TECHNICAL PAPER

Mounting a SAS® 9.4 Deployment from One Cloud Instance to Another after a Minor Operating System Release Upgrade

Last update: July 2024

Introduction

Use this document as a guide for mounting an existing SAS® 9.4 deployment on a Microsoft Azure Cloud instance to a virtual machine (VM) in a new Microsoft Azure Cloud instance where the following conditions are true:

- The underlying operating system (OS) in the target instance is running a newer minor release upgrade of the OS as compared to the source instance.
- The operating system for both the source and target Azure Cloud instances is Red Hat Enterprise Linux (RHEL).

Note: This paper augments the SAS 9.4 Disaster Recovery Policy, which addresses this use case. The Limitations and Considerations and A Note about External Systems and Data sections establish the baseline principles and considerations for mounting an existing SAS deployment from one cloud instance to another cloud instance.

Here are additional references to SAS® 9.4 administration documentation:

- SAS® 9.4 Guide to Software Updates and Product Changes
- Copying an Existing SAS 9.4 Deployment in the SAS® 9.4 Intelligence Platform: Migration Guide
- SAS® 9.4 Intelligence Platform: Installation and Configuration Guide, Second Edition
- SAS® Deployment Wizard and SAS® Deployment Manager 9.4: User's Guide

Testing Scope

SAS has validated this process with the following products and systems:

- SAS® 9.4M7 Enterprise BI Server software and SAS® Grid Manager for Platform, with a clustered metadata server, a clustered middle-tier server, and three grid nodes.

- Red Hat Enterprise Linux (RHEL) 8, and minor releases of the OS only. For information about an upgrade of a major release RHEL operation system, see Are you planning an upgrade from RHEL 7.x to RHEL 8.x or RHEL 9.x?.

- Virtual machines in Azure

- Source and target systems support server virtualization technologies that allow decoupling of the operating system disk and its infrastructure from the data disks on which the SAS deployment files, SAS configuration files, and SAS data files are deployed. An example is a cloud deployment where the SAS binaries and SAS configuration directory are deployed to externally mounted storage.

- An upgrade to SAS 9.4M8 was successful on the target system after the SAS 9.4M7 deployment was mounted to the target system.

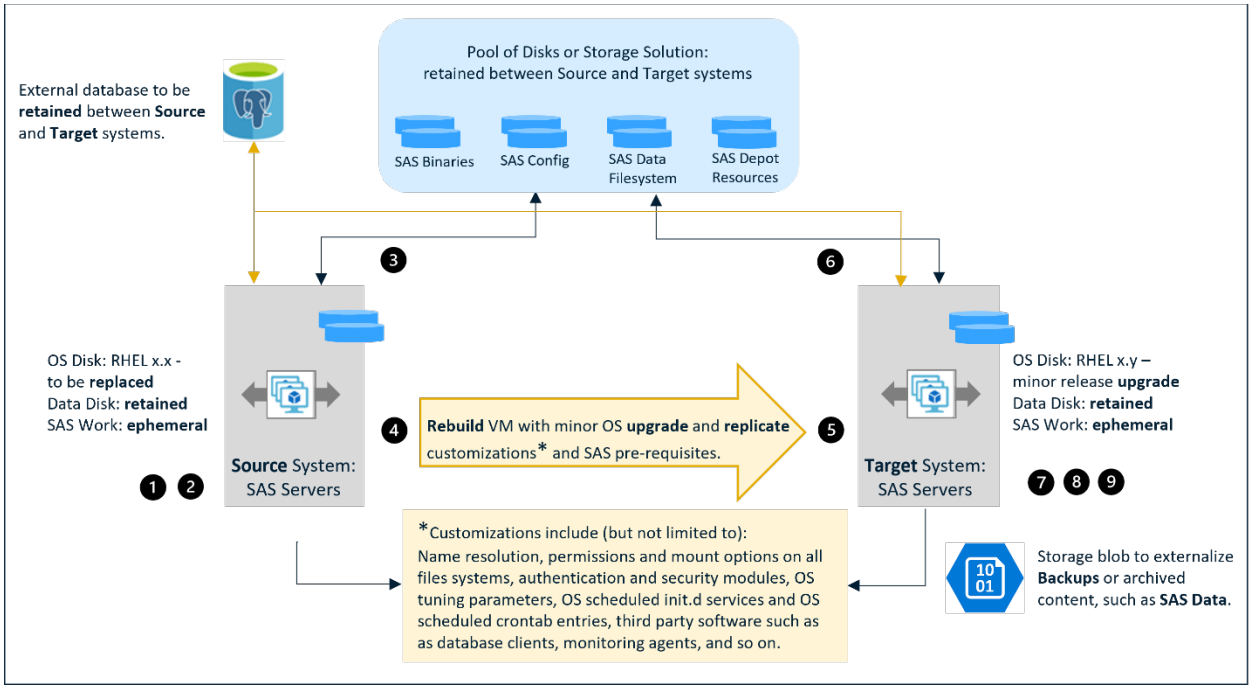
General Process to Follow

Here is the general process to follow for mounting an existing SAS 9.4 deployment to a cloud instance that has a minor OS upgrade.

- Perform the Prerequisite Steps on the Source System before you unmount a SAS 9.4 deployment from the source system.
- Perform the Prerequisite Steps on the Target System before you mount the SAS 9.4 deployment to the target system.

Note: Identical host names cannot exist within the same infrastructure. Therefore, changes must be made to one system at a time.

Use the following diagram and its numbered steps for more detail about the general process that you follow:



1. Verify that your existing SAS 9.4 deployment is fully operational on the **source** system. Confirm that you have a successful full backup and you have validated the deployment.

   See Perform the Prerequisite Steps on the Source System.

2. Stop all SAS servers on the **source** system.

3. **Unmount** the retained pool of disks that contain SAS binaries, SAS configuration files, SAS Depot, and SAS data file systems from the **source** system. (This step assumes that the SAS 9.4 deployment files are stored on data disks, and not on the OS disk. The deployment files must be mounted to an existing and operational cloud instance.)

4. Shut down the **source** system.

   Note: Host names and aliases of the **target** system must match those of the **source** system. Although you can rebuild the VMs (step 5) prior to completing steps 1-4, any host name conflicts between source and target systems must be reconciled first. To reconcile conflicts, ensure that the target system with the appropriate host names is brought online only after the sources system is offline.

5. **Rebuild** VMs with the RHEL OS minor release upgrade. **Replicate** customizations and SAS prerequisites. The **source** and **target** systems should be the same.

   See Perform the Prerequisite Steps on the Target System.

6. **Mount** the retained pool of disks that contain SAS binaries, SAS configuration files, SAS Depot, and SAS data file systems on the **target** system.

7. **Synchronize** or **mount** the contents of users' OS home directories from **source** system to **target** system.

8. Start all SAS servers on the **target** system.

9. Validate your SAS 9.4 deployment on the **target** system. Make sure that you take a full backup of the target system. See Validate the SAS 9.4 Deployment on the Target System.

Perform the Prerequisite Steps on the Source System

It is strongly encouraged that you perform a thorough validation of your source system. This allows SAS to provide support and help assure SAS customers that their SAS environment is fully operational when a SAS 9.4 deployment is unmounted from the source system cloud instance and mounted to a target system cloud instance. The following validation steps should complete successfully on the source system:

1. Validate your SAS environment. Instructions can be found in the `CONFIGDIR/Lev1/Documents/Instructions.html` file on each SAS tier. Include any customer-specific functional testing. An example is to verify access to relational databases.

2. Use SAS® Deployment Manager to successfully update passwords for every SAS internal account on each SAS tier. See Update a Managed Password for instructions.

3. Use the SAS Deployment Backup and Recovery tool to create scheduled backups. See Using the Deployment Backup and Recovery Tool for instructions.

4. Use the SAS Deployment Backup and Recovery tool to restore from a backup. See Performing a Recovery Using the Deployment Backup and Recovery Tool for instructions.

5. Validate or apply all (or at least one) available hot fixes and security updates.

6. Rebuild and redeploy web applications on the primary middle tier.

7. Re-cluster web applications on each middle tier node if applicable. See Add a Horizontal Cluster Member.

8. Validate that scheduled jobs execute as expected or reschedule those jobs and then validate their success.

IMPORTANT:

- You must perform full backups and snapshots of the source system prior to unmounting a SAS deployment from the cloud instance for recovery purposes.
- SAS binaries, SAS configuration files, third-party components provided by SAS, and user content, such as SAS code, are stored on data disks. This allows for the external storage to be unmounted and remounted to the new VM infrastructure (the target system), and no data movement or replication is required.

Perform the Prerequisite Steps on the Target System

Before you mount your SAS 9.4 deployment on the target system, ensure that the following prerequisites are met:

1. The cloud instance for the target system must be created with the minor release upgrade of the OS.

2. The target system must be equal to or larger than the source system. Source and target systems must be of the same instance type, the same network and security configuration, operating system configurations (including installed packages), subnet, proximity placement group, and so on.

3. Efforts should be made to build the target system so that it sustains or exceeds the same throughput requirements as the source system. You can use this SAS tool to perform the test.

   Note: Only the OS and ephemeral disks are mounted at this point. Use the SAS tool to measure the performance of these available disks. Use the SAS tool again after the data disks are mounted to verify throughput. Perform this test when you perform the steps described under Validate the SAS 9.4 Deployment on the Target System.

4. All SAS system requirements and prerequisites are applied to the target system. Any customizations that were done on the source system should be replicated on the target system. This includes the following customizations:
   - OS tuning parameters
   - OS scheduled init.d services
   - OS scheduled crontab entries
   - third-party software (for example, database client components or monitoring agents)
   - other SAS data that is not stored on the target file system

5. Users and the authentication mechanism that is used are the same on the source and target systems. This includes the following specifications: authentication provider and configuration, local groups and users with the same passwords (where local users and groups exist), and identical UIDs and GIDs. Keeping these specifications the same ensures that permissions on disk remain the same.

6. File systems are created to be the same as the file systems on the original hardware, and permissions on

all file systems are configured the same. See Components on Source and Target Systems for a comprehensive list of SAS components and default locations that are used for the source and target environment.

7. Host names and aliases of the new systems must match those of the old systems.

   IMPORTANT:

   Host names (including aliases) and ports are not changed because of this process. Note that switching from a fully qualified domain name (FQDN) to a short name is considered to be a host name change.

Components on Source and Target Systems

Table 1 details the various components and their locations and values on the source and target systems. It includes notes about how the transition is handled.

Table 1. Component Handling Across Source and Target Environments

Operating System Components	Source (Sample Values)	Target (Sample Values)	Method
Operating system image	x.x	x.y	Replace[1] with new minor release of the operating system disk on new infrastructure
Operating system home directories	/home	/home	Retain[2] or Replicate[3] content
Operating system boot and init processes	/etc/init.d	/etc/init.d	Replicate
Operating system authentication modules (for example, PAM in `/etc/pam.d`)	sssd, sasauth, gauth common IdP retain uid/gid	sssd, sasauth, gauth common IdP retain uid/gid	Replicate customizations

[1] Replace - a characteristic, whereby a pool of disks or a storage solution is expected to be decommissioned in favor of adopting a new version.

[2] Retain - a constraint, whereby a pool of disks or storage solution must be persisted between source and target systems (as opposed to Replicated, Rebuilt, or Recreated). In the context of this discussion, a data disk consisting of SAS binaries, configuration, and so on must be persisted by means of unmounting from source and mounting on target.

[3] Replicate - a constraint, whereby the act of replacing an operating system disk = necessitates that key content and configuration from the source operating system disk is re-created in a consistent manner to preserve the integrity of the target system.

Operating System Components	Source (Sample Values)	Target (Sample Values)	Method
Operating system prerequisites (common SAS prerequisites)	/etc/opt/vmware/vfabric	/etc/opt/vmware/vfabric	Replicate
Operating system permissions and file system mount options	selinux config Exec and noexec flags `sas` user as owner of !SASROOT	selinux config Exec and noexec flags `sas` user as owner of !SASROOT	Replicate
Operating system database libraries and ODBC configurations	Oracle client and configuration (tnsnames.ora)	Oracle client and configuration (tnsnames.ora)	Replicate
Operating system third-party software and agents for backup, monitoring, or other Enterprise Integration Technologies	Tivoli BMC Control-M Apache SOLR ESM	Tivoli BMC Control-M Apache SOLR ESM	Replicate
Operating system tuning and other common configurations that should be retained, for example, site-customized sshd parameters	selinux sshd_config nproc limits.d	selinux sshd_config nproc limits.d	Replicate
Network Components	**Source (Sample Values)**	**Target (Sample Values)**	**Method**
Networking elements like name resolution (IP address, FQDN, DNS alias, host name considerations)	hostname01 hostname01.domain.com sasmetadata01 sasmetadata01.domain.com	hostname01 hostname01.domain.com sasmetadata01 sasmetadata01.domain.com	Replicate (local IPs could be different as long as the name resolution is not impacted)
Firewalls	firewalld configuration on operating system security rules in virtual network and NACLs	firewalld configuration on operating system security rules in virtual network and NACLs	Replicate

SAS System Components	Source (Sample Values)	Target (Sample Values)	Method
Network or application load balancer	Back-end pool and health-checks to include source system	Update the back-end pool and health checks to include target system	Update
SAS binaries including IBM LSF if applicable	!SASROOT /opt/sas/software !LSFHome /opt/sas/thirdparty/pss	!SASROOT /opt/sas/software !LSFHome /opt/sas/thirdparty/pss	Retain
SAS Software Depot and deployment plan file	/opt/sas/resources/depot /opt/sas/resources/depot/plan_files/plan.xml	/opt/sas/resources/depot /opt/sas/resources/depot/plan_files/plan.xml	Retain or Replicate
SAS configuration	!SASCONFIG /opt/sas/config !LSFConfig /opt/sas/thirdparty/pss/lsf/lsfconf !JSConf /opt/sas/thirdparty/pss/pm/conf	!SASCONFIG /opt/sas/config !LSFConfig /opt/sas/thirdparty/pss/lsf/lsfconf !JSConf /opt/sas/thirdparty/pss/pm/conf	Retain
SAS Work library	/saswork	/saswork	Replicate mount options
Gridwork library	/saswork/gridwork	/saswork/gridwork	Replicate mount options (or Retain)
SAS data	/sasdata	/sasdata	Retain (or Replicate)
SAS Configuration parameters in sasv9_local.cfg and similar	UTILLOC=WORK | filename | location	UTILLOC=WORK | filename | location	Retain

SAS System Components	Source (Sample Values)	Target (Sample Values)	Method
Backup and recovery path (location used to store metadata and files) **Note:** Permissions must be identical between the source and target systems.	!SASCONFIG /Lev1/Backup/Vault /share/CentralBackupVault	!SASCONFIG /Lev1/Backup/Vault /share/CentralBackupVault	Retain
Operating system services (OSS) and scheduled jobs (init.d and crontab)	LSF and PM on boot Cleanwork Schedule	LSF and PM on boot Cleanwork Schedule	Replicate

Validate the SAS 9.4 Deployment on the Target System

1. Validate the environment as instructed in the `CONFIGDIR/Lev1/Documents/Instructions.html` on each SAS tier. Include any customer-specific functional testing. An example is to verify access to relational databases.

2. Use SAS Deployment Manager to successfully update passwords for every SAS internal account on each SAS tier. See Update a Managed Password for instructions.

3. Use the SAS Deployment Backup and Recovery tool to create scheduled backups. See Using the Deployment Backup and Recovery Tool for instructions.

4. Use the SAS Deployment Backup and Recovery tool to restore from a backup. See Performing a Recovery Using the Deployment Backup and Recovery Tool for instructions.

5. Validate or apply at least one middle-tier hot fix.

6. Rebuild and redeploy web applications on the primary middle tier.

7. Re-cluster web applications on each middle tier node if applicable. See Add a Horizontal Cluster Member.

8. Validate that scheduled jobs execute as expected or reschedule those jobs and then validate their success.

9. Any services, including SAS or Platform Load Sharing Facility (LSF), that are configured for boot setup with start-up, will need to be reinitialized. For example, if you have SAS Grid Manager for Platform and LSF services setup for boot start-up, run the `hostsetup` script.

Note: Use this SAS tool to measure the throughput of these available data disks.

Release Information Content Version: 1.0 July 2024.

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