SAS® Big Brother
Elena Muriel, Amadeus Software, UK

ABSTRACT

If, like the character from George Orwell's novel, you need to control what your users are doing and also need to report on it, then this paper is for you. Using a combination of resources available in SAS® 9.4, any administrator can control what users are allowed to perform within SAS, and then can create comprehensive and customized reports detailing what was done.

This paper discusses how metadata roles can be used to control users' capabilities. Particular attention is given to the user roles available to SAS® Enterprise Guide® and the SAS® Add-in for Microsoft Office, as well as administrator roles available to the SAS® Management Console. Best practices are discussed when it comes to the creation of these roles and how they should be applied to groups and users.

The second part of this paper explores how to monitor SAS® utilization through SAS® Environment Manager. It investigates the data collected through its extended monitoring and how this can be harvested to create reports that can track sessions launched, procedures used, data accessed, and other purpose-built reports.

This paper is for SAS Administrators who are responsible for the maintenance of systems, system architects that need to design new deployments, and users interested in an understanding of how to use SAS in a secure organization.

INTRODUCTION

More and more organizations need to control and manage the level of access that users have to their SAS® platform. This can be achieved by placing restrictions on the applications accessible and the actions that can be taken through them.

The need to impose restrictions can arise from a variety of reasons, such as:

- Users have not been trained on all SAS client applications. From using SAS® Enterprise Guide, SAS® Data Integration studio or creating reports using SAS® Visual Analytics, it can be beneficial to restrict access to client tools to only trained users.
- Users have different degrees of knowledge. You might only want statisticians to have access to the statistical analysis procedures within Enterprise Guide, or only allow skilled programmers to be able to create their own custom code in Enterprise Guide.
- Division of administrator roles when it comes to administer the SAS platform. For example, you could have the helpdesk services looking after the creation and maintenance of users and the SAS Administrators to monitor the SAS services and platform security.

Organizations can manage these restrictions through the use of Capability Roles. Capability Roles are linked to the client applications accessible through the SAS environment, and the actions that can be performed through their interfaces.

Once the restrictions are in place, there is a second part to the process that needs to be considered. This is the monitoring of activities that are taking place within the SAS state, so exceptions and violations can be reported.

This can be achieved by setting up intelligent monitoring and alert systems utilizing the data available in the Environment Manager Data Mart.
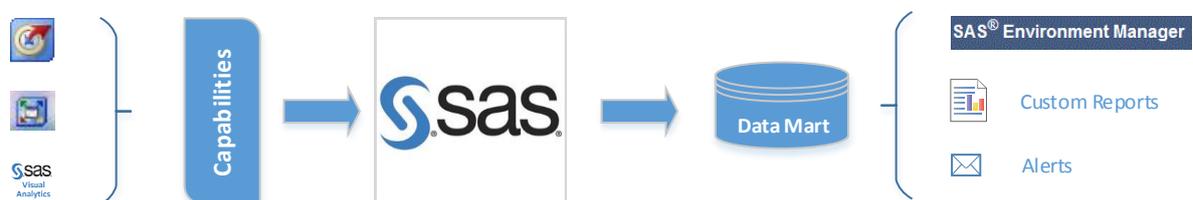
The overall process is represented in the figure below:



Figure 1 – Process overview

Therefore the analogy with George Orwell's novel 1984, where a dystopian society is controlled by their leader, named Big Brother; not only interested in dictating what people could do, but also monitoring all of the citizens movements.

First let's take a closer look at the capability roles available for some of the major client applications.
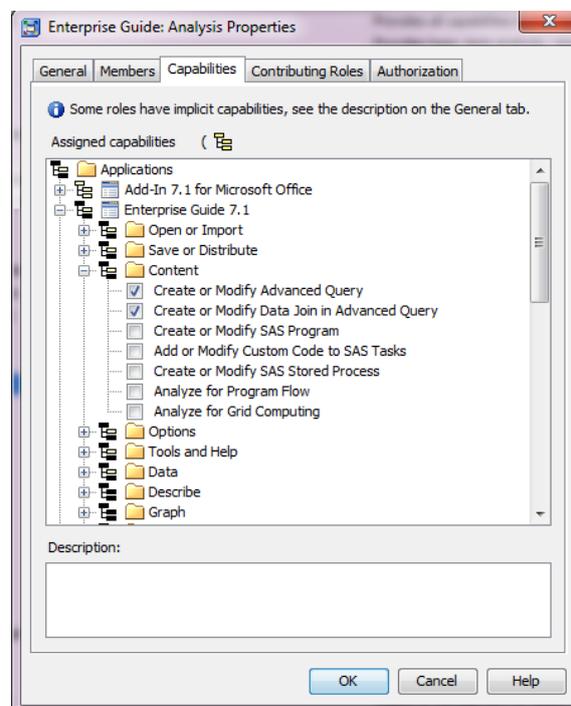
CAPABILITY ROLES

User capabilities can be controlled from within the SAS Management Console user plugin. These capabilities are assigned to Roles which can then be assigned to metadata users or groups.

The system already contains some default Roles that are based on the software installed and configured. These default roles represent common types of access required to the different client applications. For example, the role **Enterprise Guide: Programming** gives users the permission to create and modify SAS programs, when the **Enterprise Guide: Analysis** gives access to multiple analytical tasks but users cannot create custom code.
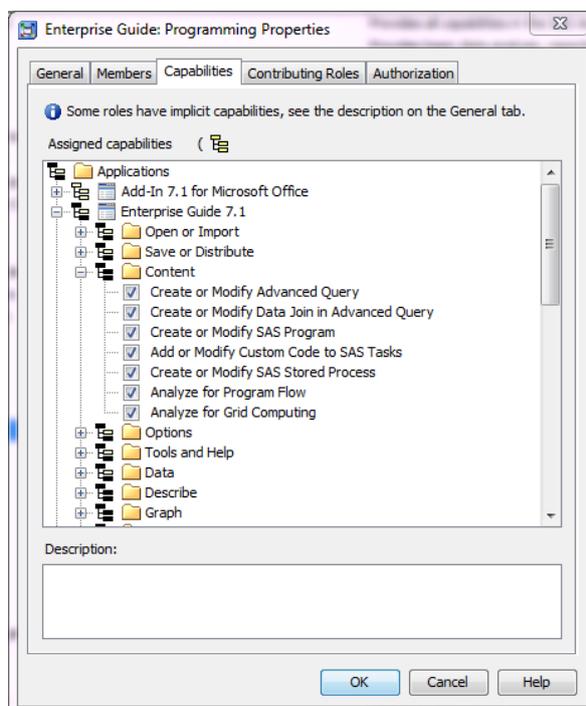
Display 1 - Enterprise Guide: Programming   **Display 2 – Enterprise Guide: Analysis**

The list of available capabilities will change based on the software configured and licensed, although capabilities linked to the use of SAS Management Console will always be present.

Some particularly interesting capabilities are grouped under the applications:

- Management Console 9.4
- Enterprise Guide 7.1 and Add-in 7.1 for Microsoft Office
- Visual Analytics 7.3

SAS MANAGEMENT CONSOLE CAPABILITIES

The capabilities available for SAS Management Console are grouped very closely to the access to each of its plugins.

Plugins	Capability Name	Description
Metacoda	Access Unregistered Plug-ins	Access plug-ins that are not registered in metadata. Such as third party plugins like Metacoda.
	Application Monitor	Monitor the activities of applications, subsystems and services.
SAS Folders	Folder View	Manage public and user folders used to store metadata objects.
Authorization Manager	Authorization Manager	Manage resource access control policies.
Data Library Manager	Data Library Manager	Manage the definitions of data libraries and database schemas.
Foundation Services Manager	Foundation Services Manager	Manage Foundation Services components.
Metadata Manager	Metadata Manager	Create and manage metadata repositories, manage the current SAS Metadata Server, and run metadata utilities.
Publishing Framework	Publishing Framework	Manage publishing framework subscribers and content channels.
Schedule Manager	Schedule Manager	Manage SAS jobs to be scheduled, create conditional events for schedules, and submit jobs for scheduling.
Server Manager	Server Manager	Create and manage server definitions (such as for SAS servers, database servers, and spawners).
User Manager	User Manager	Create and manage users, groups, roles, and capabilities.

Table 1 - SAS Management Console Capabilities

Controlling access to the plugins can be useful when organizations divide the SAS administration tasks into SAS Administrators and IT helpdesks. IT helpdesks can take on tasks such as, creating SAS metadata accounts and assigning them to groups, when it might not be such a good idea to give them access to the server or library definitions. Also you might need to grant access to some super users so they are able to access the metadata folders without seeing any other plugins.

Custom roles can therefore be created for each level of access required, and then assigned to the right Metadata group. In the case of the IT helpdesk, access to the User Manager plugin might be all that is required in order for them to perform their tasks.

SAS ENTERPRISE GUIDE AND ADD-IN FOR MICROSOFT OFFICE CAPABILITIES

SAS Enterprise Guide and the Add-in for Microsoft Office are by far the client tools that have more capabilities that can be controlled. Many of these capabilities are shared across the two client tools, although differences are also in place. Enterprise Guide has more capabilities than the Add-in for Microsoft Office, which contains a subset of those.

The following categories can be controlled in both applications:

Capability Category	EG Task Relation	Number of EG Capabilities	Number of Add-In Capabilities	Description
Open or Import	x	8	5	Controls types of files that users can open, the location (server/client) and the ability to import data
Save or Distribute	x	18	7	Controls where objects can be saved, copy and paste, and actions that imply extracting data from the system
Content	x	7	2	Controls what can be done to code, user or task created
Options	x	11	6	Controls results formats and access to options
Tools and help	✓	14	5	Controls access to tools tasks
Data	✓	24	14	Controls tasks for manipulating data, formats and download data
Describe	✓	8	8	Controls access to descriptive tasks
Graph	✓	17	17	Controls access to the graphical tasks
ANOVA	✓	5	5	Controls access to models and ANOVA analysis tasks
Regression	✓	6	6	Controls access to the regression tasks
Multivariate	✓	6	6	Controls access to the multivariate tasks
Survival Analysis	✓	2	2	Controls access to the survival analysis tasks
Capability	✓	5	5	Controls access to the capability
Control Charts	✓	8	8	Controls access to the control charts
Pareto	✓	1	1	Controls access to the Pareto charts
Time Series	✓	9	9	Controls access to the time series
Data Mining	✓	3	3	Controls access to the data mining tasks

Table 2 - SAS Enterprise Guide and Add-in for Microsoft Office Capabilities

Amadeus Software Limited, Mulberry House, 9 Church Green, Witney, Oxfordshire UK OX28 4AZ
Tel: +44 (0) 1993 848010 email:info@amadeus.co.uk

Page 4 of 13

This is over 150[1] capabilities for Enterprise Guide that can be divided into different categories:

- Enterprise Guide tasks. Many of the capability categories relate to the Enterprise Guide tasks that users have access to. The main cause for restricting access to these tasks is user training. Organizations do not want unskilled analysts applying incorrect statistics.

- Access to code. Code created by tasks can be modified by experience programmers. Organizations want to make sure that only skilled programmers have access to edit generated code or are able to create their own custom code.

- Accessibility of files. In a client-server set up, administrators can control if local files can be used in Enterprise Guide, or results can be saved locally, or enforce that programs and data can only be saved on the SAS Server. Decisions over the capability of importing and exporting files can also be controlled in here.

- Options. To control the options available on the Options menu and stop users from changing preassigned values.

Although standards installations provide four default Roles that affect Enterprise Guide, it is beneficial to analyze the user base to determine if custom roles should also be created.

VISUAL ANALYTICS CAPABILITIES

Visual Analytics is another interesting area to observe when it comes to controlling capabilities.

There are multiple application names that are grouped under the Visual Analytics umbrella. These provide control to access the different areas that form Visual Analytics.

Visual Analytics Explorer, for example, provides analysts with an ad-hoc environment where to query data in order to identify patterns and behaviors. Unlike Enterpriser Guide, Visual Analytics capabilities do not allow you at the moment to control the objects that can be used for analysis, although you can restrict access to the Explorer all together.

Application Name	Capabilities	Description

Visual Analytics Hub 7.3	Visual Analytics Hub 7.3
	  ✓ Administer Hub
	  ✓ Add and View Comments
	  ✓ Create Collections
	  ✓ Personalization
		Containing capabilities linked with the administration of the Visual Analytics central landing page or Hub.

Visual Analytics 7.3	Visual Analytics 7.3
	  ✓ View Report and Stored Process
	  ✓ Create Report
	  ✓ Explore Data
	  ✓ Build Custom Graph
	  ✓ Add and View Comments
	  ✓ Export Data
	  ✓ Export or Print as PDF
	  ✓ Email
	  ✓ Personalization
	  ⊞ Self-Service Import
	  ⊞ Advanced
		Containing capabilities linked to Visual Analytics Designer and user interactions with Visual Analytics reports.

Visual Analytics Transport Service 7.3	Visual Analytics Transport Service 7.3
	  ✓ Purge Mobile Report Data
	  ✓ Require Passcode On Mobile Devices
	  ✓ Limit Duration of Offline Access
		Containing capabilities linked to mobile device access.

---

[1] The full list of available capabilities will depend on your version of Enterprise Guide. This paper is written using Enterprise Guide 7.1.

Application Name	Capabilities	Description
Visual Analytics Explorer 7.3	Visual Analytics Explorer 7.3 ☑ Refresh Data ☑ Export as Image ☑ Export as Report ☑ Build Analytical Model	Containing capabilities linked to Visual Analytics Explorer for ad-hoc exploration of data.
Visual Analytics Admin 7.3	Visual Analytics Admin 7.3 ☑ Manage LASR Analytic Server ☑ Monitor LASR Analytic Server ☑ Manage Authorization ☑ Browse HDFS	Containing capabilities linked to the administration of the in-memory server.

Table 3 - SAS Visual Analytics Capabilities

Using a combination of some of the capacities described, the following control can be achieved:

- Administration. Controlling access to the LASR server and the ability to start and stop the server, set up security and load tables, as well as, being able to whitelist mobile devices and customize landing pages.

- Users. Depending on the type of user connecting to Visual Analytics, an administrator might want to limit what they can do:

    o View reports. Limit users to only view reports created by others.

    o Explore data. Limit access to this area to only users that have an understanding of the raw data structure.

    o Create reports and dashboards. Limit access to only advanced users who can prepare reports and dashboards to be consumed by others.

    o Prepare data. Manipulate data to best present information to the organization. This is normally done by an advanced user or somebody in charge of the data sources.

    o Allow access to download data. Control users that can extract data so it can be presented using other software tools.

With all these capabilities, it is easy to control exactly the level of access required to all users. Although the software provides some templates that represent common level of access, it is often necessary to derive unique patterns for the roles define within each organization.

CREATING YOUR OWN ROLES

Understanding all the different levels of access is crucial when you are planning to create your own personalized roles. If there is a series of roles that need to be created with slight variations (progressively granting more capabilities), then it is recommended to create a baseline role containing all the common capabilities.

The baseline role becomes your most restricted role and can be used as a template for all others. This is done by adding the baseline role as a contributing role to the rest. That way, any extra roles created will inherit the baseline, plus any extra capabilities that have been identified.

Creating a baseline role is also a good practice for maintenance reasons. If there is a change in the capabilities pattern that will affect all of the existing roles, all changes can be addressed in the same location (the template) rather than having to change all the individual ones.
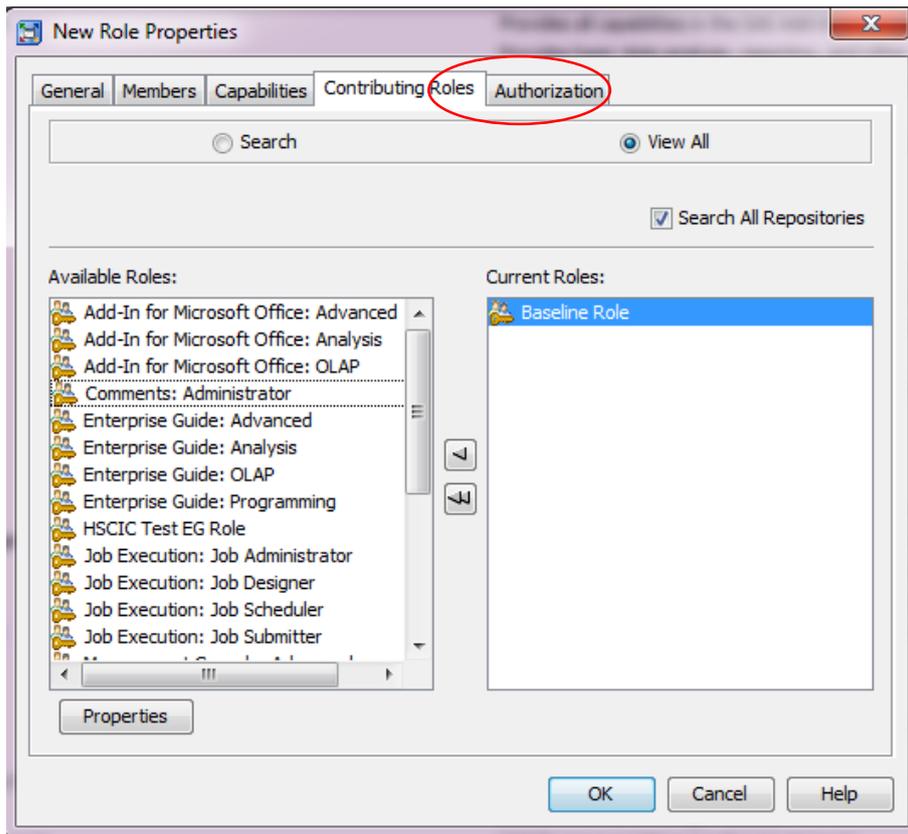
Display 3 - Contributing baseline role

Once the roles are created, they need applying to the relevant users. It is recommended to create a series of SAS metadata groups that match each of the capability roles. This way we can map 1-to-1 the capability with a group of users and the only management required is to assign specific users to their appropriate capability group.
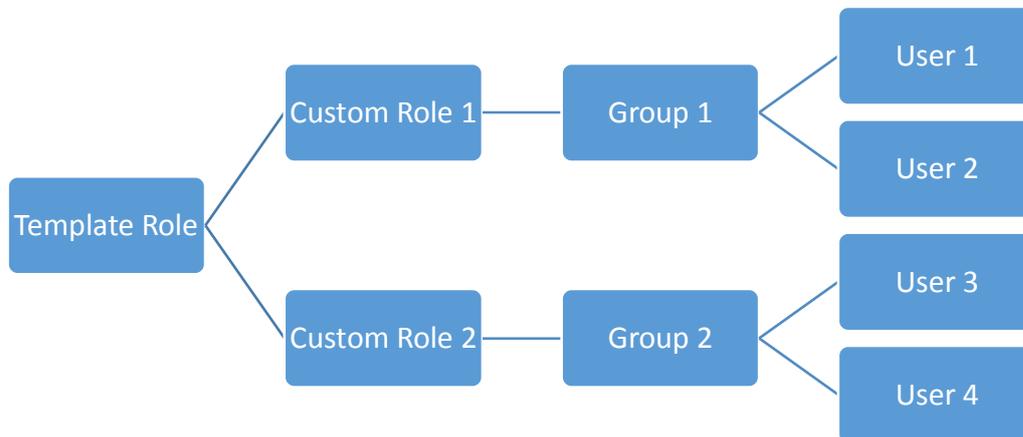

Figure 2 - Roles, groups and users relationship

When assigning custom roles to the groups, something to keep in mind are the roles that might have already be assigned to the PUBLIC and SASUSER groups, as these will overwrite any restrictions that you are trying to put in place. Check any roles assigned to these default groups when creating new ones, as otherwise your restrictions will not work!

REPORTING WITH ENVIRONMENT MANAGER

Once the capabilities are assigned to the user groups, the restrictions will take place. It is now when the monitoring process starts in order to make sure that no breaches occur to the restricted environment. Breaches can be generated from things such as: unauthorized system access, unauthorized use of client tools or access to protected data.

The best way to monitor usage of the platform is to use SAS Environment Manager (available for SAS 9.4) and particularly it's Extended Monitoring. Extended Monitoring analyses log files produced by the system in order to give you visibility of usage and resources consumed.

The data extracted is stored under a series of Data Marts. The information included in these data marts can be divided in three areas: ACM, APM and Solutions Kits, and details will be discussed in the next few sections. The volume of these tables can be large, and therefore, if you are planning to start collecting these metrics, make sure to allocate enough disk space to store them.

Extended monitoring is not configured automatically, so some extra configuration steps are required prior to use this information. For details on how to configure it, please refer to the latest SAS documentation (also included in the References section).

ACM

ACM stands for Agent Collected Metrics and captures metrics that are associated with the hardware of the SAS solution. These metrics are collected at midnight each day, and they include:

- CPU usage
- Memory usage
- I/O monitoring
- Workload

A typical chart generated using these metrics is shown below, where you see the spikes in the memory usage for a week period. This can help you identify if you hardware will need more resources in order to maintain the demand from your user base.
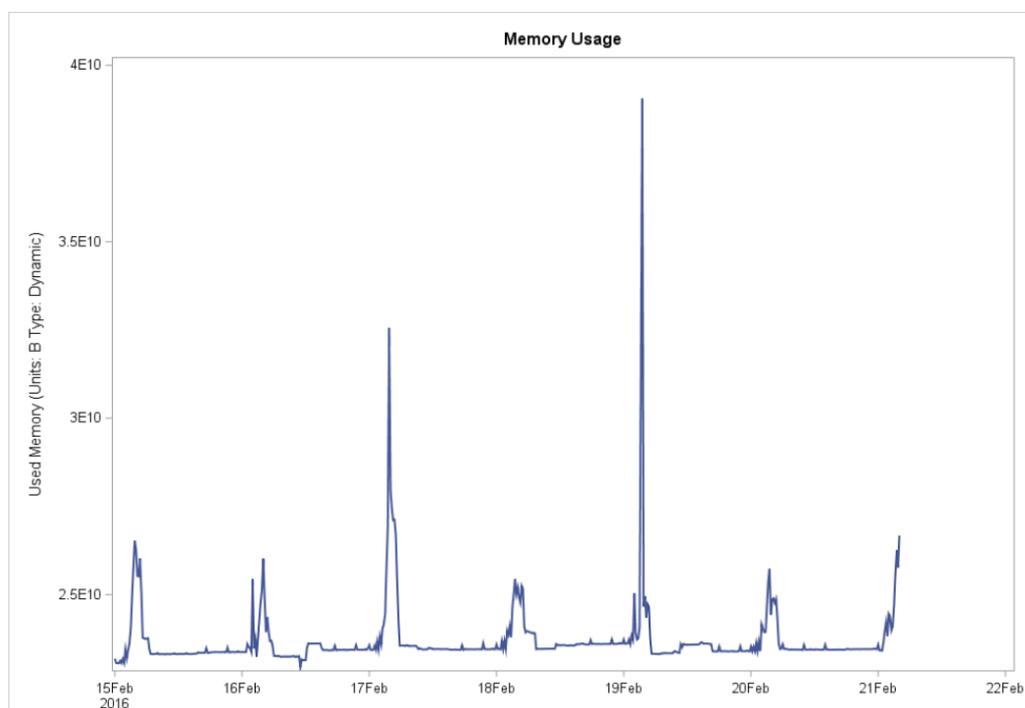
Display 4 – Environment Manager Memory Usage chart

The raw data providing this information is stored under SASEnvironmentManager\emi-framework\Datamart\acm.

This information is normally consumed by Administrators or teams responsible for looking after the SAS Infrastructure. Information that can be flagged using ACM metrics is crucial in order to maintain an optimal functioning of the SAS servers.

Through ACM metrics an administrator can easily identify those users who are consuming most of the available resources, or also see if overnight batch jobs are taking more resources to complete.

Federated Data Mart

Many organizations will be using separate servers to host different logical environments. A Federated Data Mart allows you gather information from the different systems in one place, and present a consolidated view of the ACM metrics.

Creating a Federated Data Mart requires manual configuration steps and is currently only available for the ACM metrics. All of the required steps are documented under the Environment Manager User Guide documentation.

APM

APM stands for Audit, Performance and Measurements and its metrics are collected at 1am each day. There is a clear division on the type of data that is captured by APM based on where the information originates from:

- SAS Metadata Server logs. Apart from capturing all activity recorded in the metadata logs, there is some extra information being derived from here:
  - o User accounts created, modified or deleted. Providing datetime information and the person that performed the action.
  - o Metadata group and ACT changes. Providing information on when users are added or removed to metadata groups.
  - o Authentication errors and Logons not authorized. You can track if an unauthorized person is trying to reach your environment. Data collected also includes the IP address from where the connection was attempted.
  - o Metadata connections. Providing visibility of who is connecting and from which client application.
- SAS Application Server logs. Here is where an administrator can see what the users are performing on the platform, including:
  - o Sessions launched and duration.
  - o Data sets accessed and time that they were opened.
  - o Code being executed, including the name of the procedures.

The APM data is stored under SASEnvironmentManager\emi-framework\Datamart\artifacts and some of the more important tables include:

- ARTIFACTUSAGEDETAILS. From table access, to sessions launched and procedures used, all that information is contained under this data set. A series of filters need to be used in order to extract the correct information, for example:
  - o Filtering by artifactType = TABLE gives you the names of the tables that have been accessed.
  - o Code executed through Enterprise Guide tasks correspond to artifactType = SERVER and type = TASK
  - o Sessions launched. artifactType = SERVER and type = EXECUTE. More filters can be applied for the type of server using the subtype column.
- AUDIT_TRANSACTIONS. Containing most of the information derived from the metadata server logs. This table tends to become large very quickly as it contains data on all communications done.
  - o Use the Client_Context variable to filter the connections done from different client applications.
- AUDIT_GROUPS. Contains details on when users have been added or removed to metadata groups.

A description of all the columns and tables present in the Extended Monitoring Data Mart can be found under the user guide documentation available.

Amadeus Software Limited, Mulberry House, 9 Church Green, Witney, Oxfordshire UK OX28 4AZ
Tel: +44 (0) 1993 848010 email:info@amadeus.co.uk

Page 9 of 13

SOLUTIONS KITS

If any SAS solutions have been licensed and configured, metrics collected from them can also be fed into Environment Manager. These metrics are collected at 2am each day and can contain information on logs generated, reports and artifacts used.

REPORT CENTER

The Report Center is an area accessible from within Environment Manager that provides access to a series of reports and stored processes. The content being accessed is being surfaced by the SAS Stored Process web application.

When configuring Extended Monitoring, a series of Stored Processes also become available through the Report Center.
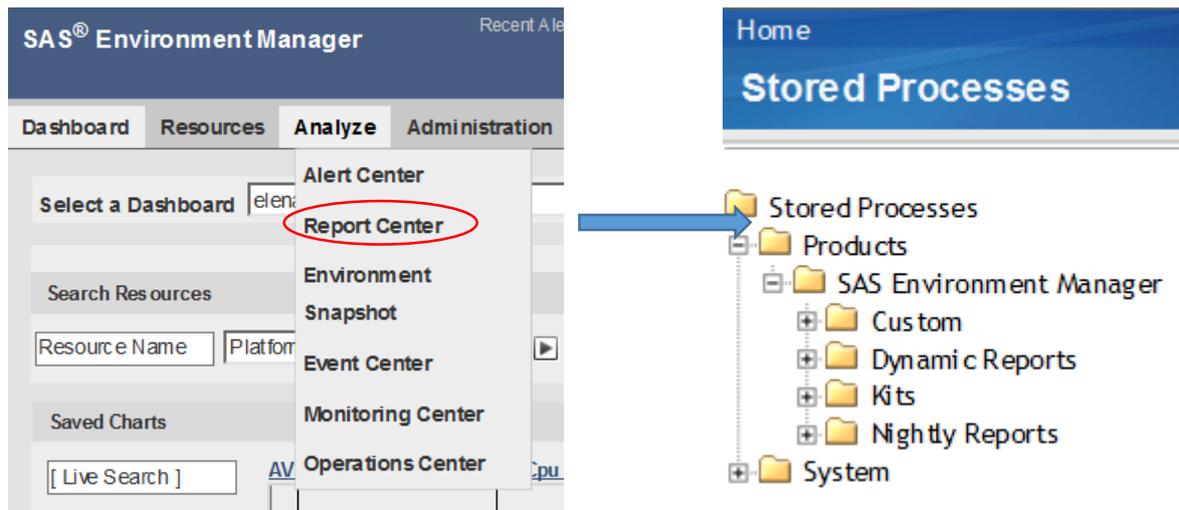
Display 5 – Environment Manager and the Web Stored Process application

The stored processes available are divided into different categories. Information relating to the areas mentioned in this paper are grouped under Nightly Reports.
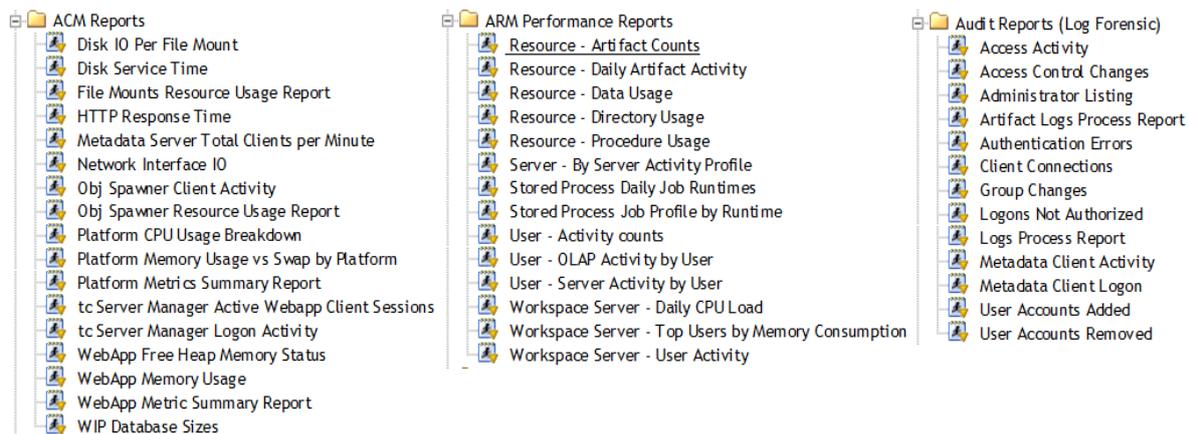
Display 6 – Available Stored Processes

There are many useful Stored Processes already available for you to use. But if there is anything else you need that is not included in here, there is nothing stopping you from creating your own custom reports or modify the existing ones.

Amadeus Software Limited, Mulberry House, 9 Church Green, Witney, Oxfordshire UK OX28 4AZ
Tel: +44 (0) 1993 848010 email:info@amadeus.co.uk
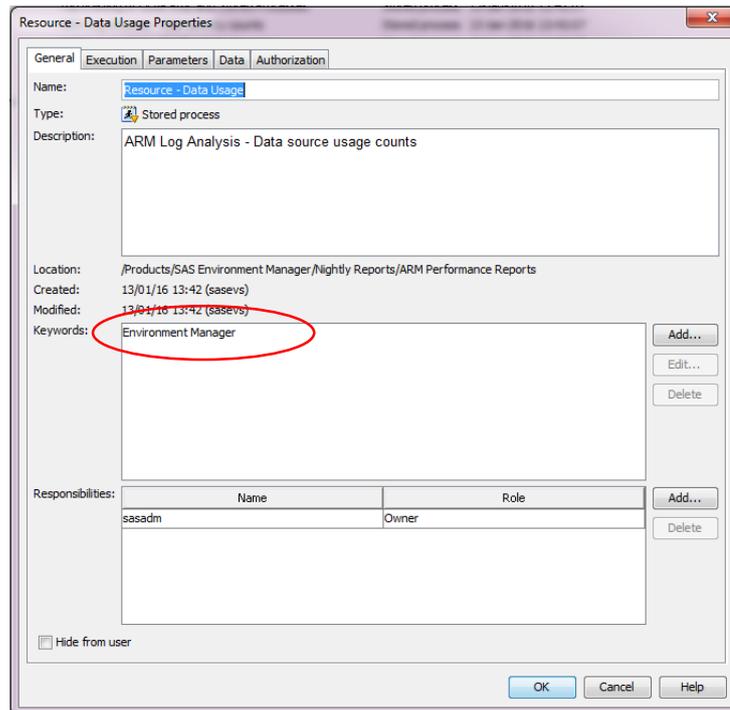
Page 10 of 13

Creating Your Own Reports

Once you know the location of the Extended Monitoring data mart, new stored processes or reports can be created.

You can reuse some of the templates generated by SAS (so your new stored processes integrate nicely with the existing ones) or simply create your own.

When creating new stored processes, there are a few things to consider:

- Add Environment Manager keywords to the new stored processes. The Stored Process web application applies a keyword filter when launched from within Environment Manager, and only those Stored Processes containing the keywords **Environment Manager** will be presented.


Display 7 – Environment Manager Keywords

Amadeus Software Limited, Mulberry House, 9 Church Green, Witney, Oxfordshire UK OX28 4AZ
Tel: +44 (0) 1993 848010 email:info@amadeus.co.uk

Page 11 of 13

- Reuse the existing Stored Processes filters. All of the pre created SAS Stored Processes have the same look and feel, including an initial screen where to select parameters that control the format and content of the output produced.

  Programmers can have a look at the existing code and the parameter configuration screens in order to use the same variable names and code structure when creating custom ones.
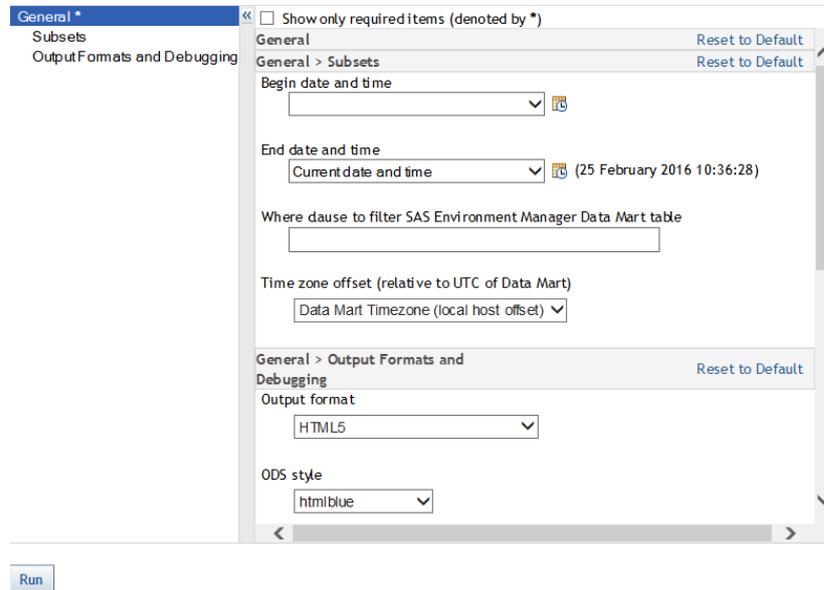
Display 8 – Stored Process parameters
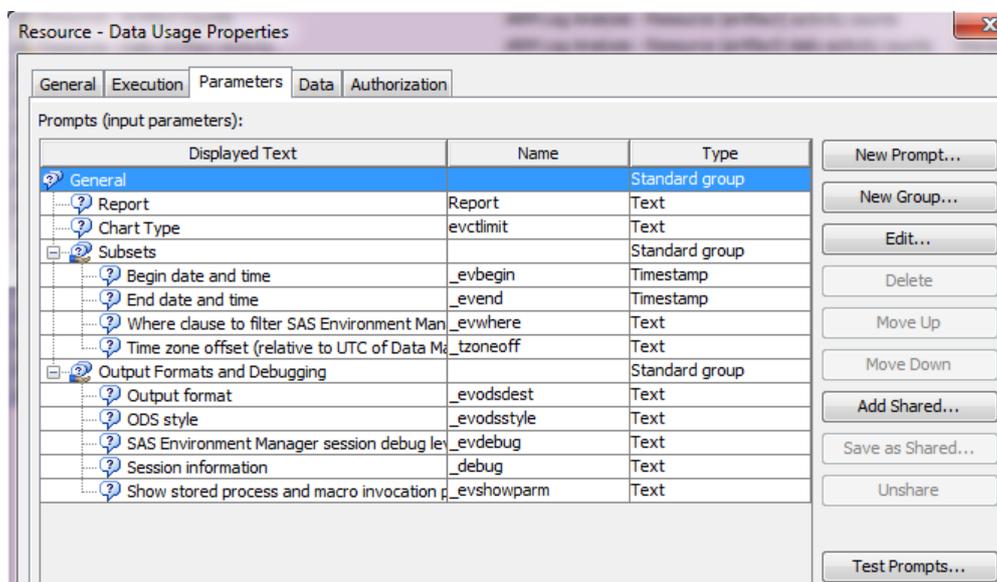
Display 9 – Stored Process parameters configuration

- Security. Remember that you should also set up permissions on any new content created (such as metadata folders) to store the stored processes.

- Giving access. Any person requiring access to these reports through Environment Manager needs to be a member of the group **SAS Environment Manager Data Mart Users** or **SAS Environment Manager Data Mart Administrators**, as otherwise they won't be able to see the associated resources.

Amadeus Software Limited, Mulberry House, 9 Church Green, Witney, Oxfordshire UK OX28 4AZ
Tel: +44 (0) 1993 848010 email:info@amadeus.co.uk

Page 12 of 13

Alerts

The Report Center is incredible useful when an administrator wants to check the activity taking place in the SAS platform. But most of the time we need to be more proactive when it comes to security breaches or incorrect use of the platform. These breaches should be flagged at least daily, and this is easily configurable as you can set up your own email alerts when certain exceptions occur.

Simply create your SAS program and schedule them to run at the relevant times (remember that the metrics get collected by default overnight, although you can change this). Your alerts can also combine other pieces of information, and you can always query the metadata server for extra information not captured on the Environment Manager tables.

CONCLUSION

The use of SAS capability roles and SAS Environment Manager provides the perfect combination for those organizations that need to protect the use of their SAS platform. Without becoming a totalitarian state, like in the novel 1984, administrators can sensible derive different access rules that protect the system from being used incorrectly.

From controlling what analysts can perform in Enterprise Guide, to a division of tasks for administering the SAS platform, using capability roles is the way forward when defining how your SAS system should be used.

Creating a series of customized reports and alerts gives you that extra monitoring that is needed to make sure that the user base is utilizing the SAS platform as it is intended.

By using Environment Manager, administrators have visibility to what happens to their systems and can keep track of the resources available, so you have a stable, secure and fit for purpose SAS environment.

REFERENCES

SAS Institute Inc. "SAS® 9.4 Intelligence Platform: Desktop Application Administration Guide, Fifth Edition" accessed February 3, 2016.

SAS Institute Inc. 2015. SAS® Visual Analytics 7.3: Administration Guide. Cary, NC: SAS Institute Inc.

SAS Institute Inc. "Initializing SAS Environment Manager Service Architecture Framework for SAS 9.4M3". Last revised July 31, 2015.

SAS Institute Inc. "SAS® Environment Manager 2.5: User's Guide" accessed February 15, 2016

CONTACT INFORMATION

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

Author Names	Elena Muriel
Company:	Amadeus Software Limited
Address:	Mulberry House, 9 Church Green, Witney, Oxon OX28 4AZ
Phone:	+44 (0) 1993 848010
Email:	elena.muriel@amadeus.co.uk
Web:	www.amadeus.co.uk

Amadeus Software Limited, Mulberry House, 9 Church Green, Witney, Oxfordshire UK OX28 4AZ
Tel: +44 (0) 1993 848010 email:info@amadeus.co.uk

Page 13 of 13