TECHNICAL PAPER

SAS 9.4 Upgrade in Place: System-Level Backup and Recovery Best Practice

Last update: October 2020

Contents

Introduction

This document recommends a best practice for backing up your SAS deployment before performing an upgrade in place (UIP) and for recovering your environment in the event of a UIP failure. For SAS software, an upgrade in place is a software update that introduces new functionality to an existing deployment, and generally involves a new release number. This best practice aligns with the SAS policy on disaster recovery, which also prescribes a method for recovery from a UIP failure. The best practices discussed in this document are mainly derived from existing SAS documentation about the backup and recovery process. To view the backup and recovery documentation directly, see Resources.

Although the effort to create these backups is nontrivial, this investment gives assurances that your SAS deployment can be backed up and restored to full normalcy in the event of an unforeseen failure. It is paramount that backups are part of any deployment process for which the configuration is being modified.

Although this best practice focuses on a UIP, it can also be used at any time that the configuration of your deployment changes. Examples are when adding a new SAS product to your deployment, removing a retired SAS product, or applying SAS hot fixes.

Note: Adjustments to these instructions might be required according to the requirements of your deployment.

Considerations for the UIP

• All SAS services and processes must be stopped before a UIP can occur.

• Upgrades cannot be selectively applied to products or tiers in the environment. Upgrades operate on the entire deployment.

• Maintenance releases have these characteristics.

  o They are cumulative (including hot fixes).

  o They cannot be undone. That is, you cannot uninstall SAS 9.4M6 in order to roll back to SAS 9.4M5.

  o They modify your deployment that is in current operation.

Prerequisites for the UIP

If your SAS topology includes SAS Web Application Server cluster nodes, then you must obtain a new deployment plan (XML file) for your new order. This plan must match the topology that you currently have deployed. You might need the plan file in order to restore and retry the UIP on the cluster nodes.

In order to obtain a new plan file, first, locate the existing plan file from the /Lev/Utilities directory. Next, share the plan file with your SAS account representative, who will then provide you with a new plan file.

You should also consider the amount of disk space available on your file system for SAS deployment backups that you will need to create. See Disk Space Requirements for more information.

Back Up the SAS Deployment

Note: Creating and keeping the backups in sync before you perform the UIP is important in case you need to restore all tiers.

1. Create a metadata backup, and temporarily modify the metadata backup retention policy:
   a. Create a metadata backup prior to shutting down processes and starting the UIP. Because you will be creating multiple metadata backups, provide a descriptive comment or label for each metadata repository backup. For example, you should back up SAS 9.4M5 before you start the UIP for SAS 9.4M6. For details, see SAS Metadata Server Backup Tasks in SAS 9.4 Intelligence Platform: System.

   b. Temporarily modify the metadata backup retention schedule and disable automatic backups. For details, see Modifying the Metadata Server Backup Schedule in SAS 9.4 Intelligence Platform: System Administration Guide.

   Note: Remember to reset the retention policy and reenable automatic backups after the UIP is complete.

2. Run the Deployment Backup and Recovery tool to back up SAS content.

   Its purpose is to enable a secondary means of content recovery after a full system restore. For details about this tool, see the following documentation:

   - Understanding the Deployment Backup and Recovery Tool in SAS 9.4 Guide to Software Updates and Product Changes
   - About the Deployment Backup and Recovery Tool in SAS 9.4 Intelligence Platform: System Administration Guide
   - Best Practices for Backing Up Your SAS Content in SAS 9.4 Intelligence Platform: System Administration Guide
   - Using the Deployment Backup and Recovery Tool in SAS 9.4 Intelligent Platform: System Administration Guide

3. Back up SAS Web Infrastructure Platform (WIP) Data Server and SAS solution data servers.

   By default, the SAS Shared Services are configured with SAS WIP Data Server, which is delivered by SAS. (SAS WIP Data Server is a PostgreSQL data server.) However, if you configured SAS WIP Data Server (or any other SAS solution data server) with a third-party database, then use the vendor-specific tools to back up the database.

   To back up SAS WIP Data Server and any SAS solution data servers, use the pg_dumpall command. For details, see Create Restore Points for Multiple Machine Deployments (step 2) in SAS 9.4 Guide to Software Updates and Product Changes.

4. Stop all SAS services and processes on all servers, in reverse order. See Starting Servers in the Correct Order in SAS 9.4 Intelligence Platform: System Administration Guide

5. To ensure that all SAS processes are fully stopped before proceeding to the next step, use the appropriate strategy:

   UNIX:

   Run the command: **ps -ef | grep** <installer-account>

   Windows:

   Use Windows Services Manager or Windows PowerShell.

   Windows Services Manager: For details, see Running Servers as Windows Services in SAS 9.4 Intelligence Platform: System Administration Guide.

   Windows PowerShell command window**: Stop-Service -Name "SAS*" -Force -Confirm**

6. Back up the file system.

   After all SAS processes have stopped, use operating system commands or third-party tools to perform a full
   operating system backup of the entire SAS deployment.

   For example, you can use snapshots, disk cloning, or disk imaging. These methods ensure that all files, including ancillary files (such as files in the install users home directory, temporary files, and so on), are properly restored.

   Note: These methods are recommended (as option A) in SAS 9.4 Policy Recovery Policy.

   A SAS deployment is the collection of machines on which you installed the <SASHome> directory and created a SAS configuration directory during the initial deployment. If you need help with identifying all the
   machines and their configurations, contact SAS Technical Support.

   After the machines in the deployment are identified, back up each instance of the <SASHome> directory and the <SASConfig> directory on each machine. Although the UIP does not modify files outside of the deployment, a best practice is to also back up any SAS components that can be installed outside of the <SASHome> directory, such as the SAS Clinical Standards Toolkit or SAS/GRAPH Java Applets. Also, back up external file systems that SAS uses or depends on, such as SAS data sources and external database instances, as appropriate.

   For SAS deployments that have been in use for a lengthy period, disk space is primarily occupied by log files. You might consider archiving logs and backing up web application resource (WAR) files prior to backing up the file system.

See Default Location for Server Logs in SAS 9.4 Intelligence Platform: System Administration Guide. Here are candidates for archive:

Metadata Server and Metadata Cluster Tier:
<SASConfig>/Lev<N>/SASMeta/MetadataServer/Logs

Compute Server Tier:<SASConfig>/Lev<N>/SASApp/BatchServer/Logs
<SASConfig>/Lev<N>/SASApp/ObjectSpawner/Logs4
<SASConfig>/Lev<N>/SASApp/StoredProcessServer/Logs
<SASConfig>/Lev<N>/SASApp/WorkspaceServer/Logs
<SASConfig>/Lev<N>/Web/gemfire/instances/ins_<instanceNumber>/*.log
<SASConfig>/Lev<N>/Logs/*.log
<SASConfig>/Lev<N>/SASApp/BatchServer/Logs
<SASConfig>/Lev<N>/SASApp/ConnectServer/Logs
<SASConfig>/Lev<N>/SASApp/OLAPServer/Logs
<SASConfig>/Lev<N>/SASApp/PooledWorkspaceServer/Logs
<SASConfig>/Lev<N>/ShareServer/Logs
<SASConfig>/Lev<N>/Web/SASEnvironmentManager/agent-5.8.0-EE/log

Web Infrastructure Platform Data Server Tiers (includes Solution Data Servers):
<SASConfig>/Lev<N>/WebInfrastructurePlatformDataServer/Logs
<SASConfig>/Lev<N>/<SolutionDataServer>/Logs
<SASConfig>/Lev<N>/Logs/*.log
<SASConfig>/Lev<N>/Web/SASEnvironmentManager/agent-5.8.0-EE/log

Web Server, Web Application Server, and Web Application Server Cluster Nodes Tier:
<SASConfig>/Lev<N>/Web/activemq/data/
<SASConfig>/Lev<N>/Web/gemfire/instances/ins_41415/*.log
<SASConfig>/Lev<N>/Web/Logs/ SASServer<N>_<M>
<SASConfig>/Lev<N>/Web/WebAppServer/SASServer<N>_<M>/logs
<SASConfig>/Lev<N>/Web/WebAppServer/SASServer<N>_<M>/sas_webapps/Backup
<SASConfig>/Lev<N>/Web/WebServer/logs
<SASConfig>/Lev<N>/Web/SASEnvironmentManager/agent-5.8.0-EE/log

Backup Methods for Windows Environments

The only backup methods for Windows environments are to use snapshots, disk cloning, or disk imaging of all disks.

Additional Backup Methods for UNIX Environments

Even though the preferred backup method is to use snapshots, disk cloning, or disk imaging of all disks, another method for UNIX environments is to use operating system commands or utilities, such as tar or zip, to back up the and directories. Make sure that your method preserves date and timestamps and file ownership. The backup

should also include any SAS components that can be installed outside of the directory, such as SAS Clinical Standards Toolkit or SAS/GRAPH Java Applets. Also, the backup should include any external file systems that SAS uses or depends on, such as SAS data sources.

Note: The risk associated with this method is that ancillary files cannot be restored, and leftover ancillary files from the failed UIP remain. Another risk is the loss of third-party software, such as Python, and third-party schedulers, such as IBM Platform LSF, that SAS must update but does not manage.

Ensure that the setuid bits for files under the directory are preserved. Preservation of setuid bits can be accomplished by the SAS installer account if it has sudo access. Otherwise, root access is required. It is critical that you preserve file permissions, ownership, date and timestamps, the setuid bit, and symbolic links.

Disk Space Requirements

After the backups are performed, ensure that you have enough remaining disk space to continue with the UIP. For example, determine the current size of your and directories, and have an equal amount of empty disk space that is available.

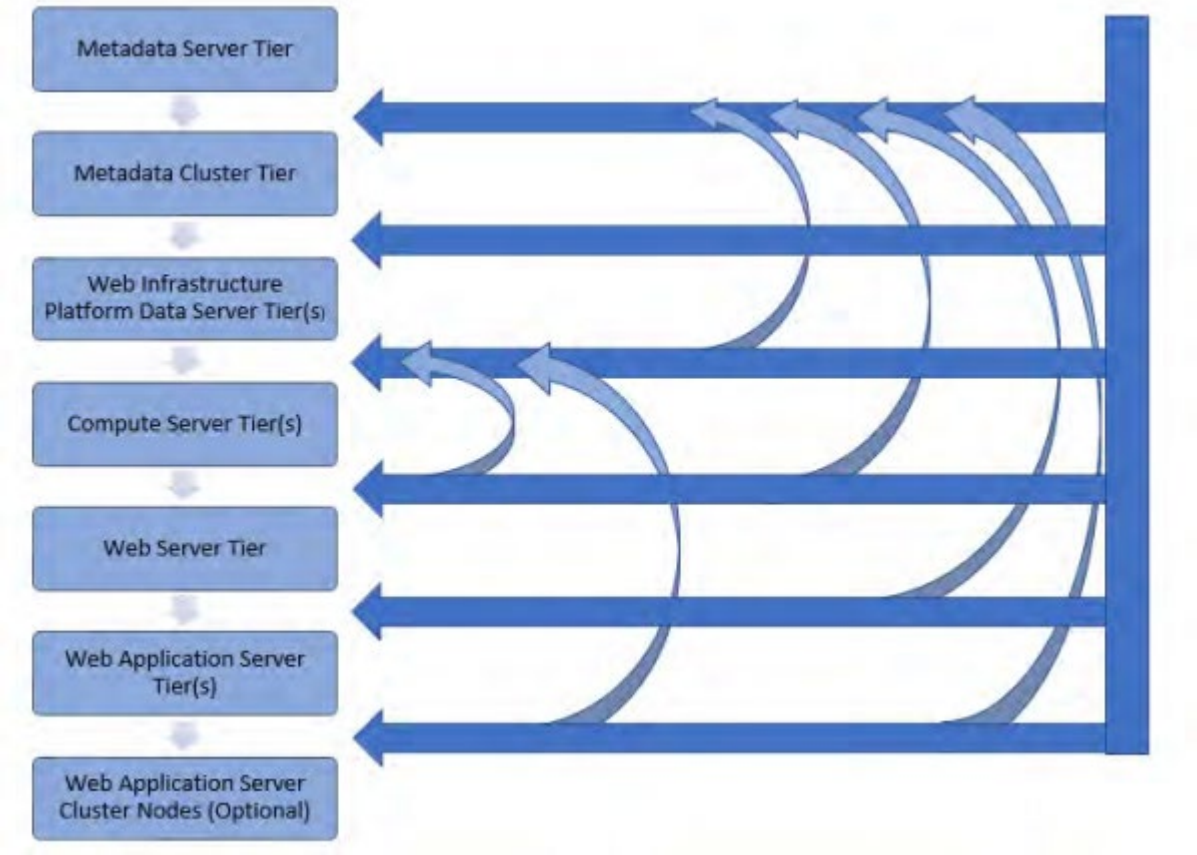
Create Restore Points during the UIP

When a SAS deployment includes multiple configured tiers, it is crucial that you create a restore point to identify each tier's UIP success. Here is an example of a complex, multiple-machine topology and the order in which each tier should be updated.

1. Metadata Server tier
2. Metadata Cluster tier
3. Web infrastructure Platform (WIP) Data Server tier
4. Compute Server tier
5. Web Server tier
6. Web Application Server tier
7. Web Application Server Cluster Nodes tier
8. Client tier

In Figure 1, the horizontal arrows in the diagram reflect the tier on which the UIP is running at that moment. The curved arrows reflect that content on another tier that is modified during that update.

Figure 1 *Complex, Multiple-Machine Topology of a SAS Deployment*



After a specific tier has been successfully upgraded, you must perform a backup of that tier and any other tier that was affected by that upgrade. Refer to Create Restore Points for Multiple Machine Deployments in SAS 9.4 Guide to Software Updates and Product Changes for specific details.

Back Up Metadata Using SAS Management Console

Use the unrestricted administrator account that is a member of role "Metadata Server: Unrestricted". Use sasadm@saspw when using SAS internal accounts.

Provide a label that helps you easily identify the point in the UIP when the metadata backup was created. An example label might be "Prior to UIP of the web application server tier."

For details, see About the Metadata Server Backup Facility in SAS 9.4 Intelligence Platform: System Administration Guide, Backing Up and Recovering the SAS Metadata Server in SAS 9.4 Intelligence Platform: System Administration Guide, and Metadata Server: Unrestricted Role in SAS® 9.4 Intelligence Platform: System Administration Guide

Back Up All Databases

Web Infrastructure and Solution Data Servers

To back up the SAS WIP Data Server and any solution data servers, run pg_dumpall again but specify a new name for the dump file. See Create Restore Points for Multiple Machine Deployments, step 2 in SAS 9.4 Guide to Software Updates and Product Changes.

Note: Typically, during the UIP of the Web Application Server tier, and occasionally during the UIP of the Compute Server tier, SAS products are written to one of the SAS data servers. Therefore, as a best practice, you should back up the data servers immediately prior to updating the Web Application Server tier and the Compute Server tier.

An alternative to backing up the SAS WIP Server Data Server and solution data servers is to use operating system commands or third-party tools to perform a full operating system or file system backup of any tier that contains the SAS WIP Data Server and solution data servers. This method requires that you stop the data server processes, and then restart them in order to proceed with the UIP.

External Databases

If you are using external databases, use the vendor-specific method to back up all databases.

Continue the UIP on the Next Tier

After the current tier has been successfully backed up, continue the UIP on the next tier.

Restore the SAS Deployment If the UIP Fails

If the UIP fails (the failure dialog box is displayed), allow SAS Deployment Manager to remain running, and consult with SAS Technical Support. Do not select **Retry**, if the option is available, and do not continue the UIP. SAS Technical Support will provide guidance on the logs to send and the next actions to perform.

If your maintenance period does not provide enough time to resolve the issue, or the issue cannot be resolved during the outage, you must restore the entire deployment to its pre-UIP state. For details, see Full Restore of the SAS Environment in the Event of a UIP Failure Back to Pre-UIP Environment.

Note: Prior to any restore, save important logs and files of the failing tier. SAS Technical Support can help identify the list of files to save. Run the System Assessment Tool to collect the important logs and files.

Partial Restore of the SAS Deployment after the UIP Failure

If you encounter a failure on a tier during the UIP, it is important that you identify the reason for the failure and attempt to resolve the problem. Contact SAS Technical Support for assistance in resolving UIP failures and performing the next steps. Beginning at 9.4M7, for some UIP failures, you can safely stop the SAS Deployment

Wizard at the point of failure and then restart SAS Deployment Manager after resolving the problem to resume the UIP at the point of failure. A restore is not needed for these types of failures. Other failures require SAS Deployment Wizard (or SAS Deployment Manager) to start the UIP of that tier from the initial state of that tier. In this case, the tier plus other portions of the environment must be restored prior to running SAS Deployment Wizard or SAS Deployment Manager again. Depending on whether the UIP failure occurs during the Install Update phase or the Update Configure phase, there are different steps that you must take to restore your SAS deployment.

UIP Failure during the Install Update Phase

If the UIP failure occurs during the Install Update phase, restore your SAS deployment from a backup before rerunning the UIP. Follow these steps to restore your SAS deployment:

Windows Deployments

1. Stop all SAS services and processes on the failed tier.

2. Restore the directory on the failed tier from the backup that was taken at the beginning of the UIP process. (A restore is accomplished with a snapshot, a disk clone, or a disk image.)

Make sure that you include any SAS components on the current tier that can be installed outside of the directory, such as SAS Clinical Standards Toolkit or SAS/GRAPH Java Applets.

UNIX Deployments

1. Stop all SAS services and processes on the failed tier.

2. Restore the directory on the failed tier from the backup that was taken at the beginning of the UIP process.

3. Make sure that you include any SAS components on the current tier that can be installed outside of the directory, such as SAS Clinical Standards Toolkit or SAS/GRAPH Java Applets. Note: If your backup method is to perform a full operating system backup (such as using snapshots, disk cloning, or disk imaging) rather than a selective restore of only the directory, then a full operating system backup is acceptable. Check date timestamps on the files under the /SASFoundation/9.4/sasexe directory and ensure that the files are being preserved. If all the files have the same date timestamp that matches the backup date or the current date, then you know that these files were not preserved. Resolve this issue before you continue with the restore.

4. Confirm that User Authentication is still configured. Check the sasperm, sasauth, and elssrv files at `<SASHome>/SASFoundation/9.4/utilities/bin/` and confirm that all three files have these setuid attributes: owned by root and 4755 permissions. If the files do not have these attributes, run the setuid.sh script with the root user ID.

Restart the UIP on the Failed Tier

1. Launch SAS Deployment Wizard. If the restore was successful, SAS Deployment Wizard should identify the need to update the installation. After the installation update is complete, SAS Deployment Wizard starts the SAS Deployment Manager Update Existing Configuration task. At this point, perform one of the following actions, which might require another backup:

    a. Note: Starting in SAS 9.4M7, SAS Deployment Wizard downloads and installs almost all hot fixes that are available for the recently updated directory. However, there are a few hot fixes that must be applied manually. Also, in SAS 9.4M7, the SAS Security update is automatically installed each time you run an install, so there is no need to re-apply security updates after applying a hot fix.

    For releases prior to SAS 9.4M7, install additional hot fixes prior to updating the configuration. If you are using the SAS Hot Fix Analysis, Download and Deployment Tool (SASHFADD) to check for and install additional hot fixes between installation and configuration, then exit the SAS Deployment Wizard, stop the SAS Deployment Agent, install the additional hot fixes, rerun the SAS Security Update utility, and create another backup of (using snapshots, disk cloning, or disk imaging), and restart the SAS Deployment Agent.

    b. If you do not stop SAS Deployment Wizard to install additional hot fixes, but instead continue the Update Configure phase, you do not need to perform a backup of the directory at this point.

UIP Failure during the Update Configure Phase

If the UIP failure occurs during the Update Configure phase and the error cannot be resolved so that the UIP can be continued, you must restore your SAS deployment to a previous working state. After the restore, validate your SAS deployment before running the UIP again.

Restore the SAS Deployment

1. Stop all SAS services and processes on the current tier.

2. Verify that all processes and services have been stopped on the current tier.

3. Restore the metadata repository to the metadata backup that was created prior to your attempt to perform the UIP of the failing tier. Refer to Figure 1 to identify other tiers that are affected by the UIP of the failing tier. If you are also restoring the directory, then you will need to launch SAS Management Console from the tier at which the UIP was successful, such as the SAS Metadata Server tier. Restore the tier using the unrestricted administrator account that is a member of role “Metadata Server: Unrestricted”. Use sasadm@saspw when using SAS internal accounts.

    a) If your metadata server is clustered and the nodes were already updated, then restore the SAS deployment by following the steps in Recovering a Clustered Metadata Server in SAS 9.4 Intelligence Platform: System Administration Guide. Otherwise, refer to Executing a Metadata Server Recovery in SAS 9.4 Intelligence Platform: System Administration Guide.

    b) If the failure occurs on the Metadata Server tier, you do not need to restore the metadata. Simply stop the metadata server and restore the configuration directory.

4. Restore the directory on the current tier from the configuration backup that was created before the UIP was started.

Note: If your backup method is a full operating system backup (such as using snapshots, disk cloning, or disk imaging) rather than a selective restore of only the and directories, then restore the full operating system backup.

Note: You will need to launch SAS Deployment Wizard on the current tier when starting the UIP again during the install phase if either of the following apply:

- You did not install hot fixes between installation and configuration.
- You did not create a snapshot between installation and configuration.

You must launch SAS Deployment Wizard during step 7, after completing steps 1 through 6.

5. Restore your databases.

During the UIP of the Web Application Server tier products, and in some cases, the Compute Server tier, the update of products causes changes to the tables in the SAS WIP Data Server, solution data server, and external databases, if applicable. Therefore, if you experience a configuration failure on the Web Application Server tier or the Web Infrastructure Data Server tier, then you must ensure that all databases are restored from the last successful UIP tier.

Refer to the PostgreSQL documentation about how to restore your databases. See the PosgreSQL 9.5 documentation for more information about the psql command.

If you are using external databases, use vendor-specific tools to restore all databases from the last successful UIP tier.

6. Validate the SAS environment.

The validation steps that you perform depend on the type of restore that was performed. Validation steps for different types of restores follow:

- Metadata Repository Restores
- Metadata Clustered Nodes Restores
- Compute Server Tier Restores
- Web Infrastructure Data Server Restores
- Web Application Server Tier Restores
- Web Server Tier Restores

Note: After you perform the validation steps for the appropriate type of restore, make sure that you restart the UIP on the failed tier (in step 7).

7. Restart the UIP on the failed tier.

   If you restored the directory as part of a full operating system backup (a snapshot, a disk clone, or a disk image), then run the UIP by launching SAS Deployment Wizard on the current tier. This action reruns the Install Update phase and transitions to the Update Configure phase.

   If you did not restore the directory, launch SAS Deployment Manager on the current tier, and choose the Update Existing Configuration option.

Validate the SAS Deployment

Complete the appropriate validation steps for the type of restore you need to perform.

Metadata Repository Restores

Verify that you can log in to SAS Management Console after restoring the repository. At this point of a restore, your deployment is back to the failed tier's pre-UIP metadata state. If the directory was not also restored, then you might receive a message that indicates the version of SAS Management Console that does not match the version of metadata. Do not change any metadata in this scenario. However, you can verify the unrestricted administrator account that is a member of role "Metadata Server: Unrestricted" (or use "sasadm@saspw" when using SAS internal accounts) to log in to SAS Management Console.

If the tier being restored is the Metadata Server tier, stop the metadata server. Otherwise, it can remain running.

Verify date timestamps and that file ownership has been preserved.

After you finish the validation, make sure that you restart the UIP on the failed tier.

Metadata Clustered Nodes Restores

Start all the metadata server nodes using your typical start procedure. After all the nodes are running, verify that all three nodes are in quorum by logging in to SAS Management Console and viewing the Active Server properties:

1. Navigate to **Environment Management → Metadata Manager → Active Server**, and right-click **Properties** on the **Cluster** tab.

2. Ensure that the **State** is QUORUM and the number of **Defined Nodes** equals the number of **Current Nodes**.

As a secondary check, open the logs for each metadata server node and check for ERROR and WARN level messages. The logs are located here:

<SASConfig>/Lev/SASMeta/MetadataServer/Logs

After you finish the validation, make sure that you restart the UIP on the failed tier.

Compute Server Tier Restores

Make these verifications:

- Verify that SAS Deployment Agent is running on the Compute Server tier.
- Verify that no other SAS processes or services are running on the restored tier.
- Verify that SAS launches from /SASFoundation.
- Verify date timestamps and that file ownership has been preserved.

After you finish the validation, make sure that you restart the UIP on the failed tier.

Web Infrastructure Data Server Restores

Temporarily start the data server and verify that you can connect to the SAS Shared Services database on SAS WIP Data Server. Check your Instructions.html files for any Solutions Data Servers in your deployment and verify your connection to those Solutions Data Servers.

Windows Deployments

1. Open a Windows command prompt and run the following command:
   \SASWebInfrastructurePlatformDataServer\9.4\bin
2. To start Postgres, run the following command:

   Note: The default account is dbmsowner, and the default port is 9432. However, use the account and port that are appropriate for your environment:

   ```
   psql -h localhost -U dbmsowner -d SharedServices -p 9432
   ```

3. You are prompted for credentials for Shared Services.
4. After you have logged in to Postgres, run the \list command.
5. To exit Postgres, enter \quit.
6. Perform a similar validation process for each solution data server that is stored in the PostgreSQL data server instance that is provided by SAS.
7. Verify that the SAS Deployment Agent is running on the SAS WIP Server tier.
8. If the failure occurred on the same tier as the SAS WIP Data Server, then stop the SAS WIP Data Server and verify that no other SAS processes or services (except for SAS Deployment Agent) are running on the restored tier. Otherwise, leave the SAS WIP Data Server running.
9. Verify that no other SAS processes or services are running on the restored tier.

UNIX Deployments

1. Open a UNIX command prompt and run the following commands to start Postgres:

```
export POSTGRES_HOME= /SASWebInfrastructurePlatformDataServer/9.4

export PATH=${POSTGRES_HOME}/bin:$PATH
```

Note: If you are using AIX UNIX, replace LD_LIBRARY_PATH with LIBPATH.

```
export LD_LIBRARY_PATH=${POSTGRES_HOME}/lib:$LD_LIBRARY_PATH

export LIBPATH=${postgres_home}/lib:$LIBPATH13
```

2. To start Postgres, run the following command:

   Note: The default account is dbmsowner, and the default port is 9432. However, use the account and port that are appropriate for your environment:

   ```
   psql -h localhost -U dbmsowner -d SharedServices -p 9432
   ```

3. You are prompted for credentials for Shared Services.
4. After you have logged in to Postgres, run the \list command.
5. To exit Postgres, enter \quit.
6. Perform a similar validation process for each solution data server that is stored in the PostgreSQL data server instance that is provided by SAS.
7. Verify that the SAS Deployment Agent is running on the SAS WIP Data Server tier.
8. If the failure occurred on the same tier as the SAS WIP Data Server, then stop the SAS WIP Data Server and verify that no other SAS processes or services (except for SAS Deployment Agent) are running on the restored tier. Otherwise, leave the SAS WIP Data Server running.
9. Verify that no other SAS processes or services are running on the restored tier. After you finish the validation, make sure that you restart the UIP on the failed tier.

After you finish the validation, make sure that you restart the UIP on the failed tier.

Web Application Server Tier Restores

Make these verifications:

- Verify that the SAS Deployment Agent is running on the SAS WIP Data Server tier.
- Verify date timestamps and that file ownership has been preserved.
- Verify that the metadata server is running and accessible.
- Verify that object spawners on Compute Server tiers are running and accepting connections.
- Verify that the SAS WIP Data Server is running and that the Shared Services database is accessible.

After you finish the validation, make sure that you restart the UIP on the failed tier.

Full Restore of the SAS Deployment after the UIP Failure

This method returns your SAS deployment to the pre-UIP deployment state.

1. Ensure that all SAS services and processes on all servers are stopped.

2. Restore the file systems on all SAS servers. Depending on the backup method taken, this is a recovery from the full operating system backups or from the backups of the and directories, and any SAS components that can be installed outside of , such as the Clinical 14 Standards Toolkit. This restores the directories for on all servers and on all logical machines. Note that the restore of the directory includes the restore of the SAS Web Infrastructure Data Server databases. Ensure that any external files system that SAS uses or depends on is also restored.

3. If using external databases, use vendor-specific tools to restore all databases.

4. Restart all SAS services and processes in all servers in the correct order. See Starting Servers in the Correct Order in SAS 9.4 Intelligence Platform: System Administration Guide.

5. Validate the SAS deployment. Check through your Instuctions.html file on each tier and perform any customer-specific user acceptance testing. Also see:

    - Checking the Status of Servers in SAS 9.4 Intelligence Platform: System Administration Guide.
    - Validate the SAS 9.4 Servers in SAS 9.4 Intelligence Platform: Installation and Configuration Guide.
    - Validate the SAS Metadata Server, SAS Workspace Servers, SAS Pooled Workspace Servers, SAS Stored Process Servers, SAS OLAP Servers, and SAS/CONNECT Servers in SAS 9.4 Intelligence Platform: System Administration Guide.
    - Validating Your SAS Foundation Deployment in SAS 9.4 Foundation and Related Software: Installation Guide for UNIX.
    - Validate the SAS Content Server in SAS 9.4 Intelligence Platform: System Administration Guide
    - Validate the SAS Content Server in SAS 9.4 Intelligence Platform: System Administration Guide
    - Step 7: Validate Your SAS Visual Analytics Deployment in SAS 9.4 Administration.
    - Using the Deployment Tester in SAS 9.4 Intelligence Platform: System Administration Guide.

6. If problems occur while validating the environment, consult with SAS Technical Support to learn about options for using the SAS Deployment Backup and Recovery tool to recover the SAS deployment content and to retry the validation. See Best Practices for Restoring Your SAS Content in SAS 9.4 Intelligence Platform: System Administration Guide.

References

SAS Support:

SAS Institute Inc. SAS 9.4 Disaster Recovery Policy. https://support.sas.com/en/technical-support/services-policies/disaster-recovery-policy.html

SAS Institute Inc. 2013. "Usage Note 15231: SAS modules that must have the setuid bit set to root in the UNIX environment." https://support.sas.com/kb/15/231.html

SAS Documentation:

SAS Institute Inc. 2020. "About Backing Up and Restoring Your SAS Content." In SAS 9.4 Intelligence Platform: System Administration Guide, Fourth Edition. Cary, NC: SAS Institute Inc. https://documentation.sas.com/?docsetId=bisag&docsetTarget=p1u29z4y7j3spvn1gaqzlyx2narb.htm&docsetVersion=9.4&locale=en

SAS Institute Inc. 2020. SAS 9.4 Guide to Software Updates and Product Changes. Cary, NC: SAS Institute Inc. https://documentation.sas.com/?docsetId=whatsdiff&docsetTarget=titlepage.htm&docsetVersion=9.4&locale=en

SAS Institute Inc. 2020. "Updating the SAS High-Performance Analytics Infrastructure." In SAS High-Performance Analytics Infrastructure 3.9: Installation and Configuration Guide. Cary, NC: SAS Institute Inc. https://documentation.sas.com/?docsetId=hpaicg&docsetTarget=p08sashpanalytics00installgd.htm&docsetVersion=3.9&locale=en

SAS Institute Inc. 2017. "Upgrading SAS Visual Analytics (Non-distributed LASR)." In SAS Visual Analytics 7.4: Installation and Configuration Guide (Non-distributed SAS® LASR(TM)). Cary, NC: SAS Institute Inc. https://support.sas.com/documentation/cdl/en/vasmicg/70710/HTML/default/viewer.htm

SAS Institute Inc. 2017. "Upgrading SAS Visual Analytics." In SAS Visual Analytics 7.4: Installation and Configuration Guide (Non-distributed SAS® LASR(TM)). Cary, NC: SAS Institute Inc. https://support.sas.com/documentation/cdl/en/vaicg/69988/HTML/default/viewer.htm

SAS Technical Papers:

SAS Institute Inc. 2020. "Modernizing Your SAS UIs: Removing Dependencies on Adobe Flash." (SAS technical paper). Cary, NC: SAS Institute Inc. https://www.sas.com/content/dam/SAS/support/en/technical-papers/modernizing-sas-ui-adobe-flash.pdf

External:

Wikibooks. "How To Backup Operating Systems." https://en.wikibooks.org/wiki/How_To_Backup_Operating_Systems. Last modified August 29, 2019.

Nadarajan, Sathish. March 28, 2019. "Windows Server 2012 – How to Create System Restore Point Using Windows Server Backup feature." https://www.sharepointpals.com/post/windows-server-2012-how-to-create-system-restore-point-using-windows-server-backup-feature/

Release Information Content Version: 1.0 October 2020

To contact your local SAS office, please visit: sas.com/offices