Paper 280-2010

SAS® Table Server and EG Project in Content Server – A Big Step Forward

Gaurav K Agrawal, GCE Solutions Inc, Bloomington, IL

ABSTRACT

In order to design a well secured SAS® BI Intelligence platform, an Architect has to think about SAS® Metadata and even Host layer security also. SAS® is very powerful and flexible to implement any kind of security model for SAS® Metadata environment. However in order to implement the Host layer security architects are dependent more on the Host (UNIX/Windows) security model.

A secured SAS® environment needs a good amount of effort to be invested in order to secure UNIX/Windows host layer also. SAS® 9.2 BI Intelligence Platform has taken a big step forward towards reducing the designing and maintenance effort required to secure host layer. SAS® 9.2 has come up with new tool called SAS® Table Server, which ease SAS® Datasets host layer security in addition to lot of other features. SAS® 9.2 also launched the concept to store SAS® Enterprise Guide project in SAS® Metadata server in order to secure the EG code/project also rather saving in host layer or LAN location during development.

1. INTRODUCTION

"SAS® 9.2 Table Server" and "SAS® Enterprise Guide project in Content Server" together brings down lot of effort required to secure the SAS® environment and make environment much easy to implement and maintain. This paper is more focused on both of the features and how they are securing SAS® Datasets and SAS® code and at the same time reducing the maintenance effort.

Point to be noticed here that SAS® Datasets and SAS® code are the two major components which brings an advance level of host layer security and reducing this effort around these imply a fast turnaround time for SAS® environment build and easy administration.

Lets discuss how mentioned features are reducing maintenance effort and how both levels (SAS® Metadata and Host layer) of security can be maintain only by SAS® Intelligence Platform Metadata environment.

2. APPROACHES TO SECURE SAS® DATASETS:

In order to better understand the new features in SAS® 9.2, lets first discuss about the traditional approach and challenges in securing the SAS® datasets at host layer. Then we'll discuss that how same can be achieved using SAS® 9.2 Table Server.

2.1 SECURITY CHALLENGES IN 9.1.3 AND EARLIER SAS® ENVIRONMENT

In SAS® 9.1.3 whenever we are designing SAS® Metadata security, we discuss about the host layer group, sub groups and all. If process is spawned by a group/division ID then in that case achieving project level security within division and group is very tough. Result of that will be that one project can access the data of other project of same division through EG because spawning ID is same.

However in case where SAS® process on UNIX being spawned by individual User ID (Host Authentication or PAM(UNIX) or LAM(AIX)) then any level of security can be implemented but it requires good amount of effort to be

invested in designing host layer security and administrator has to ensure that all UNIX groups are well maintained and designed. So whenever there is change in Metadata layer security for the user at same time security might need to be changed in Host layer also. Considering the typical organization structure and because administrator is directly dealing with SAS® security it is easy that SAS® Administrator change user permission quite fast in Metadata but in order to change the security on UNIX, administrator has to raise different kind of tickets to update the permission at host layer. Hence security change is not easy in such environment.

2.2 SECURITY ADVANTAGE BY INTRODUCING TABLE SERVER IN SAS® 9.2 ENVIRONMENT

The Advantage of SAS® 9.2 Table Server is that all SAS® datasets are being served by particular service which is running under "sas"/"sasts" ID (ID may be different and it really depends on the way SAS® Intelligence Platform architecture is implemented). Any other user or group will not have access on SAS® Datasets on host layer until or unless SAS® Architect/administrator decides to add any other groups as administrator for this table server assigned area at host layer for required maintenance. This means that any Spawned ID (other than "sas" or "sasts") will not have direct access on the SAS® Datasets. SAS® Table Server service checks the user security at Metadata layer and accordingly SAS® Datasets are served to user's process. Hence it is not required that we create many UNIX group to implement the security for SAS® Datasets and we can maintain it just by SAS® Metadata security.

Another point to consider is that SAS® 9.2 has come up with the feature called Tokenized. What is that and how it works? SAS® Tokenized will pass the actual User identity to the Spawned process even though process is spawned by group ID. Hence whenever spawned process will interact with Table Server service then actual User ID will be used to determine the user permission from Metadata and accordingly data will be accessed. SAS® architects/administrators who have good understanding about this must be remembering that to achieve this in 9.1.3, we use to pass METAUSR and METAPASS in SAS® code but now it can be implemented for complete SAS® BI platform.

There is another enhancement around the same line, in SAS® 9.1.3, in some cases SAS® Stored process was a problem around security because it was spawning the process under "sassrv" id. Because of this it was able to access Libraries even though actual users (who initiated the session) do not have access on data (not applicable to all case). In that case also now data is very much secured and it will be accessed only if actual user does have access on the data. Thanks to SAS® 9.2 Table Server and SAS® Tokenized featured.

SAS® Table Server also provides other very useful features like Column level security and Row level security, which are very easy to implement and make Table Server more powerful. SAS® Table Server can interact with approximately all the database and there are various features provides around different kind of SQLs to database.

Considering the scope of this paper other features of Table Server will not be discussed here. However below pictures shows its interaction with databases.

Please see below Figure, which depicts the above mentioned details in a pictorial formats.

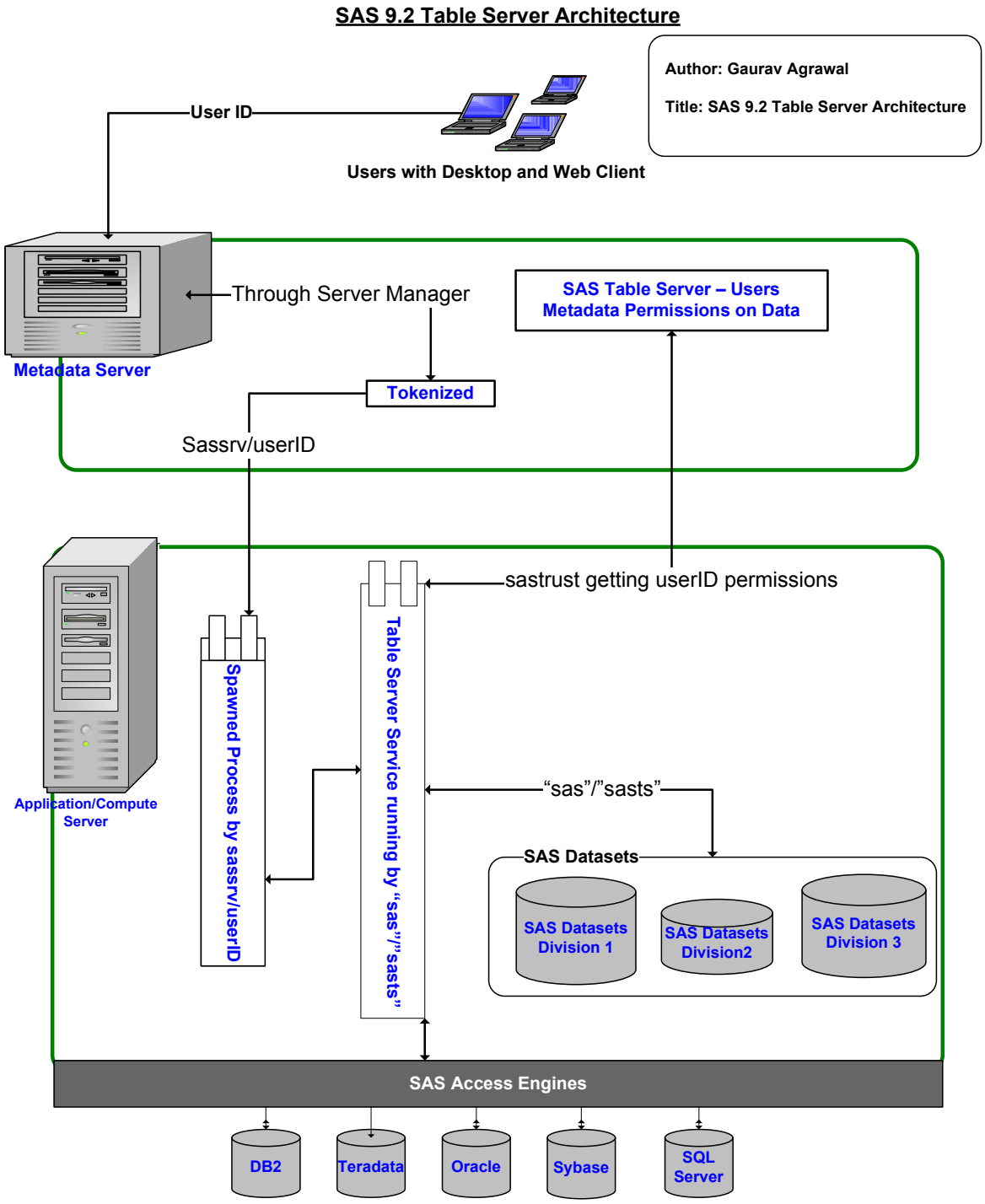

Figure 1: SAS 9.2 Table Server Architecture

Notes for Above Figure:

- ✓ SAS Datasets will be owned by "sas" and no other user do have permission on these datasets
- ✓ Every Divisions datasets will reside in separate host layer folders to differentiate the data between divisions and for easy maintenance.
- ✓ Table Server can interact with different databases and same was shown here
- ✓ In order to explain the Table Server architecture, this figure do have only Metadata Server and Compute

Server of SAS Intelligence Platform

Below steps are followed by the process in order to access SAS® datasets through table Server

- ✓ A process will spawned against group/user ID as per the designed architecture. This process is tokenized and keeping User identity secured (intact)
- ✓ Hence this process will interact with SAS® Table Service to access the data
- ✓ Table Service will take the actual user ID from Spawned process and will check its Metadata privileges in SAS® Metadata Table Server configuration
- ✓ If actual user (not Spawned ID) do have access on the Metadata/Data then as per authorization, request will be processed
- ✓ SAS® Table Server service will access the data on behalf of Spawned process and will give to SAS® Spawned process.

Note: SAS® Table Server does maintain all database related query authorization for DDL, DML and DCL queries.

Note: Some SAS® Program may/will required input from flat files also. Company may decide to put little UNIX security for those data file. Also there are many possibilities to implement security using like SAMBA drive (For UNIX flavor environment), by which even UNIX drives can be mapped to PC Windows and other such things can be implemented. As UAT and Prod environment will be more secured so process already will be automated there and only concern remains around Development environment. However if manual intervention is required in order to put the file on UAT and PROD Server then SAMBA may be good option for UNIX flavored SAS® environment.

3 APPROACHES TO SECURE SAS® ENTERPSISE GUIDE PROJECT

Lets discuss how mentioned feature ("SAS® Enterprise Guide project in Content Server") is reducing maintenance effort of security through SAS® Intelligence Platform Metadata environment during development and then by UNIX (when development is finished).

In order to understand the SAS® code or EG project security lets first defined the development cycle for such scenario/projects.

- ✓ User Start developing the SAS® code/project by opening the SAS® Enterprise Guide
- ✓ User(s) keep(s) doing the development in SAS® EG project and save the project in SAS® Metadata environment
- ✓ After the development is finished user would like to execute this code against UAT and then against Prod data
- ✓ User may request any of the two below things for codes
  - User may want that code will stay in SAS® Enterprise Guide format and only requirement is to move SAS® Enterprise Guide Project from Dev to UAT and then to PROD
  - User may also request for scheduling the code through scheduling mechanism (UNIX Cron, Windows Scheduler, LSF Scheduler or Enterprise scheduling tool)

3.1 SECURITY CHALLENGE IN 9.1.3 AND EARLIER ENVIRONMENT FOR SAS® CODE

In SAS® 9.1.3 we can save SAS® Enterprise Guide project either in Host layer or Local User computer or LAN Drive. This shows that EG project location will always be separate from the SAS® Metadata environment and should be separately secured. If project is being saved on UNIX folder then required UNIX groups to be created in order to secure the project or Code. If project is being stored on LAN then it should be secured by Windows permissions.

3.2 SECURITY ADVANTAGE BY INTRODUCING BY STORING PROJECT IN SAS® 9.2 METADTA ENVIRONMENTS

SAS® 9.2 architecture is folder based architecture and everything in Metadata belongs to a folder. Hence for every

division/group we can create division folder. Under a division folder we can create different folders for all projects belongs to a division. Same way in project folder we can create separate folder like “EG project”, “Maps” “Reports” etc. In “EG Project” folder user can save their EG project. Security permission on this folder can be implemented using the ACTs (Access Control Templates) in SAS® Metadata environment. In SAS® 9.2 you can create/manage different kind of roles for EG user itself and accordingly menus will be visible to user.

Below figure shows the different folders created inside a project for a division. In the same project folder, we can create a folder for SAS® EG Project, which will be used by SAS® EG developer of that project.

Hence during the development SAS® Enterprise Guide project is well secured inside SAS® Metadata environment and there is no required to implement separate Host layer/LAN security for the development phase.

A point comes here that after development is done then we have to handle SAS® EG project and code. As discussed below mentioned two scenarios are possible and let’s discuss each of these

- ✓ User may want that code will stay in SAS® Enterprise Guide format and only requirement is to move SAS® Enterprise Guide Project from Dev to UAT and then to PROD
- ✓ User may also request for scheduling the code through scheduling mechanism. It is up to organization that what kind of scheduling tool they have and decided to use like UNIX Cron, Windows Scheduler, LSF Scheduler or Enterprise scheduling tool

3.2.1 DIRECTLY SAS® EG PROJECT USED TO RUN JOB IN UAT AND PROD

In this scenario SAS® EG project is directly accessed by SAS® user and manually user will trigger the SAS® job. This EG project can be promoted to UAT and PROD environment using the export import utility provided in SAS® 9.2 for EG project.

This scenario does not require placing anything outside of the SAS® Metadata environment hence all security can be maintained only through SAS® Metadata Security.

3.2.2 SAS® CODE EXTRACTED FROM EG PROJECT IS SCHEDULES IN UAT AND PROD

In this case simply let SAS® Administrator know that what all jobs need to be scheduled and SAS® administrator will schedule those jobs under right credential of division to run the job. Point to be noted that in UAT and PROD normal developer will not be having any host layer access for Code development and only Administrator has to own this responsibility.

However in order to schedule developed job in SAS® Development environment it can be handed over to SAS® Administrator and/or this can be achieved using Windows Scheduler (only for development phase) to run the job at a particular point of time. If user has host access in Development environment then Unix Crontab possibility also can be used however it depends on the design of UNIX security architecture.

SAS® Administrator may also provide/consider the SAS Schedule Manager plug-in to user for scheduling the SAS® jobs.
Note: Enterprise Scheduler tool capabilities also need to be explored for Development environment.

5.6 RECOMMENDATION

This paper talked about the approach considering SAS® 9.2 Table Server and Project in SAS® Metadata Server. However I do recommend that client should discuss all available approaches and choose the best suited environment for the organization. There are lot of variation between organization requirements and structure hence its worth putting effort in discussing all approaches. SAS® Architect will play a key role in order to understand the company requirement and then will be able to present the best solution for the company.

6. CONCLUSION

"SAS® 9.2 Table Server" and "SAS® Enterprise Guide project in Content Server" together brings down lot of effort required to secure the SAS® environment and make environment much easy. SAS® Table Server also brings lots of other features in order to interact with databases and also around row and column level security. Hence considering SAS® Table Server 9.2 is worth to go for.

7. REFERENCES

1) SAS Institute, Inc. (2006), SAS® Intelligence Platform Administration Guide v9.1.3, Fifth Edition. Cary, NC: SAS Institute Inc.
2) SAS Institute, Inc. (2006), SAS® Intelligence Platform Installation Guide v9.1.3, Fifth Edition. Cary, NC: SAS Institute Inc.
3) SAS Institute, Inc. (2006), SAS® Intelligence platform Overview v9.1.3, Second Edition. Cary, NC: SAS Institute Inc.
4) SAS Institute, Inc. (2009), SAS® 9.2 Intelligence Platform Data Administration Guide
5) SAS Institute Inc. (2009), SAS® 9.2 Intelligence Platform: Web Application Administration Guide
6) SAS Institute Inc. (2009), SAS® 9.2 Intelligence Platform: Security Administration Guide.
7) Work Experience on SAS® 9.1.3 and 9.2 Intelligence Platform

8. ACKNOWLEDGMENT

I would like to give many thanks to Monika Singhal and Hitesh Sharma for reviewing this document and for making it more useful and readable for the readers.

9. RECOMMENDED READING

http://support.sas.com/documentation/

10. CONTACT INFORMATION

You can contact author at:

Name	:	Gaurav Kumar Agrawal
Address	:	1717 R T Dunn Dr, Suite# 2011 Bloomington, IL 61701
Work Phone	:	7064053450
Fax	:	7062436415
Email	:	gaurav_agrawal@yahoo.com