Paper 3730-2019

Modern, Fast, Automated and Secure Trigger-Based SAS® 9.4 Application Configuration

Timo Blomqvist, OP Services Oy; Tapio Kalmi, SAS Institute Oy

ABSTRACT

Traditional SAS® application configuration and administration has many detailed tasks for which you need deep knowledge of the SAS® Platform. When these tasks are done manually, they take a lot of time and mistakes are possible. That is the reason why we wanted to modernize the way to do it. SAS Platform administration configuration tools have been used as a quick start to automate configuration tasks. Some of the tools have been automated and integrated with the enterprise-level identity and access management process. SAS Platform user IDs, rights, and authorizations are now administered with as much automation as possible.

When user groups have been added into Active Directory for a new application, the application configuration is automatically done in the development environment in the next morning. The automation includes metadata folders, groups, ACTs, libraries and SAS® LASR™ Servers, and filesystem folders.

There is also a SAS® Stored Process interface for production administrators to promote the configuration grant for selected applications.

The benefits of this solution come in many ways. Only identity and access management integration save more than the development costs. And the process is faster than before, which improves the end-user experience by many days. Note that more savings will be achieved in the configuration part. On the technical side, this solution provides top-level naming standards and best practices for a variety of SAS technologies.

INTRODUCTION

This paper describes the main business drivers why SAS application configuration tasks have been automated at OP Group. It will also tell the design ideas and principles to make this task possible.

Sometimes it is surprising how near the needed parts are in the first place. In this case the fine tuning and advanced usage of active directory naming standards was the key to integrate identity and access management process with SAS application configuration process.

BUSINESS NEEDS FAST SERVICES

The change from the old workflows to new standards is accelerating all the time. Many companies have done modernization in enterprise level identity and access management (IAM) systems. Manual system administration tasks have been automated to digitalized self-service applications.

From SAS platform owner's perspective IAM is just the first step to enable authentication and authorization. The real task is to configure the SAS application environments properly. The rules are the same case after case. The backbone structures are the same time after

time. Many elements are common even if the application functionality and data content may vary. From that background SAS Institute Denmark developed Turbo Charge tools for SAS consultants to make application configuration faster and easier. OP Group wanted to go one step further: They needed automation for those tools. That need became evident when OP Group deployed new SAS 9.4 Grid platform with the idea of agile analytics. Any function of the organization can have their own application area for data integration and analysis. The applications can vary from few SAS Visual Analytics reports to traditional data warehouses.

We created fully automated SAS application configuration (AppConfig) which builds the environment time after time according the same design principles. That way we got rid of inconsistent human errors and different design styles. Now we have standard structures and the maintenance is easier than before. Very nice bonus is the fact that we don't need to wait for expert resources to make SAS application basic configurations anymore. Now the experts can concentrate to deploy SAS services for special cases.

The new user experience comes in many ways. Business units tell the type of needed application and the name of business function in web form. The order goes from business to SAS administration in real time and the SAS administration approval for the order is at the same time order to IAM process which is done by 3rd party. It takes 1-2 working days to get active directory updated. After that the rest is fully automated with AppConfig. The user group and application naming standards are defined so that the new SAS user group in active directory is used as trigger to configure new SAS application platform. With this solution the time from idea to development has been reduced from 1-8 weeks to 2-5 working days.

The users apply for roles (SAS user group memberships) in real time by using IAM web application. Superior and data owner use the same IAM web application to approve the roles. When needed approvals are available, the active directory is updated in real time. Active directory synchronization to SAS metadata is run 3 times per day and finally SAS users get new authorizations and permissions in 1-24 hours. If you order new role at 11 o'clock, get instant approvals and SAS Metadata update is run at 12 o'clock, it means new role delivery in one hour.

SAS administrators benefit the most from the new workflow. They just need to do one click approvals for SAS application platform initialization, SAS user role acceptance and SAS application platform promotion. Note that the most important task is still there: The administrators need to check that the new application and permissions are really needed.

PLANNING PRINCIPLES

The requirements for automated application configuration were defined as follows:

- Compliant Security Design
- Automate as much as possible
- No need to edit anything at daily basis
- Initial editing is done only once, no edits after that
- As easy initial edit as possible
- All controls in CSV files, no XML, Excel or SAS controls
- Detailed documentation in control files and in metadata
- Additional documentation only at high level as needed by Security Department, SAS Administration and SAS Application Developers

TECHNICAL SOLUTION

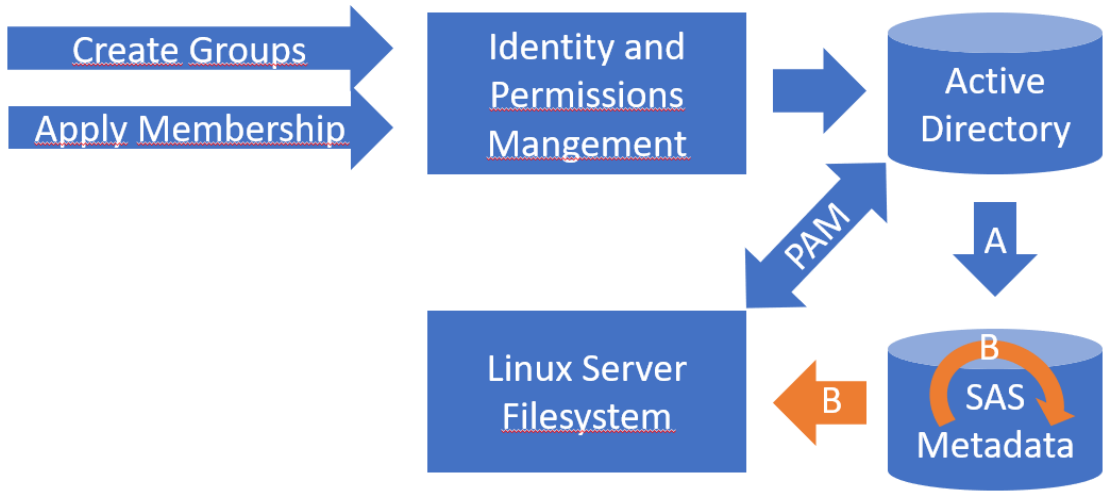


Figure 1. Overview of automated application configuration process

The IAM process updates user groups, users and user group memberships into active directory. That part is done with 3rd party enterprise level tools which have been developed for that purpose. These tools are customized according to the use cases. In our case it meant one new web form which is used to order new SAS user groups and system users. All user level actions are done with common standard procedures after the new SAS user group has been added to the system.

Linux Pluggable Authentication Modules (PAM) are configured as part of Linux installation and that needs to be done only once per SAS Platform. These modules integrate Linux and active directory tight together. This is the key element when the file system level security is implemented. All users will have own Linux user accounts when logging in to Linux.

SAS user group, user and role synchronization (A) is scheduled to run 3 times per day. You can implement that by editing the filters into SAS code which is provided with the SAS deployment package. Another solution is to use the Metacoda Identity Sync Plug-in, which allows you to easily import, check and synchronize identity-related SAS® metadata with enterprise directories without the need to edit SAS code.

The automated SAS application configuration (B, AppConfig) is run every time after the active directory synchronization. This is fully independent Base SAS code and it can be run also without the active directory synchronization at any time. %mduextr macro reads identity metadata into SAS tables and after that SAS Data Step metadata functions are used to read and write all needed metadata objects.

AppConfig compares the active directory SAS user groups with existing application names at root level of metadata folder tree. In development environment new SAS application platform is created every time, when new SAS user group is found without corresponding application folder. In other environments SAS Administrators grant the application to be promoted by using SAS Stored Process designed for that task. Application Promotion List stored process shows all SAS applications available and updates the control data according to SAS Administrator's selections.

AppConfig updates SAS metadata by using sasadm@saspw account and operating system level actions are done by sas installer user. Note that AppConfig environment should be carefully secured, because these accounts have large permissions in SAS Platform.

After AppConfig has been run the Linux script continues by using Linux root account. The filesystem level privacy is implemented by changing the ownership of the new SAS application root folder from SAS installer to SAS application's system user account and the group level permissions from SAS group to SAS Application Group. After this moment the SAS installer and SAS Administrators will not see the contents of the application folder. The script gets all needed parameters from SAS application configuration report file which is created by AppConfig.

Last but not the least part of the configuration script is to copy the updated Application ID List control data from development environment to test and production environments. It is copied next to the target environment's control data to give the needed information for the Application Promotion List stored process.

SUCCESS KEYS

Implement compliant data security design

If the environment has the requirement for data privacy, you need to secure the whole operating system so that each user is using individual user account when logging in. At Linux this means Pluggable Authentication Modules (PAM) or other technique providing the same functionality. At minimum there should be integration to enterprise level authentication domain and functionality for user account management.

Define only needed user groups

To keep SAS administration as easy as possible you need to define the user roles and user groups at the same level with the real organization roles. In Finland the organizations are tuned to be as slim as possible because of the small size of the market. Our analysts and application developers have a great variety of tasks and we have defined only one developer role for all of them. Current Data Scientist term describes this role very well.

All kind of users who use the SAS application rather than develop it, are in the consumers group. Only exception is the application level administrator role, which is used only for application's SAS Visual Analytics Server administration. Each application with SAS Visual Analytics reporting is configured to have own dedicated SAS Visual Analytics Server as well.

The system account has own group even if there is only one user. The system account has been created mainly for two reasons: to be the owner of the application and to run scheduled batch runs.

Different SAS client software metadata roles and groups are combined to customized application user groups in csv control files. AppConfig makes the metadata configurations according to these rules. This is the most efficient way to define this part: All capabilities are inherited to custom user groups from standard SAS user groups and roles. The standard SAS user groups and roles are used as is.

Follow SAS Golden Rules for Security Model Design

You need to keep also SAS Metadata security configurations as simple as possible. Even if the SAS metadata security model has many features and seems to be complicated, it can be configured by following only couple of main rules. SAS Golden Rules for Security Model Design point out the 8 golden rules to follow. This documentation is highly recommended reading before you start your metadata journey. Note that the journey doesn't end when the initial configurations have been done. No matter if the configurations are updated manually or automatically, the result needs to be tested and monitored. We have found out that Metacoda Security Plug-ins work very well for this purpose. You can automate monitoring and get alarms if some parts of metadata are not following the defined rules.

Create naming standard which helps you

The naming standards are used to integrate identity and access management process with SAS application configuration process. Active directory user group names have prefix telling if the group is SAS user group or not.

After the prefix the next part of the name tells the SAS Application type. All SAS applications are grouped using application types and the SAS application configuration control data tells which parts should be configured for each application type. If we are configuring SAS Information Delivery Portal environment, there is no SAS Visual Analytics reporting, and vice versa. SAS application providing Web Service interface for scoring has only the logic and control data which is needed for scoring, but nothing else. The SAS application areas for SAS Enterprise Miner analytics have great variety of input data sources and all data needed for modelling, but that application area is not used for direct reporting or scoring Web Services at all. The separation of these functions is part of data privacy compliant security design.

After SAS Application type the active directory user group name has the name of the function which becomes also the name of the application. Avoid special characters with the name and keep the name short: Some versions of active directory support only 20 characters for user group name. The name should be informative, because this part of the active directory name will be used in metadata folder name with the SAS application id.

Create unique SAS Application ID

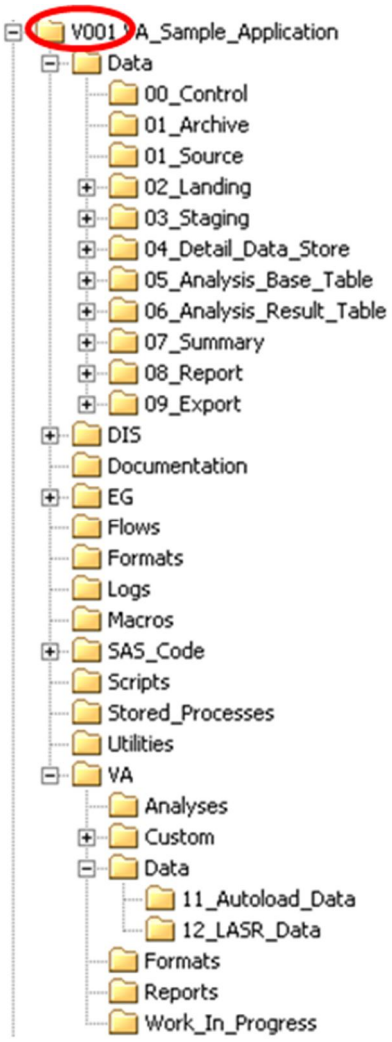
The unique SAS application ID is needed for SAS naming standards. When we have many SAS applications in the same SAS metadata side by side and the developers can't see them all, there is no other way than naming standard to keep the environment working properly. Especially you need to design the SAS metadata object naming very carefully, because SAS metadata requires unique metadata object names. That's because the SAS metadata promotion routines use metadata object names to match source and target environment metadata objects. When all metadata object names start with the unique application id, there should not be any naming conflicts across applications. And developers can check the naming inside the application they are developing.

Remember modularity and reusability

When designing the control data for configurations there are many general parts which needs to be designed only once. Then there are parts which should have general default values and a way to define application group level exceptions to defaults. At some cases it is best to define fully separate controls for each application group. This way the development of new application group configuration doesn't have any impact to the existing application groups. For optimal solution you need to find the balance between integration and separation.

Most of the cases can be configured with the application group default settings. Then there are some special cases at application level design. The special cases vary a lot and therefore we have left the automation of these parts to be done later. We will wait and see, which special cases are most common. These should be the best candidates for further automation in the coming versions of AppConfig.

UNIQUE SAS APPLICATION ID



The main idea is to keep different SAS applications separate from each other in one environment. This is done with application specific and unique SAS application id.

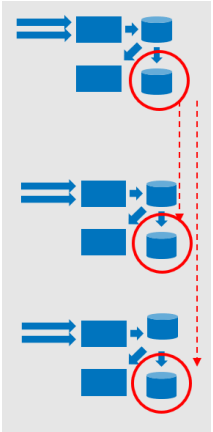
Figure 2 shows the sample SAS metadata folder structure. The application id V001 is only in the root of the folder tree structure. This is enough, because all subdirectory paths have the upper level pathname parts to make up unique SAS metadata pathname.

NOTE: This sample shows also the selected data libraries for sample SAS application group (V). The programs are stored below SAS client specific folders: DIS for SAS Data Integration Studio jobs, EG for SAS Enterprise Guide projects and SAS_Code for Base SAS programs. Below each application specific folder there is the same subfolder structure as below data folder. This way the navigation from data folder to the program folder is as easy as possible.

NOTE: All metadata object names should start with application id: The library reference for control data SAS library in V001 application would be v001_ctl, the name of the control table would be v001_ctl.daily_run_parameters and the name of the control initialization job would be v001_ctl.daily_run_parameters_init. Library and table metadata should be stored into Data/00_Control subfolder and the job should be stored into DIS/00_Control subfolder.

On the other hand the application id should be the same for one application in all environments. This enables the SAS metadata promotion tools to find the match when importing metadata objects from one environment to another.

Figure 2. Sample metadata folder tree



In development environment AppConfig creates SAS application ID for each application and initializes the application platform for all new applications automatically. This behavior is set in AppConfig control parameters.

The configuration script copies the list of SAS application IDs from development environment into test and production environments as well.

In test and production environments AppConfig control parameters are set to wait the grant from SAS administrators before the configuration is done for new SAS application platform.

Another name for this grant is SAS Application Platform Promotion.

Figure 3. Unique SAS Application ID and SAS Application Platform Promotion

SAS APPLICATION PLATFORM PROMOTIONTHE SELECTED NEW

SAS application platform promotion is our own term for SAS application configuration grant. We have implemented SAS Stored Process for SAS administrators for this task. The Stored Process lists the SAS Application IDs, names and configuration timestamps from two environments. The list tells which applications are available in the source environment and which have not been configured in the target environment. If the user clicks ”Promote” link the SAS stored process asks if you really want to grant the promotion for the selected application. If you answer Yes, the Stored process updates the control data so that AppConfig will create the new SAS application platform in the next run.

The list acts also as a summary of the SAS application platform configurations. The timestamps tell when the applications have been configured in different environments, “Promote” text tells that configuration is not granted yet. “Promoted, not configured” text tells that the grant is given, but the configuration has not been run yet.

APP_CONFIG Application Promotion List
SAS Deployment: OP VA GRID

ID	Application Name	UAT Configured	PROD Configured
S001		20180518_135609	Promote
V001		20180518_135609	20180518_135609
V002		20180518_135609	20180518_135609
V003		20180518_135609	Promote
V004		20180518_135609	Promoted, not configured.
V005		20180518_135609	20180518_135609
V006		20180518_135609	Promote
V007		20180518_135609	20180518_135609
V008		20180518_135609	20180518_135609
V009		20180518_135609	20180518_135609
V010		20180518_135609	Promote
V011		20180518_135609	Promote

Figure 4. SAS Application Platform Promotion List

ALL BASIC PLATFORM STRUCTURES CREATED AT ONCE

AppConfig creates all the basic structures for the new SAS application. The most important part is the new SAS Application ID. It needs to be created first, because the id is used in SAS Application home folder name as well as in all metadata object names.

After configuration is run the SAS metadata will have all basic folder and pathname structures. These include SAS library definitions for all common data areas and pathnames for all common SAS Data Integration Studio deployment directories for jobs and stored processes.

All application specific identity and authorization metadata objects are created. These include user groups metadata with members, groups and roles; the access control templates with all defined permission settings; and authorization settings to link the created access control templates with the created application root folder and SAS application servers.

Dedicated SAS Visual Analytic Server and SAS LASR Library are created for the new SAS application into metadata only if the application group controls tell that these components need to be configured.

The SAS application folders are created also on the filesystem side. SAS application server specific SASApp_server_autoexec_usemods.sas program is updated to include the new application level Application_autoexec_usermods.sas program, which is created into application root folder. These programs append the application specific pathnames to fmtsearch and mautocall option configurations. AppConfig csv controls tell the SAS application server context for each application group.

CONCLUSION

Automation is more and more common in modern installations and configurations. Cloud solutions make it easier to get new hardware resources and SAS deployments in place. But still after the SAS Platform level installations there is wide range of configuration tasks which needs to be done at application level. These tasks can and need to be automated as well.

The automation of application level configurations creates a new setup where the basic structures and naming standards are common across the whole enterprise. The benefits of fast application configuration are immediate, but there is more than that. When the basic structures are the same, also the maintenance and development tasks are more homogenous than before. The developers can change from one application to another faster than before, because the basic ideas are common. This will save more time and resources.

This case is also good story about how to help others by helping yourself. When SAS administrators build tools for themselves they can make a difference.

ACKNOWLEDGMENTS

Credits of the successful project belong to the whole team. The Linux server administration tasks were done and scripts were created by Tieto Ostrava, SAS Team. Especially Jaromir Mielec, Matej Baloga and Filip Pinter have been in the major role. More specialized questions about SAS installations have been resolved with the help of Ilkka Maristo from SAS Finland Technical Architecture Services.

The idea of fully automated SAS application configuration was born after we had used the best practices and configuration tools which were created by SAS Institute Denmark consulting and SAS Global Enablement and Learning Team.

RECOMMENDED READING

- *Linux Pluggable Authentication Modules (PAM)*

  http://www.linux-pam.org/

- *SAS Golden Rules for Security Model Design*

  https://communities.sas.com/t5/SAS-Communities-Library/Golden-Rules-for-Security-Model-Design/ta-p/373542

- *Metacoda SAS plug-ins and tools*

  https://www.metacoda.com/en/

- *SAS® 9.4 Metadata Model: Reference*
- *SAS® 9.4 Intelligence Platform: Security Administration Guide, Third Edition, Metadata Authorization Model*
- *SAS® 9.4 Language Interfaces to Metadata, Third Edition, DATA Step Functions*

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Timo Blomqvist
OP Services Oy
timo.blomqvist@op.fi

Tapio Kalmi
SAS Institute Oy
tapio.kalmi@sas.com