS Viya Deployment Assistant for Windows can also configure Kerberos to meet SAS Viya requirements. If you run the tool with the `-remediate` option, it compares the existing configuration of Kerberos to the requirements and attempts to fix any deficiencies that it finds.

Running SAS Viya Deployment Assistant for Windows will assist you in fulfilling the following requirements:

- A user account that can be used as a service account for the HTTP proxy server (the Apache HTTP Server) must exist in Active Directory.
- A service principal name (SPN) must be mapped to the service account for the Apache HTTP Server. The HTTP SPN must follow the convention HTTP/*host-name*, where *host-name* is the fully qualified domain name of the Apache HTTP proxy server in the deployment.

  The domain account that functions as a service account is the owner of the SPN. Multiple SPNs can be added to the account if aliases are required.
- The SPN must be mapped to the principal name.
- A keytab file is required, with a filename in the format *host-name*.keytab. Access to the Kerberos utilities is required to generate this file.
- An SPN for the CAS server is required. The CAS SPN must follow the convention sascas/*host-name*, where *host-name* is the fully qualified domain name of the machine where the CAS server is running. The SPN must be registered on the service account that is running the CAS server (the cas account).

  If desired, you can designate the same service account that was used to register the HTTP SPN for this purpose.
- The cas account must be trusted for delegation to any service.
- The machine object must be trusted for delegation to any service.

The sasboot user account is used to configure Kerberos authentication in SAS Environment Manager after the deployment process has completed. For more information, see Configure Kerberos.

Transport Layer Security

The deployment process provides a default level of security by enabling TLS on connections to the Apache HTTP Server. However, this level of security requires you to block external connections to the server on port 80. You can also enforce HTTPS for access to SAS Viya by redirecting port 80 to 443 for web browser access.

The certificate that the deployment provides to secure the Apache HTTP Server is self-signed. SAS recommends that you enhance the security by replacing this certificate with a custom certificate that is generated according to the security standards at your organization.

How Default Security Is Applied

An Apache HTTP server is used as a reverse proxy server to secure your environment. By default, TLS is enabled for Apache httpd, and the server is secured with a self-signed certificate (sas.crt) and a private key (sas.key) that the deployment process generates.

TLS is not enabled on the CAS server by default. However, after the deployment has completed, a system administrator can enable TLS by running a PowerShell script that is provided with SAS Viya. This script creates a certificate file (sas_encrypted.crt), a private key file (sas_encrypted.key), and a passphrase file (encryption.key) for the private key file. It also configures the CAS server and Windows to use these files in order to enable TLS.

The deployment process provides a default level of encryption for data in motion (transmitted data). SAS Viya attempts to use the highest level of the TLS protocol that the operating system library supports, up to TLS 1.3. Microsoft SChannel is used for TLS protocols. SAS Viya attempts to use the cipher suites that ensure Perfect Forward Secrecy and that provide the highest level of security that the host can support. For more information, see TLS Encryption.

You can replace the self-signed certificate that is used to enable TLS for the CAS server. For details, see Update Certificates and Configure TLS on CAS in *Encryption in SAS Viya: Data in Motion*.

You can also replace the self-signed certificate that is used to enable TLS for the Apache HTTP Server. For details, see Update Apache HTTP Server TLS Certificates and Cryptography in *Encryption in SAS Viya: Data in Motion*.

Replacing the certificates will require you to restart the Apache and CAS servers. This will cause a brief outage. If you do not add custom certificates and instead keep the default security settings and certificates, users will see a standard web browser warning message. SAS recommends that you replace the certificates that are created by the deployment before you give users access to the software.

Enhance Default Security Settings

SAS recommends that you enhance the default security that is applied by the deployment process. For more information about configuring additional security settings, see Tasks to Harden Security for Your Windows Deployment in *Encryption in SAS Viya: Data in Motion*.

As a best practice, follow these steps as soon as the deployment process has completed:

1. Secure the Apache HTTP Server by adding certificates that conform to the policies at your enterprise.
2. Enable TLS for the CAS server.
3. If you are using SAS/CONNECT to access data from earlier versions of SAS 9.4, enable TLS for SAS/CONNECT.

For more information, see Configure SAS/CONNECT to Use TLS (Windows) in *Encryption in SAS Viya: Data in Motion*.

4 Enforce HTTPS for access to SAS Viya by blocking external connections to port 80 and by redirecting port 80 to 443 for browser access.

5 Prevent administrators from altering the default permissions on subdirectories of `Program Files\SAS\Viya` and `ProgramData\SAS`. Use your preferred network monitoring or security tool to monitor permissions on these subdirectories after the deployment has completed.

Client Requirements

Operating Systems and Web Browsers

UNIX and 64-bit Windows operating systems are supported.

SAS Viya user interfaces include some advanced features that require recent versions of popular web browsers. For information about supported web browsers and the corresponding platforms to access SAS user interfaces, see: https://support.sas.com/en/documentation/third-party-software-reference/viya/35/support-for-web-browsers.html.

Mobile Platform Support

The SAS Visual Analytics App is supported on iOS and Android smartphones and tablets. The SAS Visual Analytics App is also supported on Windows 10. The app is written specifically for the selected operating system and provides native support for these devices so you can view and explore reports anywhere, anytime on your mobile device. You can download the app for free from the Apple App Store, Google Play, or the Microsoft Store.

When the SAS Visual Analytics App for iOS, Android, or Windows is installed on a mobile device, users of the following SAS Viya products can view and explore reports on that device:

- SAS Visual Analytics
- SAS Visual Statistics
- SAS Visual Data Mining and Machine Learning

Users of SAS Visual Investigator can license and install the SAS Mobile Investigator app. It is supported on iOS and Android smartphones and tablets.

Note: Some SAS user interfaces are not currently supported on mobile devices. Touch-enabled interactions with SAS Viya web applications on mobile devices are not supported.

Database Drivers

Make sure that each client where users will access SAS software has the required database drivers already installed.

Screen Resolution

The minimum screen resolution for each client machine that will access the SAS Viya user interfaces is 1280 x 1024.

3

Pre-installation Tasks

Create a Mirror Repository

A mirror repository is required for all SAS Viya deployments on SUSE Linux. For other platforms, it is optional.

Overview

SAS Mirror Manager is a command-line utility for synchronizing a collection of software repositories from SAS. Its primary purpose is to create and manage mirror repositories for software deployment. Mirror repositories are useful if your deployment does not have access to the internet, or if you must always deploy the same version of software (such as for regulatory reasons).

SAS Mirror Manager downloads the software that you ordered and creates a mirror repository. It can create the mirror repository in a specified location, such as a shared NFS mount point or a web server that serves the files with HTTP. The default location for the files that SAS Mirror Manager will download is the `sas_repos` directory in the installation user's home directory. Make sure that the default location or another location that you select has adequate space. Also ensure that the machine where the mirror repository will be located has adequate space.

This guide refers to the default location as `sas_repos`. If you specify a different mirror destination, replace instances of `sas_repos` that are used in this guide with the actual location that you select.

The directories and files that are downloaded to `sas_repos` are explained as follows:

- The entitlements.json is a list of the repositories to which you are entitled.
- The location_group_declarations.json file and the sasmd directory contain data that is used by the SAS Orchestration CLI to create the order-specific tools for your deployment.
- Any remaining directories are the software repositories, organized by native deployment tools:
  - repos contains yum files for Linux.
  - win contains MSI files for Windows.
  - deb contains APT files for Debian.

By default, SAS Mirror Manager downloads the contents of all repositories to which your order entitles you. However, the tool provides options to download software selectively, based on the target platform for the installation. If you run SAS Mirror Manager without options, make sure that the machine where the software is downloaded has adequate disk space to accommodate all platforms:

Table 3.1 *Minimum disk space required for the mirror repository*

Platform	Command Option	Required Disk Space
All platforms	None	159 GB
Linux on Power Power only	ppc64le-redhat-linux-7	54 GB
Red Hat Enterprise Linux or equivalent, such as Oracle Enterprise Linux, only	x64-redhat-linux-6	89 GB
SUSE Linux Enterprise Server only	x64-suse-linux-12	70 GB
Windows only	x64-microsoft-windows-61	38 GB

Using SAS Mirror Manager

To create a mirror repository with SAS Mirror Manager:

1. The Software Order Email (SOE) indicated that you should save the SAS_Viya_deployment_data.zip file attachment. If you have not already saved the file, save it now.

2. Download SAS Mirror Manager from the SAS Mirror Manager download site to the machine where you want to create your mirror repository.

   Note: If you use Microsoft Edge to download the Linux or Macintosh version, save the file as a .tgz file instead of a .gz file.

3. Uncompress the downloaded file.

4. (Optional) Add the location of SAS Mirror Manager to your PATH environment variable.

   Note: This step is not required. However, the example SAS Mirror Manager commands in this section assume that you have added the recommended location to your PATH.

5. Run the following basic command to create the mirror repository in the default location:

   Note: All the software to which your order entitles you is downloaded if you use the basic command.

   ```
   mirrormgr mirror --deployment-data path-to-SAS_Viya_deployment_data.zip
   ```

   By default, the repositories are placed in the `sas_repos` directory in the installation user's home directory. Use the `--path` option, followed by the full directory location of the mirror destination, to change this location.

   ```
   mirrormgr mirror --deployment-data path-to-SAS_Viya_deployment_data.zip --path location-of-mirror-repository
   ```

   Note: If you have an HTTPS proxy, you might also need the `--cacert` option, followed by the location of the certificate (PEM file) that the proxy will use. The proxy certificate is one that your organization manages.

6. (Optional) If your mirror repository is being created on a machine that is secured by TLS (HTTPS), use the `--trusted-certificate` option to define the Certificate Authority chain (such as a file named ca_cert.pem):

   ```
   mirrormgr mirror --deployment-data path-to-SAS_Viya_deployment_data.zip --path location-of-mirror-repository
   --platform platform --latest --trusted-certificate cert-file-name.pem
   ```

7 (Optional) After the initial download is complete, move the file structure to a web server or shared NFS mount. The destination machine does not have to be connected to the internet.

Using SAS Mirror Manager with a Proxy Server

If your environment requires a proxy server and is set up to use it, the SAS Mirror Manager commands will work automatically. However, if your environment is not set up to send data through the proxy, you can add an environment variable to the command to run SAS Mirror Manager. The environment variable identifies where the proxy is located and what is required to send data through it.

Use the environment variable that is appropriate for the target of the query that passes through the proxy. For example, if you are trying to reach a SAS repository, you should use the HTTPS environment variable because the SAS repository is on an HTTPS site. In most cases, the HTTPS environment variable is appropriate.

Here are some examples of SAS Mirror Manager commands that include environment variables.

Example 1: An HTTPS site.

```
set https_proxy=http://user-name:password@internet-proxy-server-FQDN:proxy-port
```

For example:

```
set https_proxy=http://proxyid:password@proxy.company.com:3129
```

Note: If you use the https_proxy variable, the command for SAS Mirror Manager might also require the `--cacert` option, which indicates the location of the certificate that the proxy will use. The proxy certificate will be one that your organization manages.

Example 2: An HTTP site.

```
set http_proxy=http://user-name:password@internet-proxy-server-FQDN:proxy-port
```

For example:

```
set http_proxy=http://proxyid:password@proxy.company.com:443
```

Specify a Log Location

The default location for the logs for SAS Mirror Manager is `%LOCALAPPDATA%\mirrormgr\mirrormgr.log` on Windows and *`user-home-directory`*`/.local/share/mirrormgr/mirrormgr.log` on Linux. To specify an alternative log location:

Note: Specify the command on a single line. Multiple lines are used here to improve readability.

```
mirrormgr.exe mirror --deployment-data path-to-
SAS_Viya_deployment_data.zip --path location-of-mirror-repository --
log-file location-of-logs\mirrormgr.log --latest
```

Create the Deployment Scripts

The SAS Orchestration Command Line Interface (CLI) uses the order information that was included in your Software Order Email (SOE) to create deployment scripts for your SAS Viya software. The SAS Orchestration CLI can be run on Linux or Windows and it requires the Java Runtime Environment 1.8.*x* It also requires access to the internet, unless you are deploying from a mirror repository.

Before you use the SAS Orchestration CLI, ensure that the SAS_Viya_deployment_data.zip file attachment from your SOE is copied to a directory on a machine that runs the Linux, Macintosh, or Windows operating system.

Download the SAS Orchestration CLI

1. The SOE indicated that you should save the SAS_Viya_deployment_data.zip file attachment. If you have not already saved the file, save it now.
2. Go to the SAS Orchestration CLI download site and download the SAS Orchestration CLI for the operating system where you stored the ZIP file. The SOE recommended that you save the ZIP file to a machine that runs Windows, which is where you will install your SAS Viya software. But you could also store it on a machine that runs Macintosh or Linux. If you use Microsoft Edge to download the Linux or Macintosh version, save the file as a .tgz file instead of a .gz file.
3. Uncompress the .tgz file (Linux or Macintosh) or ZIP file (Windows) in the same location where you downloaded it. The result is a file named sas-orchestration on Linux or Macintosh or a file named sas-orchestration.exe on Windows.

Create the Deployment Scripts with the SAS Orchestration CLI

Basic Command

To create the deployment scripts, use the command that is appropriate for the operating system where the SAS Orchestration CLI is located.

Note: The following commands are organized by the operating system where the SAS Orchestration CLI runs, rather than by the operating system where your SAS Viya software is deployed. After you create the deployment scripts, you can move them to the machine where you deploy your software.

Linux or Macintosh

```
./sas-orchestration build --input location-of-ZIP-file-including-file-name
```

Windows

```
.\sas-orchestration.exe build --input location-of-ZIP-file-including-file-name
```

Using the SAS Orchestration CLI creates a new file named sas-viya-deployment-script.zip.

Options

Use a Proxy Server

If you use an unauthenticated proxy to reach the internet, you must add the following option to the run command in order to make an outgoing connection:

```
--java-option "-Dhttps.proxyHost=proxy-server-IP-address-or-host-name"
```

In addition, if the proxy server is not using the default proxy port of 80, you must also add the following option:

```
--java-option "-Dhttps.proxyPort=proxy-server-port-number"
```

If you use both options, they should not be combined into a single option. Here is an example of using both options on a Linux machine:

```
./sas-orchestration --java-option "-Dhttps.proxyHost=my.proxy.com
--java-option "-Dhttps.proxyPort=1111" build
--input /tmp/SAS_Viya_deployment_data.zip
```

The `--java-option` tags must come before the `build` command.

Specify the Deployment Type

You can perform either of two types of deployment for SAS Viya software:

- Full deployment

  Includes all the software to which you are entitled.

- Programming-only deployment

  Excludes SAS Drive, most graphical user interfaces, and most services. It is the simplest and smallest type of deployment.

SAS typically recommends a full deployment. However, if your software includes SAS Data Science, it must be deployed as programming-only.

To deploy your software as programming-only, add the `--deployment-type` option, as shown in this example:

```
.\sas-orchestration build --input c:\sas\install
\SAS_Viya_deployment_data.zip
--deployment-type programming
```

Use a Mirror Repository

If you created a mirror repository with SAS Mirror Manager, you must include its location with the `--repository-warehouse` option.

```
.\sas-orchestration build --input c:\sas\install
\SAS_Viya_deployment_data.zip --repository-warehouse URL-to-mirror-
repository-content
```

Here is an example:

```
.\sas-orchestration build --input c:\sas\install
\SAS_Viya_deployment_data.zip --repository-warehouse
c:\DeploymentFiles\sas_repos
```

Note: If your mirror repository has a secured URL (HTTPS), you must define the Certificate Authority chain (such as a file named ca_chain.pem) using the `--trusted-certificate` option.

Here is an example:

```
.\sas-orchestration build --input c:\sas\install
\SAS_Viya_deployment_data.zip --repository-warehouse HTTPS-URL-to-
mirror-repository-content --trusted-certificate ca_chain.pem
```

For more information about SAS Mirror Manager, see "Create a Mirror Repository" on page 29.

Help with Options

The SAS Orchestration CLI includes several options. To learn about all the options for the SAS Orchestration CLI, use the appropriate command:

Linux or Macintosh

```
./sas-orchestration build --help
```

Windows

```
.\sas-orchestration.exe build --help
```

Store the Deployment Scripts

As a best practice, create a directory where you can store the files that are used to deploy and maintain your software. SAS recommends using **`C:\sas\install`**. This guide assumes that you will use **`C:\sas\install`**. Otherwise, replace those references with the actual location that you select.

Save the deployment scripts to your hard drive.

1. If necessary, move the sas-viya-deployment-script.zip file to the machine where you will deploy your software. The recommended location is **`C:\sas\install`**.

2 In the same directory where you have saved sas-viya-deployment-script.zip, uncompress it.

Deployment Scripts and Security

The deployment scripts that are created by the SAS Orchestration CLI are PowerShell scripts. The PowerShell scripts are not digitally signed because they are created at deployment time based on your software order and the options that you set when you run the SAS Orchestration CLI. If your organization requires that PowerShell scripts be digitally signed, you must sign the created scripts yourself. For information about how to digitally sign PowerShell scripts, see "About Signing" at the Microsoft PowerShell support site.

By default, the deployment scripts bypass any PowerShell security policy that might be set up. However, to enforce a PowerShell security policy:

1 Open one of the multiple .bat files from the uncompressed ZIP file. If you accepted the defaults, those files are located in **`C:\sas\install\powershell-deployment`**.

2 Locate the following line:

```
set ARGS=%ARGS% -ExecutionPolicy Bypass
```

3 Revise the line using one of the following methods:

- Disable the command. Add `rem` (remark) to the beginning of the line.

  ```
  rem set ARGS=%ARGS% -ExecutionPolicy Bypass
  ```

  Later, you can restore the command by removing the remark from the line.
- Delete the line completely.

4 Save and close the .bat file.

5 Repeat these steps for each .bat file in the directory.

Required Ports

The following ports are used by SAS Viya and should be available before you begin to deploy your software. The same ports should also be available for any firewalls that are configured on the operating system or the network.

Table 3.2 Ports to Be Made Available

Process	Required Port	Requires Allowed Inbound Traffic From	Notes
Apache HTTP Server	80 (internal) 443 (external)	anywhere (workstation)	See note below.
Erlang Port Mapper Daemon (epmd) port	4369		
SAS Infrastructure Data Server	5430–5439		For a single server deployment with no failover, ports 5430-5432 must be opened in order to use the PostgreSQL tools, pgAdmin and pgpoolAdmin. Additional standby nodes each get the next available port number sequentially up to 5439.
CAS Server	5570	workstation	Used by clients to make binary connections to CAS.
SAS Message Broker	5672, 15672, 25672		
SAS Studio	7080		Required only for SAS Studio 4.4 and for programming-only deployments.
SAS Configuration Server	8300, 8301, 8302, 8500, 8501		SAS uses HashiCorp Consul as its configuration server. Ports 8301, 8302, and 8600 are open for both UDP and TCP traffic.
Object Spawner	8591		
CAS Server Monitor	8777		Used by clients to make REST HTTP calls to CAS, as with the Python REST interface.

Process	Required Port	Requires Allowed Inbound Traffic From	Notes
SAS Cache Locator	10334		Provide a distributed cache technology for SAS Viya.
SAS Cache Server	14443		Provide a distributed cache technology for SAS Viya.
SAS/CONNECT Spawner management	17541	anywhere (SAS 9.X servers, workstation)	Used to monitor the health of the SAS/CONNECT Spawner
SAS/CONNECT Spawner	17551	anywhere (SAS 9.X servers, workstation)	
SAS Job Execution launcher context	18501–18600		Use a range of ports. The compute server gets the port range from the launcher during start-up and attempts to use an open port in the range.

Note: In order to secure web access to your SAS Viya software, only port 443 (HTTPS) should be open externally on the machine where SAS Viya is deployed, and port 80 should be blocked externally. After the deployment process has completed, port 80 must be open internally. For more information, see Options for Port 80.

If your order included SAS Event Stream Processing, any ports that will be used for ESP servers must be open to HTTP traffic. For more information, see Setting Up and Using the ESP Server in *SAS Event Stream Processing*.

The ports in the ephemeral port range on each machine in the deployment must be open to enable SAS Viya services to communicate. Update the port range. From a command prompt, run the following commands:

```
netsh int ipvn set dynamicport tcp start=32768 num=32767
netsh int ipvn set dynamicport udp start=32768 num=32767
```

where *n* indicates the IP addressing system, either 4 or 6. After you run the command, restart Windows.

You can also use SAS Viya Deployment Assistant for Windows to update the required ports automatically. For more information, see “Evaluate the Kerberos Configuration and Windows Tuning” on page 48.

Tune Your Windows System

Update the Windows Registry

Microsoft recommends performing a system backup before editing the registry.

1. At a command prompt, type `REGEDIT`. The **Registry Editor** opens.
2. Go to the **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`** registry subkey.
3. Add the `DWORD` value with a name of `TcpTimedWaitDelay` and a value of **`30 Decimal`**.
4. Go to the **`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\PriorityControl`** registry subkey.
5. Add the `DWORD` value with a name of `Win32PrioritySeparation` and a value of **`36 decimal`**.
6. Go to the **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters`** registry subkey.
7. Add the following `DWORD` values:

Name	Recommended Value
EnableDynamicBacklog	1 decimal
MinimumDynamicBacklog	20 decimal
MaximumDynamicBacklog	1000 decimal
DynamicBacklogGrowthDelta	10 decimal

   The recommended values specify the number of connections that you want to be available. These values request a minimum of 20 and a maximum of 1000 available connections. The number of available connections is increased by 10 each time

8. Modify the SubSystems registry value.

Note: If you are performing a programming-only deployment, skip this step.

a Go to the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\Windows** registry subkey. Here is an example of the value:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768...
```

b Right-click the `Windows` registry name and select **Modify**. The Edit String window appears.

c Change the value for the third number in the `SharedSection` entry according to 20480. Here is an example of the revised entry:

```
%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,20480 ...
```

9 Click **OK**.

10 Close the **Registry Editor**.

11 Restart Windows.

Additional Tuning Suggestions

The following list includes general recommendations for configuring Windows systems:

- Disable Windows indexing on any directories that are used by SAS software.
- Set Windows performance settings so that background processes are favored.
- Set the maximum power profile in the system BIOS for all systems, except Intel Sandy Bridge.
- Disable the C1E BIOS setting on Dell systems.

Set Environment Variables for SAS Event Stream Processing

You must set several environment variables before you install SAS Event Stream Processing. Some variables are required to support core product features. Others are required only to support optional components and features. If your order did not include SAS Event Stream Processing, you can skip this section.

1 Open the Control Panel from the **Start** menu. Navigate to **System and Security**.

2 Click **System** ⇨ **Advanced System Settings** in the left pane.

The System Properties dialog box appears. Click **Environment Variables**.

3 Click **New** to add the following variable definitions. Or select the variable from the list and click **Edit** to modify an existing variable definition:

Variable	Value
DFESP_HOME	C:\PROGRA~1\SAS\Viya \SASEventStreamProcessingEngine*version* The setting for this variable does not affect the default installation location, which is `C:\Program Files\SAS \Viya`. For *version*, specify the appropriate version of the SAS Event Stream Processing software, such as 6.2. If you installed in a location other than the default, update the path to match the installation directory.
PATH	%PATH%;%DFESP_HOME%\bin;C:\PROGRA~1\SAS \Viya\SASFoundation\sasexe;C:\PROGRA~1\SAS\Viya \SASEventStreamProcessingEngine*version*\ssl\bin For *version*, specify the appropriate version of the SAS Event Stream Processing software, such as 6.2. If you installed in a location other than the default, update the path to match the installation directory.
(Optional) SV_ENABLE_DATA_SHARING	Set to “true” to enable data sharing. This variable disables CSRF protection so that you can embed charts and import data from this instance of SAS Event Stream Processing Streamviewer.
(Optional) PYTHONPATH or PYTHONHOME Enables you to use the Anaconda Python support in SAS Micro Analytic Service.	Add the Python Lib directory to PYTHONPATH. Or set PYTHONHOME to the top-level Python directory: ■ PYTHONPATH=C:\Program Files\Miniconda3\envs \python*version*\Lib ■ PYTHONHOME=C:\Program Files\Miniconda3\envs \python*version*

4 Click **OK** to save your variable settings.

SAS Event Stream Processing includes the internal component SAS Micro Analytic Service. To use the Anaconda Python support in SAS Micro Analytic Service, you must set one of the optional variables listed in the table for your version of Python. For more information, see *SAS Micro Analytic Service: Programming and Administration Guide*, which is available on the SAS Event Stream Processing product page.

4

Installing SAS Viya

Specify Credentials for the cas User Account

Use a deployment script to save the credentials for the cas user account that you created previously. For more information, see “Additional Required User Accounts” on page 19. Be sure to complete these steps before you start the deployment process.

Note: The name for this user account, cas, is recommended. However, you might have selected another name for this account when you created it.

1. Navigate to the directory where you extracted the contents of the sas-viya-deployment-script.zip file that you created using the SAS Orchestration CLI.

   The recommended location is **`C:\sas\install`**.

2. In the **`C:\sas\install\powershell-deployment`** directory, verify the presence of the encryptCasUser.bat script.

   Note: The setup.bat script and the encryptCasUser.bat script must be in the same directory.

3. From that directory, run the following command:

   ```
   .\encryptCasUser.bat
   ```

4. The script prompts you for the user ID and password of the cas user account. Since the cas user account is a domain account, the user name should include the domain.

   ```
   domain-name\user-name
   ```

   The script creates a file named casUser.xml in the same directory.

   Note: Do not delete the casUser.xml file. Deployment components continue to use it after the deployment process has completed. Similarly, do not delete the cas user account. It becomes the owner of the CAS service.

Specify Credentials for the postgres User Account

Note: This section is applicable only if you have a full deployment. If you have a programming-only deployment, skip this section.

Use a deployment script to save the credentials for the postgres user account that you created previously. This user account enables the SAS Infrastructure Data Server, which runs on PostgreSQL, to start automatically. For more information, see "Additional Required User Accounts" on page 19. Be sure to complete these steps before you start the deployment process.

Note: The name for this user account, postgres, is recommended. However, you might have selected another name for this account when you created it.

1. Navigate to the directory where you extracted the contents of the sas-viya-deployment-script.zip file that you created using the SAS Orchestration CLI.

The recommended location is **C:\sas\install**.

2 In the **C:\sas\install\powershell-deployment** directory, verify the presence of the encryptPostgresUser.bat script.

Note: The setup.bat script and the encryptPostgresUser.bat script must be in the same directory.

3 From that directory, run the following command:

```
.\encryptPostgresUser.bat
```

4 The script prompts you for the user ID and password of the postgres user account. If you are using a localhost account, you should provide only the user name. If you are using a domain account, the user name should include the domain name.

domain-name\user-name

As the script runs, it creates a file named postgresUser.xml in the same directory.

Note: Do not delete the postgresUser.xml file. Deployment components continue to use it after the deployment process has completed. Similarly, do not delete the postgres user account.

Modify Deployment Variables

The configuration settings for your deployment are contained in the vars.psd1 file, located at **C:\sas\install**.

Modify the PostgreSQL Settings

Note: This section is applicable only if you have a full deployment. If you have a programming-only deployment, skip this section.

SAS Viya uses PostgreSQL as the SAS Infrastructure Data Server. For SAS Viya 3.5 on Windows, the PostgreSQL deployment consists of one data node. You can modify the settings for the PostgreSQL deployment in the vars.psd1 file.

1 Open the vars.psd1 file in a text editor.

2 Locate the `Postgres invocation definitions` section.

```
# Postgres invocation definitions.
NODE_DATA_ROOT_DIR = "<configDir>\data\sasdatasvrc"
PG_PORT = "5432"
```

3 Replace the default values with the values that you want to use.

```
# Postgres invocation definitions.
NODE_DATA_ROOT_DIR = "PostgreSQL-data-files-directory"
PG_PORT = "port-used-by-clients-for-database-connections"
```

4 Save and close the vars.psd1 file.

Change the CAS Server Monitor Port Number

By default, the SAS Cloud Analytics (CAS) server listens for REST HTTP calls through port 8777. To change the port number:

1 Open the vars.psd1 file in a text editor.

2 Locate the `cas_httpport` variable.

```
# HTTP port in cas.settings file.
cas_httpport = "8777"
```

3 Change the default value to the one that you want to use.

```
# HTTP port in cas.settings file.
cas_httpport = "new-HTTP-port-number"
```

4 Save and close the vars.psd1 file.

Disable Pre-deployment Validation

The setting of the VERIFY_DEPLOYMENT variable determines the extent of the pre-deployment validation that the deployment script performs. If the variable is set to true (the default), the following validation tests occur:

- to verify that the deployment scripts are compatible with the version of the software being installed
- to verify that the version of PowerShell meets the requirements to deploy your software

If the variable is set to false, only the PowerShell version check is performed. To set the variable to false:

1 Open the vars.psd1 file in a text editor.

2 Locate the `VERIFY_DEPLOYMENT` variable.

```
# The option used to turn on/off pre-flight checks.
VERIFY_DEPLOYMENT = "true"
```

3 Change the default value to false.

```
# The option used to turn on/off pre-flight checks.
VERIFY_DEPLOYMENT = "false"
```

4 Save and close the vars.psd1 file.

Change the CAS Server Port Number

By default, clients make binary connections to the CAS server through port 5570. To change the port number:

1. Open the vars.psd1 file in a text editor.
2. Locate the `cas_port` variable.

```
# Port in cas.settings file.
cas_port = "5570"
```

3. Change the default value to the one that you want to use.

```
# Port in cas.settings file.
cas_port = "new-CAS-port-number"
```

4. Save and close the vars.psd1 file.

Modify the Kerberos Settings

To modify your Kerberos configuration settings in order to accurately reflect your system:

1. Open the vars.psd1 file in a text editor.
2. Locate the settings for `kerberos_kdc` and `kerberos_realm`.

```
# Kerberos configuration settings.
kerberos_kdc = ""
kerberos_realm = ""
```

3. For these variables, specify the appropriate values within the quotation marks.
   - For `kerberos_kdc`, use the fully qualified domain name for the Kerberos authentication server.
   - For `kerberos_realm`, use the name of the Kerberos authentication administrative domain. The realm is typically the DNS domain and is specified in all uppercase letters.

   Note: For information about the values to use, contact your system administrator.

   Here is an example:

```
# Port in cas.settings file.
cas_port = "5570"
kerberos_kdc = "ldap.kdc.company.com"
kerberos_realm = "NA.COMPANY.COM"
```

4. Save and close the vars.psd1 file.

Set Up the CAS Data Directory

Note: If you are performing an upgrade, skip this section.

By default, product caslibs are written to **C:\ProgramData\SAS\Viya\data\cas\default**, which is often hosted on a single hard disk drive with limited storage. To ensure proper performance of your SAS solutions, SAS recommends that the CASDATADIR option be configured to point to a high-performance storage platform. Examples of high-performance storage platforms include SAN, NVMe, and multiple drive disk arrays. The storage platform that you use must be owned by the cas user.

Optimizing the performance of the CAS data directory is especially useful for solutions that can be resource-intensive, such as SAS Visual Forecasting, SAS Visual Data Mining and Machine Learning, and SAS Visual Text Analytics.

To set up a different CAS data directory:

1. Open the vars.psd1 file.
2. Add the following line to the end of the file.

   ```
   casdatadir = "path-to-CAS-data-directory"
   ```

   Note: The CAS data directory must be accessible from the CAS controller.

3. Save and close the vars.psd1 file.

Post-Deployment Configuration

After the software has been deployed, you cannot make changes to the configuration using the vars.psd1 file. For information about changing the configuration after deployment, see Reference in *SAS Viya Administration: SAS Cloud Analytic Services*.

Evaluate the Kerberos Configuration and Windows Tuning

SAS Viya Deployment Assistant for Windows is a utility for evaluating an installation of Kerberos to determine whether it meets the requirements for deploying SAS Viya. In addition, a user with the appropriate rights can configure security principals and keytabs, as necessary. Also, the SAS Viya Deployment Assistant for Windows can evaluate whether the host meets the system requirements and has the appropriate system settings.

Requirements for SAS Viya Deployment Assistant for Windows

SAS Viya Deployment Assistant for Windows has the following requirements:

- The Active Directory computer account must be trusted for delegation.
- The following service principals must exist:
  - HTTP/Service Principal Name (SPN)
  - sascas/SPN
- The Kerberos keytab must contain HTTP SPN information.
- The Local Security Policy must grant the service account rights to log on as a service and to replace a process-level token.

Deploy SAS Viya Deployment Assistant for Windows

1. Go to the SAS Viya Deployment Assistant for Windows for SAS Viya 3.5 page.
2. Download the sas-wvda-windows.zip file to the Windows machine where you will deploy your SAS Viya software.
3. Unzip the sas-wvda-windows.zip file in the same location.

Validation Tests

The following is the list of the validation tests that are performed by SAS Viya Deployment Assistant for Windows. Each test is followed by information about manually modifying your host to pass the test. If you prefer that SAS Viya Deployment Assistant for Windows programmatically remediate the issues that it finds, then see “Configure the Kerberos Environment and Tune Windows Programmatically” on page 53.

Operating System

The operating system is a 64-bit environment.
See “Supported Operating Systems” on page 13.

The operating system is a supported version of Microsoft Windows.
See “Supported Operating Systems” on page 13.

Third-Party Software

JAVA_HOME points to a 64-bit version of Java 8.
See "Java Requirements" on page 15.

The installed version of Microsoft .NET Framework is 4.6 or higher.
See "Additional Software Requirements" on page 14.

The installed version of PowerShell is 5.1 or higher.
See "Windows PowerShell Requirements" on page 13.

The Microsoft Visual C++ 2013 Redistributable (x64) is installed.
See "Additional Software Requirements" on page 14.

The Microsoft Visual C++ 2015 Redistributable (x64) is installed.
See "Additional Software Requirements" on page 14.

Active Directory

The host is part of a Windows domain.
Your domain administrator should add the host to a Windows domain.

The host is a member of an Active Directory.
Your Active Directory administrator should add the host to an Active Directory.

The host account for the machine being installed on is trusted for delegation in Active Directory.
Your Active Directory administrator should add the machine to the Trusted for Delegation security policy in Active Directory.

The sascas/Service Principal Name has been added to Active Directory.
Your Active Directory administrator should add the Service Principal Name to Active Directory.

The http/Service Principal Name has been added to Active Directory.
Your Active Directory administrator should add the Service Principal Name to Active Directory.

Additional Users

A cas user account exists on the host.
See "Additional Required User Accounts" on page 19.

The cas user ID and password are valid.
See "Additional Required User Accounts" on page 19.

The cas user and password are encrypted.
See "Specify Credentials for the cas User Account" on page 43.

The cas user account has the Log on as a Service privilege.
See "Additional Required User Accounts" on page 19.

The cas user account has the Replace Process Level Token privilege.
See "Additional Required User Accounts" on page 19.

A PostgreSQL user account exists on the host.
See "Additional Required User Accounts" on page 19.

The PostgreSQL user ID and password are valid.
See "Additional Required User Accounts" on page 19.

The PostgreSQL user and password are encrypted.
See "Specify Credentials for the postgres User Account" on page 44.

The PostgreSQL user account is a member of the local users group and not a local administrator.
See "Additional Required User Accounts" on page 19.

The PostgreSQL user account has the Log on as a Service privilege.
See "Additional Required User Accounts" on page 19.

Tuning

The third parameter of the SharedSystem registry subkey is set to 20480 or greater.
See "Update the Windows Registry" on page 39.

The TcpTimedWaitDelay registry subkey is set to 30.
See "Update the Windows Registry" on page 39.

The Win32PrioritySeparation registry subkey is set to 36.
See "Update the Windows Registry" on page 39.

The TCP ephemeral port range starts with port 32768 or lower.
See "Required Ports" on page 36.

The TCP ephemeral port quantity is 32767 or greater.
See "Required Ports" on page 36.

Certificates

The SAS public code signing certificates are installed.
Note that this required only if you are running PowerShell with an execution policy of AllSigned. See "Install the SAS Signing Certificates" on page 54.

Keytab

The keytab is usable by Java-based services.
The domain or Active Directory administrator needs to create a working keytab file. See "Authentication Requirements" on page 24.

Evaluate Your Windows System

From the directory where you unpacked the ZIP file, use the following command to run the utility:

```
sas-wvda.ps1 -keyTabPath keytab-location -validate option
```

The *keytab-location* is the path to the keytab that contains credentials for the HTTP/*host-name* principal.

Here are the values for the `-validate` option:

adconfig
Validates that the domain entities are correctly configured.

all
Performs all validations.

host
Validates the host configuration.

keytab
Validates that the keytab can be used successfully by kinit. If you use this option, you must also use the `-keyTabPath` option.

postgres
Validates that the postgres service account is correctly configured.

sas
Validates the credentials for the CAS server and PostgreSQL (see "Specify Credentials for the cas User Account" on page 43 and "Specify Credentials for the postgres User Account" on page 44 for more information). It also validates that the CAS server credentials match the account that owns the sascas/*host-name* SPN.

tuning
Validates that the recommended tuning has been applied to this host. (See "Tune Your Windows System" on page 39 for more information.)

If the value for `-validate` is `sas` or `all`, the `-DeployDir` argument must also be used. Here is an example:

```
sas-wvda.ps1 -keyTabPath keytab-location -validate all
-DeployDir path-to-user-XML-files
```

The path that is used should be the path to the postgresUser.xml and casUser.xml files described in "Specify Credentials for the cas User Account" on page 43 and "Specify Credentials for the postgres User Account" on page 44.

The output of this command is a list of the validation tests that were performed and the results (success or failure).

Configure the Kerberos Environment and Tune Windows Programmatically

You can use SAS Viya Deployment Assistant for Windows to remediate any issue that is identified when `-validate` is used.

```
sas-wvda.ps1 -keyTabPath keytab-location -remediate [options-for-addressing-issues]
```

SAS Viya Deployment Assistant for Windows essentially performs a validation using `-validate all` as it remediates the system. When it finds an issue that fails the validation, it attempts to remediate the issue. Here are additional options that can be used with `-remediate`:

-CASAcct <*string*>
If the string is specified, the name of the CAS domain account name will match the string. If the string is not specified, the name will be *`svcAcctPrefix-host-name-CCAS`*. If that is longer than 20 characters, the NETBIOS name will be truncated to 20 characters.

-CASPassword <*string*>
If the string is specified, the password for the CAS domain account will match the string. If the string is not specified, the password will be random.

-cmdFileOnly
Specifies that the utility should not attempt to create Active Directory entities at execution time. Instead, a script will be created to perform any remediation. This can be helpful for situations where the SAS Administrator is a local server administrator but not a domain administrator. The script can be provided to a domain admin. The output of the script is a ZIP file that the domain administrator should return to the SAS administrator for subsequent use during deployment of SAS Viya.

-cmdFilePath <*string*>
Specifies the output path and filename of the command file script.

By default the script will be placed in the current directory and be named SASViyaADEntitySetup.ps1.

-createADEntities
Specifies that the utility should attempt to create any Active Directory entities that are not found.

Note: This flag requires that account running the utility has administrative permission to create and modify accounts in Active Directory.

-createKeytab
Creates the keytab file that contains the HTTP/SPN.

-HTTPAcct <*string*>
If the string is specified, the name of the domain account used by the HTTP service will match the string. If the string is not specified, the name will be *`svcAcctPrefix-host-name-HTTP`*. If that is longer than 20 characters, the NETBIOS name will be truncated to 20 characters.

-HTTPPassword <*string*>
If the string is specified, the password for the domain account used by the HTTP service will match the string. If the string is not specified, the password will be random.

-PostgresAcct <*string*>
If the string is specified, the name of the account for the local PostgreSQL will match the string. If the string is not specified, the name will be `svcAcctPrefixpostgres`.

-PostgresPassword <*string*>
If the string is specified, the local PostgreSQL account password will match the string. If the string is not specified, the password will be random.

pwLength <*Int32*>
The default is 20.

If accounts are created with random passwords, specifies the length of the password.

-pwNumSpecialChars <*Int32*>
The default is 8.

If accounts are created with random passwords, specifies the number of special characters that can be used in the password.

-svcAcctOUName <*string*>
The default is `Default: OU=serviceAccounts`.

If domain accounts are created, specifies the location within the structure of Active Directory to house the accounts. The distinguished names (DNs) for the realm of the host will be added to this string. If the specified location does not exist, the default location for your Active Directory will be used.

-svcAcctPrefix <*string*>
The default is `svc-sas-`

Specifies the account name prefix for all default account names that are created.

-svcAcctSuffix <*string*>
The default is an empty string.

Specifies the account name suffix for all default account names that are created.

Install the SAS Signing Certificates

All PowerShell scripts from SAS are signed using SAS signing certificates. If your PowerShell installation has an execution policy of AllSigned, PowerShell must confirm that those scripts originate from SAS. Therefore, SAS has included signing certificates in the ZIP file that contains the SAS Viya Deployment Assistant for Windows. The certificates must be installed in the TrustedPublisher certificate store on the Windows machine where the scripts will be run.

As an administrator, install the certificates using the following command:

```
certutil -addstore "TrustedPublisher" .\SAS_Code_Signing_Certs.p7b
```

Install SAS Viya

1. Navigate to the `C:\sas\install\` directory where you uncompressed the sas-viya-deployment-script.zip file that you created.
2. Locate the setup.bat file in the `C:\sas\install\powershell-deployment` directory. You can use this file in one of two ways:
   - Right-click the file, and select **Run as Administrator** from the menu. Using this method does not include command options. The software is downloaded and installed on the local machine, then the script configures and starts any necessary services.
   - Open a command prompt (being sure to select **Run as administrator**) from the Windows **Start** menu. Run the following command:

     `setup.bat` *`options`*

     When the command is run without options, the script downloads and installs software on the local machine and then configures and starts any necessary services. Descriptions of the optional flags follow.

     - -install

       Only installs the software and services. If you use this option, the software and services will not be configured and the services will not be started.

     - -config

       Configures the installed software, and configures and starts the services. This option fails if you run the command before the software and services have been installed.

   As the batch job runs, a `\Downloads` folder is created in the directory where you are running the batch script. The software is downloaded from secure repositories to this new folder on your computer.

To conserve space, after the setup.bat script has been run and the deployment is complete, you can delete the .msi files in the `C:\sas\install\powershell-deployment\downloads` directory.

If the deployment process fails, but you are able to recover from the error, be sure to restart the deployment using the appropriate deployment commands. In addition, if you receive a message to reboot during the deployment process, make sure that use the same deployment commands.

5

Post-installation Tasks

Configure Security

Configure Your Environment with SAS Environment Manager

Note: The tasks in this section are applicable if you deployed all of your software. If you deployed the programming interface only, skip this section.

Sign In as the sasboot User

Your SAS environment is deployed with an initial administrator account that is named sasboot. The password for this account has expired by default, so you must reset the password before you can sign in.

To reset the password:

1. Locate the most recent log for the SAS Logon service in the **C:\ProgramData\SAS\Viya\var\log\saslogon\default** directory.
2. Search the log for the characters, **sasboot**.

   Here is a typical message:

   ```
   Reset password for initial user sasboot using link:
   ```

3. Sign in from a URL with this format:

   ```
   https://reverse-proxy-server/SASLogon/reset_password?code=password
   ```

   Make a note of this URL to share with other administrative users of your SAS Viya software, as described in "Share Important Deployment Information with the Administrators" on page 89.

4. Follow the instructions on the web page that is displayed in order to reset the password.

   Note: If the URL has expired, stop and start the SAS Logon Manager Service.

   Then return to the log and obtain the new URL. The URL expires 24 hours after the SAS Logon service restarts. For security purposes, the URL that is specified in a browser or in a text editor also expires, even if the password is not reset.

   After you reset the password, SAS Environment Manager automatically opens in your browser.

5. Click **Yes** to opt in to all the assumable groups so that you have the permissions to perform subsequent tasks.

Configure the Connection to Your Identity Provider

After completing the installation of SAS Viya, you must configure the connection to your identity provider before your users can access SAS Environment Manager and SAS Visual Analytics.

While signed in as sasboot, configure the connection to your identity provider:

Note: Only LDAP-based identity providers are supported. You need to have basic familiarity with LDAP administration. For more information about the properties that

are relevant for this procedure, see "sas.identities.providers.ldap" in *SAS Viya Administration: Configuration Properties*.

1 Select the 🔧 from the side menu to open the Configuration page.

2 On the Configuration page, select **All Services** from the list, and then select the **Identities service** from the list of services.

3 To configure user properties, in the **sas.identities.providers.ldap.user** section, click **New Configuration**:

   a Specify a value for the **baseDN** required field. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

   For each property that represents a user-level field in SAS, specify a corresponding property in the LDAP server software.

   > **TIP** Consider specifying a custom filter to limit the user accounts that SAS Viya returns from your LDAP server.

   b Click **Save**.

4 To configure group properties, in the **sas.identities.providers.ldap.group** section, click **New Configuration**. In the New Configuration window:

   a Specify a value for the **baseDN** required field. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

   For each property that represents a group-level field in SAS, specify a corresponding property in the LDAP server software.

   > **TIP** Consider specifying a custom filter to limit the accounts that SAS Viya returns from your LDAP server.

   b Click **Save**.

5 To configure connection properties, in the **sas.identities.providers.ldap.connection** section, click **New Configuration**. In the New Configuration window:

   a Specify values for the following required fields: **host**, **password**, **port**, **url**, and **userDN**. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

   b Click **Save**.

6 To verify user and group information, from the SAS Environment Manager side menu, select 👥 to open the Users page.

   On the Users page, select **Users** from the list in the toolbar. Your users should appear after a few minutes. It is not necessary to restart any servers or services. Then select **Groups** from the list to display your groups.

7 Verify that user and group information is displayed correctly. If not, make any necessary changes to the identities service properties then restart the Identities and SAS Logon Manager services:

Note: When using the LDAP protocol, passwords are transmitted over the network as clear-text. To secure the deployment, SAS recommends that you configure encrypted LDAP connections. For more information, see Encrypt LDAP Connections in *Encryption in SAS Viya: Data in Motion*.

Set Up Administrative Users

CAUTION
Be sure to complete these steps before you configure Kerberos as the identity provider. Kerberos authentication will prevent you from signing in as sasboot. You will have to use one of these administrative accounts to access the system when Kerberos has been enabled.

While you are signed in to SAS Environment Manager as the sasboot user, set up at least one SAS Administrator user, as follows:

1 On the Users page in SAS Environment Manager, select **Custom Groups** from the list in the toolbar.

2 In the left pane, click **SAS Administrators**.

3 In the **Members** section of the right pane, click , and add one or more members to the group (including your own account, if applicable).

4 Sign out from SAS Environment Manager so that you are no longer signed in as the sasboot user.

5 Test the configuration by signing back in to SAS Environment Manager. If you added your own account to the SAS Administrators group, you can sign in using that account. Otherwise, sign in as one of the administrative users that you have added.

   Open SAS Environment Manager from a URL with the following format:

   `https://reverse-proxy-server/SASEnvironmentManager/`

TIP Because SAS Administrators is an assumable group, the following prompt is displayed: `Do you want to opt in to all of your assumable groups?` Select **Yes** if you want to enable the additional permissions that are associated with the SAS Administrators group. The selection remains in effect until you sign out.

Configure Kerberos

After performing a new SAS Viya deployment, you must configure the connection to Kerberos before your users can access SAS Environment Manager and SAS Visual Analytics. To configure Kerberos, see Configure Kerberos (Windows Full Deployment) in *SAS Viya Administration: Authentication*.

> **IMPORTANT** Complete those steps while you are signed in as the sasboot user. However, be aware that as soon as Kerberos is enabled, the sasboot account can no longer be authenticated. Therefore, it is important that you create at least one SAS Administrator, as explained in "Set Up Administrative Users" on page 60 before you enable Kerberos authentication. Otherwise, you cannot access SAS Viya after Kerberos is enabled.

Sign In Using Kerberos

Open SAS Environment Manager from a URL with the following format:

`https://reverse-proxy-server/SASEnvironmentManager/`

Sign in as one of the SAS Administrators that you set up in "Set Up Administrative Users" on page 60.

Configure the Connection to the Mail Service

After installing a new SAS Viya deployment, you must configure the connection to your mail service. Complete these steps while you are signed in as one of the SAS Administrators.

1. Select the 🔧 from the side menu to open the Configuration page.
2. On the Configuration page, select **All Services** from the list, and then select **Mail service** from the list of services.
3. In the **sas.mail** section, click . In the Edit Configuration window, follow these steps:
   a. Specify a value for the following required fields: **host** and **port**. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.
   b. Click **Save**.
4. (Optional) To enable the health check for the mail service:

a Select the 🔧 from the side menu to open the Configuration page.

b On the Configuration page, select **All Services** from the list, and then select **Mail service** from the list of services.

c In the **management.health.mail** section, click .

d Turn the **enabled** toggle to `on`.

e Click **Save**.

When this toggle is set, health checks will be enabled after the mail service is restarted. If the mail host is not configured or is configured incorrectly, or if it cannot connect to the SMTP mail server, the mail service will indicate it is in a failed state.

Disable the Password Reset Feature and Reset the sasboot Password

When you have finished setting up Kerberos and the initial administrative users, you should reset the password for the sasboot user. For additional security, you can then disable the password reset feature. This action prevents password reset links from being written to the log each time the SASLogon service is restarted.

1 Sign in to SAS Environment Manager as an administrative user and select 🔧 from the side menu to open the Configuration page.

2 On the Configuration page, select **Definitions** from the drop-down list.

3 In the left pane, select **sas.logon.initial**. Then click the **New Configuration** button at the top of the right pane. If a definition already exists, you can select to edit the existing definition.

4 In the New sas.logon.initial Configuration window or the Edit sas.logon.initial Configuration window, set **reset.enabled** to `off`.

5 Click **Save**.

6 Restart the SAS Logon service. For more information, see General Servers and Services: Operate (Windows) in *SAS Viya Administration: General Servers and Services*.

Note: After you disable this feature, you can still change the sasboot password if the existing password is known. Enter the URL for SAS Viya with the path `/SASLogon/change_password`. If you are already signed in as another user, first sign out and then sign back in as sasboot using the current password. You can then complete the steps to change the password.

Configure SAS Viya to Encrypt the LDAP Connection

SAS Viya supports encrypted connections between the LDAP client and server. To configure a secure LDAP connection, see Encrypt LDAP Connections in *Encryption in SAS Viya: Data in Motion*.

Change the Administrative User Password for SAS Message Broker

Note: The tasks in this section are applicable only if you deployed all your software. If you deployed the programming interface only, skip this section.

You must change the administrative user password for SAS Message Broker as soon as possible after you have deployed SAS Viya. When you execute the following steps, the administrative password is updated in SAS Configuration Server (Consul).

1. Using the installer user ID, open a Windows PowerShell with the `Run As Administrator` privilege. Do not use the same PowerShell you used to install your software. If that PowerShell is still open, close it and open a new one.

2. Change to the following directory:

   ```
   cd  C:\Program Files\SAS\Viya\bin
   ```

3. Run the message broker account tool:

   ```
   .\sas-rabbitmq-acct-admin.ps1 change_passwd -t account-type -u user-ID
   -promptpw
   ```

   -t *account-type*
   specifies the account user type, which is always the **`client`** type. The client user has full administrative rights. These rights can change in future releases.

   -u *user-ID*
   identifies the client user ID for SAS Message Broker. By default, the user ID is *sasclient*.

   -promptpw
   prompts for the new password for the client user ID for SAS Message Broker. The password that you enter is hidden, by default.

   Here is an example that changes the password for the default administrative user:

   ```
   .\sas-rabbitmq-acct-admin.ps1 change_passwd -t client -u sasclient -
   promptpw
   ```

4. Open the Services Window.

5 Restart the SAS Message Broker. You must change the administrative user password for SAS Message Broker as soon as possible after you have deployed SAS Viya.

6 Restart all SAS Viya services. Restarting the SAS Viya services activates the changes to the credentials for SAS Message Broker.

For more information, refer to SAS Viya Administration: General Servers and Services.

Configure the Machines

Create a Backup Configuration

The tasks in this section are applicable only if you deployed all your software. If you deployed the programming interface only, skip this section. For information about backing up a programming-only deployment, see Backing Up and Restoring Programming-Only Deployments in *SAS Viya Administration: Backup and Restore*.

1 In SAS Environment Manager, confirm that the DEFAULT_BACKUP_SCHEDULE has been created. For details, see Initial Tasks in the *SAS Viya Administration: Backup and Restore* .

2 Check the logs at **`C:\ProgramData\SAS\Viya\var\log\deploymentBackup\default`** and **`C:\ProgramData\SAS\Viya\var\log\backupagent\default`**. If the following message is in the deploymentBackup log, restart the deploymentBackup service.

```
ServiceSchedule] c.sas.backup.util.BackupScheduleManager  :
service [BACKUP_SCHEDULT_ERROR] Cannot schedule backup since maximum retry attempt
is reached and one of the dependent services is still not running
```

Restart the deploymentBackup service. Confirm that the following message is now in the log:

```
ServiceSchedule] c.sas.backup.util.BackupScheduleManager  :
service Default schedule created for BackupService to run backup job every Sunday 1AM
```

3 Set the sharedVault location and ensure that the permissions on the designated location are set. For details, see Initial Tasks in the *SAS Viya Administration: Backup and Restore* .

4 In SAS Environment Manager, click **Jobs**.

5 Right-click the DEFAULT_BACKUP_SCHEDULE and then select **Run** from the pop-up menu to immediately run the backup.

6 To confirm that the backup ran successfully, in the **Jobs** list, click the **Monitoring** tab.

7 On the **Monitoring** tab of the **Jobs** page, ensure that the jobs are running without any warnings and errors.

(Optional) Create a Local Copy of Documentation

You can configure your software to give your users access to local documentation. Here are two instances where access to local documentation would be useful:

- You have customized your documentation.
- Your SAS system is highly secure, and it does not have access to the internet. Because the SAS documentation is cloud-hosted, it cannot be reached without internet access.

Note: The cloud-hosted SAS documentation is frequently updated. The SAS administrator should refresh the local copy on a regular basis to ensure that your users have up-to-date information.

You can download PDF versions of the documentation, or you can create customized versions of the documentation. Create an HTML page with links to all documents that make up your local documentation collection, and create a link to this page.

To configure local documentation:

1 Access SAS Environment Manager.

2 Select **Configuration** from the left navigation bar.

3 Under the **View** menu, select **Definitions**.

4 Select the sas.htmlcommons definition.

5 Click **New Configuration**.

6 On the New sas.htmlcommons Configuration pane, click **Add Property** to add the following two properties:

   - **additionalHelpMenuUrl** — Specify the path to the HTML page that contains links to your local documentation.
   - **additionalHelpMenuLabel** — Provide a meaningful label for the link that your users can access.

     If you do not provide this parameter, a default label of **Additional Help** is used.

7 Click **Save** on the New htmlcommons Configuration pane.

Users see a new item in the **Help Menu** list, between the **Help Center** and **About** entries. Clicking this link opens the specified HTML page.

Configure Locale and Encoding

Overview

SAS Viya supports most of the SAS session encodings that are available in SAS 9.4. By default, SAS Foundation is configured to use UTF-8 as the SAS session encoding and en_US, for English (United States), as the default SAS LOCALE. You can change the SAS LOCALE option, the ENCODING option, or both options to configure SAS Foundation. For more information, see Data Migration to UTF-8 Encoding in the *SAS 9.4 and SAS Viya Programming Documentation*.

SAS Foundation Configuration

The primary configuration file for SAS Foundation is located in the **`C:\Program Files\SPRE\SASFoundation\sasv9.cfg.`** file. After deployment, this file contains a single option setting:

```
-CONFIG "!SASROOT\nls\u8\sasv9.cfg"
```

The ENCODING and LOCALE options are set in the sasv9.cfg file, which is referenced by the -CONFIG option.

Changing the LOCALE

If you want to use UTF-8 as the SAS Foundation encoding, and you want to change the LOCALE setting, edit the **`C:\ProgramData\SAS\SPRE\SASFoundation\sasv9_local.cfg`** file. Change the LOCALE option setting so that it contains the following line:

```
-LOCALE five-character-POSIX-locale-code
```

Here is an example that sets the LOCALE option to French:

```
-LOCALE fr_FR
```

The POSIX locale must be one that is supported by SAS Foundation. For a list of SAS locales, see the Values for the LOCALE= System Option table in the *National Language Support (NLS): Reference Guide*, and locate the appropriate POSIX locale that you want to use.

Note: The -ENCODING option in the nls/u8/sasv9.cfg file must always be set to UTF-8.

Changing the ENCODING

Before you change the SAS Foundation encoding for SAS Viya, be aware that any character data that you migrate to CAS must be transcoded to UTF-8. The section Data Migration to UTF-8 Encoding in the *SAS 9.4 and SAS Viya Programming Documentation* gives guidelines and features that will help you migrate your data successfully.

If you want to configure SAS Foundation to use a different session encoding, you must modify the `C:\ProgramData\SAS\SPRE\SASFoundation\sasv9_local.cfg` file. You can set the -CONFIG option to a different sasv9.cfg file. Select the sasv9.cfg that contains resources to support the encoding that you want to use.

The following table lists the NLS directories that are included with your SAS Foundation deployment. The table also lists the LOCALE and ENCODING options that are set in the sasv9.cfg file.

Table 5.1 *LOCALE and ENCODING Options*

NLS Subdirectory	Default LOCALE	Default ENCODING
u8	en_US	UTF-8
1d	ja_JP	shift-jis[1]
ar	Arabic	warabic
da	Danish	wlatin1
de	German	wlatin1
en	en_US	wlatin1[1]
es	Spanish	wlatin1
fr	French	wlatin1
hu	Hungarian	wlatin2
it	Italian	wlatin1
iw	Hebrew	whebrew
ja	ja_JP	shift-jis
ko	ko_KR	euc-kr
nl	Dutch	wlatin1
no	Norwegian	wlatin1

NLS Subdirectory	Default LOCALE	Default ENCODING
pb	pt_BR	wlatin1
pl	Polish	wlatin2
pt	Portuguese	wlatin1
ru	Russian	wcyrillic
sv	Swedish	wlatin1
tr	Turkish	wturkish
zh	zh_CN	euc-cn
zt	zh_TW	ms-950

[1]Change the ENCODING option in the sasv9.cfg files in the `nls/1d` or `nls/en` directory. You must choose an encoding that is supported by the option settings in the file. Refer to the list of Windows Encoding Values in the *National Language Support (NLS): Reference Guide*.

- The `nls/en/sasv9.cfg` file includes resources to support single-byte encodings, which are listed in the table that is titled Single-byte Encodings for Windows.
- The `nls/1d/sasv9.cfg` file includes resources that can support double-byte encodings, which are listed in the table that is titled Windows Double-Byte Encodings.
- ENCODING should be set to UTF-8 in the `nls/u8/sasv9.cfg` directory.

If you change the ENCODING option, you must ensure that the locale is compatible with the encoding that you select. The table that is titled Values for the LOCALE= System Option located in the *National Language Support (NLS): Reference Guide* maps the POSIX Locale ID to the Windows encoding that supports characters for the locale.

(Optional) Enable GPU Functionality

The SAS GPU Reservation service aids SAS processes in resource sharing and utilization of the GPUs that are available on a system. It is required if you want to take advantage of additional GPU functionality. A check is performed to detect supported GPUs in the environment. If a GPU is detected, the service is started automatically on that machine.

You can add a GPU to your deployment at a later time. It is not necessary to perform the SAS software deployment again in order to add GPU functionality. However, the initial software deployment must have been performed on the machine. Otherwise, some requirements would not be met.

To enable GPU functionality:

1. Using a user account that has administrator privileges, log on to the machine where the GPU has been installed.
2. Verify that the SAS GPU Reservation service (sasgpud) has been installed in `%ProgramData%\SAS\Viya\etc\sasgpud\default` by a previous deployment.
3. Install the GPU Reservation service as a Windows service. Type `cmd` in the Search window of the Start menu to open a command prompt.
4. Run the following command:

   ```
   C:\ProgramData\SAS\Viya\etc\sasgpud\default\sasgpud.bat install
   ```

5. If that command is successful, run the following command:

   ```
   C:\ProgramData\SAS\Viya\etc\sasgpud\default\sasgpud.bat start
   ```

6. Set the start type of the service to Manual:

   ```
   sc config sas-viya-sasgpud-default start=demand
   ```

The service starts. If the system is restarted, the service restarts automatically.

Configure SAS Data Access

(Optional) Configure Java for the ACCELWHERE Option

> **IMPORTANT** If you want to configure your Java installation to improve Hadoop cluster processing speed, perform these tasks.

The ACCELWHERE option that is available with SAS Scalable Performance Data Engine leverages MapReduce when interacting with HDFS. It improves processing speed by optimizing data subsetting that occurs in the Hadoop cluster. For more information about the ACCELWHERE option, see WHERE Processing Optimization with MapReduce in *SAS 9.4 and SAS Viya Programming Documentation: Storing Data in the Hadoop Distributed File System*.

To enable the ACCELWHERE option for your Java installation:

1. Go to the location where Java is installed. If you are unsure of the location, the value for the JAVA_HOME environment variable is the fully qualified pathname of the top level of the Java directory tree.
2. Determine whether the `JAVA_HOME\lib\tools.jar` file exists. If it exists, then the ACCELWHERE option is already enabled and no further action is required. If it does not exist, continue with these steps to copy a tools.jar file to the appropriate location.
3. At the top level of the JAVA_HOME directory, create a subdirectory named `lib`.

```
mkdir lib
```

4. Find out the version of Java that you are using. Most deployments of Java have a version number in the name of the directory that is used as JAVA_HOME. For example, if the directory is named **`jre1.8.0_144`**, you are using Java version 1.8.0_144. Similarly, if the directory is named **`jdk1.8.0_161`**, you are using Java version 1.8.0_161. If the directory name does not contain a version number, you should consult with your system administrator to find out the version of Java that is installed.

5. Locate a copy of the tools.jar file from the version of the JDK that matches the version of Java that is installed. Here are two methods for locating a copy of the tools.jar file:
   - Download the correct version of the JDK from the Oracle web site and unpack the downloaded file to find the tools.jar file.
   - Look in an existing Java installation for the correct version of the JDK.

6. Copy the located tools.jar file to the `lib` directory that you created.

7. Repeat these steps for each machine that runs SAS software.

Configure SAS Data Science

Software Order Associated with SAS Data Science

One other software order is associated with deploying SAS Data Science. The software order contains SAS Embedded Process for Hadoop and SAS Embedded Process for Teradata on Linux. The Software Order Email (SOE) specifies the location of the deployment documentation: SAS Embedded Process: Deployment Guide. You should deploy this order only if you are using SAS in-Database Technologies for Hadoop or SAS in-Database Technologies for Teradata.

Note: The SOE for the associated order does not refer to SAS Data Science explicitly.

Configure SAS Event Stream Processing

Complete SAS Event Stream Processing Setup

If your order included SAS Event Stream Processing, take a few steps to complete the deployment. Otherwise, you can skip this section.

Enable Metering for ESP Servers

The deployment process applies the product license on each machine where you have deployed SAS Event Stream Processing. However, additional steps are required in order to enable the license. You must set up and run at least one metering server to track the number of incoming events and to maintain event counts.

The metering server aggregates counts that are based on the license, the source window, and the hour of day. It stores aggregated results so that a client can query and track the total volume of messages that are processed. Enabling the metering server ensures that your ESP server is in compliance with the terms of its license. Event metering is not required on development servers because they do not contribute to the event volume that is assigned to a license.

1. Log on to the Windows server as an administrator.
2. Type `cmd` in the Windows Search box. In the search results, right-click **Command Prompt** and select **Run as Administrator**.
3. Run the following command:

   ```
   %DFESP_HOME%\bin\dfesp_metering.bat -d
   ```

   The -d argument creates a log file in the configuration directory.

For more information about the metering server, see Setting Up and Using the Metering Server in the SAS Event Stream Processing user documentation.

Start SAS Event Stream Processing Studio and Log On

Additional steps might be required to use SAS Event Stream Processing Studio, which provides a user interface for creating models. It is automatically started during the installation. However, you can start it manually if you find that the service is not running.

1. Verify that you have set the required environment variables. For more information, see "Set Environment Variables for SAS Event Stream Processing" on page 40.

2. (Optional) Verify that the SAS Event Stream Processing Studio service is running. Click **Start**, and enter *services.msc* in the **Search** box. Select **services.msc** from the search results.

   The **Services** panel is displayed.

3. Scroll through the list of services and locate the **SAS Event Stream Processing Studio** service. If required, click the **Start** link to start the service.

4. When the service is running, you can access the SAS Event Stream Processing Studio user interface from a web browser that is running on Windows or Linux:

   ```
   scheme://reverse-proxy-server/SASEventStreamProcessingStudio
   ```

   In a programming-only deployment, the scheme is http. In a full deployment, the scheme is https.

   For *reverse-proxy-server*, specify the hostname of the machine where you installed SAS Viya.

5. Start the ESP server. For more information, see "Start the ESP Server" on page 72.

Start the ESP Server

When the deployment script has completed, the SAS Event Stream Processing processes are already running. Before you can open or create a model in SAS Event Stream Processing Studio, you must start the ESP server.

If you plan to use SAS Event Stream Manager to manage your environment, take some additional steps to set up a connection between the ESP server and SAS Event Stream Manager when you start the ESP server. For more information, see "Configure the ESP Server for SAS Event Stream Manager" on page 74.

To start an ESP server:

1. Open a command prompt by clicking **Start** and entering *cmd* in the **Search** box.

2. Start the ESP server. Here is an example of the command:

   ```
   %DFESP_HOME%\bin\dfesp_xml_server
   ```

   The values that provide server start-up instructions are defined in the esp-properties.yml configuration file. For more information, see Server Configuration Properties.

3. The following message is displayed:

   ```
   Access control disabled (permissions.yml not present)
   ```

   The file that is referenced is required only to enable access control on the ESP server. You can ignore this message.

For more information about the ESP server, see SAS Event Stream Processing: Setting Up and Using the ESP Server.

Log on to SAS Event Stream Processing Streamviewer

SAS Event Stream Processing Streamviewer is a web-based client that visualizes events that stream through event stream processing models. SAS Event Stream Processing Streamviewer is installed automatically along with SAS Event Stream Processing.

When the deployment process has completed, take the following steps to access SAS Event Stream Processing Streamviewer:

1. The Streamviewer service is started automatically during the deployment. If it is not running, start the service from the Windows Services panel.
2. Open the following URL:

   http://*ESP-server-host-name*/SASEventStreamProcessingStreamviewer

   For *ESP-server-host-name*, substitute the host name of the machine where SAS Event Stream Processing Streamviewer is installed.
3. Enter your user ID and password and click **Sign in**.

When you successfully log on to SAS Event Stream Processing Streamviewer, the home page appears.

Encryption and Authentication Options

SAS Event Stream Processing provides optional encryption and authentication features. You can enable encryption on TCP/IP connections within an event stream processing engine. You can also configure ESP servers to require client authentication for SAS TCP/IP clients.

To enable encryption, the OpenSSL libraries must be installed on all computer systems that run the ESP server and clients. Version 1.0.2 or later of the Transport Layer Security (TLS) Protocol is required in order to take advantage of ECDH support for encryption ciphers used in encrypted connections.

Authentication and encryption apply to the following ESP server APIs:

- The ESP server (XML Server) HTTPS API
  - Connections that are created by a client to communicate with an ESP server
  - Connections that are created by a file and socket connector or adapter that acts as a socket client or server
  - Connections that are created by the SAS Event Stream Processing Streamviewer component (streamviewer.html) to communicate with the ESP server using the HTTPS protocol
- C, Java, or Python Publish/Subscribe API
  - Connections that are created by a client that uses the C, Java, or Python Publish/Subscribe API to communicate with an ESP server

- Connections that are created by an adapter to communicate with an ESP server

Configuration of these security options has been greatly simplified in recent releases of SAS Event Stream Processing. For more information about enabling security for an ESP server or for SAS Event Stream Processing Streamviewer, see SAS Event Stream Processing: Security.

Complete SAS Event Stream Manager Setup

If you plan to use SAS Event Stream Manager, you must complete setup after the installation has completed. Otherwise, skip this section.

Log On to SAS Event Stream Manager

SAS Event Stream Manager is installed in your environment automatically. SAS Event Stream Manager uses SAS Logon Manager for logon functionality.

1. Open SAS Event Stream Manager from a URL with the following format:

   `https://reverse-proxy-server/SASEventStreamManager`

   For *reverse-proxy-server*, use the host name of the machine where the Apache HTTP server is running.

   The Sign In to SAS window is displayed.

2. Enter your user ID and password, and click **Sign In**.

Successful logon to the SAS Event Stream Manager user interface indicates that the software has been installed correctly.

Configure the ESP Server for SAS Event Stream Manager

When the deployment script has completed, the SAS Event Stream Processing processes are already running. Before you can open or create a model in SAS Event Stream Processing Studio, you must start the ESP server.

In addition, to manage SAS Event Stream Processing instances with SAS Event Stream Manager, you must manually locate and define ESP servers that are running in your environment. However, you can start your ESP servers with some additional instructions that enable secure, persistent sockets between SAS Event Stream Manager and ESP servers. If you plan to use SAS Event Stream Manager, the optional steps are recommended.

To start an ESP server:

1. Provide SAS Logon Manager with a client ID and client secret for SAS Event Stream Manager. First, obtain the value of the SAS Configuration Server

(Consul) token for your environment. The Consul token is located in the following directory:

C:\ProgramData\SAS\Viya\etc\SASSecurityCertificateFramework\tokens\consul\default\client.token

2 Run a curl command to request a registration token for a new client. In this example, the client is named app:

Note: Install curl if necessary.

```
curl -X POST "http://localhost/SASLogon/oauth/clients/consul?callback=false&serviceId=app" -H "X-Consul-Token: X-Consul-Token-value"
```

For *X-Consul-Token-value*, substitute the value for the Consul token, which you obtained from the previous step.

Note: Specify the command on a single line. This request must pass a `callback=false` query string parameter and authenticate directly by passing a Consul token. If the Consul token that you specified in the command is valid, SAS Logon Manager returns the OAuth access token for registration in the response.

3 Use the registration token to register the client ID. This step establishes the ESP server as a new client of SAS Logon Manager. Run the following curl command:

```
curl -X POST http://localhost/SASLogon/oauth/clients -H
"Content-Type: application/json"
-H "Authorization: Bearer token-from-previous-step"
    -d '{
         "client_id": "client-id",
         "client_secret": "client-secret",
         "scope": ["openid", "*"],
         "resource_ids": "none",
         "authorities": ["uaa.none"],
         "authorized_grant_types": ["password"]
         }'
```

Note: You can find more information about the required steps to configure a new client for SAS Logon Manager in Obtain an Access Token Using Password Credentials in *SAS Viya Administration: Authentication*.

4 Create an XML file with filename esm.xml. Make sure that it uses the required syntax.

Here is an example:

```
<esm>
a <server name="SAS-Event-Stream-Manager-host">
b      <url>http://reverse-proxy-server</url>
c     <port>port-number</port>
d      <context-path>path-to-SAS-Event-Stream-Manager</context-path>
        <auth>
e             <clientId>client-id</clientId>
f             <clientSecret>client-secret</clientSecret>
```

```
g           <user>user-name</user>
h           <password>password</password>
        </auth>
    </server>
</esm>
```

a For *SAS-Event-Stream-Manager-host*, substitute the host name of the machine where SAS Event Stream Manager is running.

b For *reverse-proxy-server*, substitute the fully-qualified host name of the machine where the SAS Viya HTTP proxy server is running.

c (Optional) For *port-number*, substitute the port where SAS Event Stream Manager is listening. This parameter is only needed if your instance is running without the SAS Viya HTTP proxy service.

d (Optional) For *path-to-SAS-Event-Stream-Manager*, substitute the full path to your instance of SAS Event Stream Manager that is running as a stand-alone product (deployed on a separate machine).

e For *client-id*, substitute the client ID that you provided to SAS Logon Manager for the SAS Event Stream Manager instance.

f For *client-secret*, substitute the client secret that you provided to SAS Logon Manager for SAS Event Stream Manager.

g For *user-name*, substitute a user name for an LDAP user account that is valid for use with SAS Logon Manager.

h For *password*, substitute the password that corresponds to the user account that you specified.

Repeat the `<server></server>` section of the file as many times as required to accommodate all SAS Event Stream Manager servers.

5 Save the file in a network-accessible directory.

6 Open a command prompt by clicking **Start** and entering *cmd* in the **Search** box.

7 Start the ESP server. Here is an example of the command:

```
%DFESP_HOME%\bin\dfesp_xml_server -esm file:\\full-path-to-file
\esm.xml
```

The `-esm file:\\esm.xml` argument instructs the ESP server to read the contents of the esm.xml file. Other values that provide server start-up instructions are defined in the esp-properties.yml configuration file. For more information, see Server Configuration Properties.

8 The following message is displayed:

```
Access control disabled (permissions.yml not present)
```

The file that is referenced is required only to enable access control on the ESP server. You can ignore this message.

When it is started with the optional `-esm file:\\esm.xml` argument, the ESP server automatically registers with SAS Event Stream Manager, which can then manage it. The esm.xml file instructs the ESP server where to locate SAS Event Stream Manager. The ESP server registers itself with SAS Logon Manager as a new client with a new secret. SAS Logon Manager can then provide a token that

enables the ESP server to set up a persistent web socket for secure communications with SAS Event Stream Manager.

For more information about the ESP server, see SAS Event Stream Processing: Setting Up and Using the ESP Server.

6

Validating the Deployment

Verify Access to SAS Logon and SAS Drive

Note: The following information applies only if you are performing a full deployment. If you are performing a programming-only deployment, skip this section.

To verify that you can access SAS Logon and SAS Drive:

1. To verify SAS Logon, open it using a URL with this format:

   `http://reverse-proxy-server/SASLogon`

2. To verify SAS Drive, open it using a URL with this format:

```
http://reverse-proxy-server/SASDrive
```

For more information about SAS Drive, see Introduction to SAS Drive in *SAS Drive*.

Log On to Your Version of SAS Studio

Your version of SAS Studio depends on which type of deployment you performed:

- If you deployed a programming-only environment, your environment contains SAS Studio (Basic).
- If you deployed a full environment, your environment contains both SAS Studio (Basic) and SAS Studio (Enterprise). By default, you log on to SAS Studio (Enterprise) to perform deployment tasks.

To ensure that your default version of SAS Studio has been deployed correctly and is working, log on to it:

1. Open SAS Studio from a URL with this format:
   - or SAS Studio (Basic) in a programming-only environment:

     ```
     http://hostname/SASStudio
     ```

   - For SAS Studio (Enterprise) in a full environment:

     ```
     http://hostname/SASStudioV
     ```

   Make a note of this URL to share with any other users of your SAS Viya software, as described in "Share Important Deployment Information with the Administrators" on page 89.

2. Log on using the credentials for your operating system account.

Note: To log off from SAS Studio, click **Sign Out** on the toolbar. Do not use the **Back** button on your web browser.

SAS Viya File Locations

After the deployment process has completed, default directories will be populated with installation and configuration files. The following table lists default directory and file locations that you can verify as part of deployment validation. The table also describes recommended locations for installation files to assist you in locating them later:

Table 6.1 *Default Directory and File Locations*

Directory Path	Description
`%ProgramFiles%\SAS\Viya`	SAS Viya home directory, which contains the application files. The default location is typically `C:\Program Files\SAS\Viya`.
`%ProgramData%\SAS\Viya`	SAS Viya configuration directory.
`%ProgramFiles%\SAS\SPRE`	Home directory for the SAS Foundation programming runtime environment and files to support SAS 9.4 integration. The default location is typically `C:\Program Files\SAS\SPRE`.
`%USERPROFILE%\sas_repos`	Default location of the SAS software repositories that are created and populated, based on your order, when you create a mirror repository.
`%LOCALAPPDATA%\mirrormgr\mirrormgr.log`	Default location for SAS Mirror Manager logs.
`%ProgramData%\sas\viya\data\cas\default`	Default location for persistent storage for the predefined system caslibs and the Public caslib.
`C:\sas\install`	Recommended location where you can uncompress the sas-viya-deployment-script.zip file. You created this ZIP file when you used the SAS Orchestration CLI to create the deployment scripts.
`C:\sas\install\sas-viya-deployment-script\powershell-deployment`	Location for all files (EXE and BAT) that are required for the deployment. Individual files that provide configuration options are stored in subdirectories of `\powershell-deployment`. When you uncompress the sas-viya-deployment-script.zip file, it creates and populates these subdirectories.
`C:\sas\install\sas-viya-deployment-script\downloads`	Directory that is created automatically when you run the setup.bat script to install SAS Viya. This directory is used for temporary storage of installation files that are downloaded from SAS secure repositories. To conserve space, you can delete the MSI files in the `\downloads` directory after the deployment has been completed.
`%ProgramData%\SAS\Viya\var\log\`*`service`*`\default\*.log`	Directories where logs are generated. For *service*, substitute the name of the microservice, such as Identities, or the name of the service, such as Consul.

Directory Path	Description
`%ProgramData%\SAS\SPRE\var\log\service\default\*.log`	**Note:** The SPRE directories contain files for the SAS Programming Runtime and for the SAS Foundation programming environment.
`%ProgramData%\SAS\Viya\etc\SASSecurityCertificateFramework`	Default location of SAS-provided TLS certificates to enable encryption of data in motion.
`%ProgramData%\SAS\Viya\backup`	Also referred to as "local vault." The location where the backup files for data sources are created. The local vault location cannot be changed. As a last step in the backup process, the contents of the local vault are moved to the shared vault. The SAS Viya administrator sets the location of the shared vault parameter in SAS Environment Manager as a post-deployment step. For more information, see Concepts in *SAS Viya Administration: Backup and Restore*.
`%ProgramData%\SAS\Viya\var\log\deploymentBackup\default` `%ProgramData%\SAS\Viya\var\log\backupagent\default`	Locations for backup activity logs.

Note: The ProgramData directory location might be hidden by default in Microsoft Windows File Explorer.

Access CAS Server Monitor

Note: This section is applicable only if you have a programming-only deployment. If you have a full deployment, skip this section.

To verify that CAS Server Monitor has been successfully deployed, access it by opening a web browser and entering the URL in the address field in the following format:

```
http://reverse-proxy-server/cas-shared-default-http
```

Here is an example:

```
http://host1.sas.com/cas-shared-default-http
```

Log on using one of the SAS Administrator users that you established in "Set Up Administrative Users" on page 60.

Access SAS Environment Manager

Note: This section is applicable only if you have a full deployment. If you have a programming-only deployment, skip this section.

1. Open SAS Environment Manager from a URL with the following format:

   `https://reverse-proxy-server/SASEnvironmentManager/`

2. Sign on as one of the SAS Administrators that you set up in "Set Up Administrative Users" on page 60.

Verify SAS Message Broker

Note: This section is applicable only if you have a full deployment. If you have a programming-only deployment, skip this section.

1. Open a browser and go to the following address:

   Note: For information about resetting credentials, see "Change the Administrative User Password for SAS Message Broker " on page 63.

   - If HTTPS is enabled:

     `https://RabbitMQ-IP-address:15672/#/`

     Note: If you did not add compliant certificates and instead kept the default security settings and certificates, you will see the `Your connection is not private` message. SAS recommends that you replace the certificates before you give end users access to SAS Viya. For details, see HTTPS Access to SAS Message Broker.

   - If HTTP is enabled:

     `http://RabbitMQ-IP-address:15672/#/`

   If the RabbitMQ logon window appears, then SAS Message Broker is functioning as expected.

Verify SAS Infrastructure Data Server

Note: This section is applicable only if you have a full deployment. If you have a programming-only deployment, skip this section.

Use these steps to verify that SAS Infrastructure Data Server has been deployed correctly.

1. Open a Windows PowerShell Integrated Scripting Environment (ISE).
2. Change the directory to the sasdatasvrc script directory. By default, it is the **C:\Program Files\SAS\Viya\libexec\sasdatasvrc\script** directory.

   ```
   cd "C:\Program Files\SAS\Viya\libexec\sasdatasvrc\script"
   ```

3. To verify the database, call the function by running the following command:

   ```
   .\Invoke-PostCheckPostgres.ps1 -batchJob
   ```

   Here are typical results:

   ```
   Config Environment Variable file located:
    C:\ProgramData\SAS\Viya\etc\sasdatasvrc\postgres\node0
   \ConfigEnvironmentVariables.psd1
   abccom16:5432 - accepting connections
   Postgres server check was successful
   ```

Overview of Data Access Verification

Overview

After starting a CAS session, run the SAS code as specified in the verification section for your data connector(s). If any of the verification steps for data access return an error, perform the appropriate configuration steps again.

Verify with SAS Studio 5.2 in a Programming-Only Deployment

To verify the SAS Data Connectors:

1. Open SAS Studio from a URL with this format:

`http://hostname/SASStudio`

2 Log on using the credentials for your operating system account.

3 Start a new CAS session.

   a In the navigation pane, open the **Snippets** section.

   b Select **SAS Snippets** ⇨ **SAS Viya Cloud Analytic Services** .

   c Right-click **Create CAS Connection** and select **Open**. The snippet opens in the code editor.

   In the code, specify the cashost and the casport. (Default is casport of 5570).

   d In the toolbar, click  to run the new CAS session code.

   e Right-click **New CAS Session** and select **Open**. The snippet opens in the code editor.

   f In the toolbar, click  to run the new CAS session code.

Run the SAS code as specified in the verification section for your data connector(s). If any of the verification steps for data access return an error, perform the appropriate configuration steps again.

Verify with SAS Studio 5.2 in a Full Deployment

1 Open SAS Studio from a URL with this format:

`http://hostname/SASStudioV`

2 Log on using the credentials for your operating system account.

3 Start a new CAS session.

   a In the left navigation pane, click on the **Snippets** icon.

   b Select **SAS Snippets** ⇨ **SAS Viya Cloud Analytic Services** .

   c Right-click **New CAS Session** and select **Open**. The snippet opens in the code editor.

   d In the toolbar, click  to run the new CAS session code.

Run the SAS code as specified in the verification section for your data connector(s). If any of the verification steps for data access return an error, perform the appropriate configuration steps again.

Verify SAS/ACCESS Interface to ODBC

Note: The information in this section is applicable only if you ordered SAS/ACCESS Interface to ODBC (on SAS Viya).

1. From SAS Studio, edit and run the following SAS code to verify the SAS/ACCESS to ODBC LIBNAME statement:

   ```
   libname olib odbc dsn="DSN-from-odbc.ini" user="user-ID"
   password="password";
   ```

   If SAS/ACCESS to ODBC was successfully deployed, the execution of the LIBNAME statement returns results without error.

2. From SAS Studio, edit and run the following SAS code to verify SAS Data Connector to ODBC:

   ```
   caslib odbclib datasource=(srctype="odbc", username="user-ID",
   password="password", odbc_dsn="DSN-from-odbc.ini");

   proc casutil;
   list files incaslib="odbclib";
   run;
   ```

   If the data connector was successfully deployed, the results are the names of the tables in ODBC.

If an error was returned on the execution of the LIBNAME statement or no table information was returned for the data connector, you should perform the configuration steps again.

Verify SAS/ACCESS Interface to Snowflake

Note: The information in this section is applicable only if you ordered SAS/ACCESS Interface to Snowflake (on SAS Viya).

To verify that SAS Data Connector to Snowflake was successfully deployed:

1. From SAS Studio, edit and run the following SAS code to verify the SAS/ACCESS to Snowflake LIBNAME statement:

   ```
   libname snowlib sasiosnf server="Snowflake-server-address" user="user-
   ID"
   password="password";
   ```

If SAS/ACCESS to Snowflake was successfully deployed, the execution of the LIBNAME statement returns results without error.

2 From SAS Studio, edit and run the following SAS code to verify SAS Data Connector to Snowflake:

```
caslib snowLib datasource=(srctype="Snowflake", username="user-ID",
password="password",server="Snowflake-server-address",
database="database-name");

proc casutil;
list files incaslib="snowLib";
run;
```

If the data connector was successfully deployed, the results are the names of the tables in ODBC.

7

Completing the Deployment

Share Important Deployment Information with the Administrators

If other persons are responsible for administering your SAS deployment, share the following important information with them:

- The deployment type: Did you deploy the programming interface only, or did you perform a full deployment? The type was determined by whether you used programming-only orchestration (see "Specify the Deployment Type" on page 34).
- The location of the directory on each machine where you stored deployment and maintenance files. For more information about this directory, see "Store the Deployment Scripts" on page 35.
- The URL to access the software: What products did you deploy?
  - If you deployed products from the SAS Event Stream Processing Family, share the URL for SAS Event Stream Processing Studio:

    https://*reverse-proxy-server*/SASEventStreamProcessingStudio.

    Share the following URL for SAS Event Stream Manager:

    https://*reverse-proxy-server*/SASEventStreamManager
  - If you deployed the programming interface only, your administrators should use SAS Studio (Basic). The URL is http://*reverse-proxy-server*/SASStudio.
  - If you performed a full deployment, your administrators should use SAS Environment Manager. You used SAS Environment Manager to configure your environment for a full deployment as described in "Configure Your

Environment with SAS Environment Manager" on page 57. Use the same URL that you used in that section.

Next Steps for SAS Event Stream Processing Users

If your order included SAS Event Stream Processing, you might need to consult some additional documentation. SAS Event Stream Processing provides three client user interfaces and an add-on product:

- Get help using the main product user interface, SAS Event Stream Processing Studio, by reading Using SAS Event Stream Processing Studio.
- SAS Event Stream Processing Streamviewer is a graphical user interface that enables you to visualize events as they stream through event stream processing models. For a complete guide to SAS Event Stream Processing Streamviewer usage, see Using SAS Event Stream Processing Streamviewer.
- If you plan to use SAS Event Stream Manager to automate the deployment of SAS Event Stream Processing projects and monitor their health, start by reading the user documentation. Find a full set of instructions in Using SAS Event Stream Manager.
- If your order included SAS Event Stream Processing for CAS, you now have the option to use an additional CAS action set, espCluster. A second SAS Event Stream Processing action set, loadStreams, is included with all SAS Viya orders. For more information, see Using SAS Event Stream Processing with SAS Cloud Analytic Services Actions.
- Read additional documentation about SAS Event Stream Processing. Links to all SAS Event Stream Processing documentation are available on the SAS Event Stream Processing product page. All product user documentation is also available from the login ID in each client user interface.

SAS has provided examples to help you write SAS Event Stream Processing applications. You can find them on the SAS Support website here.

The examples include files for XML, Python, and Java, with a brief description of each example and its usage. SAS recommends that you copy the files that you require to a writable directory on the local computer so that you can run them.

Refer to Additional Documentation

- To perform initial administrative tasks, see SAS Viya Administration: Initial Tasks.
- To locate administration and additional documentation for solutions and offerings, go to the SAS Viya documentation page:

  http://support.sas.com/documentation/onlinedoc/viya/index.html

- To locate usage information, refer to the Help that is available from the SAS Viya product and administrative interfaces.

8

Managing Your Software

Overview

What Is an Update?

An update replaces some or all of your deployed software with the latest versions of that software. Updated software is intended to be compatible with existing configuration, content, and data. To perform an update, you will run the same tools that were run during the initial deployment. You do not need a new order to perform an update. You might determine that your software needs updating or you might be notified by SAS that updates are available.

What Is an Add-On Product?

An add-on product is new software that you can order and then install with your currently deployed software. You will need a new order for an add-on product.

Because an add-on product is added to the currently deployed software in an environment, you might need to expand your environment's capacity before installing an add-on product.

What Is an Upgrade?

An upgrade adds significant feature changes or improvements to your deployed software. To perform an upgrade, you will run the same tools that were run during the initial deployment. You will need a new order to upgrade your deployed software. Add-on products that are included in the order are installed as part of the upgrade process. An upgrade might require changes to the deployed software's configuration.

You might determine that your software needs upgrading or you might be notified by SAS that upgrades are available. SAS recommends creating a backup of the deployed software environment before performing an upgrade.

Updating Your SAS Viya Software

Overview

IMPORTANT After 15 November 2022, the first update to your deployment will cause the existing encryption, MD5, to be changed to scram-sha-256. The database users' passwords deployed by SAS Viya will be converted to scram-sha-256 as well. If your deployment uses any database users that were not deployed by SAS Viya, you must change the hashing of those database users' passwords manually.

An update replaces some or all of your deployed software with the latest versions of that software. You perform the update with the same command that was used to install SAS Viya and use the same software order.

- To see what updates are available for your deployed software, go to the SAS Viya Hot Fix Availability web page at https://tshf.sas.com/techsup/download/hotfix/HF2/Viya_home.html.
- If you are updating a SAS Viya deployment that used a mirror repository and you want to use a mirror repository again, download the current version of SAS Mirror Manager. For more information, see "Create a Mirror Repository" on page 29.
- You can update your deployment from programming-only to full. See "Update the Deployment Type" on page 99.
- SAS Data Science is deployed as programming-only. However, to obtain the visual interface for the components of SAS Data Science, different products must be licensed. The resulting order should be deployed using the instructions in "Add to Your SAS Viya Software" on page 100. Contact your SAS account representative to determine the exact products that are required.

An outage period is required during which all SAS Viya services must be stopped and then restarted.

Note: The process preserves any user-modified configuration values in the vars.psd1 file, but changes made to other files in the deployment might be lost. Therefore, SAS recommends that you make changes to vars.psd1 when possible in order to avoid any loss of customizations that you made to other files.

Before you begin, review the Chapter 1, "Introduction," on page 1, the Chapter 2, "System Requirements," on page 7, and and Chapter 3, "Pre-installation Tasks," on page 29 chapters of this guide.

You will need the location of the directory on each machine where you stored deployment and maintenance files. For more information about this directory, see "Store the Deployment Scripts" on page 35.

See SAS Note 64084 to determine whether a symbolic link was used during your deployment of SAS Viya to place the configuration files into a location other than the default `%ProgramData%\SAS` directory. Refer to SAS Note 64084 before performing the tasks in this section if a symbolic link was used for your deployment.

If you are using a PDF version of this guide, go to the Deployment Guides web page at https://support.sas.com/en/documentation/install-center/sas-viya/deployment-guides.html and verify that you have the latest version of the deployment documentation before you start the update process. The release date of each document is located in the bottom right corner of the front page.

User Requirements

You must have administrator privileges for the machine.

(Optional) List the Packages That Are Available for Update

Deployments without a Mirror Repository

To list the packages that are available for the update process:

1. To list the packages that are available for the update process, run the following command:

   ```
   setup.bat -update
   ```

   Available updates are displayed, followed by a prompt.

2. At the prompt `Do you wish to download updates? [yes/no]`, review the available updates and then enter `no`.

Deployments with a Mirror Repository

IMPORTANT How you list packages for deployments with a mirror repository depends on whether you have internet access.

With Internet Access

To list packages in a mirror repository in a deployment with internet access:

1. To list the packages that are available for the update process, run the following command on the machine where the mirror repository is located:

   ```
   mirrormgr mirror diff --deployment-data path-to-deployment-zip-file-from-SOE
   --path path-to-mirror-destination --latest
   ```

2. To synchronize the deployment's mirror repository with the SAS mirror repository, run the following command on the machine where the mirror repository is located:

   ```
   mirrormgr mirror --deployment-data path-to-deployment-zip-file-from-SOE
   --path path-to-mirror-destination --latest
   ```

Without Internet Access

To list packages in a mirror repository in a deployment without internet access:

1. To list the packages that are available for the update process, run the following command on the machine where the connected mirror repository is located:

   ```
   mirrormgr mirror diff --deployment-data path-to-deployment-zip-file-from-SOE
   --path path-to-mirror-destination --latest
   ```

2. Before performing an update, synchronize the mirror repository with SAS. To synchronize, run the following command on the machine where the connected mirror repository is located:

   ```
   mirrormgr mirror --deployment-data path-to-deployment-zip-file-from-SOE
   --path path-to-mirror-destination --latest
   ```

3. Move the files from the machine where the connected mirror repository is located to the machine where the unconnected mirror repository is located.

Prepare to Update SAS Viya Software

If you did not perform the original deployment, or if the passwords for the cas or postgres accounts have changed, you must regenerate the casUser.xml and postgresUser.xml files using the encryptCasUser.bat and encryptPostgresUser.bat scripts, as appropriate. See "Specify Credentials for the cas User Account" on page 43 and "Specify Credentials for the postgres User Account" on page 44.

Update Your SAS Viya Software

To update a SAS Viya deployment on Windows, perform one of the following two options for each Windows machine in the deployment.

Review Available Updates Before Updating

1. Stop all SAS Viya services. For more information, see Start and Stop Servers and Services in *General Servers and Services:SAS Viya Administration*.
2. To verify that the Windows deployment is correctly configured:
   a. Download and install the current version of SAS Viya Deployment Assistant for Windows. See "Deploy SAS Viya Deployment Assistant for Windows" on page 49.
   b. To programmatically remediate settings in your Windows deployment, run the SAS Viya Deployment Assistant for Windows using `-remediate` in the command line. See "Configure the Kerberos Environment and Tune Windows Programmatically" on page 53.
3. To list the packages that are available for the update process, run the following command:

   ```
   setup.bat -update
   ```

4. If no updates are available, the following prompt is displayed:

   ```
   No updates available
   Press any key to continue . . .
   ```

   Press any key to exit the update prompt.

5. If updates are available, a prompt similar to the following example is displayed:

   ```
   Updates found:
   Package                 Installed Version ->       Update Version
   msiespstvwr                       5.3.0.1 ->              5.3.1.1
   Do you wish to download updates? [yes/no]
   ```

6. To download and install the updates, enter `yes`.
7. The following prompt is displayed:

   ```
   Downloading packages...
   Downloading msiespstvwr
   Download complete
   Install complete.
   Press any key to continue . . .
   ```

   Press any key to exit the update prompt.

8. To configure the updated products and start all of the services:

   ```
   setup.bat -config
   ```

Update without Reviewing Available Updates

1. Stop all SAS Viya services. For more information, see General Servers and Services: Operate (Windows) in *SAS Viya Administration: General Servers and Services*.
2. To verify that the Windows deployment is correctly configured:
   a. Download and install the current version of SAS Viya Deployment Assistant for Windows. See "Deploy SAS Viya Deployment Assistant for Windows" on page 49.
   b. To programmatically remediate settings in your Windows deployment, run the SAS Viya Deployment Assistant for Windows using `-remediate` in the command line. See "Configure the Kerberos Environment and Tune Windows Programmatically" on page 53.
3. Run the following command:

   ```
   setup.bat -update -noprompt
   ```

   Available updates are displayed, downloaded, and installed.
4. To configure the updated products and start all of the services, run the following command:

   ```
   setup.bat -config
   ```

Update the Deployment Type

You can update your deployment from programming-only to full.

Note: If you make changes to the proxy.conf file and then rerun the deployment script, those changes are overwritten. A copy of the proxy.conf should be created in the **`/etc/httpd/conf.d`** directory when you rerun the deployment script. Use this copy with the instructions inChapter 5, "Post-installation Tasks," on page 57 to make changes to the updated proxy.conf file.

To update a SAS Viya deployment from programming-only to full:

1. Complete the task in "Create the Deployment Scripts" on page 33.

   Note: Do not select the programming-only option in the SAS Orchestration CLI when generating the new playbook. The default deployment script that is generated is for a full deployment.

2 To change from a programming-only deployment to a full deployment, complete the configuration for the visual attributes of the deployment. For more information, see Chapter 5, “Post-installation Tasks,” on page 57.

Note: When the programming-only interface is deployed, SAS Studio is accessible on port 7080. However, when updating from a programming-only deployment to a full deployment, SAS Studio uses a dynamically assigned port.

Add to Your SAS Viya Software

Overview

IMPORTANT After 15 November 2022, the first update to your deployment will cause the existing encryption, MD5, to be changed to scram-sha-256. The database users' passwords deployed by SAS Viya will be converted to scram-sha-256 as well. If your deployment uses any database users that were not deployed by SAS Viya, you must change the hashing of those database users' passwords manually.

Here are some common scenarios for adding SAS Viya software to your existing deployment:

- Adding new software from your initial SAS Viya order

  You ordered software and did not install all of it.

- Deploying additional software from a new SAS Viya order

  The additional software is not a part of your original SAS Viya order. You might have made another order and now have to download and deploy the new order.

An outage period is required during which all SAS Viya services must be stopped and then restarted.

Note: The process preserves any user-modified configuration values in the vars.psd1 file, but changes made to other files in the deployment might be lost. Therefore, SAS recommends that you make changes to vars.psd1 when possible in order to avoid any loss of customizations that you made to other files.

Note: To preserve data from the current deployment, verify that the settings in the vards.psd1 file for the new deployment scripts match the values that are used in the current deployment. Variable `NODE_DATA_ROOT_DIR` contains the location of the database that stores data that includes reports, authorization rules, and user preferences. Therefore, if the new value for `NODE_DATA_ROOT_DIR` is different from the previous value of this variable, then the prior data will not be available in the new deployment. If the optional setting for the variable `casdatadir` was used in the

current deployment, be sure to include this setting in the vars.psd1 file of the new deployment scripts.

Before you begin, you should review the Chapter 1, “Introduction,” on page 1, the Chapter 2, “System Requirements,” on page 7, and and Chapter 3, “Pre-installation Tasks,” on page 29 chapters of this guide.

You will need the location of the directory on each machine where you stored deployment and maintenance files. For more information about this directory, see “Store the Deployment Scripts” on page 35.

See SAS Note 64084 to determine whether a symbolic link was used during your deployment of SAS Viya to place the configuration files into a location other than the default `%ProgramData%\SAS` directory. Refer to SAS Note 64084 before performing the tasks in this section if a symbolic link was used for your deployment.

If you are using a PDF version of this guide, go to the Deployment Guides web page at https://support.sas.com/en/documentation/install-center/sas-viya/deployment-guides.html and verify that you have the latest version of the deployment documentation before you start the update process. The release date of each document is located in the bottom right corner of the front page.

User Requirements

You must have administrator privileges for the machine.

Prepare to Add SAS Viya Software

SAS recommends that you create a backup of the deployed software environment before adding SAS Viya software to an existing deployment.

To prepare to add SAS Viya software:

1. If you did not perform the original deployment, or if the passwords for the cas or postgres accounts have changed, you must regenerate the casUser.xml and postgresUser.xml files using the encryptCasUser.bat and encryptPostgresUser.bat scripts, as appropriate. See “Specify Credentials for the cas User Account” on page 43 and “Specify Credentials for the postgres User Account” on page 44.

2. If you are adding SAS Viya software to a SAS Viya deployment that used a mirror repository and you want to use a mirror repository again, download the current version of SAS Mirror Manager. For more information, see “Create a Mirror Repository” on page 29.

3. When you add SAS Viya software, you receive a new Software Order Email (SOE) from SAS. Use your SOE to download the SAS Orchestration CLI.

4. Using the SAS Orchestration CLI that you downloaded, create new deployment scripts using the instructions on the SAS Orchestration Command Line Interface (CLI) download site. For more information, see “Create the Deployment Scripts” on page 33.

5 Extract the new deployment scripts to a location that is different from that of your original deployment scripts. For example, if you extracted your original deployment scripts to `C:\ProgramData\SAS`, you might extract the new deployment scripts to `C:\ProgramData\SASasddon` instead. Extract the new deployment scripts to a location that is different from the one that you used for your deployment for these reasons:

   - To preserve the original vars.psd1 file.
   - To ensure that the directory that contains the deployment scripts correctly reflects what is delivered. If the new deployment scripts are accidentally extracted over existing deployment scripts, the files that were removed in the new deployment scripts would still be available and could negatively affect the process for researching and resolving deployment issues.

   To extract the new deployment scripts, see "Create the Deployment Scripts" on page 33.

6 Copy the casUser.xml and postgresUser.xml files that are used to store the encrypted passwords for the cas and postgres user accounts from the previously generated deployment scripting directory to the newly generated deployment scripting directory.

7 Follow the steps that are described in "Tune Your Windows System" on page 39 on the target machine before starting the add SAS Viya software process.

8 System requirements for RAM, CPU, and disk space are likely to change with each SAS Viya release. Verify that your environment meets the requirements that are listed in Chapter 2, "System Requirements," on page 7.

Merge the User-Modified Files

Merging user-modified files includes the following actions:

- compare the existing deployment's vars.psd1 file with the new vars.psd1 file
- find any post-deployment edits in the existing deployment's vars.psd1 file
- update the new vars.psd1 file with any post-deployment edits in the existing deployment's vars.psd1 file

You will find or create original, unedited versions of the vars.psd1 file from the original deployment. You will compare the three vars.psd1 files described here and edit the new vars.psd1 file.

This guide refers to the three types of vars.psd1 files as follows:

- vars_original.psd1 — the vars.psd1 file for the original SAS Viya deployment as it was received from SAS or created by SAS tools.
- vars_current.psd1 — the vars.psd1 file for your current SAS Viya deployment that might contain post-deployment edits.
- vars.psd1 — the new vars.psd1 file as it was received from SAS or created by SAS tools.

To merge the user-modified files:

1. Locate the existing vars.psd1 for your current SAS Viya deployment that might contain post-deployment edits, and save a copy of the file by renaming the file as vars_current.psd1.
2. Perform one of the two following steps:
   - If you have the original and unedited vars.psd1 that was generated by the SAS Viya Orchestration CLI during the original deployment, copy that unedited vars.psd1 file and save it with the name vars_original.psd1.
   - Otherwise, run the SAS Viya Orchestration CLI from the original deployment to create new and unedited SAS Viya deployment scripts using the original SOE attachments. Extract the vars.psd1 from the newly created deployment scripts. Name it vars_original.psd1.
3. Compare the file that is currently in use, vars_current.psd1, to the new file, vars.psd1.
4. Make a list of any variables that are present in vars_current.psd1 that are not present in vars.psd1.
5. Compare the list of variables that you made to vars_original.psd1.
   - Any variable in the list that is not present in vars_original.psd1 is probably a customization that you want to retain. Add the variable to vars.psd1.
   - Any variable in the list that is present only in vars_original.psd1 represents a deprecated variable. Do not add these variables to vars.psd1.
6. If you created a sitedefault.yml in the previous deployment, copy it to `sitedefault_original.yml` to use as reference for any future deployments.

   Note: Do not edit sitedefault.yml or sitedefault_original.yml.

7. If TLS is enabled for the Windows deployment, perform the following steps.
   a. To preserve the output of the Enable-CAS-TLS.ps1 script, in **`C:\ProgramData\SAS\Viya\etc\cas\default`**, locate the following environment variables in casconfig.lua:

   ```
   env.CAS_CLIENT_SSL_REQUIRED=true
   env.CAS_CLIENT_SSL_CERTSERIAL="190000AB8122B4DEC1D0AD1A7800000000AB5
   7"
   env.CAS_CLIENT_SSL_CERTISS="Company SHA2 Issuing CA02"
   ```

   b. Copy these environment variables and their values from casconfig.lua to the end of the casconfig_usermods.lua file, also located in **`C:\ProgramData\SAS\Viya\etc\cas\default`**.

   For information about the Enable-CAS-TLS.ps1 script, see Configure CAS TLS to Use SAS Viya Default Certificates (Windows) in *Data in Motion: SAS Viya Administration*.

Add SAS Viya Software

To add SAS Viya software and update a SAS Viya deployment:

1. Stop all SAS Viya services. For more information, see General Servers and Services: Operate (Windows) in *General Servers and Services: SAS Viya Administration*.

2. If you have deployed SAS Event Stream Processing, perform the following steps:

   a. Stop the SAS Event Stream Processing Studio service from the Windows Services panel.

   b. If Streamviewer 5.2 is part of the current deployment, stop the Streamviewer 5.2 process:

   ```
   dfesp_xml_client -url "http://host-name:http-port/exit"
   ```

   Replace *host-name* with the host name of the machine where Streamviewer 5.2 is running.

   Replace *http-port* with the port number that you provided when you started Streamviewer 5.2 with the start-up script. For more information, see Examples for Starting Streamviewer on Windows.

   c. Stop the metering server:

   ```
   dfesp_xml_client -url "http://host-name:port/SASESP/exit"
   ```

   Replace *host-name:port* with the host name and port of the machine where the metering server is running. By default, it uses port 31001.

3. Complete the tasks in "Data Source and Storage Requirements" on page 17, as appropriate.

4. To verify that the Windows deployment is correctly configured:

   a. Download and install the current version of SAS Viya Deployment Assistant for Windows. See "Deploy SAS Viya Deployment Assistant for Windows" on page 49.

   b. To programmatically remediate settings in your Windows deployment, run the SAS Viya Deployment Assistant for Windows using `-remediate`in the command line. See "Configure the Kerberos Environment and Tune Windows Programmatically" on page 53.

5. Run the following command:

   ```
   setup.bat
   ```

   Available updates and newly added products are downloaded and installed.

6. If any SAS Viya services are running, the following message is displayed:

   ```
   Viya services are still running.
   Please shut down all Viya services before an install or update.
   See 'General Servers and Services: Start and Stop All Servers and
   Services' in the 'SAS Viya Administration' documentation for
   instructions on shutting down Viya services.
   ```

   Stop all services as described in Step 1 on page 104, and then run `setup.bat`.

7. At the end of the process, one of the following events occurs:

   - If a reboot is not required, setup.bat exits to a prompt.
   - If a reboot is required, the following message is displayed:

```
You must reboot in order to complete install
```

Reboot the machine, and then run `setup.bat -config` to configure the new products and start all of the services.

8 After you install the software, complete the post-installation tasks that are appropriate for your deployment.

   a "Configure the Connection to the Mail Service" on page 61.

   b If SAS Event Stream Processing was added, set environment variables for SAS Event Stream Processing on page 40 and complete SAS Event Stream Processing setup on page 71.

   c If the output of the Enable-CAS-TLS.ps1 script was not preserved as shown in Step 7 on page 103, and TLS needs to be enabled, re-run the Enable-CAS-TLS.ps1 script. See Configure CAS TLS to Use SAS Viya Default Certificates (Windows) in *Data in Motion: SAS Viya Administration*.

   d If the default Apache HTTP Server certificates were replaced by custom certificates, then add the CA root certificate and intermediate certificates to the SAS Viya truststores. To add the certificates to the truststore, see Add Certificates to the Trustedcerts Files in *Data in Motion: SAS Viya Administration*.

   e If the default CAS TLS certificates were replaced by custom certificates, then add the CA root certificate and intermediate certificates to the SAS Viya truststores. To add the certificates to the truststore, see Add Certificates to the Trustedcerts Files in *Data in Motion: SAS Viya Administration*.

   f See Chapter 6, "Validating the Deployment," on page 79.

   g See Chapter 7, "Completing the Deployment," on page 89.

   h Configure additional SAS products as appropriate.

9 To access the software changes that were added to your deployment, users must log back in to any running SAS Studio session or CAS session. If the data mining service is deployed, restart all data mining service instances.

Upgrade to PostgreSQL Version 15

PostgreSQL no longer releases security patches nor bug fixes for PostgreSQL 9.4 and 11. See PostgreSQL's Versioning Policy for more information.

SAS strongly recommends that you upgrade your PostgreSQL to version 15, which is available in the November 2023 release of SAS Viya 3.5. To determine if you have already downloaded or deployed PostgreSQL 15, see SAS Note 70482.

For the instructions to upgrade PostgreSQL, see Upgrading PostgreSQL in SAS Viya in *SAS Viya Administration: Infrastructure Servers*.

Upgrading Your SAS Viya Software

Overview

IMPORTANT After 15 November 2022, upgrading to SAS Viya 3.5 will cause the existing encryption, MD5, to be changed to scram-sha-256. The database users' passwords deployed by SAS Viya will be converted to scram-sha-256 as well. If your deployment uses any database users that were not deployed by SAS Viya, you must change the hashing of those database users' passwords manually.

An upgrade adds significant feature changes or improvements to your deployed software. To perform an upgrade, you will run the same tools that were run during the initial deployment. You will need a new software order to upgrade your deployed software. An upgrade might require changes to the deployed software's configuration.

You might determine that your software needs to be upgraded or you might be notified by SAS that upgrades are available.

Add-on products that are present in the order are installed as part of the upgrade process.

An outage period is required during which all SAS Viya services must be stopped and then restarted.

This chapter includes all the steps that are required for the upgrade process regardless of the version of the source environment or the software installed.

Note: The process preserves any user-modified configuration values in the vars.psd1 file, but changes made to other files in the deployment might be lost. Therefore, SAS recommends that you make changes to vars.psd1 when possible in order to avoid any loss of customizations that you made to other files.

Note: To preserve data from the current deployment, verify that the settings in the vards.psd1 file for the new deployment scripts match the values that are used in the current deployment. Variable `NODE_DATA_ROOT_DIR` contains the location of the database that stores data that includes reports, authorization rules, and user preferences. Therefore, if the new value for `NODE_DATA_ROOT_DIR` is different from the previous value of this variable, then the prior data will not be available in the new deployment. If the optional setting for the variable `casdatadir` was used in the current deployment, be sure to include this setting in the vars.psd1 file of the new deployment scripts.

Before you start the upgrade, it is recommended that you review all the steps to determine the tasks that are applicable to your deployed software. During your

review, identify the tasks that can be performed before a scheduled outage and those that must be performed during a scheduled outage.

First, review the Chapter 1, “Introduction,” on page 1, the Chapter 2, “System Requirements,” on page 7, and and Chapter 3, “Pre-installation Tasks,” on page 29 chapters of this guide.

You will need the location of the directory on each machine where you stored deployment and maintenance files. For more information about this directory, see “Create the Deployment Scripts” on page 33.

See SAS Note 64084 to determine whether a symbolic link was used during your deployment of SAS Viya to place the configuration files into a location other than the default `%ProgramData%\SAS` directory. Refer to SAS Note 64084 before performing the tasks in this section if a symbolic link was used for your deployment.

If you are using a PDF version of this guide, go to the Deployment Guides web page at https://support.sas.com/en/documentation/install-center/sas-viya/deployment-guides.html and verify that you have the latest version of the deployment documentation before you start the upgrade process. The release date of each document is located in the bottom right corner of the front page.

User Requirements

You must have administrator privileges for the machine.

Prepare to Upgrade SAS Viya Software

SAS recommends that you create a backup of the deployed software environment before performing an upgrade.

To prepare to upgrade a SAS Viya deployment:

1. If you did not perform the original deployment, or if the passwords for the cas or postgres accounts have changed, you must regenerate the casUser.xml and postgresUser.xml files using the respective encryptCasUser.bat and encryptPostgresUser.bat scripts, as appropriate. See “Specify Credentials for the cas User Account” on page 43 and “Specify Credentials for the postgres User Account” on page 44.

2. If you are upgrading a SAS Viya deployment that used a mirror repository and you want to use a mirror repository again, download the current version of SAS Mirror Manager. For more information, see “Create a Mirror Repository” on page 29.

3. When you upgrade SAS Viya, you receive a new Software Order Email (SOE) from SAS. Use your SOE to download the SAS Orchestration CLI.

4. Using the SAS Orchestration CLI that you downloaded, create new deployment scripts using the instructions on the SAS Orchestration Command Line Interface (CLI) download site. For more information, see “Create the Deployment Scripts” on page 33.

5 Extract the new deployment scripts to a location that is different from that of your original deployment scripts. For example, if you extracted your original deployment scripts to `C:\ProgramData\SAS`, you might extract the new deployment scripts to `C:\ProgramData\SASupgrade` instead. Extract the new deployment scripts to a location that is different from the one that you used for your deployment for these reasons:

   - To preserve the original vars.psd1 file.
   - To ensure that the directory that contains the deployment scripts correctly reflects what is delivered. If the new deployment scripts are accidentally extracted over existing deployment scripts, the files that were removed in the new deployment scripts would still be available and could negatively affect the process for researching and resolving deployment issues.

   To extract the new deployment scripts, see "Create the Deployment Scripts" on page 33.

6 Copy the casUser.xml and postgresUser.xml files, which are used to store the encrypted passwords for the cas and postgres user accounts, from the previously generated deployment scripting directory to the newly generated deployment scripting directory.

7 Follow the steps that are described in "Tune Your Windows System" on page 39 on the target machine before starting the upgrade process.

8 System requirements for RAM, CPU, and disk space are likely to change with each SAS Viya release. Verify that your environment meets the requirements that are listed in Chapter 2, "System Requirements," on page 7.

Merge the User-Modified Files

Merging user-modified files includes the following actions:

- compare the existing deployment's vars.psd1 file with the new vars.psd1 file
- find any post-deployment edits in the existing deployment's vars.psd1 file
- update the new vars.psd1 file with any post-deployment edits in the existing deployment's vars.psd1 file

You will find or create original, unedited versions of the vars.psd1 file from the original deployment. You will compare the three vars.psd1 files described here and edit the vars.psd1 file for the upgrade.

This guide refers to the three types of vars.psd1 files as follows:

- vars_original.psd1 — the vars.psd1 file for the original deployment as it was received from SAS or created by SAS tools.
- vars_current.psd1 — the vars.psd1 file for your current deployment that might contain post-deployment edits.
- vars.psd1 — the vars.psd1 file for the deployment as it was received from SAS or created by SAS tools.

To merge the user-modified files:

1. Locate the existing vars.psd1 for your current deployment that might contain post-deployment edits, and save a copy of the file by renaming the file as vars_current.psd1.
2. Perform one of the two following steps:
   - If you have the original and unedited vars.psd1 that was generated by the SAS Orchestration CLI during the original deployment, copy that unedited vars.psd1 file and save it with the name vars_original.psd1.
   - Otherwise, run the SAS Orchestration CLI from the original deployment to create new and unedited deployment scripts using the original SOE attachments. Extract the vars.psd1 from the newly created deployment scripts. Name it vars_original.psd1.
3. Compare the file that is currently in use, vars_current.psd1, to the file from the deployment scripts, vars.psd1.
4. Make a list of any variables that are present in vars_current.psd1 that are not present in vars.psd1.
5. Compare the list of variables that you made to vars_original.psd1.
   - Any variable in the list that is not present in vars_original.psd1 is probably a customization that you want to retain. Add the variable to vars.psd1.
   - Any variable in the list that is present only in vars_original.psd1 represents a deprecated variable. Do not add these variables to vars.psd1.
6. If you created a sitedefault.yml in the previous deployment, copy it to `sitedefault_original.yml` to use as reference for any future deployments.

   Note: Do not edit sitedefault.yml or sitedefault_original.yml.

7. If TLS is enabled for the Windows deployment, perform the following steps.
   a. To preserve the output of the Enable-CAS-TLS.ps1 script, in **`C:\ProgramData\SAS\Viya\etc\cas\default`**, locate the following environment variables in casconfig.lua:

      ```
      env.CAS_CLIENT_SSL_REQUIRED=true
      env.CAS_CLIENT_SSL_CERTSERIAL="190000AB8122B4DEC1D0AD1A7800000000AB5
      7"
      env.CAS_CLIENT_SSL_CERTISS="Company SHA2 Issuing CA02"
      ```

   b. Copy these environment variables and their values from casconfig.lua to the end of the casconfig_usermods.lua file, also located in **`C:\ProgramData\SAS\Viya\etc\cas\default`**.

      For information about the Enable-CAS-TLS.ps1 script, see Configure CAS TLS to Use SAS Viya Default Certificates (Windows) in *Data in Motion: SAS Viya Administration*.

Prepare to Upgrade SAS Event Stream Processing

If you are upgrading SAS Event Stream Processing software:

1. If you are upgrading from a version earlier than SAS Event Stream Processing 6.1, check for configuration files that have been customized.

   With SAS Event Stream Processing 6.1 and later, a single configuration file, esp-properties.yml, is used. Some customizations that you have made to an earlier version will not be used after the upgrade process has completed unless you merge them into the new file.

   On the machine where SAS Event Stream Processing is installed, compare any modified files with the copies that were included with the older version of the software. Run the following commands:

   Note: Specify each command on a single line. Multiple lines are used here for improved readability.

   ```
   fc /N "%DFESP_HOME%\etc\connectors.excluded" C:\ProgramData\SAS
   \Viya\etc\SASEventStreamProcessingEngine\default
   \connectors.excluded
   ```

   ```
   fc /N "%DFESP_HOME%\etc\connectors.excluded" C:\ProgramData\SAS
   \Viya\etc\SASEventStreamProcessingEngine\default\esp-logger.xml
   ```

   ```
   fc /N "%DFESP_HOME%\etc\connectors.excluded" C:\ProgramData\SAS
   \Viya\etc\SASEventStreamProcessingEngine\default\metatags.conf
   ```

   ```
   fc /N "%DFESP_HOME%\etc\connectors.excluded" C:\ProgramData\SAS
   \Viya\etc\SASEventStreamProcessingEngine\default\security-
   properties.yml
   ```

2. Save the results of the commands to a file. You will consult this file when you are ready to merge the configuration changes into esp-properties.yml. For more information, see "Complete SAS Event Stream Processing Upgrade Steps" on page 112.

3. Copy the postgresUser.xml file that is used to store the encrypted passwords for the postgres user account from the previously generated deployment scripting directory to the new deployment scripting directory.

4. Locate the sitedefault.yml file from the previous deployment. Make a copy of it with a new file name, `sitedefault_original.yml`. You will use it as a reference for any future deployments.

   Note: Do not edit sitedefault.yml or sitedefault_original.yml.

5. Stop the metering server:

   ```
   dfesp_xml_client -url "http://host-name:port/SASESP/exit"
   ```

   Replace *host-name:port* with the host name and port of the machine where the metering server is running. By default, it uses port 31001.

Upgrade Your SAS Viya Software

To upgrade a SAS Viya deployment on Windows, perform the following steps:

1. Stop all SAS Viya services. For more information, see General Servers and Services: Operate (Windows) in *General Servers and Services: SAS Viya Administration*.

2. Complete the tasks in "Data Source and Storage Requirements" on page 17, as appropriate.

3. To verify that the Windows deployment is correctly configured:

   a. Download and install the current version of SAS Viya Deployment Assistant for Windows. See "Deploy SAS Viya Deployment Assistant for Windows" on page 49.

   b. To programmatically remediate settings in your Windows deployment, run the SAS Viya Deployment Assistant for Windows using `-remediate` in the command line. See "Configure the Kerberos Environment and Tune Windows Programmatically" on page 53.

4. To upgrade a SAS Viya deployment, run the following command:

   ```
   setup.bat
   ```

   Available upgrades are downloaded and installed.

5. If any SAS Viya services are running, the following message is displayed:

   ```
   Viya services are still running.
   Please shut down all Viya services before an install or update.
   See 'General Servers and Services: Start and Stop All Servers and
   Services' in the 'SAS Viya Administration' documentation for
   instructions on shutting down Viya services.
   ```

   Stop all services as described in Step 1 on page 111, and then run `setup.bat`.

6. At the end of the upgrade, one of the following events occur:

   - If a reboot is not required, setup.bat exits to a prompt and the upgrade is complete.
   - If a reboot is required, the following message is displayed:

     ```
     You must reboot in order to complete install
     ```

     Reboot the machine, and then run `setup.bat -config` to configure the upgraded products and start all the services.

7. After you install the software, complete the post-installation tasks that are appropriate for your deployment.

   a. "Configure the Connection to the Mail Service" on page 61.

   b. If the output of the Enable-CAS-TLS.ps1 script was not preserved as shown in Step 7 on page 109, and TLS needs to be enabled, re-run the Enable-CAS-TLS.ps1 script. See Configure CAS TLS to Use SAS Viya Default Certificates (Windows) in *Data in Motion: SAS Viya Administration*.

   c. If the default Apache HTTP Server certificates were replaced by custom certificates, then add the CA root certificate and intermediate certificates to the SAS Viya truststores. To add the certificates to the truststore, see Add Certificates to the Trustedcerts Files in *Data in Motion: SAS Viya Administration*.

Note: Skip this step if the custom certificates were placed in `C:\ProgramData\SAS\Viya\etc\SASSecurityCertificateFramework\cacerts` and the certificate files are base64-encoded and have a `.crt` extension.

d If the default CAS TLS certificates were replaced by custom certificates, then add the CA root certificate and intermediate certificates to the SAS Viya truststores. To add the certificates to the truststore, see Add Certificates to the Trustedcerts Files in *Data in Motion: SAS Viya Administration*.

Note: Skip this step if the custom certificates were placed in `C:\ProgramData\SAS\Viya\etc\SASSecurityCertificateFramework\cacerts` and the certificate files are base64-encoded and have a `.crt` extension.

e See Chapter 6, “Validating the Deployment,” on page 79.

f See Chapter 7, “Completing the Deployment,” on page 89.

g If you are upgrading SAS Event Stream Processing, complete the steps in “Complete SAS Event Stream Processing Upgrade Steps” on page 112.

h Configure additional SAS products as appropriate.

8 To access the software changes that were added to your deployment, users must log back in to any running SAS Studio session or CAS session. If the data mining service is deployed, restart all data mining service instances.

Upgrade to PostgreSQL Version 15

PostgreSQL no longer releases security patches nor bug fixes for PostgreSQL 9.4 and 11. See PostgreSQL's Versioning Policy for more information.

SAS strongly recommends that you upgrade your PostgreSQL to version 15, which is available in the November 2023 release of SAS Viya 3.5. To determine if you have already downloaded or deployed PostgreSQL 15, see SAS Note 70482.

For the instructions to upgrade PostgreSQL, see Upgrading PostgreSQL in SAS Viya in *SAS Viya Administration: Infrastructure Servers*.

Complete SAS Event Stream Processing Upgrade Steps

Earlier, you were instructed to compare versions of SAS Event Stream Processing configuration files and save a file reflecting the differences between them. Now merge the newer information in the configuration files into the new configuration file for SAS Event Stream Processing 6.2, named esp-properties.yml.

1. Open the file that contains the results of the fc commands that you saved in "Prepare to Upgrade SAS Event Stream Processing" on page 109.
2. Use your preferred text editor to modify the following file: **`%ProgramData%\SAS\Viya\etc\SASEventStreamProcessingEngine\default\esp-properties.yml`**.
3. For the customizations that you found in connectors.excluded, locate the connectors: section of esp-properties.yml. For each connector that you excluded, set the connector's value to false.
4. For the customizations that you found in esp-logger.xml, copy the changes from your comparison file to the logging: section of esp-properties.yml.
5. For the customizations that you found in metatags.conf, copy the changes from your comparison file to the meta: section of esp-properties.yml.
6. For the customizations that you found in security-properties.yml, copy the changes from your comparison file to the security: section of esp-properties.yml.
7. When you have completed the modifications, save esp-properties.yml.
8. Set environment variables for SAS Event Stream Processing on page 40.
9. Complete the tasks that are described in Complete SAS Event Stream Processing Setup on page 71

9

Uninstalling SAS Viya

Overview

You can remove your SAS Viya software by using the remove.bat script or by using the Windows control panel. After the software is removed, you must clean up the deployment by performing a few steps.

Use the Software Removal Script

1. Navigate to the `C:\sas\install\` directory where you uncompressed the sas-viya-deployment-script.zip file that you created.

   SAS Viya software is installed in the `C:\Program Files\SAS` and `C:\ProgramData\SAS` directories.

2. Locate the remove.bat file in the `C:\sas\install\powershell-deployment` directory. You can use this file in one of two ways:

   - Right-click the file, and select **Run as Administrator** from the menu.
   - Open a command prompt (being sure to select **Run as administrator**) from the Windows **Start** menu. Run the following command:

     ```
     remove.bat
     ```

The services will be stopped, and the SAS Viya software and services will be uninstalled.

Use the Windows Control Panel

1. Go to the Control Panel for your Windows machine and select either **Add/Remove Programs** or **Programs and Features**, whichever is appropriate for the version of Windows that you are using.
2. Select **SAS Viya**, right-click, and select **Uninstall**.

The services will be stopped, and the SAS Viya software and services will be uninstalled.

Final Cleanup Steps

1. After most of the software is removed, the SAS Package Manager for Windows will still be installed. To remove SAS Package Manager for Windows:
   a. Go to the Control Panel for your Windows machine and select either **Add/Remove Programs** or **Programs and Features**, whichever is appropriate for the version of Windows that you are using.
   b. Select **SAS Package Manager for Windows**, right-click, and select **Uninstall**.
2. Manually remove the `C:\Program Files\SAS` and `C:\ProgramData\SAS` directories.

   Note: `C:\ProgramData` is a hidden directory. If it is not viewable, go to the **View** tab on Windows Explorer and select **Hidden Items** under **Show/hide**.

   After the directories are manually removed, the removal of your SAS Viya deployment is complete.

Appendix 1

Troubleshooting

Setup Fails When PostgreSQL Starts Up

Explanation

While attempting to deploy, the setup failed with the following message:

```
Start-Service : Service 'SAS Infrastructure Data Server - Postgres -
  Datanode0 (sas-viya-sasdatasvrc-postgres-datanode0)' cannot be started
  due to the following error: Cannot start service sas-viya-sasdatasvrc
  -postgres-datanode0 on computer '.'
```

Resolution

Review the messages in the Windows event viewer and correct any pre-installation, installation, or configuration steps, and then retry the deployment.

From Any Browser: Connection Is Not Private

Explanation

The default self-signed certificates are not in the operating system truststore by default. The Apache Web Server is configured to use a certificate that is signed by this Certificate Authority (CA). When you open any SAS URL and navigate to the web server from a machine that does not have this CA in the truststore, you will receive the message `Your connection is not private`. The message does not indicate that there is any problem with the SAS deployment.

Resolution

SAS recommends that you replace the certificates before you give end users access to SAS Viya. For details, see the Security section of the System Requirements chapter.

From Google Chrome: Connection Is Not Private

Error

When attempting to access SAS Viya software from Google Chrome, the following message is displayed:

```
Your connection is not private.
```

Explanation

If you have previously accessed a website using https, when you access the website again, Google Chrome automatically redirects to https.

Resolution

To reset Google Chrome so that it does not redirect to https:

1. In the Chrome address bar, enter this command:

   `chrome://machine-name//#hsts`

2. Under **Query domain**, in the **Domain** box, enter the name of the machine that was used in the URL that you were attempting to access.
3. Click **Query** to determine whether the machine is known to the browser.
4. If the machine is known to the browser, under **Delete domain**, enter that machine name in the **Domain** box. Click **Delete**.

The corrected URL should now work with the HTTP protocol.