

A Practical Approach to Managing a Multi-Tenant SAS® Intelligence Platform Deployment

Jim Fenton, Robert Ladd, SAS Institute Inc., Cary NC

ABSTRACT

Modernizing SAS® assets within an enterprise is key to reducing costs and improving productivity. Modernization implies consolidating multiple SAS environments into a single shared enterprise SAS deployment. While the benefits of modernization are clear, the management of a single-enterprise deployment is sometimes a struggle between business units who once had autonomy and IT that is now responsible for managing this shared infrastructure. The centralized management and control of a SAS deployment is based on SAS metadata. This paper provides a practical approach to the shared management of a centralized SAS deployment using SAS® Management Console. It takes into consideration the day-to-day needs of the business and IT requirements including centralized security, monitoring, and management. This document defines what resources are contained in SAS metadata, what responsibilities should be centrally controlled, and the pros and cons of distributing the administration of metadata content across the enterprise. This document is intended as a guide for SAS Administrators and assumes that you are familiar with the concepts and terminology introduced in SAS® *9.4 Intelligence Platform Security Administration Guide*.

INTRODUCTION

The central point of control for a SAS server deployment is SAS Metadata, which houses all the SAS environment assets. Depending on the SAS deployment type, managing and administering SAS Metadata takes on different responsibility levels.

In a small single user environment, like a training class, the individual user must take on all administrative responsibilities. On a department sized deployment, a single user might take on the administrative role, or leave the basic administrative responsibilities up to individual users. In enterprise-level SAS deployments individual departments become tenants in a single shared SAS environment, and centralization of many administrative responsibilities is needed to manage access to resources and changes. Some administrative responsibilities can be distributed to select individuals across the organization allowing timely and efficient operation.

This paper defines what SAS Metadata is, the tools for administering it, and it outlines the pros and cons of providing access to components within the administrative user interface for an enterprise-level SAS deployment.

For this paper, the SAS Administrator is defined as the overall SAS environment administrator, like the unrestricted SAS Administrator. The SAS Group Administrator can represent a distributed group administrator, a SAS Group Developer or any custom administrative role. Administrator is a general definition for either of these administrative classes.

SAS METADATA

The SAS Intelligence Platform core is SAS Metadata. SAS client interfaces and SAS servers depend on it for vital information about the SAS environment. There are three main SAS Metadata components: The SAS Metadata Repository, the SAS Metadata Server and SAS Management Console. SAS Management Console depends on the SAS Metadata Repository and SAS Metadata Server for the capabilities it provides for SAS administration.

SAS METADATA REPOSITORY

The SAS environment information assets are managed in a common metadata layer called the SAS Metadata Repository. This repository stores objects such as library and table definitions, information maps, stored processes, SAS jobs and schedules; it is a central point of control over the quality and consistency of data definitions, business rules, and defined processes. The repository also stores

information about system resources such as servers, the users who access data and metadata, and the rules that govern what a user can access and do inside the SAS environment.

SAS METADATA SERVER

The SAS Metadata Server is a multi-user service that provides access to the SAS Metadata Repository that is shared by all SAS applications and users in the environment. This server process executes the controls established in the SAS Metadata Repository to provide access to resources stored inside. It also provides centralized management and security capabilities to ensure that all users and applications access appropriate and consistent information.

SAS MANAGEMENT CONSOLE

SAS Management Console is a user interface, typically installed on an Administrator's desktop, to view and manage the metadata objects that are stored in the SAS Metadata Repository. SAS Administrators can manage and monitor SAS servers, explore and manage metadata objects, manage user and group accounts, administer security and provide methods for organizing and securing SAS content across multiple user groups.

SAS Management Console includes three tabs highlighted in Figure 1 for organizing or finding content within the SAS Metadata Repository. The Plug-ins tab provides access to environment and administrative resources using named plug-in modules for handling specific tasks in the SAS environment. Plug-in management and administration is explored in more detail in the following sections.

The Folders tab is a hierarchical structure designed to organize and secure SAS content used by applications and users in the SAS environment. Library definitions and job schedules are two examples of metadata content that are stored in metadata folders and secured. Details on the administration and security model for SAS Folders can be found in SAS Global Forum Paper 311-2010, "A Practical Approach to Securing a SAS® 9.2 Intelligence Platform Deployment" and in the *SAS® Intelligence Platform: Security Administration Guide*.

The Search tab provides detailed capabilities for finding metadata objects in the repository. While Search is not a focus of this paper, managing access to this tab can be controlled through Role assignments discussed later in this paper.

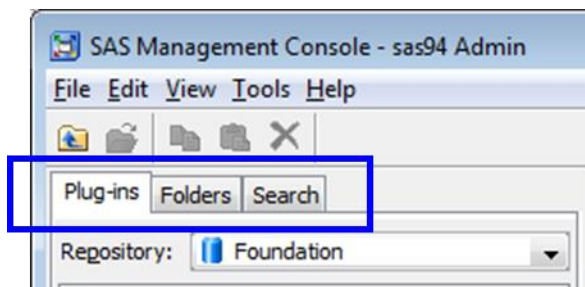


Figure 1 SAS Management Console Tabs

SAS MANAGEMENT CONSOLE PLUG-INS

The Plug-ins tab contains application modules, or plug-ins, designed to create and maintain metadata for a specific resource type. Figure 2 shows a full list of plug-ins provided in the SAS deployment used in this paper. As the term plug-in implies, plug-ins can be added to support additional metadata types that are needed to manage and administer a SAS environment.

The plug-ins are grouped into two basic categories: registered and unregistered. Registered plug-ins have an associated Role Capability that can be assigned to a user or group of users, like SAS Group Administrators. The unregistered plug-ins do not have an associated capability by default and must be administered in other ways. The plug-in administration and security is discussed in later sections.

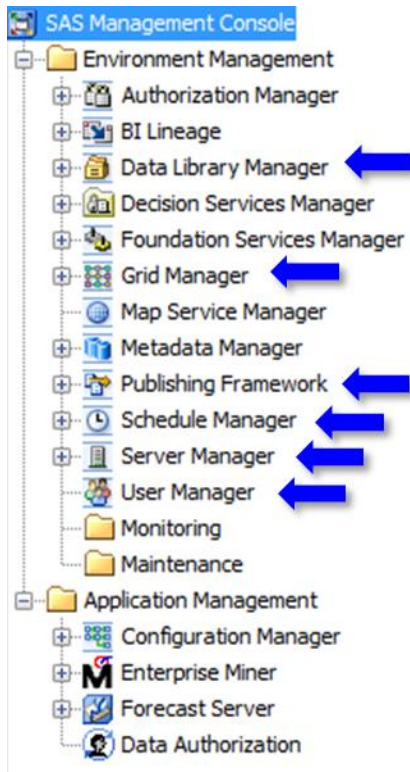


Figure 2 SAS Management Console Plug-ins

When SAS is initially deployed, the plug-ins in Figure 2 that fall into the Registered category are:

- **Authorization Manager** defines rules to control access to SAS metadata objects.
- **Data Library Manager** contains definitions for SAS Libraries and database schemas.
- **Foundation Services Manager** holds deployment configurations for infrastructure and services used by SAS applications.
- **Metadata Manager** contains the administrative components for the SAS Metadata Server.
- **Publishing Framework** includes subscriber lists and channels for publishing content.
- **Schedule Manager** houses schedule objects for executing SAS jobs.
- **Server Manager** contains the definitions for all the physical server and service resources in the SAS environment.
- **User Manager** houses definitions for Users, Groups, and Roles.

Plug-ins in Figure 2 that are considered Unregistered are:

- **BI Lineage** identifies connections between BI objects from data to report in SAS metadata.
- **Decision Services Manager** is a framework for managing models and the workflows that are associated with model projects.
- **Grid Manager** provides management capabilities for grid hosts, jobs, and queues.
- **Map Service Manager** holds configurations for ESRI ArcGIS map services to support SAS OLAP.

- **Application Management** is a folder containing plug-ins for configuring SAS applications, like:
 - **Configuration Manager** contains configuration attributes for many SAS applications.
 - **Enterprise Miner** provides the ability to customize metadata objects associated with the product.
 - **Forecast Server** provides a graphical interface for managing product resources and content.
 - **Data Authorization** manages access to the Forecast Analyst Workbench solution data mart.

USING PLUG-INS TO DISTRIBUTE ADMINISTRATIVE RESPONSIBILITIES

There are core plug-ins to consider when evaluating what administrative responsibilities to assign to SAS Group Administrators. These plug-ins are highlighted in Figure 2 and discussed in further detail below.

DATA LIBRARY MANAGER PLUG-IN

This plug-in provides the ability to create and maintain SAS libraries across the SAS environment. Libraries are logical connections to physical data resources. Administrators use this plug-in to connect to data for use in projects and applications. During library creation, the library definition metadata is assigned to a metadata folder under the Folders tab. This folder is secured by an Access Control Template (ACT) governing access to the library definition and data resources for the target user population.

The ACTs applied to the metadata folders to secure content extend to the Data Library Manager plug-in. This provides the same access level for SAS Group Administrators to view and work with the library definitions that apply to their group. Figure 3 illustrates the difference in content that is available at the plug-in level between the SAS Administrator and the Group A Administrator. Notice the absence of GrpB – Data and GrpC – Data library definitions from the Group A Administrator's view. These definitions are contained in folders that only members of Group B and Group C, respectively, can access.

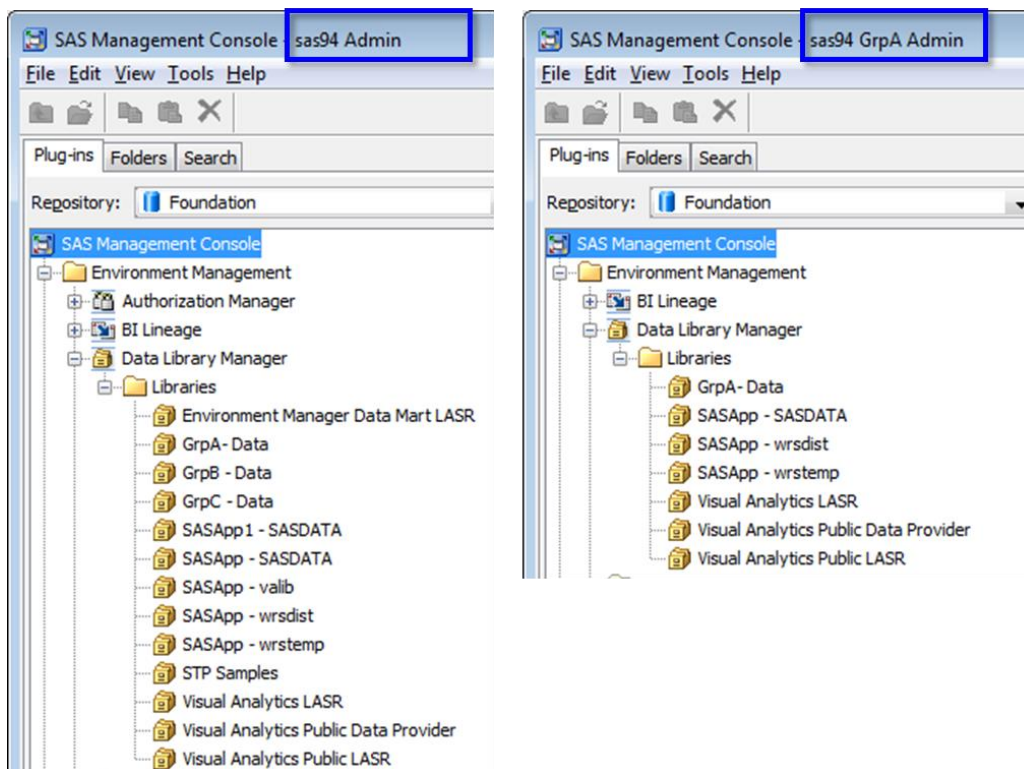


Figure 3 Data Library Manager Views for SAS Administrator and Group A Administrator

Metadata Bound Libraries

New in SAS 9.4 is the ability to bind physical library contents to SAS Metadata. This provides an additional security layer to SAS data sets over standard operating system authorizations. Access to any SAS data set in this physical library location first requires authentication to the metadata server binding the library, then metadata authorization for the access permissions to the content.

From a SAS administration perspective, this becomes a two-step process to create a metadata-bound library. The first step in the process is to bind the physical library to metadata. The second step is to create a traditional SAS library definition pointing to this same physical library location using the Data Library Manager plug-in. The second step is covered above, the binding step is covered below.

The binding step is performed on the Folders tab, not in the Data Library Manager plug-in. Metadata bindings are created inside the Secured Libraries folder located under the System folder. By default, only SAS Administrators Group members have access to this folder. To enable SAS Group Administrators to create and manage their respective metadata-bound libraries, folders must be created under the Secured Libraries folder and the ACTs used to secure standard library contents applied to secure individual group content.

Figure 4 is a Folders tab view of the metadata binding in the main illustration and the traditional library definition in the inset. The Group A Secure Data folder was created to hold the group's metadata bindings. This folder is secured using the same ACT applied to the Group A folder that stores the traditional library definitions for the group. Under the Group A Secured Data folder is a metadata-bound library definition for GrpA – MBL Forecasts. The right pane of the main illustration shows the current SAS data sets bound in this library location. Metadata-bound libraries have their own specific access controls governing this metadata. Refer to the *SAS®9.4 Guide to Metadata-Bound Libraries, Second Edition* referenced at the end of this paper for more detail. Adding the Select permission to the Group A ACT securing the group's content, allows Group A members to see the metadata-bound content.

In summary, the binding step follows the same security and administration model as other SAS metadata stored under the Folders tab.

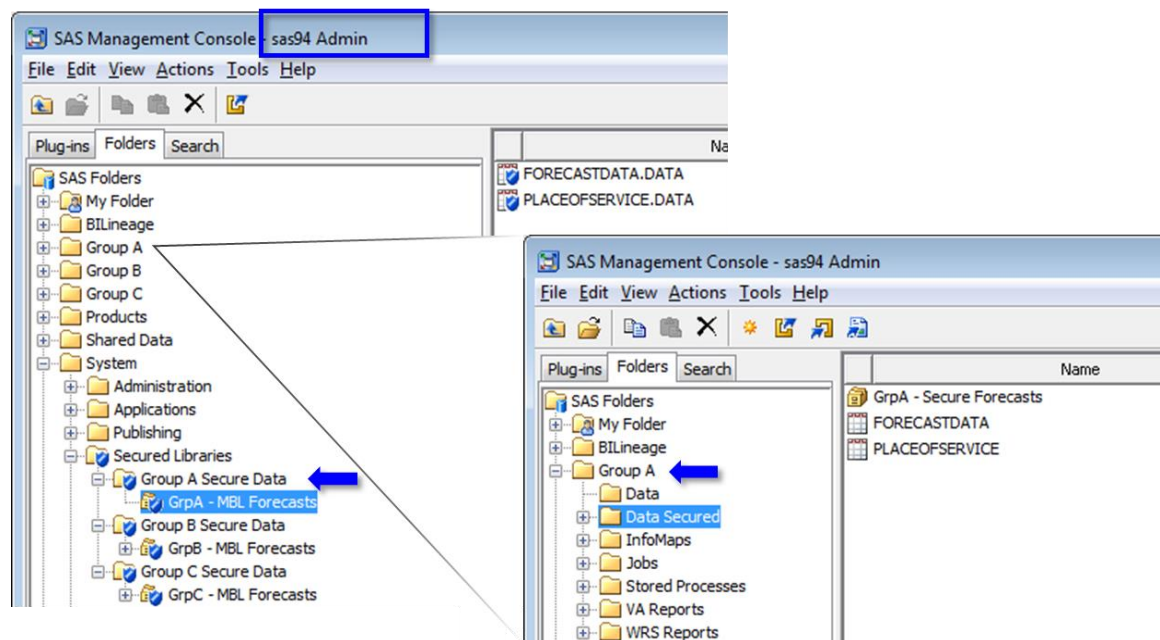


Figure 4 Metadata-Bound Libraries and Traditional Library Metadata

GRID MANAGER PLUG-IN

The Grid Manager plug-in enables an Administrator to monitor and manage SAS jobs, hosts, and queues in a SAS grid environment. The information inside the plug-in is organized into three categories: Job Information, Host Information, and Queue Information. The Job Information node provides the ability to view, terminate, suspend, or resume individual jobs. The Host Information node is used to view, close, or reopen computing host resources in the grid. Using the Queue Information node, the Administrator can open, activate, or inactivate job queues in the grid.

These capabilities are dependent on the authorizations granted to the user in the SAS Grid configuration. At a minimum, a user with access to the Grid Manager plug-in can view and administer their individual SAS jobs on the grid. The SAS Administrator typically has authorization to manage all jobs, hosts, and queues in the grid. A SAS Group Administrator could have authorized access to manage all jobs associated with their group. More SAS grid administration detail can be found in the *Administering Platform LSF* manual referenced at the end of this paper.

Platform RTM (Report Track Monitor) for SAS is a web-based user interface used in many deployments as an alternative to the Grid Manager plug-in. In addition to Host, Queue, and Job management capabilities provided with this plug-in, RTM also provides the ability to manage the policies and grid configuration. This robust tool monitors job performance and grid efficiency enabling Administrators to optimize usage and grid performance using a single interface.

PUBLISHING FRAMEWORK PLUG-IN

This plug-in is a repository for managing and administering the Publishing Framework. It contains a node for Subscribers and another node for subscription Channels. When SAS is initially deployed, only SAS Administrators group members, like the SAS Administrator, have permission to create content in this plug-in. The default permissions for the Publishing Framework is set at the Foundation repository level, but it can be modified using Access Control Templates at any level below it.

Once a subscriber profile is created, it can be maintained by the individual user through the SAS Information Delivery Portal web application to set delivery transport method, update email address or filter on subscription content to be received. Subscriber Groups can be established by SAS Administrators group members to simplify assigning subscribers to publishing channels, but this is solely an administrative function. Providing SAS Group Administrator's access to the Publishing Framework plug-in provides access to all user and group content inside the Subscribers node, except for groups restricted using Access Control Templates.

The Channels node is used to organize the subscription content. Subscription channels can be organized into folders to group similar content and they can be secured using Access Control Templates to provide SAS Group Administrators the ability to create channels and manage all publishing content appropriate to their group. Applying ACTs to channels or folders also restricts a user's subscription ability to channels that they have been granted access to view.

The left illustration in Figure 5 shows the Channels node as seen by the SAS Administrator. At the top of the node there are two channels, Global Distribution Channel and Group B Content. All subscribers can see and subscribe to the Global Distribution Channel, but only the SAS Administrator can manage it with the default authorizations at the Channels node level. The Group B Content folder has been secured using the Group B ACT, providing only Group B users access to this single channel and the Group B Administrator the ability to manage the content published to it. The remaining folders have been secured using Access Control Templates to limit access to the appropriate groups. The right illustration in Figure 5 shows the Channels that Group A users can access. By leveraging folders and Access Control Templates, SAS Group Administrators have full access to create and manage all publishing content inside their group folders.

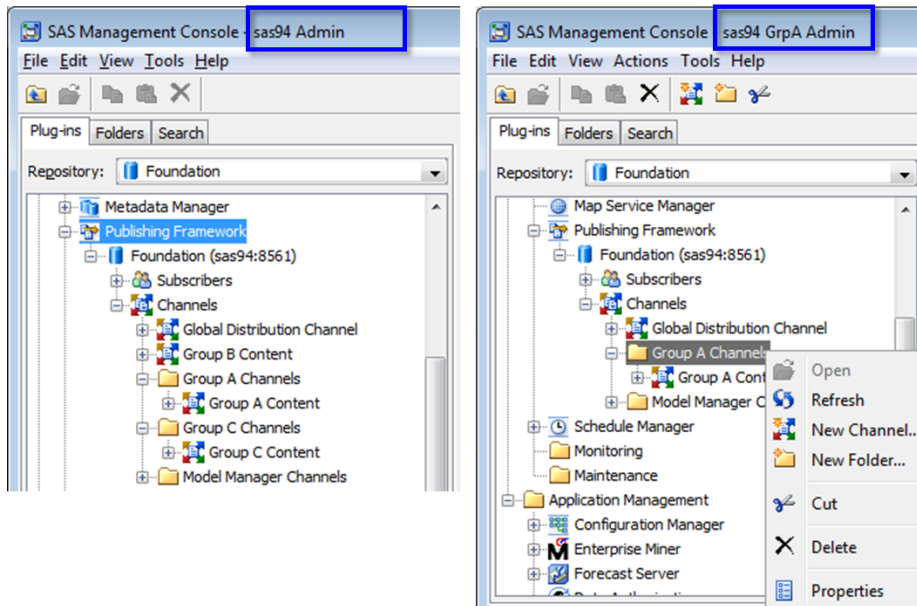


Figure 5 Publishing Framework Plug-in

SCHEDULE MANAGER PLUG-IN

The Schedule Manager plug-in works with scheduling servers like Platform Suite for SAS to schedule jobs created in SAS applications or in open SAS code. Administrators use this plug-in to create and edit process flows that contain one or more jobs, define job dependencies, job exception rules, and manually run any scheduled job.

Schedules and jobs are stored in metadata folders, which are secured using Access Control Templates. Using ACTs, SAS Group Administrators have visibility into the schedules and jobs for their group.

When scheduling jobs in an enterprise-level SAS environment, it is important to understand job timings. Executing too much workload on a server could exceed computing capacity and optimal processing performance. SAS Grid Manager mitigates scheduling concerns by providing workload management to ensure that computing resources are protected, optimized for performance, and scheduled SAS jobs are prioritized and executed as compute resources become available.

Figure 6 shows the Schedule Manager Plug-in for the Group A Administrator and the properties for a scheduled job, highlighting its secured metadata folder location.

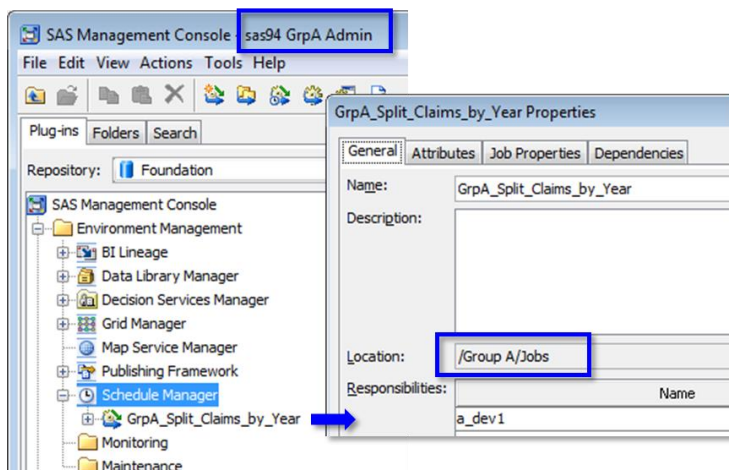


Figure 6 Scheduling Manager Plug-in with Properties for a Group A Scheduled Job

SERVER MANAGER PLUG-IN

The Server Manager plug-in is used to define and maintain logical server definitions to the physical resources for compute servers and databases. SAS Administrators use this plug-in to manage server contexts or server groupings, logical server definitions, define specific resources like memory allocations, then associate computing needs such as SAS jobs and stored processes to these resources. Administrators can view processes that are running under each server category and start, stop, pause, or resume most processes running under these server definitions.

Server definitions are rarely modified after the initial deployment and might sometimes be associated with multiple user groups. Access Control Templates can be applied to logical server definitions within this plug-in, limiting SAS Group Administrators access and management capabilities to specific server resources. SAS Group Administrators need to understand the impact of adding and modifying server resources on the larger user community when resources are shared. Through best practice development and defined administrative responsibilities, SAS Group Administrators can provide effective server resource management.

USER MANAGER PLUG-IN

The User Manager plug-in is used to create and maintain definitions for Users, Groups, and Roles. Administrators add new SAS users to the environment, assign them to their respective groups based on job responsibilities, and provide access to roles within the SAS user interfaces that are appropriate to their skillset.

Access to this plug-in provides access to all Users, Groups, and Roles defined in SAS Metadata. There is no ability to efficiently limit Users or Groups to a SAS Group Administrator's domain of responsibility. By developing best practices defining administrative responsibilities, SAS Group Administrators can provide efficient User, Group, and Roles administration for users within their area of responsibility.

As an alternate to manually defining Users and Groups, SAS provides the ability to bulk load and synchronize User and Group assignments from LDAP repositories like Active Directory. This does not eliminate all the administrative responsibilities, especially more granular authorizations and role assignments that might be required within the SAS environment, but it does ensure that basic user and group assignments are in sync with corporate definitions. As changes are made to LDAP configurations, SAS Group Administrators could manually run the scheduled metadata synchronization jobs with appropriate permissions in the Schedule Manager plug-in.

SECURING SAS MANAGEMENT CONSOLE PLUG-INS

Upon careful review of the plug-ins described above, access patterns associated with Metadata Folders and Access Control Templates begin to emerge along with the use of best practices. Access to metadata contained in the Data Library Manager and Schedule Manager are controlled through Metadata Folder security using ACTs. The Publishing Framework and Server Manager plug-ins leverage ACTs to control access and authorization to metadata inside these plug-ins. Grid Manager and User Manager rely on policies and best practices developed to manage the roles of administrators using these plug-ins. Other plug-ins not discussed in this paper also follow these basic patterns to manage access to metadata within the plug-in.

Primary access to SAS Management Console plug-ins is controlled through Roles. SAS Management Console capabilities are located in the Role's Capabilities tab under the Management Console 9.4 tree. Access to Registered plug-ins is controlled by selecting one or more of the standard plug-in capabilities from the list.

A best practice when designing roles to meet a specific need is to create custom roles rather than modifying the standard roles that come with the SAS Metadata Repository. The SAS – Group Administrators role shown in the left side of Figure 7 was created for this paper and contains an initial selection of Management Console plug-in capabilities to meet the SAS Group Administrator's needs.

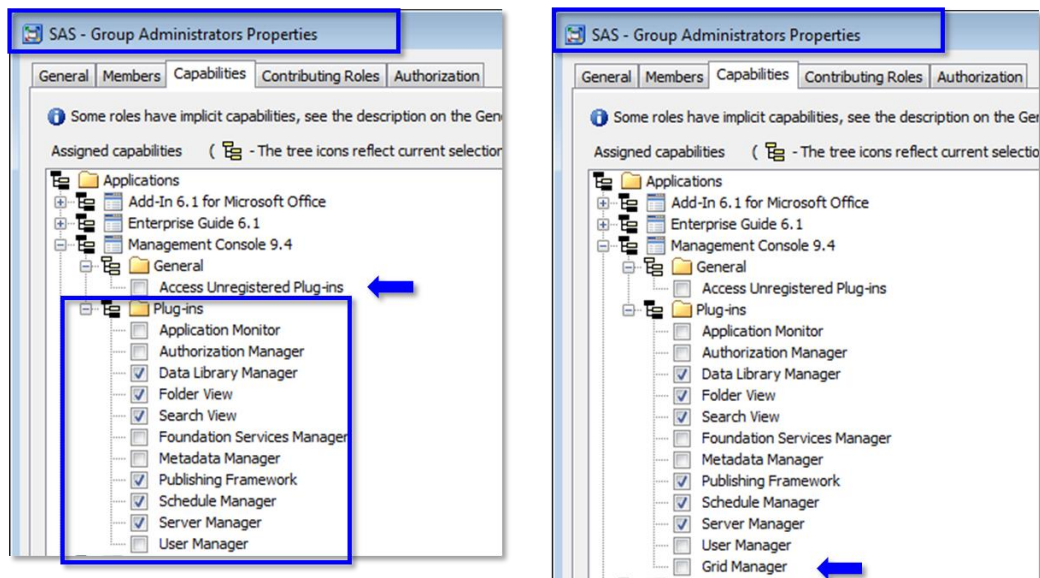


Figure 7 SAS Management Console SAS-Group Administrator Custom Role

Access to plug-ins not listed in Figure 7 is controlled by the Access Unregistered Plug-ins capability highlighted in the left side of the figure. Providing access to Unregistered Plug-ins provides access to all unregistered plug-ins installed with the SAS Management Console application. One means to control unregistered plug-ins is through the plug-in selections made in the SAS Deployment Manager during the installation of SAS Management Console.

Another way to manage unregistered plug-ins is by registering them. The unrestricted SAS Administrator has the ability to register any unregistered plug-in using the Plug-in Manager application listed under the Tools menu in SAS Management Console. Figure 8 shows the default selections made in Plug-in Manager at an initial SAS deployment. Note that all plug-ins, both registered and unregistered, are available in this list. When the SAS Administrator selects the Grid Manager plug-in for registration, it is immediately available for selection in the Management Console 9.4 Plug-ins capability list, as highlighted in the right illustration of Figure 7.

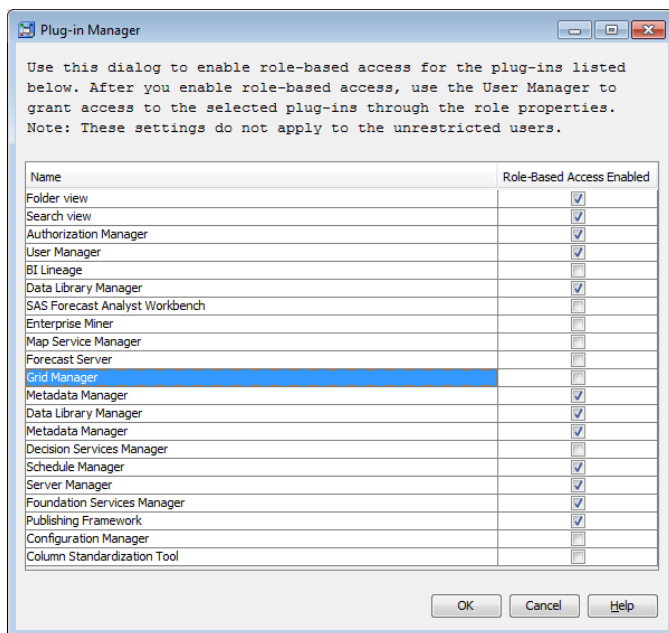


Figure 8 SAS Management Console Plug-in Manager

CONCLUSION

In an enterprise SAS deployment, administering the daily activities of multiple business groups is a large responsibility. As business needs evolve, these groups need the ability to adapt quickly. Business groups that had the agility to change direction on a dime in their individual SAS environments are looking for that same ability in the enterprise SAS analytical environment.

This paper defined key resources contained within SAS Management Console and how to manage their distribution for business groups to administer and maintain their SAS analytical needs. Distributing administrative responsibilities closer to the source provides efficient workflow processing and relieves the administrative burden of daily business group activities on the SAS Administrator. With responsible design and the application of best practices, the delegation of responsibilities across the organization can be possible without disrupting the integrity of the SAS environment.

REFERENCES

Platform Computing, an IBM Company. May 2012. *Platform RTM Administrator Guide for SAS®, Version 2.0.8*. Platform Computing, an IBM Company.

Available at: <http://support.sas.com/rnd/scalability/platform/index.html>

IBM Corporation. 2013. Platform LSF, Version 9 Release 1.1: *Administering Platform LSF*, IBM Corporation. Available at: <http://support.sas.com/rnd/scalability/platform/index.html>

SAS Institute Inc. 2013. *SAS® 9.4 Publishing Framework: Developer's Guide*. Cary, NC: SAS Institute Inc. Available at: <http://support.sas.com/documentation/onlinedoc/inttech/index.html>

Fenton, Jim and Ladd, Robert. 2010. "A Practical Approach to Securing a SAS® 9.2 Intelligence Platform Deployment." *Proceedings of the SAS® Global Forum 2010 Conference*, Seattle, WA: SAS Institute Inc.

SAS® 9.4 Intelligence Platform Administration Documentation available at <http://support.sas.com/documentation/onlinedoc/intellplatform/index.html>, in particular these references:

SAS Institute Inc. 2014. *SAS® 9.4 Intelligence Platform: Desktop Application Administration Guide, Fourth Edition*. Cary, NC: SAS Institute Inc.

SAS Institute Inc. 2013. *SAS® 9.4 Intelligence Platform: Security Administration Guide, Second Edition*. Cary, NC: SAS Institute Inc.

SAS Institute Inc. 2014. *SAS® 9.4 Intelligence Platform: System Administration Guide, Second Edition*. Cary, NC: SAS Institute Inc.

SAS Institute Inc. 2013. *SAS® 9.4 Management Console: Guide to Users and Permissions*. Cary, NC: SAS Institute Inc.

SAS Institute Inc. 2013. *Scheduling in SAS® 9.4*. Cary, NC: SAS Institute Inc.

SAS Institute Inc. 2014. *Grid Computing in SAS® 9.4, Third Edition*. Cary, NC: SAS Institute Inc.

SAS Institute Inc. 2013. *SAS® 9.4 Guide to Metadata-Bound Libraries, Second Edition*. Cary, NC: SAS Institute Inc.

ACKNOWLEDGMENTS

Many thanks to Diane Hatcher for her feedback and review of this paper.

The authors would like to acknowledge Matt Clarke and Alpesh Patel from Kaiser Permanente for their valuable input and experiences using SAS in a large enterprise.

CONTACT INFORMATION

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

Jim Fenton
SAS Institute, Inc.
Cary, NC
(919) 531-9761
Jim.Fenton@sas.com

Robert Ladd
SAS Institute, Inc.
Dallas, TX
(919) 531-9352
Robert.Ladd@sas.com

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration.

Other brand and product names are trademarks of their respective companies.