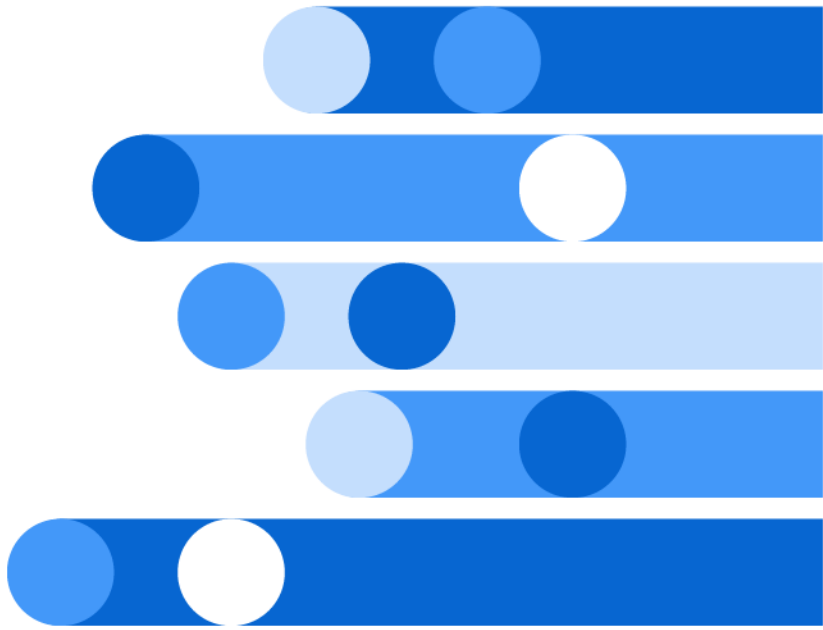
Instructions for the SAS Response to Log4j Vulnerabilities

1.0*



* This document might apply to additional versions of the software. Open this document in SAS Help Center and click on the version in the banner to see all available versions.

SAS® Documentation
September 25, 2024

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2021. *Instructions for the SAS Response to Log4j Vulnerabilities*. Cary, NC: SAS Institute Inc.

Instructions for the SAS Response to Log4j Vulnerabilities

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

September 2024

1.0-P1:log4j

Contents

Chapter 1 / Introduction **1**
About This Document 1

Chapter 2 / Automated Approach: Loguccino **3**
Introduction to Loguccino 3
Instructions for Loguccino 4
Troubleshooting Loguccino 10
How to Stop and Start a Deployment 14

Chapter 3 / Platform-Level Instructions **19**
SAS Viya 2020.1 and Later 19
SAS Viya 3.5 21
SAS Viya 3.4 21
SAS Viya 3.3 22
SAS 9.4 22

Chapter 4 / Product-Specific Instructions **29**
SAS Business Orchestration Services 29
SAS Enterprise GRC 31
SAS Fraud Management 31
SAS Risk Governance Framework 36
SAS Visual Investigator 37

1

Introduction

About This Document 1

About This Document

The instructions in this document help you implement the guidance that is provided in SAS Security Bulletin Remote Code Execution Vulnerability (CVE-2021-44228).

Here are key points:

- This document is updated when additional information becomes available.
- Before you complete any product-specific instructions, complete all instructions for the applicable platform.
- The absence of a particular product from this document does not indicate that the product has no associated vulnerabilities.
- To determine which tasks are applicable for your SAS software, see the security bulletin. To determine how to complete applicable tasks, use this document.

2

Automated Approach: Loguccino

Introduction to Loguccino . . . 3
About Loguccino . . . 3
Supported Platforms . . . 4
Instructions for Loguccino . . . 4
Summary . . . 4
Prepare . . . 5
Scan and Patch on Linux . . . 6
Scan and Patch on Other Hosts . . . 7
Product-Specific Steps . . . 9
Reference . . . 9
Troubleshooting Loguccino . . . 10
Java 1.8 Is Not Available . . . 10
Services Do Not Restart (SAS Viya 3.x) . . . 10
The --no-compress Option Was Not Used (SAS Viya 3.x) . . . 11
The Help Command Does Not Work . . . 11
False Positive Files . . . 12
Unreadable Files . . . 12
How to Stop and Start a Deployment . . . 14
SAS Viya 3.5 . . . 15
SAS Viya 3.4 . . . 16
SAS Viya 3.3 . . . 16
SAS 9.4 . . . 17

Introduction to Loguccino

About Loguccino

Loguccino remediates the Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046 in the specified supported platforms. SAS recommends that you

use loguccino, where supported, instead of completing manual mitigation or remediation tasks.

In general, the manual instructions in this document are intended for sites that either choose to not use loguccino or have software versions that loguccino does not support. If you use loguccino, you can ignore the manual instructions in other chapters of this document, except where otherwise noted.

IMPORTANT The instructions in this document use loguccino to remediate software from SAS in the supported platforms that are specified in the following section. These instructions do not remediate software from other providers, even if that software is on the same system as your SAS software.

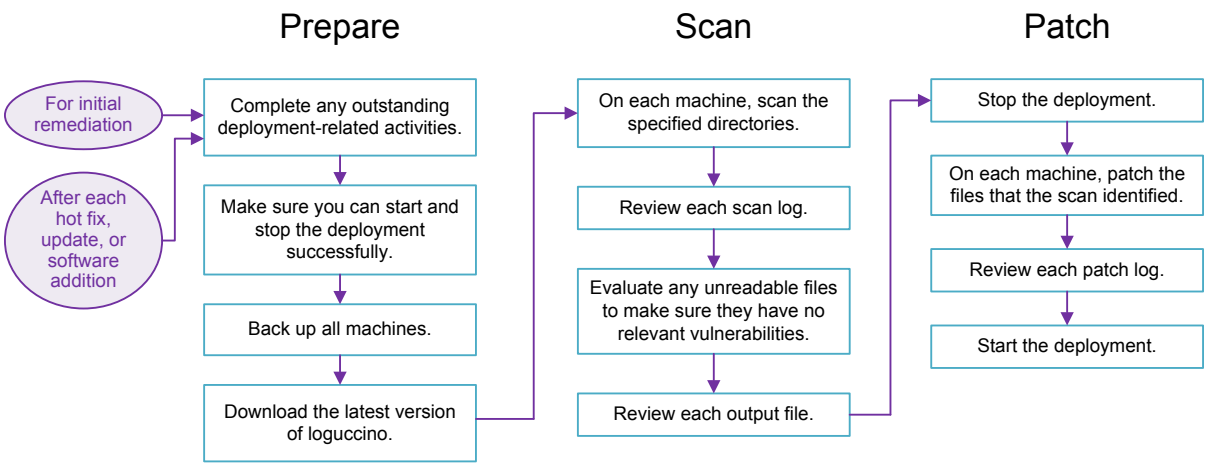
Supported Platforms

Loguccino is supported for SAS 9.4 and SAS Viya 3.3, SAS Viya 3.4, and SAS Viya 3.5 (referred to as SAS Viya 3.x).

Instructions for Loguccino

Summary

The following figure summarizes the workflow for using loguccino.



Note: A *relevant vulnerability* is either of the Log4j version 2 vulnerabilities that loguccino remediates (CVE-2021-44228 and CVE-2021-45046).

The following sections provide step-by-step instructions and essential details.

Prepare

1 Verify that you can stop and start your deployment successfully. See "How to Stop and Start a Deployment".

2 Back up all machines in your environment. You will run loguccino on all machines.

Before you make any changes, SAS strongly recommends that you have a solid, repeatable, and completely tested backup and recovery process that includes all machines in your deployment. Here are references:

SAS Viya 3.5	SAS Help Center: Backup and Restore: Perform a Backup SAS Support: SAS Disaster Recovery Policy for SAS Viya 3.5
SAS Viya 3.4	SAS Help Center: Backup and Restore: Performing a Backup SAS Support: SAS Disaster Recovery Policy for SAS Viya 3.4
SAS Viya 3.3	SAS Help Center: Backup and Restore
SAS 9.4	SAS Help Center: Understanding the Deployment Backup and Recovery Tool

3 Download the appropriate executable or JAR from https://github.com/sassoftware/loguccino.

- For Red Hat Enterprise Linux 7 and later with glibc 2.17, use the native image that is named loguccino.

  Issue the command `chmod +x` on the executable.

  ```
  chmod +x loguccino
  ```

- For other platforms (Windows, AIX, Solaris, z/OS, and so on) and UNIX releases with older releases of glibc, use the JAR file that is named loguccino-*version*.jar.

  Note: Java Runtime Environment (JRE) 1.8+ is required to run loguccino.

  The JAR file can be run with the command `java -jar` on Java Runtime Environment 1.8 or later.

4 Read loguccino's README. It contains important information that you need to know before you use the tool.

Scan and Patch on Linux

The following instructions are for Red Hat Enterprise Linux 7 and later with glibc 2.17. Repeat the scan and patch process after every install activity.

How to Scan on Linux

Note: Loguccino writes files to the current directory. Therefore, you should run loguccino from a location other than SAS Home, the SAS configuration directory, or a Program Files folder. This prevents you from writing files to another application's installation directory.

On each machine, issue the following commands:

1 Scan specified directories.

- For SAS 9.4:

```
./loguccino scan --output path-to-myOutput.csv path-to-SAS-Home
```

```
./loguccino scan --output path-to-myOutput.csv path-to-config
```

- For SAS Viya 3.x:

```
./loguccino scan --output path-to-myOutput.csv /opt/sas
```

This traverses all subdirectories in the specified path or paths, including recursively traversing all nested .tar.gz, .tgz, .tar, .zip, .ear, .war and .jar archives.

2 Review the log that is written to the current directory (for example, loguccino-23122021213438.log). Evaluate any unreadable files.

3 Review the output.

How to Patch on Linux

Note: Loguccino writes files to the current directory. Therefore, you should run loguccino from a location other than SAS Home, the SAS configuration directory, or a Program Files folder. This prevents you from writing files to another application's installation directory.

On each machine where vulnerabilities were found, run the patch command as the SAS Installer user (on SAS 9.4) or the 'sas' user (on SAS Viya 3.x).

Note: On SAS 9.4, do not run the patch command as root.

1 Stop your deployment.

2 Issue the following command:

- For SAS 9.4:

```
./loguccino patch path-to-myOutput.csv
```

- For SAS Viya 3.x if you are running loguccino 3.2.0:

```
./loguccino patch --no-compress path-to-myOutput.csv
```

For SAS Viya 3.x if you are running an older release of loguccino:

```
umasktmp=$(umask)
umask 022
./loguccino patch --no-compress path-to-myOutput.csv
umask ${umasktmp}
```

> **IMPORTANT** The --no-compress option is required with a SAS Viya 3.x system.

3 Start your deployment. See "How to Stop and Start a Deployment".

4 In the current directory, remove the **patch-*[timestamp]*** directory, which contains a backup of each JAR file that was patched.

Scan and Patch on Other Hosts

The following instructions are for hosts such as Windows, AIX, Solaris, z/OS, and UNIX releases that have older releases of glibc. Repeat the scan and patch process after every install activity.

How to Scan on Other Hosts

Note: Loguccino writes files to the current directory. Therefore, you should run loguccino from a location other than SAS Home, the SAS configuration directory, or a Program Files folder. This prevents you from writing files to another application's installation directory.

On each machine, issue the following commands:

1 Scan specified directories.

- For SAS 9.4:

```
path-to-bin-java -jar loguccino-version.jar scan -o path-to-
myOutput.csv path-to-SAS-Home
```

```
path-to-bin-java -jar loguccino-version.jar scan -o path-to-
myOutput.csv path-to-config
```

Here is an example of ***path-to-bin-java*** if you are using the SAS Private JRE to run loguccino on Windows:

```
"C:\Program Files\SASHome\SASPrivateJavaRuntimeEnvironment\9.4\jre
\bin\java.exe"
```

- For SAS Viya 3.x on Windows:

  path-to-bin-java -jar loguccino-*version*.jar scan -o *path-to-myOutput*.csv "C:\Program Files\SAS"

  path-to-bin-java -jar loguccino-*version*.jar scan -o *path-to-myOutput*.csv C:\ProgramData\SAS

- For SAS Viya 3.x on other hosts:

  path-to-bin-java -jar loguccino-*version*.jar scan -o *path-to-myOutput*.csv /opt/sas

This traverses all subdirectories in the specified path or paths, including recursively traversing all nested .tar.gz, .tgz, .tar, .zip, .ear, .war and .jar archives.

2 Review the log that is written to the current directory (for example, loguccino-23122021213438.log). Evaluate any unreadable files.

3 Review the output.

How to Patch on Other Hosts

Note: Loguccino writes files to the current directory. Therefore, you should run loguccino from a location other than SAS Home, the SAS configuration directory, or a Program Files folder. This prevents you from writing files to another application's installation directory.

On each machine where vulnerabilities were found, run the patch command as the SAS Installer user (on SAS 9.4) or the 'sas' user (on SAS Viya 3.x).

Note: On SAS 9.4, do not run the patch command as root.

1 Stop your deployment.

2 Issue the following command:

- For SAS 9.4:

  path-to-bin-java -jar loguccino-*version*.jar patch *path-to-myOutput*.csv

  Here is an example of ***path-to-bin-java*** if you are using the SAS Private JRE to run loguccino on Windows:

  ```
  "C:\Program Files\SASHome\SASPrivateJavaRuntimeEnvironment\9.4\jre
  \bin\java.exe"
  ```

- For SAS Viya 3.x:

```
path-to-bin-java -jar loguccino-version.jar patch --no-compress
path-to-myOutput.csv
```

3 Start your deployment. See "How to Stop and Start a Deployment".

4 In the current directory, remove the **loguccino-patch-** ***[timestamp]*** directory, which contains a backup of each JAR file that was patched.

Product-Specific Steps

See also any product-specific instructions that are applicable for your deployment.

Note: When you use loguccino for platform-level mitigation, some product-specific steps are completed (if applicable to your deployment).

Reference

Output from a Scan

The scan creates a vulnerabilities CSV file that contains the following columns:

AffectedFile
: Full path on the file system to the file that contains the vulnerability.

NestedPath
: Path within the archived file where the vulnerability was found.

AffectedVersion
: Version of Log4j in the affected file.

Patched
: Indicates whether the vulnerable file has been patched. Values are true or false.

Directories to Target

For SAS Viya 3.x on Windows, scan the Program Files and ProgramData directories.

For SAS Viya 3.x on other hosts, scan the SAS directory (**/opt/sas**).

For SAS 9.4, scan the SAS Home and SAS configuration directories.

CAUTION

Do not target your SAS Software Depot. Modifying any file in a SAS Software Depot creates checksum errors that might make future installation activities fail. Instead of modifying files in your SAS Software Depot, re-run loguccino after each installation activity. (You might have Log4j files in your SAS Software Depot that are within the scope of CVE-2021-44228 or CVE-2021-45046. The presence of those files in that location does not constitute an exploitable instance of those vulnerabilities.)

When to Repeat the Process

Each time you perform a SAS installation activity (such as upgrading, updating, hot fixing, or adding software), repeat the entire workflow. Repetition is necessary to ensure that installation activities do not reintroduce vulnerabilities.

Troubleshooting Loguccino

Java 1.8 Is Not Available

Issue: When you issue a loguccino command, the following message is returned: `Exception in thread "main" java.lang.UnsupportedClassVersionError: com/sas/vulnerabilities/Loguccino : Unsupported major.minor version 52.0`

Explanation: The system that you are using does not have Java 1.8 or later.

Resolution: Install Java 1.8 on your system and try again.

Services Do Not Restart (SAS Viya 3.x)

Issue: After you use the patch command, services do not restart and you get the following message in the log of the service: `java.lang.IllegalStateException: Unable to open nested entry 'WEB-INF/lib/logback-core-1.1.7.jar'.`

Explanation: The JAR has been compressed and nested JAR files must be stored without compression.

Resolution: Check the mechanism that was used to create your executable JAR file.

The --no-compress Option Was Not Used (SAS Viya 3.x)

Issue: The --no-compress option was not used when patching a SAS Viya 3.x system.

Explanation: The --no-compress option is required with SAS Viya 3.x.

Resolution: Complete the following steps:

1. Scan the system again. The resulting CSV file indicates the system is already patched. Edit the resulting CSV file, and change **true** to **false** in the Patched column for each row. This allows the system to be patched again.
2. Edit all rows. For example, change:

   ```
   /opt/sas/viya/home/libexec/searchindex-service-1.2.0.jar",
   "/opt/sas/viya/home/libexec/searchindex-service-1.2.0.jar::
   lib/log4j-core-2.4.1.jar","2.4.1","true"
   ```

   to

   ```
   "/opt/sas/viya/home/libexec/searchindex-service-1.2.0.jar",
   "/opt/sas/viya/home/libexec/searchindex-service-1.2.0.jar::
   lib/log4j-core-2.4.1.jar","2.4.1","false"
   ```

3. Run the patch command, making sure to include the --no-compress option (as sas user). Restart services.

The services should now start without issue.

The Help Command Does Not Work

Issue: The Help command returns unexpected results instead of usage information.

Explanation: If you use the wrong syntax in the help command, loguccino might interpret the command as an input file. Here are two examples of *incorrect* syntax for the help command:

```
./loguccino scan help
```

```
java jar ./loguccino/your-jar-version.jar scan help
```

Incorrect results from the help command do not begin with the string `Usage`. Here is an example of the first part of an incorrect result:

```
$ ./loguccino scan help
 ?? Scanning /r/vfiler04/vol/vol50/cxt/logpresso/3.0.0_released/help
INFO: Results written to CSV file: /r/vfiler04/vol/vol50/cxt/logpresso/
3.0.0_released/loguccino-23122021072158.csv
```

Resolution: Here are two examples of the correct syntax for the help command:

```
./loguccino help scan
```

```
java jar ./loguccino/your-jar-version.jar help scan
```

Results from the help command should begin with `Usage` and provide options and additional information. Here is an example of the first part of a correct result:

```
Usage: loguccino scan...
```

False Positive Files

Third-party scanning tools often base their results on the version information of the JAR file and do not account for JAR files that have been patched in this manner. You might continue to see false positives depending on how your tool is designed to detect remediation.

Ensure that loguccino does not need to be run again for recent deployment activity before ascertaining that files are false positives.

Unreadable Files

Issue: The log indicates that some files are unreadable.

Explanation: If the scan command encounters files that it cannot read, it writes those files to a log in the current directory (for example, loguccino-23122021213438.log). The log lists unreadable files in a format that is similar to the following:

```
22.12.2021 16:03:19.172 INFO  Failed to read 26 files:
22.12.2021 16:03:19.172 INFO   1) /install/tmp/tmp_log4j2_scan_manually/snmp-1.0.2.tar
```

Resolution: Evaluate each unreadable file. In the unusual circumstance in which an unreadable file has a relevant vulnerability, contact SAS Technical Support.

Note: A *relevant vulnerability* is either of the Log4j version 2 vulnerabilities that loguccino remediates (CVE-2021-44228 and CVE-2021-45046).

The first step in evaluating an unreadable file is to determine whether that file *might* have relevant vulnerabilities. Certain unreadable files are known to not have relevant vulnerabilities. For those files, no action is necessary. Here is the list of those files:

- agent-5.8.0.tar.gz
- agent-win32-5.8.0.zip
- agent-x86-64-linux-5.8.0.tar.gz
- agent-x86-64-win-5.8.0.zip
- agent-x86-linux-5.8.0.tar.gz

- fmatrans.tar

  Note: This is not a TAR file. It is a SAP transport package that is used to transfer data from one SAP installation to another.

- hyperic-hqee-agent-noJRE-5.0.0.tar.gz
- hyperic-hqee-agent-noJRE-5.8.0.tar.gz
- server-5.0.0.tar.gz server-5.8.0.tar.gz
- rt-1.0.2.tar.gz (whether embedded in another file or not)
- snmp-1.0.2.tar.gz (whether embedded in another file or not)

Other unreadable files might have relevant vulnerabilities. For such files, further evaluation is necessary. Complete the following explode, scan, and evaluate steps for each unreadable file that might have relevant vulnerabilities:

1 Explode the file.

- On UNIX, complete the following steps:

  1 Copy the unreadable file to a temporary directory that has enough disk space to explode the file.

  2 Open a command prompt, and navigate to the temporary directory.

  3 Issue the appropriate command for the UNIX file type:

Type	Command and Result
GZ	`gzip -d filename.gz` A *filename*.tar appears in the temporary directory, and the *filename*.gz disappears.
TAR	`tar -xf filename.tar` A directory by the same name as *filename* appears. The *filename*.tar remains on disk.
ZIP	`unzip filename.zip -d filename` A directory as specified by the `-d` option appears. The *filename*.zip remains on disk.

- On Windows, complete the following steps:

  1 Download and install 7-Zip.

  2 Add the installation directory (default **`C:\Program Files\7-Zip`**) to the Path Environment Variable or use the full path to the executable in the example commands.

  3 If you have not done so, create a temporary directory where you want to extract these archives and copy them to that location.

4 Start PowerShell with **Run as Administrator**, and navigate to the temporary directory that you created.

5 Issue the appropriate command for the Windows file type:

Note: As an alternative to using the following example commands, you can use the 7-Zip GUI or the Windows Explorer pop-up menu (when you right-click on the archive) to extract the contents.

Type	Command and Result
GZ	`7z x .\filename.gz` A *filename*.tar appears in the temporary directory. The *filename*.gz remains on disk.
TAR	`7z x .\filename.tar` A directory by the same name as *filename* appears in the temporary directory. The *filename*.tar remains on disk.
ZIP	`7z x .\filename.zip` A directory by the same name as *filename* appears. The *filename*.zip remains on disk.

2 Examine the contents of the directory that was created by exploding the file.

a Issue the scan command against the directory.

b If the scan log identifies additional unreadable files within the directory, repeat the evaluate, explode, and scan process for each of those files.

In the unusual circumstance in which an unreadable file has a relevant vulnerability, contact SAS Technical Support.

How to Stop and Start a Deployment

Note: These instructions do not contain solution-specific stop and start steps. If you need solution-specific stop and start steps, see your solution documentation.

SAS Viya 3.5

Linux Stop and Start Instructions

Restart all the services on the machine in one of two ways:

- Using the SAS Viya Administration Resource Kit.
- Manually:
  - Stop all services on the machine.

    ```
    sudo /etc/init.d/sas-viya-all-services stop
    ```

  - Start all services on the machine.

    ```
    sudo /etc/init.d/sas-viya-all-services start
    ```

CAUTION

There is a sequence for starting and stopping SAS Viya servers and services. You must follow this sequence to avoid operational issues. The SAS Viya start and stop scripts, including the sas-viya-all-services script, do not span multiple machines. You must run the appropriate script, in the correct sequence, on each machine in your SAS Viya topology. If you have a multi-machine deployment, then start or stop your services by running the SAS Viya Multi-Machine Services Utilities playbooks. Do not run the sas-viya-all-services script on a multi-machine deployment.

For more information about starting and stopping services in multiple machine environments, please refer to the General Servers and Services: Operate (Linux) in the SAS Viya 3.5 Administration guide.

Windows Stop and Start Instructions

Stop and start the Windows services.

1. Bring up Windows Services by entering **`services`** in the Windows search box.
2. Search for the **`SAS Services Manager`** service.
3. Double-click on it and stop the service. Wait for all SAS Viya services to stop. Refresh the Windows Services window if needed to verify. After all SAS Viya services are stopped, proceed.
4. Retart the SAS Services Manager service.

SAS Viya 3.4

Linux Stop and Start Instructions

- Stop all services on the machine.

```
sudo /etc/init.d/sas-viya-all-services stop
```

- Start all services on the machine.

```
sudo /etc/init.d/sas-viya-all-services start
```

CAUTION
There is a sequence for starting and stopping SAS Viya servers and services. You must follow this sequence to avoid operational issues. The SAS Viya start and stop scripts, including the sas-viya-all-services script, do not span multiple machines. You must run the appropriate script, in the correct sequence, on each machine in your SAS Viya topology. If you have a multi-machine deployment, then start or stop your services by running the SAS Viya Multi-Machine Services Utilities playbooks. Do not run the sas-viya-all-services script on a multi-machine deployment.

For more information about starting and stopping services in multiple machine environments, please refer to the General Servers and Services: Operate (Linux) in the SAS Viya 3.4 Administration guide.

Windows Stop and Start Instructions

Stop and start the Windows services.

1. Bring up Windows Services by entering **`services`** in the Windows search box.
2. Search for the **`SAS Services Manager`** service.
3. Double-click on it and stop the service. Wait for all SAS Viya services to stop. Refresh the Windows Services window if needed to verify. After all SAS Viya services are stopped, proceed.
4. Retart the SAS Services Manager service.

SAS Viya 3.3

- On Linux, stop all services on the machine.

```
sudo /etc/init.d/sas-viya-all-services stop
```

- On Linux, start all services on the machine.

```
sudo /etc/init.d/sas-viya-all-services start
```

CAUTION
There is a sequence for starting and stopping SAS Viya servers and services. You must follow this sequence to avoid operational issues. The SAS Viya start and stop scripts, including the sas-viya-all-services script, do not span multiple machines. You must run the appropriate script, in the correct sequence, on each machine in your SAS Viya topology. If you have a multi-machine deployment, then start or stop your services by running the SAS Viya Multi-Machine Services Utilities playbooks. Do not run the sas-viya-all-services script on a multi-machine deployment.

For more information about starting and stopping services in multiple machine environments, please refer to the General Servers and Services: Operate in the SAS Viya 3.3 Administration guide.

SAS 9.4

Linux Stop and Start Instructions

See Operating Your Servers for general information about stopping and starting services, including the *Overview of Server Operation* section for information about shutdown and start-up order if needed.

- Use the sas.servers command to stop services on each machine:

```
SAS-configuration-directory/LevN/sas.servers stop
```

- Use the sas.servers command to start services on each machine:

```
SAS configuration directory/LevN/sas.servers start
```

Windows Stop and Start Instructions

See Operating Your Servers for general information about stopping and starting services, including the *Overview of Server Operation* section for information about shutdown and start-up order if needed.

- Use Windows Services to stop your SAS services.
- Use Windows Services to start your SAS services.

z/OS Stop and Start Instructions

On z/OS environments, see Using the sas.servers Script on UNIX or z/OS to Start or Stop All Servers for information about stopping and starting SAS services on z/OS.

3

Platform-Level Instructions

SAS Viya 2020.1 and Later 19
Original Instructions 19
Open Distro for Elasticsearch 20
SAS Viya 3.5 21
SAS Viya 3.4 21
SAS Viya 3.3 22
SAS 9.4 22
Current Instructions 22
Prior Instructions 23

SAS Viya 2020.1 and Later

As of February 24, 2022, all supported versions of SAS Viya 2020.1 and later are patched with Log4j 2.17.1. SAS recommends that you use a supported version with all available patches applied. No other mitigation measures are needed.

If you previously completed other mitigation steps, there is no need to undo those changes. See also any product-specific instructions that are applicable for your deployment.

Original Instructions

If you cannot immediately update your deployment to a supported version with the necessary patches, complete the following steps:

1. Log on to SAS Environment Manager with an administrator account. (For example, https://my.sas.viya.url/SASEnvironmentManager.)
2. When prompted in the Assumable Groups window about whether to opt in to all of your assumable groups (SASAdministrators), select **Yes**.

3 Select Configuration.

4 Ensure that **All Services** is selected from the drop-down list, and then select **Global**.

5 Determine whether a jvm configuration exists. If it does, edit the configuration by clicking the pencil to the right. Skip to step 8 for edits. Otherwise, proceed.

6 Select **New Configuration**.

7 Select **jvm**.

8 Select **Add property**.

9 For **Name**, enter `java_global_option_disable_log4jlookups`.

10 For **Value**, enter `-Dlog4j2.formatMsgNoLookups=true`.

11 Click **Save** in the Add Property window.

12 Click **Save** in the New jvm Configuration window.

The affected services do not automatically restart. A full restart is required after making these changes. For more information about restarting all services, see Starting and Stopping a SAS Viya Deployment. Make sure to choose the appropriate version of the documentation.

Open Distro for Elasticsearch

If your deployment includes Open Distro for Elasticsearch, and you cannot immediately upgrade to SAS Viya 2021.2.2 (or later), make sure you are using a supported version of SAS Viya, with the latest patches.

Note: Prior instructions for using a JVM option to mitigate Open Distro for Elasticsearch have been removed. If you previously completed those instructions, there is no need to undo those changes.

Is Open Distro for Elasticsearch Present?

To determine whether a SAS Viya deployment contains Open Distro for Elasticsearch, examine the result of the following command:

```
kubectl -n namespace get pods | grep sas-opendistro
```

If pods are identified in the namespace by this command, Open Distro for Elasticsearch is included in the deployment.

SAS Viya 3.5

If you cannot update your software immediately, use loguccino to find and patch occurrences of vulnerable Log4j version 2 jars.

When you are ready to update your software, complete the following steps:

1 Update to the latest version of SAS Viya 3.5.

Note: See SAS Viya Hot Fix Availability.

2 Use loguccino to find and patch any remaining occurrences of vulnerable Log4j version 2 jars.

If loguccino does not find any remaining occurrences of vulnerable Log4j version 2 jars, the remediation is complete.

Otherwise, proceed to the next step.

3 Complete any additional product-specific instructions that are applicable for your deployment.

4 When the next update to SAS Viya 3.5 becomes available, repeat the preceding steps.

Note: See How to learn about hot fixes to SAS software.

Prior instructions to set a JRE argument (-Dlog4j2.formatMsgNoLookups=true) have been removed from this topic.

SAS Viya 3.4

If you cannot update your software immediately, use loguccino to find and patch occurrences of vulnerable Log4j version 2 jars.

When you are ready to update your software, complete the following steps:

1 Update to the latest version of SAS Viya 3.4.

Note: See SAS Viya Hot Fix Availability.

2 Use loguccino to find and patch any remaining occurrences of vulnerable Log4j version 2 jars.

If loguccino does not find any remaining occurrences of vulnerable Log4j version 2 jars, the remediation is complete.

Otherwise, proceed to the next step.

3 Complete any additional product-specific instructions that are applicable for your deployment.

4 When the next update to SAS Viya 3.4 becomes available, repeat the preceding steps.

Note: See How to learn about hot fixes to SAS software.

It is not necessary to undo any previous mitigations.

Prior instructions to set a JRE argument (-Dlog4j2.formatMsgNoLookups=true) have been removed from this topic.

SAS Viya 3.3

Use loguccino to find and patch occurrences of vulnerable Log4j version 2 jars. See also any product-specific instructions that are applicable for your deployment.

Prior instructions to set a JRE argument (-Dlog4j2.formatMsgNoLookups=true) have been removed from this topic.

SAS 9.4

This topic applies to SAS 9.4M6 and SAS 9.4M7. (For the M0, M1, M2, M3, M4, and M5 maintenance releases of SAS 9.4, no platform-level mitigation is needed.)

Current Instructions

IMPORTANT If you have SAS Fraud Management, see SAS KB0036357. Do not complete the following steps.

1 Apply the SAS Security Updates that are available on March 31, 2022.

a Open the SAS Security Updates and Hot Fixes page.

b In the first paragraph on the page, click SAS Security Updates and Hot Fixes.

A PDF file titled *README--Security Updates and Hot Fixes* opens.

c In your browser's address bar, make sure the file name is **`security-update-2022-03.pdf`** (or later). Follow all applicable instructions in the file.

2 Use loguccino to find and patch any remaining occurrences of vulnerable Log4j version 2 JAR files.

3 If an additional update that is relevant to your deployment becomes available, repeat the preceding steps. Continue this process until no exploitable occurrences of vulnerable Log4j version 2 JAR files are found.

Note: Each hot fix creates a backup of any file that it replaces. After you apply a hot fix that replaces vulnerable Log4j files, you might find residual instances of those files in a TAR file in your backup directory. It is not necessary to remove that TAR file. Removing that TAR file does not cause any problems.

Here are additional details:

- If you cannot immediately apply SAS Security Updates, use loguccino to find and patch occurrences of vulnerable Log4j version 2 JAR files.
- If you previously completed other mitigation steps, there is no need to undo those changes.

Prior Instructions

IMPORTANT If you complete the instructions in the preceding section, there is no need to complete the instructions in this section.

Overview

Here is a summary of the steps that are documented in detail in the following sections:

- Stop all SAS sessions, processes, services, and servers.
- Remove the JndiLookup class from any log4j-core-2.14 (or earlier) JAR files in the SAS Home directory or the SAS configuration directory.

CAUTION

Do not modify files in your SAS Software Depot. Modifying any file in a SAS Software Depot creates checksum errors that might make future installation activities fail. Instead of modifying files in your SAS Software Depot, repeat these mitigation steps after each installation activity. (You might have Log4j files in your SAS Software Depot that are within the scope of CVE-2021-44228 or CVE-2021-45046.

The presence of those files in that location does not constitute an exploitable instance of those vulnerabilities.)

- Restart all SAS sessions, processes, services, and servers.

If you choose to use these prior instructions, you must repeat the entire process every time you perform any install activity.

Stop Your System

Stop all SAS services in your environment. See Operating Your Servers for general information about stopping services, including the *Overview of Server Operation* section for information about shutdown and start-up order if needed.

1. On UNIX environments, the sas.servers command can be used to stop services on each machine:

   ```
   SAS-configuration-directory/LevN/sas.servers stop
   ```

2. On Windows environments, use Windows Services to stop your SAS services.
3. On z/OS environments, see Using the sas.servers Script on UNIX or z/OS to Start or Stop All Servers for information about stopping and starting SAS services on z/OS.

Search for log4j JAR Files

Search your SAS Home and SAS configuration directories for any log4j-core-2.* JAR files.

1. On UNIX:

   ```
   find -L SAS-installation-directory -name log4j-core-2.*.jar
   ```

   ```
   find -L SAS-configuration-directory -name log4j-core-2.*.jar
   ```

   On z/OS, you must run the commands in the UNIX System Services (USS) operating environment:

   ```
   find SAS-installation-directory -name log4j-core-2.*.jar
   ```

   ```
   find SAS-configuration-directory -name log4j-core-2.*.jar
   ```

   On Windows, use Windows Explorer to find the log4j JAR files. In the **Search** field, enter **`log4j-core-2.*.jar`**.

   Or, on Windows, use PowerShell:

   ```
   Get-ChildItem -Path SAS-installation-directory -Recurse -Include log4j-core-2.*.jar | Select-Object FullName | Format-Table -AutoSize
   ```

   ```
   Get-ChildItem -Path SAS-configuration-directory -Recurse -Include log4j-core-2.*.jar | Select-Object FullName | Format-Table -AutoSize
   ```

2. With your search results handy, proceed to the next section.

Remove the JndiLookup class

For each log4j-core JAR file where the release is 2.14 or earlier, remove the JndiLookup class. Navigate to each directory containing the applicable log4j-core-* JAR files found in the previous *Search for log4j JAR Files* section, and run the following commands (specific to your system) from that directory to remove the class. This step needs to be repeated for each log4j-core-* JAR file where the release is 2.14 or earlier.

1 On UNIX, issue the following command for each JAR file:

```
zip -q -d path-to-JAR-file org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

2 On AIX, for each JAR file:

Note: The JAR command comes with the Java Development Kit (JDK).

a Extract the contents of the JAR file to a temporary location.

1 Change to the directory that contains the JAR file.

2 Create a temporary directory, and navigate to the temporary directory.

```
mkdir /tmp/newjar
```

```
cd /tmp/newjar
```

3 Extract the contents of the JAR file.

```
jar -xvf complete-path-to-JAR-file
```

b Remove the JndiLookup.class.

```
rm ./org/apache/logging/log4j/core/lookup/JndiLookup.class
```

c Rebuild the JAR file.

```
jar -cvf complete-path-to-jar-file .
```

d Change to the directory that contains the temporary directory, and remove the temporary directory.

```
cd ..
```

```
rm *
```

3 On Windows, for each JAR file:

a In Windows Explorer, navigate to the JAR file, and rename it with a ZIP extension.

b Open the ZIP file in Windows Explorer.

c Navigate to **org/apache/logging/log4j/core/lookup**, and delete the JndiLookup.class file.

d Navigate back to JAR file location, and rename the ZIP file with a JAR extension.

4 On z/OS, for each JAR file:

Note: The JAR command comes with the Java Development Kit (JDK). On z/OS, you might have to install the IBM provided JDK.

a Extract the contents of the JAR file to a temporary location.

1 Change to the directory that contains log4j-core-2.1.jar

2 Create a temporary directory, and navigate to the temporary directory.

```
mkdir tmp
cd tmp
```

3 Extract the contents of the JAR file.

```
jar -xvf ../log4j-core-2.1.jar
```

b Remove the JndiLookup.class.

```
find ./ -name JndiLookup.clas
rm JndiLookup_class_location
```

c Rebuild the JAR file.

```
jar -cvf ../log4j-core-2.1.jar *
```

d Change to the directory that contains the temporary directory, and remove the temporary directory.

```
cd ..
rm -rf tmp
```

Product-Specific Steps

Check the product-specific sections of this document for any product-specific steps that you now need to perform.

Restart Your System

Once you have completed all of the above steps, restart all SAS services in your environment. See Operating Your Servers for general information about starting services, including the *Overview of Server Operation* section for information about shutdown and start-up order if needed.

On UNIX environments, the sas.servers command can be used to start services on each machine:

```
SAS configuration directory/LevN/sas.servers start
```

On Windows environments, use Windows Services to start your SAS services.

On z/OS environments, see the z/OS instructions here for information about starting SAS services on z/OS.

4

Product-Specific Instructions

SAS Business Orchestration Services 29
Instructions for Versions 10.1 and 10.1 HF1 29
Instructions for Versions 1.2 and 1.3 30
Further Assistance 30
SAS Enterprise GRC 31
SAS Fraud Management 31
Current Instructions 31
Prior Instructions 31
Original Instructions 32
SAS Risk Governance Framework 36
SAS Visual Investigator 37
Instructions for Versions 10.6, 10.7, 10.7 Update, and 10.8 (on SAS Viya 3.5) 37
Instructions for Versions 10.4, 10.5, and 10.5.1 (on SAS Viya 3.4) 37

SAS Business Orchestration Services

Instructions for Versions 10.1 and 10.1 HF1

For every instance of SAS Business Orchestration Services (10.1 or 10.1 HF1) that runs on your servers, SAS recommends that you use loguccino.

Note: Prior mitigation instructions have been removed from this topic. If you previously completed other mitigation steps, there is no need to undo those changes. You can use loguccino to make sure no instances of the JndiLookup class were missed.

Instructions for Versions 1.2 and 1.3

Note: You cannot use loguccino as an alternative to completing the following instructions.

For every instance of SAS Business Orchestration Services (1.2 or 1.3) that runs on your servers, complete the following steps:

1. Verify that the zip utility is available on the system where SAS Business Orchestration Services is running. If it is not available, install it. For example:

   ```
   sudo yum install -y zip unzip
   ```

2. Stop SAS Business Orchestration Services.

3. Change directory to **`/usr/local/EOP/EOP-`*`version`*`/lib`**. For example:

   ```
   cd /usr/local/EOP/EOP-1.3.0/lib
   ```

4. List all versions of the `log4j-core` jar file that are found in that directory:

   ```
   ls -l | grep log4j-core
   ```

5. For each version of the `log4j-core` jar file found in that directory, remove the `JndiLookup` class by executing the following command:

   ```
   sudo zip -q -d log4j-core-version.jar org/apache/logging/log4j/core/
   lookup/JndiLookup.class
   ```

   For example:

   ```
   sudo zip -q -d log4j-core-2.6.2.jar org/apache/logging/log4j/core/
   lookup/JndiLookup.class
   sudo zip -q -d log4j-core-2.7.jar org/apache/logging/log4j/core/lookup/
   JndiLookup.class
   ```

6. Verify that the `JndiLookup` class has been removed from the jar files. For example:

   ```
   sudo unzip -l log4j-core-2.6.2.jar | grep JndiLookup.class
   sudo unzip -l log4j-core-2.7.jar | grep JndiLookup.class
   ```

   These commands should return no results.

7. Restart SAS Business Orchestration Services.

Further Assistance

If you require assistance with this matter please email SAS Business Orchestration Services Technical Support at bosstechsupp@sas.com.

SAS Enterprise GRC

Note: SAS Governance and Compliance Manager was formerly known as SAS Enterprise GRC.

If you have SAS Enterprise GRC 6.1 and have applied Hot Fix T04013 or later, SAS recommends that you use loguccino to find and patch occurrences of vulnerable Log4j version 2 JAR files. SAS Enterprise GRC 6.1 runs on SAS 9.4M2.

SAS Fraud Management

Current Instructions

See SAS KB0036357.

If you previously completed other mitigation steps, there is no need to undo those changes.

Prior Instructions

IMPORTANT If you complete the instructions in SAS KB0036357, there is no need to complete the instructions in this section.

You can use loguccino to find and patch occurrences of vulnerable Log4j version 2 JAR files.

If you previously completed other mitigation steps, there is no need to undo those changes. You can use loguccino to make sure no instances of the JndiLookup class were missed.

Note: The loguccino instructions do not provide solution-specific details for stop and start. If you need those details, see the steps for stop and start in the instructions below.

Original Instructions

IMPORTANT If you complete the instructions in either of the preceding sections, there is no need to complete the instructions in this section.

If you choose to use these original instructions, you must complete any manual steps for your maintenance release of SAS 9.4 and then complete the steps in the appropriate section below.

Instructions for Version 6.1

The following instructions assume that SAS Fraud Management 6.1 is the only SAS product that has been installed in the environment where the mitigation is being applied, and that the default directories were used for installation.

Complete the following steps for every instance of SAS Fraud Management 6.1 running on your servers:

1 Stop the SAS Fraud Management servers and processes.

   a Stop the OnDemand Decision Engine (ODE) server(s).

   ```
   cd CONFIGDIR/Lev1/Applications/SASFraudManagement/6.1/Auth-Domain/
   engine/Servern/bin
   ./ose.sh stop
   ```

   b Stop the Transactional Analysis Server (TAS).

   ```
   cd CONFIGDIR/Lev1/Applications/SASFraudManagement/6.1/Auth-Domain/
   analysis/bin
   ./tas.sh stop
   ```

   c Stop all batch jobs and processes running against the SAS Fraud Management databases.

   d Stop all rule estimations.

2 Stop the SAS servers.

   ```
   ./sas.servers stop
   ```

3 Update log4j-core-2.*.jar:

   Note: In the instructions below, substitute your version of log4j for the * in the JAR name. The version of the JAR file might differ depending on the software version and hot fixes that are applied.

   a Change the directory.

```
cd CONFIGDIR/Lev1/Web/WebAppServer/SASServer8_1/sas_webapps/
sas.finserv.frdmgmt6.1.war/WEB-INF/lib/
```

b Remove the offending class file from the JAR file.

```
zip -q -d log4j-core-2.*.jar org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

c Change the directory to the location of log4j-core-2.*.jar in SASVersionedJarRepository.

```
cd SASDIR/SASVersionedJarRepository/eclipse/plugins/Log4J2_2.*
```

d Remove the offending class file from the JAR file.

```
zip -q -d log4j-core-2*.jar org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

e Update the log4j-core-2.*.jar in each ***CONFIGDIR*/Lev1/Web/WebAppServer/SASServer*n*_1/lib** directory where n represents a number specifying the various directories. If the default installation options were used, there are three **SASServer*n*_1/lib** directories .

1 Change the directory.

```
cd CONFIGDIR/Lev1/Web/WebAppServer/SASServern_1/lib
```

For n, substitute 1, 2, and 8 for the number of the SAS Web Application Server.

2 Remove the offending class file from the JAR file.

```
zip -q -d log4j-core-2.*.jar org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

4 Start the SAS Fraud Management servers.

a Start the SAS servers using the sas.servers script located in the ***CONFIGDIR*/** Lev1 directory:

```
./sas.servers start
```

b Start the SAS Fraud Management servers.

1 Start the TAS server. Confirm that there are no errors in the log.

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/6.1/Auth-Domain/
analysis/bin
./tas.sh start
```

2 Start the ODE server(s). Confirm that there are no errors in the log.

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/6.1/Auth-Domain/
engine/Servern/bin
./ose.sh start
```

3 Start any batch jobs that were stopped before the installation.

Instructions for Version 4.4M1

The following instructions assume that SAS Fraud Management 4.4M1 is the only SAS product that has been installed in the environment where the mitigation is being applied, and that the default directories were used for installation.

Complete the following steps for every instance of SAS Fraud Management 4.4M1 running on your servers:

1 Stop the SAS Fraud Management servers and processes.

   a Stop the OnDemand Decision Engine (ODE) server(s).

   ```
   cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.4/Auth-Domain/
   engine/Servern/bin
   ./ose.sh stop
   ```

   b Stop the Transactional Analysis Server (TAS).

   ```
   cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.4/Auth-Domain/
   analysis/bin
   ./tas.sh stop
   ```

   c Stop all batch jobs and processes running against the SAS Fraud Management databases.

   d Stop all rule estimations.

2 Stop the SAS servers.

   ```
   ./sas.servers stop
   ```

3 Update log4j-core-2.*.jar:

   Note: In the instructions below, substitute your version of log4j for the * in the JAR name. The version of the JAR file might differ depending on the software version and hot fixes that are applied.

   a Change the directory.

   ```
   cd CONFIGDIR/Lev1/Web/WebAppServer/SASServer8_1/sas_webapps/
   sas.finserv.frdmgmt4.4.war/WEB-INF/lib/
   ```

   b Remove the offending class file from the JAR file.

   ```
   zip -q -d log4j-core-2.*.jar org/apache/logging/log4j/core/lookup/
   JndiLookup.class
   ```

   c Change the directory to the location of log4j-core-2.*.jar in SASVersionedJarRepository.

   ```
   cd SASDIR/SASVersionedJarRepository/eclipse/plugins/Log4J2_2.*
   ```

   d Remove the offending class file from the JAR file.

   ```
   zip -q -d log4j-core-2*.jar org/apache/logging/log4j/core/lookup/
   JndiLookup.class
   ```

   e Change the directory.

```
cd CONFIGDIR/Lev1/Web/WebAppServer/SASServer1_1/lib
```

f Remove the offending class file from the JAR file.

```
zip -q -d log4j-core-2.*.jar org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

4 Start the SAS Fraud Management servers.

a Start the SAS servers using the sas.servers script located in the ***CONFIGDIR***/Lev1 directory:

```
./sas.servers start
```

b Start the SAS Fraud Management servers.

1 Start the TAS server. Confirm that there are no errors in the log.

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.4/Auth-Domain/
analysis/bin
./tas.sh start
```

2 Start the ODE server(s). Confirm that there are no errors in the log.

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.4/Auth-Domain/
engine/Servern/bin
./ose.sh start
```

3 Start any batch jobs that were stopped before the installation.

Instructions for Version 4.3

The following instructions assume SAS Fraud Management 4.3 is the only SAS product that has been installed in the environment where the mitigation is being applied and that the default directories were used for installation.

Complete the following steps for every instance of SAS Fraud Management 4.3 running on your servers:

1 Stop the SAS Fraud Management servers and processes.

a Stop the OnDemand Decision Engine (ODE) server(s).

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.3/Auth-Domain/
engine/Servern/bin
./ose.sh stop
```

b Stop the Transactional Analysis Server (TAS).

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.3/Auth-Domain/
analysis/bin
./tas.sh stop
```

c Stop all batch jobs and processes running against the SAS Fraud Management databases.

d Stop all rule estimations.

2 Stop the SAS servers.

```
./sas.servers stop
```

3 Update log4j-core-2.*.jar:

Note: In the instructions below, substitute your version of log4j for the * in the JAR name. The version of the JAR file might differ depending on the software version and hot fixes that are applied.

a Change the directory.

```
cd CONFIGDIR/Lev1/Web/WebAppServer/SASServer8_1/sas_webapps/
sas.finserv.frdmgmt4.3.war/WEB-INF/lib/
```

b Remove the offending class file from the JAR file.

```
zip -q -d log4j-core-2.*.jar org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

c Change the directory to the location of log4j-core-2.*.jar in SASVersionedJarRepository.

```
cd SASDIR/SASVersionedJarRepository/eclipse/plugins/Log4J2_2.*
```

d Remove the offending class file from the JAR file.

```
zip -q -d log4j-core-2*.jar org/apache/logging/log4j/core/lookup/
JndiLookup.class
```

4 Start the SAS Fraud Management servers.

a Start the SAS servers using the sas.servers script located in the ***CONFIGDIR***/Lev1 directory:

```
./sas.servers start
```

b Start the SAS Fraud Management servers.

1 Start the TAS server. Confirm that there are no errors in the log.

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.3/Auth-Domain/
analysis/bin
./tas.sh start
```

2 Start the ODE server(s). Confirm that there are no errors in the log.

```
cd CONFIGDIR/Lev1/Applications/SASFraudManagement/4.3/Auth-Domain/
engine/Servern/bin
./ose.sh start
```

3 Start any batch jobs that were stopped before the installation.

SAS Risk Governance Framework

This topic applies to the 7.4 version of SAS Risk Governance Framework.

First, complete the instructions for SAS 9.4. Then, complete the following steps:

1 Apply hot fix D4Z017 or a later hot fix.

2 If you have set up the Apache Solr server for search capabilities, make sure your version of Apache Solr server is at least 8.11.1.

   Here are additional details:

   - One of the issues that is resolved in hot fix D4Z017 enables SAS Risk Governance Framework to use Apache Solr 8.11.1. That resolution is supported in SAS 9.4M6 and later. See Usage Note 68740.
   - Apache Solr provides impact analysis for CVE-2021-44228 and related CVEs in Apache Solr affected by Apache Log4J CVE-2021-44228.
   - If you need to upgrade, see https://solr.apache.org/downloads.html.
   - Apache Solr server 8.11.1 has Log4j 2.16.

Note: If you previously completed other mitigation steps, there is no need to undo those changes.

SAS Visual Investigator

Instructions for Versions 10.6, 10.7, 10.7 Update, and 10.8 (on SAS Viya 3.5)

For SAS Viya 3.5 platform-level mitigation, SAS recommends that you use loguccino to scan and patch occurrences of vulnerable Log4j version 2 JAR files.

Note: Prior mitigation instructions have been removed from this topic. If you previously completed other mitigation steps, there is no need to undo those changes.

Instructions for Versions 10.4, 10.5, and 10.5.1 (on SAS Viya 3.4)

For SAS Viya 3.4 platform-level mitigation, SAS recommends that you use loguccino to scan and patch occurrences of vulnerable Log4j version 2 JAR files.

Note: Prior mitigation instructions have been removed from this topic. If you previously completed other mitigation steps, there is no need to undo those changes.