Paper SAS1918-2018

Recent SAS® 9.4 Middle-Tier Platform Updates for Fun and Profit

Zhiyong Li and Qing Gong, SAS Institute Inc.

ABSTRACT

The SAS® middle tier includes the middle-tier infrastructure software such as SAS® Web Server, SAS® Web Application Server, Java Message Service broker, and the system management software such as SAS® Environment Manager, all of which are critical to all SAS products with a web frontend and all SAS middle-tier services. Since the last SAS® Global Forum, we have made a lot of updates and significant improvements to the middle tier that are driven by customer requirements and input from consultants and SAS technical support. We believe it is extremely important to provide a detailed review of the updates so that SAS administrators can better manage their SAS middle-tier environment and satisfy their corporate IT requirements with improved confidence and fun. This paper first reviews the key components of the SAS middle tier, and then discusses updates made in recent SAS® 9.4 releases (mainly SAS® 9.4M4 and SAS 9.4M5). We specifically discuss the following topics: changes to SAS Web Server, SAS Web Application Server, and Java Message Service Broker; changes to SAS® Private Java Runtime Environment; a new process for updating your horizontal cluster node the right way; SSL library updates to address your concerns about OpenSSL vulnerability; how to preserve your manual SSL configurations; improvements to hardening your environment to enforce TLSv1.2 protocol; and changes to system management and SAS® Environment Manager.

INTRODUCTION

A majority of SAS products have a web frontend and hence need a middle tier. This middle tier is typically built based on the SAS middle-tier platform. The SAS middle-tier platform includes middle-tier infrastructure software such as SAS® Web Server, SAS® Web Application Server, Java Message Service Broker, Java Runtime Environment, and system management software such as SAS Environment Manager. The infrastructure software provides the run-time environment to run the SAS products. SAS Environment Manager offers rich management functions to help manage the SAS products.

Java Runtime Environment. The SAS middle-tier environment includes a Java Runtime Environment (JRE) that is included with the SAS 9.4 software deployment. This JRE is used for all SAS middle-tier and foundation products. The products that are based on Java Web Start (JWS) are allowed to use JREs installed in the client machines and hence do not have to use SAS JRE. SAS continues to evaluate future revisions and patches to the JRE as they become available. SAS also packages and delivers the revisions and patches to SAS customers as necessary to address security issues and to ensure that the functionality of SAS applications is correct and complete.

SAS Web Server. SAS Web Server is an HTTP server that is based on Pivotal Web Server. Pivotal Web Server is a commercial distribution of the Apache HTTP web server. The pivotal distribution of the Apache HTTP server is backed with enterprise support. This gives SAS customers the proven stability of the Apache HTTP server coupled with the support infrastructure that enterprise applications require.

SAS Web Application Server. SAS Web Application Server is a lightweight server that provides enterprise-class features for running SAS web applications. It is a specialized, extended configuration of Pivotal tc Server. Pivotal tc Server has Apache Tomcat at its core and provides the highly scalable, lightweight application server that customers require, along with enterprise support. Tomcat is the most frequently used web application server in existence today. It powers numerous very large-scale, mission-critical web applications across a diverse range of industries and organizations. All SAS middle-tier applications are running in SAS Web Application Server instances. You can find which instance a specific SAS web application runs on this page: http://go.documentation.sas.com/?docsetId=biwaag&docsetTarget=n1fojaysjal45on1wio1kpd3u8as.htm&docsetVersion=9.4&locale=en

Java Message Service Broker. The Java Message Service (JMS) Broker is based on Apache ActiveMQ. A JMS Broker enables web applications to quickly respond to client requests without requiring the client to wait for completion of all the work that the request requires. The JMS Broker is the queuing entity that tracks the requested items from the time that they are requested until they are completed. Some SAS web applications use JMS connection factories, queues, and topics for implementing business logic. These resources are configured in SAS Web Application Server for use by SAS web applications.

Cache Locator. The cache locator is part of Pivotal vFabric GemFire. The software is used by SAS applications on server-tier and middle-tier machines to locate other members and form a shared data cache. When the SAS Web Application Server starts, it contacts one of the locators to initialize communication with the distributed cache. With that information, SAS Web Application Server instances form the cache that is needed to share run-time information across server instances, which might be on different machines. A locator is configured on the server tier to provide access to the data cache for stand-alone client applications such as SAS® Web Infrastructure Platform Scheduling Services.

SAS Environment Manager. The SAS middle-tier environment includes SAS Environment Manager. SAS Environment Manager is based on VMware vFabric Hyperic, an enterprise system management and monitoring system. Hyperic has capabilities to monitor and manage system and application resources, including OS platforms, services running on the system, different types of servers such as database servers and web application servers, and services implemented in the servers. It also has alert, event, and log management capabilities. With the extensible architecture of SAS Environment Manager, it is possible to write additional plug-ins to manage servers, services, and applications in the SAS deployment.

Further details about the SAS middle-tier infrastructure and architecture can be found in my 2014 paper: Migrating SAS Java EE Applications from WebLogic, WebSphere, and JBoss to Pivotal tc Server.

It is important for customers to understand the updates to the SAS middle-tier platforms. These updates address high-priority customer requirements and issues including security issues that are increasingly important due to stricter corporate IT requirements.

CHANGES TO SAS WEB SERVER, SAS WEB APPLICATION SERVER, AND JAVA MESSAGE SERVICE BROKER

SAS Web Server: Even though our out-of-the-box installation is still at the Apache HTTP server 2.2 level, we have upgraded it many times in that release boundary. In SAS 9.4M5, we upgraded the SAS Web Server to the newest Pivotal Web Server 5.5.4, which includes the updated OpenSSL libraries. This upgrade fixed many security issues and hence compliance with the increased security requirements of corporate IT departments. This upgrade also makes sure we are consistent with many SAS Web Server patches we issued for the previous SAS 9.4 maintenance releases. Unfortunately, this upgrade breaks the FIPs compliance. If FIPs compliance is needed and configured in your environment, you might not want to upgrade this version.

We have also recently provided hot fixes to upgrade customers to Pivotal Web Server 6.5 for all SAS 9.4 maintenance releases. That version of Pivotal Web Server uses the Apache HTTP server 2.4. See the OpenSSL section of this paper for details of updates over the last few years.

SAS Web Application Server: SAS Web Application Server is upgraded to the Pivotal tc Server 3.2.5 release in SAS 9.4M5. With this upgrade, we also switch from using Tomcat 7 to Tomcat 8. This is a significant change that fixed many security issues and also addressed many bugs. This upgrade does have a negative impact for preserving customer settings. With this change, some of the configuration files for ActiveMQ and GemFire are re-created and hence some of the customer settings are not preserved. You can find those settings from the backup we created. All SAS solutions have been verified to work with this new version of SAS Web Application Server. All but four solutions will need to issue hot fixes to comply with the upgraded SAS Web Application Server.

The following table lists the upgrades we made to SAS Web Application Server. The table also includes the Pivotal tcServer version and the corresponding Tomcat server version. Keep in mind, Pivotal tc Server packages are for two levels of Tomcat. That is why you see Tomcat A and Tomcat B columns. The last row in the table is for the hot fixes.

SAS Web Application Server			tc Server		Tomcat A	Tomcat B
Version	Date	JRE	Version	Date	Version	Version
SAS 9.4M0 13w26	06/13	7	2.8.0	10/12	7.0.30*	6.0.35
SAS 9.4M1 13w51	12/13	7	2.8.0	10/12	7.0.30*	6.0.35
SAS 9.4M2 14w32	04/14	7	2.8.0	10/12	7.0.30*	6.0.35
SAS 9.4M3 15W29	07/15	7	3.0.0	08/14	8.0.9	7.0.55*
SAS 9.4M4 16w48	10/16	7	3.0.0	08/14	8.0.9	7.0.55*
SAS 9.4M5 17w38	08/17	7	3.2.5	01/17	8.5.13*	7.0.76
Tc server HF W43006	02/18	7	3.2.8	10/17	8.5.23*	7.0.82*

Versions that are marked with * signify the versions actually used in SAS releases.

Java Message Service Broker: This is upgraded in SAS 9.4M4 but not in 9.4M5. The upgrade addresses many security issues reported by scanning reports from customers.

Java Message Service Broker is also upgraded as a hot fix due to the Java deserialization vulnerability and customers' security hardening requirements.

ActiveMQ version information:

SAS Web Application Server	ActiveMQ	
Version	Version	Security Fixes
SAS 9.4M0 SE13W26	5.7.0	yes
SAS 9.4M4 SE16W48	5.12.2	yes

CHANGES TO SAS PRIVATE JRE

Many SAS products continue to rely on Java 7 technology. For the SAS 9.4 releases, SAS expects customers to use the Java versions distributed by SAS to support middle-tier components and SAS web applications. The SAS Private JRE is delivered with standard SAS 9.4 software releases and maintenance updates. SAS also makes updates available to customers who are still running SAS 9.3.

SAS Private JRE is updated in each maintenance release, and we also issue hot fixes quarterly based on the vendors' quarterly JRE security updates. JRE on other platforms such as IBM AIX and HP-UX follows a similar process.

SAS Research and Development (R&D) contacts retrieve the appropriate Java 7 files, and analyze the content to determine applicability to the constrained use of the SAS Private JRE. If a Critical Path Update (CPU) contains security updates that are applicable to the SAS Private JRE, R&D delivers updated content for the SAS Private JRE to SAS Technical Support.

SAS Technical Support prepares the SAS Private JRE for the SAS download site. Final testing is performed for multiple operating systems and for multiple SAS®9 releases. The team updates the download instructions and SAS Notes when the download is posted. For awareness, SAS posts the availability of the updated SAS Private JRE on the Security Bulletins site – Java updates section: https://support.sas.com/en/security-bulletins.html, and to the SAS Hot Fix Announcements community.

The distribution of Java that SAS delivers to customers is determined by the OS platform. Windows, Linux, and Solaris systems will use a distribution based on Azul starting from February 27, 2018. Customers can either upgrade to a later update or apply JRE quarterly hot fixes to switch the JRE from Oracle to Azul. To receive the new JRE content when they download a quarterly update, following the guidelines in SAS Note 56203.

AIX and HP-UX use Java distributions that are customized by their vendors: these updates are typically released after the new releases or quarterly updates are available from Oracle.

JRE version information:

SAS 9.4M4

Platform	Java Version	Address Space
HP-UX	7.0.11	64-bit
Linux	1.7.0_111	64-bit
AIX	Java 7 SR9 FP50	64-bit
Solaris	1.7.0_111	64-bit
Solaris for x64	1.7.0_111	64-bit
Windows 32 bits	1.7.0_111	32-bit
Windows 64bits	1.7.0_111	64-bit
z/OS	Java 7	31-bit

SAS 9.4M5

Platform	Java Version	Address Space
HP-UX	7.0.11	64-bit
Linux	1.7.0_151	64-bit
AIX	Java 7 SR9 FP50	64-bit
Solaris	1.7.0_151	64-bit
Solaris for x64	1.7.0_151	64-bit
Windows 32 bits	1.7.0_151	32-bit
Windows 64 bits	1.7.0_151	64-bit
z/OS	Java 7	31-bit

NEW PROCESS TO UPDATE YOUR HORIZONTAL CLUSTER NODE

There is much confusion about what is the right process to update the cluster members after different SAS maintenance and management tasks. Here are examples:

- Apply hot fixes
- Update in place (UIP)
- Add-ons
- Migration
- Other changes such as rebuilding the web applications

The confusion is caused by many different reasons. First, clustering is a complicated configuration, and we are trying to make it simple and transparent for end users. Over the last several years, we have given different instructions, and those instructions are found in various documents such as *SAS Middle-Tier Administration Guide*; *SAS Intelligence Platform Installation and Configuration Guide*, *SAS Guide to Software Updates*, SAS Notes, and SAS hot fix instructions. Some of them contain either out-of-date or even conflicting information.

SAS R&D has been working with the SAS Technical Support over the last year to make the process consistent and clear, which we will discuss in this paper.

The general flow for keeping a middle-tier horizontal cluster machine up-to-date is as follows:

1. Apply updates to the primary middle-tier machine.
2. Update all middle-tier horizontal cluster machines.

For example, next we will discuss how you should update your cluster node after applying hot fixes.

Applying Hot Fixes

Overview

1. Apply all hot fixes to the middle-tier primary machine.
2. Run SAS® Deployment Manager and rebuild and redeploy all web applications.
3. Apply all hot fixes to all horizontal cluster machines.
4. Run SAS Deployment Manager and run the target “Update existing configuration” on all horizontal cluster machines.

Steps to Perform on the Primary Middle-Tier Machine

1. Install all hot fixes on the primary node using SAS Deployment Manager. For details about installation, see the section "Applying Hot Fixes" in *SAS Deployment Wizard and SAS Deployment Manager 9.4: User's Guide.*
2. Perform any post-installation tasks listed in the documentation that accompanies each hot fix that was applied.
3. Rebuild the SAS web applications. For details, see the section “Rebuilding the SAS Web Applications” topic ("Chapter 8: Administering SAS Web Applications") in the *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide*.
4. Redeploy the SAS Web Applications . For details, see the section “Redeploying the SAS Web Applications” (Chapter 8: Administering SAS Web Applications”) in the *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide.*

Once these steps have been completed on the primary middle-tier node, follow the steps below to configure each middle-tier cluster node.

Steps to Perform on Each Additional Horizontal Middle-Tier Cluster Machine

Note: Steps 1-4 above must already have been performed on the primary node before starting the steps below. Do not perform the steps below on the primary node.

1. Ensure that the primary middle-tier node has all of the required components running (for example, the SAS® Web Infrastructure Platform Data Server, SAS® Metadata Server, SAS Web Server, the SAS cache locator, the SAS Java Message Server (JMS) Broker, SAS Web Application Server instances, and the SAS® Deployment Agent).
2. For each middle-tier, horizontal cluster node, stop all SAS sessions, daemons, spawners, servers, and agents.
3. Apply all web application hot fixes to the horizontal middle-tier machine.
4. Perform any post-installation tasks that are listed in the documentation that accompanies each hot fix applied.
5. Start the SAS Deployment Agent on the horizontal middle-tier machine.
6. If you are configuring your cluster with Java deserialization fixes, you must first remove the existing SAS Environment Manager Agent configuration. Follow instructions in the *SAS 9.4 Intelligence Platform: Installation and Configuration Guide* for details about how to remove configuration for SAS Environment Manager Agent.
7. Start SAS Deployment Manager and, under the **Administration Tasks,** select **Update Existing Configuration.**

For further details about how to upgrade your cluster node, see the updated *SAS Middle-Tier Administration Guide,* which has a new section about the cluster node update process.

SSL LIBRARY UPDATES TO ADDRESS YOUR CONCERNS ABOUT OPENSSL VULNERABILITY

Security vulnerability has been reported for the OpenSSL very frequently, and that has required us to upgrade OpenSSL libraries. Here is the partial list of OpenSSL library upgrades over the last few releases. SAS Web Server originally came from VMware vFabric Web Server (vFWS). Later, it was based on Pivotal Web Server (PWS). The first column in the table lists the VMware and Pivotal version numbers.

VFWS/PWS	Date	Apache	Date	Security Fixes	OpenSSL	SAS Web Server	Date	Notes
5.2.0	16 Oct 2012	2.2.23		yes	1.0.1c	9.4 M0 SE13W26	June 2013	Initial SAS delivery.

5.2.1	24 Jan 2013	2.2.23		yes				VFWS updated APR to 1.4.6, but same Apache version.
5.3.0	24 Apr 2013	2.2.24		yes	1.0.1e			
5.3.1	06 Aug 2013	2.2.25	Jul 2013	yes				
5.3.2	19 Nov 2013	2.2.25	Jul 2013	yes				This was released the day after Apache 2.2.26, but is still based on 2.2.25.
5.3.3	07 Jan 2014	2.2.26	18 Nov 2013	no	1.0.1h	9.4 M2 SE14W28		Re-introduces the session draining patch required by SAS.
5.4.3	29 Oct 2014	2.2.29	02 SEP 2014	yes	1.0.1j	9.4 M3 SE15W29	June 2014	
5.5.0	August2015	2.2.31	July 2015	yes	1.0.1p	Hot Fixes	August 2015	
5.5.1	May 2016	2.2.31-1	July 2015	yes	1.0.1t	Hot Fixes: S47004, S47006,	June 2016	

						V77007		
5.5.2	Oct 2016	2.2.31-1	July 2015	yes	1.0.1u	9.4 M4 SE16W48 Hot Fixes	Dec 2016	
5.5.2	Mar 2017	2.2.31-1	July 2015	yes	1.0.2j	Hot Fixes: V77010 S1314611	Mar 2017	
5.5.4	August 2017	2.2.34.0-64	Jan 2017	yes	1.0.2l	9.4 M5: S1336946	June 2017	

PRESERVATION OF YOUR MANUAL SSL AND REVERSE PROXY CONFIGURATIONS

SAS Web Server, SAS Web Application Server, and SAS Environment Manager all can be secured with SSL configurations.

For the SAS Web Server, the SSL configuration can be easily done during the SAS® Deployment Wizard installation and configuration process. In SAS 9.4M4, an improvement was made to automatically enable SAS Web Server SSL when it was not enabled during the original configuration and later enabled manually (called manual SSL configuration). This SSL enablement will become permanent and will be carried on during future upgrades.

SAS Web Application Server requires manual changes to enable SSL by following instructions in the *SAS Middle-Tier Administration Guide*. Before SAS 9.4M4, customers who had manually configured SSL for SAS Web Application Servers were required to go through a tedious and error-prone process during the upgrade. This includes unconfiguring and reconfiguring of SSL for the SAS Web Application Server. To improve customer experience, in 9.4M4, we introduced a new feature to automatically restore manual SSL configurations for the SAS Web Application Server. To achieve this goal, the manually configured SSL settings are backed up before the new SAS Web Application Server configuration. At the end of the configuration, manual SSL settings are programmatically restored into the current configuration files.

For customers who manually set up the reverse proxy, these settings would also be lost if an upgrade configuration is run for SAS Web Application Server. In 9.4M4, we added a feature to automatically restore such settings during an upgrade.

The restoration of the manual SSL configuration for SAS Web Application Server and manual reverse proxy configurations are entirely transparent to the user during an upgrade. In 9.4M5, further enhancement and bug fixes were added to this feature.

IMPROVEMENT ON HARDENING YOUR ENVIRONMENT TO ENFORCE THE TLSV1.2 PROTOCOL

SAS 9.4M5 has many improvements to harden the SAS environment including the enablement of the TLSv1.2 protocol across the board. Most parts of the SAS components are enforced with the TLSv1.2 protocol. However, to guarantee system component compatibility, some components can be configured to a state that is TLSv1.2 ready (enabled). To accomplish this, during the SAS Deployment Wizard configuration process, we inserted appropriate security settings into the configuration files. These settings are either used immediately, or can be used when certain manual configurations are completed. Some of the specific changes are described below.

- For SAS Web Application Server, the related TLSv1.2 attributes are inserted into the corresponding server.xml files.
- TLSv1.2 compatible Cipher suites are added into the SAS Web Server and SAS Web Application Server configuration files.
- SAS Environment Manager has complete TLSv1.2 enablement after the out-of-the-box SAS Deployment Wizard configuration for all its components. This includes SAS Environment Manager Server, SAS Environment Manager Agents, and the SAS Environment Manager Administration User Interface. In addition to configuration file changes, code changes are actually needed to enforce the TLSv1.2 protocol.
- The upgraded SAS Private JRE supports security options on the client such as the -Djdk.tls.client.protocols to enforce client TLSv1.2 protocols when needed.

CHANGES TO THE SYSTEM MANAGEMENT OR SAS ENVIRONMENT MANAGER

We have made significant changes to SAS Environment Manager in the last two maintenance releases, and those changes can be summarized in the following areas:

- Plug-in changes to accommodate the corresponding software updates such as SAS Web Server upgrade
- User interface changes to address the defects reported
- Third-party components such as Spring framework and commons-beanutils upgrades to address the security concerns
- SSLv1.2 hardening changes to enforce SSLv1.2
- Compliance with the findings of the AppScan security scanning
- Complete redesign of automated SSL configuration for SAS Environment Manager

Next, we will discuss the detailed changes to the SSL configuration.

SSL configuration for SAS Environment Manager has been error-prone and confusing. The new design is based on several years of feedback from consultants who worked with end users and the SAS Technical Support team that gets customer inquiries all the time. The goal of the redesign and implementation is to simplify the SSL configuration for customers and make it streamlined and easy to follow.

When we use SAS Deployment Wizard to configure middle-tier products, two products can be automatically configured to communicate using SSL: SAS Web Server and SAS Environment Manager. SAS Environment Manager consists of SAS Environment Manager Server and SAS Environment Manager Agents. Each of them can be configured to support SSL.

Before SAS 9.4M5, SSL configurations for SAS Web Server and SAS Environment Manager were independent. That means, you were asked to answer the SSL configuration prompts separately, and sometimes those prompts had duplicate questions. Similarly, SSL configurations for SAS Environment

Manager Server and Agents might contain duplicate questions. With the complexity of SSL configuration, these additional prompts or questions made the configuration tasks even more confusing.

Part of this problem also came from the fact that SAS Environment Manager Server doesn't use SAS Web Server as the reverse proxy server, SAS Environment Manager has its own HTTP and HTTPS endpoints. Hence, it cannot take advantage of SAS Web Server's SSL configuration directly like other SAS web applications can. For those other SAS middle-tier components that use SAS Web Server as the reverse proxy server, all communications between the user's browser and client come to SAS Web Server first. If SAS Web Server is configured with SSL, all the other middle-tier components are running behind an SSL-enabled server and hence it might not be necessary to be configured to support SSL.

However, this independence does not mean we should not consider to configure SSL configuration consistently between them. Actually, our major design change is to follow the SAS Web Server SSL selection for SAS Environment Manager. Further, we want to configure SSL for SAS Environment Manager server and the web server using the same certificate whenever possible.

Considering also the fact that SAS Web Server is optional and SAS Web Server and SAS Environment Server might be not on the same machine, we have three principal cases that we need to consider in order to decide how to configure SSL:

- SAS Web Server is configured to use SSL.
  - SAS Web Server and SAS Environment Manager Server are configured on the same machine.
  - SAS Web Server and SAS Environment Manager Server are configured on different machines.
- SAS Web Server is not configured for SSL.
- SAS SWeb Server is not included in the plan.

With the above cases, there are still large combinations of possible supported configuration scenarios that we would like to limit and simplify. In SAS 9.4M5, we limited combinations to the following supported scenarios and also followed our design principle: follow the SAS Web Server SSL selection for SAS Environment Manager and use the same certificates whenever possible:

Both on Same Machine ?	**Web Server TLS?**	**Environment Manager SSL?**	**Required Configuration**
Yes	Yes	Yes	SAS Environment Manager should use the same customer-supplied, site-signed certificate as SAS Web Server. The keystore is generated from the key and certificate that are used by SAS Web Server. The password is set to **hyperic**.
Yes	Yes	No	This scenario is possible only during an update in place. During an update in place, the communication protocol for SAS Environment Manager defaults to the protocol for SAS Environment Manager on the source system. Although SAS Deployment Wizard displays a prompt for the Configured Protocol (which defaults to HTTP), you should not change it. If you do change the protocol to HTTPS, the underlying protocol is still HTTP, matching the SAS Environment Manager protocol on the source system.

Yes	No	No	No additional configuration is required.
No	Yes	Yes	SAS Deployment Wizard prompts for the customer-supplied, site-signed certificate and for the SAS Environment Manager keystore and password.
No	Yes	No	This scenario is possible only during an update in place. During an update in place, the communication protocol for SAS Environment Manager defaults to the protocol for SAS Environment Manager on the source system. SAS Deployment Wizard displays a prompt for the Configured Protocol, which defaults to HTTPS when SAS Web Server and SAS Environment Manager are installed on different machines. You must change the protocol to HTTP, so that it matches the protocol of SAS Environment Manager on the source system. If you kept the communication protocol as HTTPS (which you are allowed to do), the underlying protocol is still HTTP, matching the SAS Environment Manager protocol on the source system.
No	No	No	No additional configuration is required.

For the SAS Environment Manager Agent, since multiple agents are possible, we can’t follow the same principle as we did for SAS Environment Manager Server. However, we do encourage you to use self-signed certificates for Agent SSL configuration since those communication channels are likely to be internal to the customer’s firewall. Self-signed certificates should normally be sufficient. For details about agent SSL configuration, see the section “Middle-Tier Security” in *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide*.

CONCLUSION

This paper gives an update about the SAS middle-tier infrastructure changes over the last few years. Some of the changes, such as supporting the Apache HTTP 2.4 releases and using a different SAS Private JRE, are rather recent and might have a large impact on your environments. Other changes, such as security updates, are welcome topics for many SAS administrators as they are facing increasing numbers of questions from their corporate IT security departments. Even though we have updated our middle-tier administration guide, users guide, and installation guide and even though the SAS Technical Support website reflects these changes, we believe that a complete overview in the important areas will be extremely valuable for the SAS administrators and all SAS users as well. It is our hope that they will feel more comfortable in working with the SAS middle-tier environment after understanding what they are getting--as described in this paper.

In summary, we believe that by understanding these updates, you, as a SAS administrator, can have much better knowledge about SAS middle-tier architecture and can implement and manage your SAS environment with more confidence and might also find it is fun to deploy and manage your SAS environment as well.

REFERENCES

SAS Institute Inc. 2017. *What's New in SAS 9.4.* Cary, NC: SAS Institute Inc. Available at http://go.documentation.sas.com/?docsetId=whatsnew&docsetTarget=whatsnew.pdf&docsetVersion=9.4&locale=en

SAS Institute Inc. 2015. *SAS 9.4 Intelligence Platform: Installation and. Configuration Guide.* Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/cdl/en/biig/69172/PDF/default/biig.pdf

SAS Institute Inc. 2016. *SAS Environment Manager 2.5 User's Guide.* Cary, NC: SAS Institute Inc. Available at http://go.documentation.sas.com/api/collections/evcdc/2.5_M1/docsets/evug/content/evug.pdf?locale=en#nameddest=titlepage

SAS Institute Inc. 2017. *SAS 9.4 Intelligence Platform: Middle-Tier Administration Guide.* Cary, NC: SAS Institute Inc. Available at http://go.documentation.sas.com/api/docsets/bimtag/9.4/content/bimtag.pdf

Peters, Amy, Bonham, Bob, and Li, Zhiyong. 2013, "Monitoring 101: New Features in SAS 9.4 for Monitoring Your SAS Intelligence Platform." *Proceedings of the SAS Global Forum 2013 Conference*. Cary, NC: SAS Institute Inc. Available at https://support.sas.com/resources/papers/proceedings13/463-2013.pdf

Li, Zhiyong, and Fernandez, Alec. 2014, "Migrating SAS Java EE Applications from WebLogic, WebSphere, and JBoss to Pivotal tc Server." *Proceedings of the SAS Global Forum 2014 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings14/SAS357-2014.pdf

Li, Zhiyong, and Thorland, Mike. 2015, "Your Top Ten SAS Middle-Tier Questions." *Proceedings of the SAS Global Forum 2015 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings15/SAS1904-2015.pdf

Li, Zhiyong, and Chrzaszcz, Giles. 2016, "Advanced Topics in SAS Environment Manager." *Proceedings of the SAS Global Forum 2016 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings16/SAS5680-2016.pdf

Li, Zhiyong 2017, "Frequently Asked Questions about SAS Environment Manager on SAS 9.4." *Proceedings of the SAS Global Forum 2017 Conference*. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/resources/papers/proceedings17/SAS0575-2017.pdf

ACKNOWLEDGMENTS

We thank Mike Thorland for the initial writeup of the clustering sections, Donna Bennett for providing the materials for the JRE-related sections, and Fred Li for the design and implementation of the SAS Environment Manager SSL configuration.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the authors:

Zhiyong Li
100 SAS Campus Drive
Cary, NC 27513
SAS Institute Inc.
Zhiyong.Li@sas.com
http://www.sas.com

Qing Gong
100 SAS Campus Drive

Cary, NC 27513
SAS Institute Inc.
Qing.Gong@sas.com
http://www.sas.com