Global Enablement & Learning

Recommended SAS® 9.4 Security Model Design: Visual Analytics

First Edition

Contact Information

Name: David Stern

Title: Principal Technical Architect, SAS Global Enablement & Learning

Phone Number: +44 1628 490851 Cell: +44 7775 754259

E-mail address: David.Stern@sas.com

THE POWER TO KNOW.

Revision History

Version	By	Date	Description
0.1	David Stern	August 2016	Initial creation
0.2	David Stern	September 2016	Added content on server definitions, libraries and config files, and minor restructure
0.3	David Stern	November 2016	Updates in response to review feedback
1.0	David Stern	December 2016	Published
1.1	David Stern	December 2016	Granted permission to share with customers

References

Ref	Document Title	By	Date	Description and source
Ref 1	Metadata Security in SAS® 9.4 – Step-by-Step	Johannes Jørgensen, Cecily Hoffritz	September 2013	Fourth version of Metadata Security in SAS® – Step-by-Step, for SAS® 9.4. Contains a best practice for security implementation and [at the time of publication] has been the de facto standard [for implementation of SAS metadata security] for more than 7 years in Denmark. Source: http://misksapm.na.sas.com/KnowledgeSharingApplication/AdvSearchDisplayArtifact.jsp?Entry_ID=4156

Table of Contents

1 Introduction

1.1 Series Overview

Figure 1 below is an overview of this series of papers, which together represent the GEL recommended practices for security model design in SAS 9.4.

GEL is an abbreviation used widely in these papers, to refer to the SAS Global Enablement and Learning team, part of SAS Global Consulting Services.

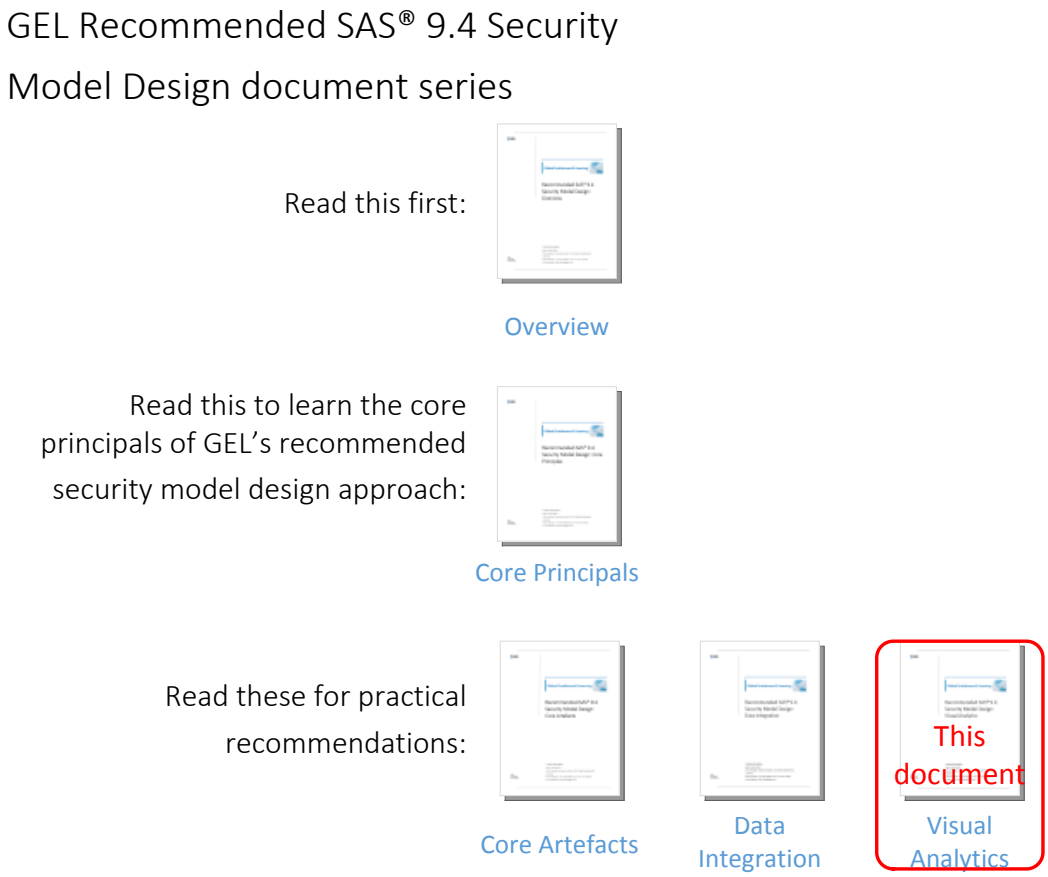


Figure 1 - Overview of papers in this series

1.2 Purpose of this paper

This paper is the first edition of the GEL Recommended SAS 9.4 Security Model Design for **Visual Analytics**.

It is one of a series of papers discussing recommended practices for security model design in SAS 9.4. This paper covers SAS 9.4 security model concepts that apply specifically to SAS platforms where SAS Visual Analytics is present. If you have not done so already, you should start by reading the

Recommended SAS® 9.4 Security Model Design: **Core Principles**. Then, follow the guidance in the GEL Recommended SAS 9.4 Security Model Design: **Core Artefacts** paper. We intend that this paper be used as an extension of the guidance in those two documents, rather than as an alternative, or as a standalone document.

In this paper, we recommend a template pattern of metadata folders and filesystem directories, group, ACTs and permissions, which you should implement on all SAS deployments with Visual Analytics.

See other papers in the "Recommended SAS® 9.4 Security Model Design" series for solution-specific recommendations for other solutions.

You may find this process quicker and easier if you use the set of scripts that we have developed to 'turbocharge' (i.e. speed up) your security model setup. The GEL Turbo scripts and accompanying resources are discussed in the **Core Principles** paper.

1.3 Assumptions

This paper assumes you have read the Recommended SAS® 9.4 Security Model Design: Core Principles, and have some awareness of SAS Visual Analytics.

This paper also assumes that you can make a consistent system-wide backup, from which you know you can successfully restore, before you make any changes recommended in this paper. We further assume that you have done so immediately before you begin making changes, and may make additional backups at sensible points throughout the process of making these changes.

1.4 Distributed vs Non-Distributed LASR Servers

The GEL recommended security model design for SAS Visual Analytics has no significant differences between:

- non-distributed (single-server, symmetric multiprocessing, or SMP) deployments, and
- distributed (massively parallel processing, MPP or massively multiprocessing, MMP) deployments

Metadata and filesystem security for SAS deployments with either type of LASR in-memory analytics server should be approached in the same way.

1.5 Permission to share this document

2 Naming conventions for multitenancy and multi-environment ecosystems

The Core Principles paper discusses naming conventions for objects in security models in general terms, and in particular, for security models in SAS deployments that currently (or will, in the future) support some form of multitenancy. You should adopt and follow clear naming convention for objects implementing your security model, because each tenant of the platform will have its own set of similar objects, and you must be able to identify them easily and distinguish between the ones belonging to each tenant.

The naming convention below allows for consistent naming throughout an *ecosystem* of related SAS deployments: for example, a Development, Test and Production environment which are all related to each other, and form a 'route to live' for application content. However, it is unusual to have Development and Test deployments of SAS Visual Analytics. Many customers only use Visual Analytics in a Production deployment, so for Visual Analytics artefacts, naming to support multiple related deployments is less important than for some other solutions. You can easily cater for an *ecosystem* of related environments in these naming conventions, if necessary, so long as each environment has a distinct name.

We recommend names in this paper that take follow patterns illustrated in the following examples. This is not an exhaustive list, but the following examples are enough to illustrate the pattern:

1. LDAP-synchronised dynamic group named "**SAS Prod Rigel Dept1 Report Developers**" (where 'Rigel' is the name of an example tenant organisation)
2. Static shadow group named "**Rigel Dept1 Report Developers**"
3. ACT named "**Rigel Dept1 Report Developers ACT**"
4. Libref "**RigelV10**"

In the table which follows, we break down the components of each of those example names, to explain what each component is, and when and why they are needed.

Ex.	Object Type	Full Object Name	Component	Explanation
1	Group (LDAP-synch-ronised dynamic group)	SAS Prod Rigel Dept1 Report Developers	SAS	A group of this name should exist in the customer's Active Directory system, and a group of this name should also exist in SAS metadata. The 'SAS' prefix helps AD administrators identify the group as being important for SAS, and means that it sorts alphabetically together with other SAS groups in Active Directory. The 'SAS' prefix also serves the purpose of identifying the LDAP-synchronised corresponding group in SAS Metadata as having come from Active Directory synchronisation; there is no other reason to prefix a group name in SAS metadata with 'SAS'!
			Prod	The second component of this name signifies that this group should contains users of the SAS Production environment, in an organisation where there is an ecosystem of related Dev, Test and Prod environments. SAS Visual Analytics deployments are sometimes found in Development and Test environments, but not always. Allows users to be put in a group like Dept1 Report Developers in different environments, so that the permissions assigned to the static *group* can be consistent across all environments in the ecosystem, but one *user* does not necessarily get the same permissions in all environments.
			Rigel	Important for SAS ecosystems which support multitenancy, the long name of the 'tenant' organisation.

				Distinguishes this group from another tenant's Dept1 Report Developers. **Optional if your SAS deployment is always going to be strictly single-tenant.**
			Dept1	For SAS Visual Analytics deployments which support multiple Departments, Projects, Teams, Subject Areas, Data Topics, or Organisations *per tenant*, a name which indicates this. Dept1 is not meant to be used *literally* in the actual group name: it is meant as a *placeholder* for the name of the actual department name, e.g. you could replace it with any of: Oscar, Marketing, Credit Risk, Clinical Trials Data, or Northern Europe. We use Dept1 throughout the GEL Recommended SAS 9.4 Security Model Design for Visual Analytics, and in the GEL Turbocharge scripts' example CSV data for VA, as a *placeholder* for *a real name* of one of those types. The impersonal, nonspecific name *Dept1* should not end up in your actual SAS security model, when you have documented, implemented and handed it over to a customer!
			Report Developers	Indicates what members of this group do: in this example, they develop reports for the department named in the previous component of this group name.
2	Group (static shadow group)	Rigel Dept1 Report Developers	Rigel	Important for SAS ecosystems which support multitenancy, the long name of the 'tenant' organisation. Distinguishes this group from another tenant's DI Developers. **Optional if your SAS deployment is always going to be strictly single-tenant.** The shadow group is static, in the sense that it can't be accidentally deleted if the Active Directory group 'SAS Prod Rigel Dept1 Report Developers' is deleted or if synchronisation with LDAP fails. This group is therefore safe to use in ACTs.

				No 'SAS' prefix: this group only exists inside SAS metadata, so does not need to be labelled as 'SAS'. No 'Prod' prefix: within this metadata repository, everything belongs to the same SAS deployment, so no qualification is necessary. This also keeps the name of this group consistent across all deployments in the ecosystem: it exists with the exact same name in each one (if it exists at all – for Visual Analytics, this group may not be needed anywhere outside Production).
			Dept1	For SAS Visual Analytics deployments which support multiple Departments, Projects, Teams, Subject Areas, Data Topics, or Organisations *per tenant*, a name which indicates this. Dept1 is a *placeholder* for the real name.
			Report Developers	Indicates what members of this group do.
3	ACT	Rigel Dept1 Report Developers ACT	Rigel	Important for SAS ecosystems which support multitenancy, the long name of the 'tenant' organisation. Distinguishes this tenant's DI Developers ACT from another tenants' DI Developers ACTs. **Optional if your SAS deployment is always going to be strictly single-tenant.**
			Dept1	As above.
			Report Developers	Indicates which group this ACT features.

			ACT	This suffix is redundant when discussing ACTs only, but in a broader context when we may discuss ACTs together with groups and folders, helps identify this object as an ACT.
4	Libref	RigelV10	Rigel	Librefs are limited to 8 characters. We allow up to 5 characters for a short version of the tenant or project's name. If there are multiple tenants, and each has multiple projects/teams/data topics etc, this part of a libref name can become very condensed: you may need to design a naming convention where e.g. the first three characters indicate the tenant organisation, and the next two indicate the project/team/data topic.
			V	Librefs are limited to 8 characters. We allow up to 3 characters for an abbreviation of the library name: the first letter for a VA-specific BASE Engine library is V, indicating that it belongs to SAS Visual Analytics. Other letters used in this character position include L, for a LASR library, and H for a Hadoop library.
			1	This character indicates that the library belongs to Dept1, or rather, the first department in this instance of the security model structure. The next department will take number 2 in this position of its librefs, and so on. Since the ordinal number to department/project/team/etc relationship is not going to be at all intuitive in most designs, document and publicise the relationship between number and team.
			0	Indicates the first BASE Engine library per instance of the repeated structure, for example, Source Data.

				Other BASE Engine libraries in the reporting data structure (if you decide to create any more as part of your design) could take successive numerals in this position, e.g. Target Data could take number 1, Reporting Mart number 3 and so on.

Table 1 – Example object names illustrating our recommended naming convention

You should use the structure above if it will work for your customer. Apart from providing a regular naming convention that allows you to name a large number of objects in a multi-tenant ecosystem of related SAS deployments, another benefit of following this naming convention in particular is that SAS staff who are familiar with these recommendations will immediately understand it, and you will waste less time explaining your naming convention to them.

If the structure described above will not work for your customer (e.g. because your customer has some more complex internal organisation which must be represented in more complex object names), you may absolutely deviate from the naming convention above. However, you should then document your naming convention clearly, and use it consistently across all the SAS deployments that belong together in an ecosystem, for this customer.

3 Static metadata groups

'Static metadata groups' in SAS metadata are static in the sense that the process of synchronising groups with Active Directory or another LDAP provider does not create or destroy them.

See the discussion of dynamic groups synchronised from LDAP, and their corresponding Static Groups in the Recommended SAS® 9.4 Security Model Design: **Core Principles** section titled "Identify groups of users who will use the assets".

For SAS deployments that include Visual Analytics, create one of each of the following groups for each 'tenant' organisation in each SAS deployment in your ecosystem. If this SAS deployment will **never** need to support multitenancy, omit the 'tenant' part of each group name. Otherwise substitute the tenant's name for [Tenant] in each group name below.

Many of the group names also include [Dept1], a placeholder for the name of a Department, Project, Team, Subject Area, Data Topic, or sub-organisation etc. For simplicity, we will refer to these as departments, but please think of a 'department' as being potentially any of those things, and [Dept1] as a placeholder name for any one such thing. Your design should have one of each such group, per department, for the tenant.

The idea is that a given tenant may have multiple separate departments, who have their own separate work areas (with their own departmental groups, ACTs, folders etc.). There are also 'All' groups which should include all of the corresponding departmental groups.

Altogether, the group structure presented below is designed to support both multitenancy and a multidepartmental (or multi-project, multi-team etc.) organisational structure for each tenant, at the same time.

Metadata Group	Description
[Tenant] All Users	Super-group containing all the 'All' groups below for this tenant, and thereby all users who have any access whatsoever to content belonging to this tenant organisation. Used to restrict access to the tenant organisation's top level folder in metadata so that other tenants cannot see it.
[Tenant] All Report Developers	Super-group containing each of the separate departmental Report Developers groups for this tenant.
[Tenant] All Analysts	Super-group containing each of the separate departmental Analysts groups for this tenant.

[Tenant] All LASR Administrators	Super-group containing each of the separate departmental LASR Administrators groups for this tenant.
[Tenant] All Consumers	Super-group containing each of the separate departmental Consumers groups for this tenant.
[Tenant] All [Dept1]	Super-group containing all members of each of the [Dept1] departmental groups belonging to this tenant.
[Tenant] [Dept1] Report Developers	Create one group like this per Tenant, per department. Contains expert users of SAS Visual Analytics who create reports on LASR data belonging to this department, for other users in the same department (etc.) or outside it to consume. Preferred applications: • SAS® Enterprise Guide® • SAS® Add-In for Microsoft Office • SAS® Visual Analytics Explorer • SAS® Visual Analytics Report Designer • SAS® Programming in an editor
[Tenant] [Dept1] Analysts	Create one group like this per department belonging to each tenant of the SAS deployment. Contains expert users who use SAS Visual Analytics and other applications to perform many types of analysis on data belonging to this single department. Preferred applications: • SAS® Enterprise Guide® • SAS® Add-In for Microsoft Office • SAS® Visual Analytics Explorer • SAS® Visual Analytics Report Designer • SAS® Programming in an editor
[Tenant] [Dept1] LASR Administrators	Create one group like this per department belonging to each tenant of the SAS deployment.

	Contains all LASR Administrator responsible for managing (creating, starting, stopping) the LASR Servers, for loading and unloading LASR tables, and for managing Autoload for this specific department (etc.). Preferred applications: • SAS® Management Console • SAS® Visual Analytics Data Management • SAS® Programming in an editor
[Tenant] [Dept1] Consumers	Create one group like this per department belonging to each tenant of the SAS deployment. Contains all users belonging to this department (etc) who consume reports created by members of the corresponding [Tenant] [Dept1] Report Developers group. Preferred applications: • SAS® Visual Analytics

Table 2 – Metadata Groups for SAS Visual Analytics, describing the users belonging to each group

3.1 Metadata group structure

Figure 2 below shows illustrates how these groups should be organized, if they were instantiated for a tenant named “Rigel”, who has two departments. The department names in this figure have not been substituted with example names, and have been left as Dept1 and Dept2. However, in practice, you would also replace those placeholder names with the actual department names.

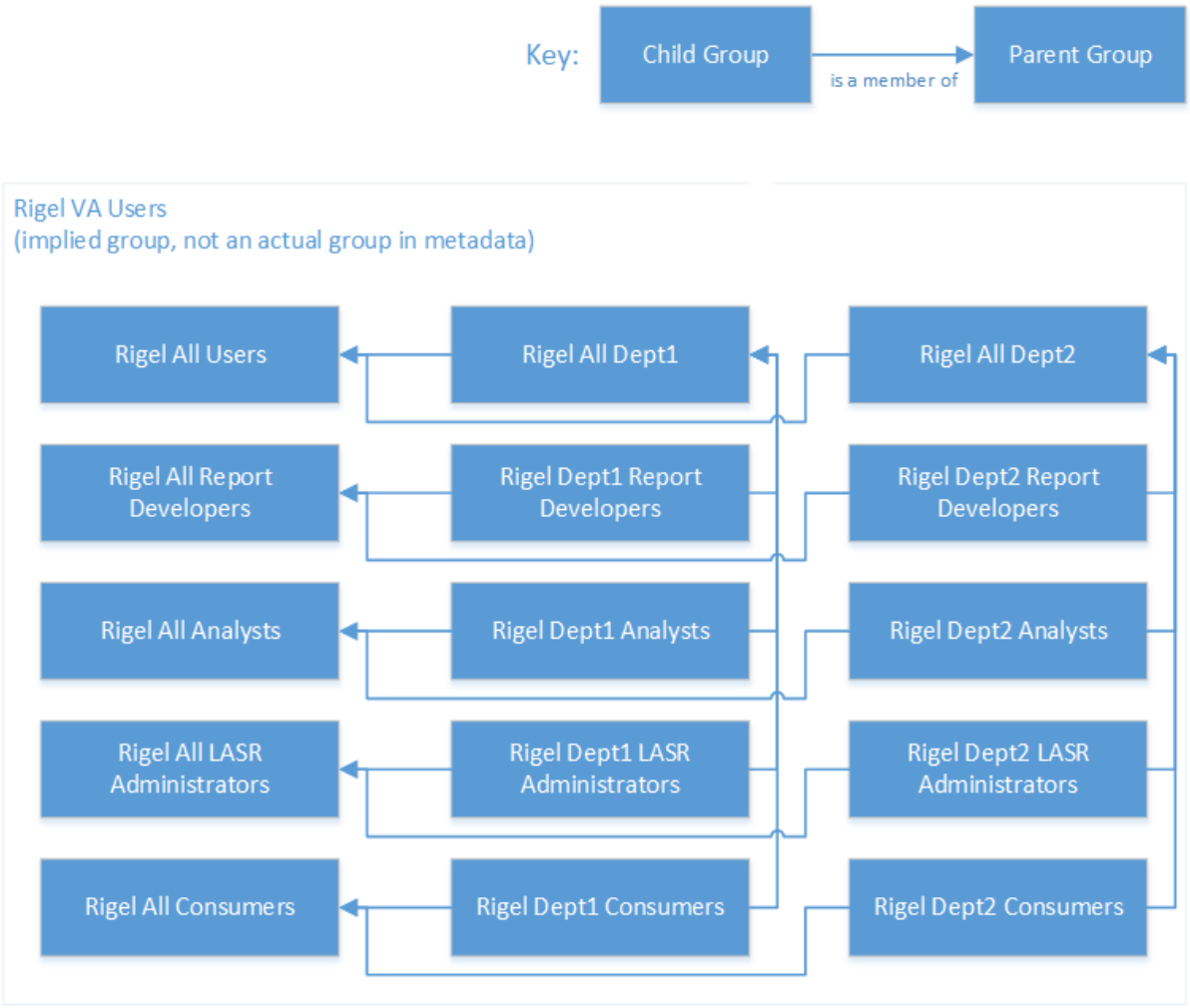


Figure 2 – Example representation of VA groups for a tenant named "Rigel". The placeholder department names Dept1 and Dept2 have not been substituted with example department names in this figure.

4 Metadata folders

For SAS deployments that include Visual Analytics, create one of each of the following metadata folder structures for each tenant organisation in your SAS deployment. If this SAS deployment will **never** need to support multitenancy, create one copy of this metadata folder structure, which should NOT be inside a top-level folder named after the organisation or project. Since Visual Analytics users are more akin to end users than to developers, they should be offered as shallow a folder structure as possible. If this SAS deployment will have multiple tenants, you have no alternative but to group each instance of the metadata folder structure below inside a top-level folder, named for the tenant.

In this folder structure, you will see a folder labelled [Dept1], with subfolders below it. This is meant to represent a repeated structure of folders for a series of Departments, Projects, Teams, Subject Areas, Data Topics, Organisations, or any other 'unit' of a tenant's business which makes sense – each having its own similar set of subfolders. As in section 3 above, we will simply call any of these things 'departments', but when you see the term department, remember that it could represent any of those things, and you should create one such folder structure for each one of them that this tenant has. Again, [Dept1] is intended as a placeholder for the actual name of each instance of any of those things belonging to this tenant.

SAS Folders	Top metadata folder
[Tenant]	Only place the following Visual Analytics folders under a grouping folder like this if there will be multiple tenants of this SAS deployment. To put it another way, the flatter the folder structure the better, so do not include this folder in the structure for Visual Analytics if it is not required. Even if not required for Visual Analytics folders below, this folder may still exist as part of your overall metadata folder design, to contain Data Integration content. That is not our main concern here, in this paper. If there will only be one tenant in the SAS deployment, please place the Visual Analytics folders listed in the rest of this table *directly* beneath the SAS Folders folder, and not beneath this folder, to minimise the number of levels of folder hierarchy that Visual Analytics users see.
[Dept1]	Top level of a sub-structure of folders for data and reports developed for a single department. You should name each instance of this folder after its respective department, and not name them Dept1, Dept2 etc.

	Normally only users in a [Dept1] metadata group will see this folder and its subfolders. Duplicate this folder and the structure of folders below it for each separate department in this tenant organisation.
Analyses	Metadata folder for ad-hoc analysis of data specific to [Dept1].
Data	Data for reports specific to [Dept1].
Formats (optional)	Optional. If required, metadata folder for tables used to populate formats, used in preparing data specific to [Dept1], which is loaded into LASR.
LASR Data	Metadata folder for LASR libraries and tables specific to [Dept1].
Source Data	BASE Engine libraries and tables containing data specific to [Dept1] that is prepared for loading into LASR.
Reports	Published reports specific to [Dept1].
Work In Progress	Reports and Data Explorations specific to [Dept1], which are not yet ready to be published.
Global	Top level of a sub-structure of folders for data and reports developed for an audience across the whole tenant organisation. Everyone in the tenant organisation can see reports in the Global Reports folder.
Analyses	Metadata folder for ad-hoc analysis of global data (used across the whole tenant organisation).
Data	Data for reports which are globally-accessible (across all departments for this tenant).
Formats (optional)	Optional. If required, metadata folder for tables used to populate formats, used in preparing data loaded into LASR.
LASR Data	Metadata folder for LASR libraries and tables.
Source Data	BASE Engine libraries and tables containing data which is prepared for loading into LASR.
Reports	Published reports on global data (across the whole tenant organisation).
Work In Progress	Reports and Data Explorations that are not yet ready to be published.

Table 3 – Metadata Folders for SAS Visual Analytics

In contrast with the folder structure recommended for SAS deployments which include SAS Data Integration Studio, this folder structure is flatter, and does not have numeric prefixes before folder names. Users of SAS Visual Analytics are end-users of the SAS deployment, and tend to prefer as flat a metadata folder structure as possible, for simplicity.

Also, the several groups of SAS Visual Analytics users each can see different subsets of this metadata folder structure, so numbering the folders would lead to potential confusion for the users who can only see folders prefixed e.g. 01_ and 03_: they would wonder what happened to a folder prefixed 02_. We avoid this potential for confusion by not numbering Visual Analytics folders.

The next section describes a similar structure of filesystem folders.

5 Filesystem folders

For SAS deployments that include Visual Analytics, create one of each of the following filesystem folder structures for each 'tenant' organisation in your SAS deployment. If this SAS deployment will **never** need to support multitenancy, you should NOT group these folders inside a common top-level folder named after the tenant project or organisation. If this SAS deployment will have multiple tenants, you have no alternative but to group each instance of the filesystem folder structure below inside a top-level folder, named for the tenant.

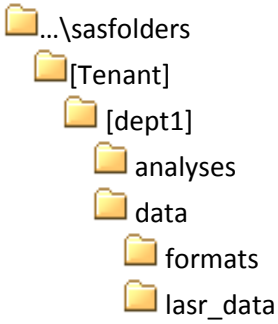
We recommend that filesystem folders are named in all lowercase, on both Windows and Unix.

In the table below, the top level folder is shown as …\sasfolders. This is intended to mean that you should create a folder called 'sasfolders' in an appropriate place on a filesystem accessible from all the SAS servers (Workspace Server, Stored Process Server) in your SAS deployment's main Application Server Contexts (e.g. SASApp). For example, on Unix you may place this folder at /opt/sas/data/sasfolders, or on Windows you may place it at D:\sasfolders.

You may choose another name for the 'sasfolders' folder if you prefer. The suggested name is meant to mirror the "SASFolders" top-level folder in metadata.

The use and meaning of the filesystem folders is the same as the corresponding metadata folders: they are intentionally similar. The only differences (in the recommended standard structure) are that filesystem folders are named in all lowercase, and underscores are used instead of spaces to separate names of more than word.

As for the metadata folder structure in the previous section, you will see a folder labelled [Dept1], with subfolders below it in the table below. Again, this is meant to represent a *repeated* structure of folders for a series of Departments, Projects, Teams, Subject Areas, Data Topics, Organisations, or any other 'unit' of a tenant's business which makes sense – each having its own similar set of subfolders. As in section 3 above, we will simply call any of these things 'departments', but when you see the term department, remember that it could represent any of those things, and you should create one such folder structure for each one of them that this tenant has. Again, [dept1] is intended as a placeholder for the actual name of each instance of any of those things belonging to this tenant.



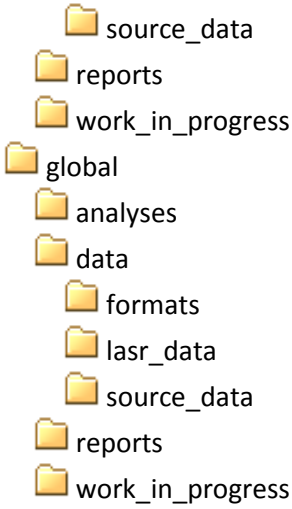


Table 4 – Filesystem Folders for SAS Visual Analytics

6 Libraries

6.1 Base Libraries

For SAS deployments that include Visual Analytics, create one of each of the following BASE libraries for each 'tenant' organisation in your SAS deployment. In this table:

- The placeholder string [TEN] should be replaced with a maximum 5-letter abbreviation for the tenant organisation name in the libref.
- The placeholder string [Tenant] should be replaced with the longer name of the tenant organisation.
- Create one copy of each of the libraries containing the placeholder string [Dept1] for each department (etc.) that a given tenant has.

To learn which filesystem folder each Filesystem Alias refers to, see section 7 below.

Librefs are constrained to a maximum length of 8 characters. In our naming convention, five of these characters are reserved to contain an abbreviation of the name for the tenant organisation. The remaining 3 characters in each libref (e.g. VG0, V1F) are used for a somewhat cryptic-looking 3 letter code identifying the library. While they are not intuitive to an uninformed reader, we intend them to make the library somewhat recognisable to an informed reader who knows what these 3-letter codes are, by the libref alone. They should be useable in this format so long as a tenant does not have more than 10 departments (or projects, teams etc.), taking the numbers 0-9 (notice that G=Global, leaving you with all 10 single numerals for the departments). However, for tenants with more than 10 departments (or 16 if you choose to use a single hexadecimal digit!), this naming convention will not work well. You may have to come up with another naming convention for the last 3 characters in each libref, such as a 3-character serial code, and a lookup table translating the serial code into a more meaningful name for the library. That would allow 1000+ departments per tenant, at the cost of some loss of transparency.

Libref	Library Name	Metadata Folder	Filesystem Alias	Description
[TEN]VG0	[Tenant] Global Source Data_[TEN]VG0	/[Tenant]/Global/Data/Source Data	![Tenant]_gbl_0	Contains BASE engine source tables which can be loaded into LASR for use in Global reports. In the code VG0 making up the last 3 characters of the libref:

				V=Visual Analytics Base Library G=Global 0=Source Data
[TEN]V10	[Tenant] [Dept1] Source Data_[TEN]V10	/[Tenant]/[Dept1]/Data/Source Data	![Tenant]_[dept1]_0	Contains BASE engine source tables which can be loaded into LASR for use in [Dept1] reports. In the code V10 making up the last 3 characters of the libref: V=Visual Analytics Base Library 1=[Dept1], 2=[Dept2] etc. 0=Source Data
[TEN]VGF	[Tenant] Global Formats_[TEN]VGF	/[Tenant]/Global/Data/Formats	![Tenant]_gblfmt	SAS Format Library for use in Global reports. In the code VGF making up the last 3 characters of the libref: V=Visual Analytics Base Library G=Global F=Formats
[TEN]V1F	[Tenant] [Dept1] Formats_[TEN]V1F	/[Tenant]/[Dept1]/Data/Formats	![Tenant]_[dept1]fmt	SAS Format Library for use in [Dept1] reports. In the code V1F making up the last 3 characters of the libref: V=Visual Analytics Base Library 1=[Dept1], 2=[Dept2] etc.

				F=Formats

Table 5 – GEL Recommended 'VA' Base and Format Libraries to include in security model designs for deployments which include SAS Visual Analytics

6.2 LASR Servers

For SAS deployments that include Visual Analytics, create one of each of the following LASR Servers for each 'tenant' organisation in your SAS deployment. In this table:

- The placeholder string [Tenant] should be replaced with the longer name of the tenant organisation.
- Create one copy of each of the LASR servers containing the placeholder string [Dept1] for each department (etc.) that a given tenant has.

LASR Server Name
[Tenant] – Global LASR Server
[Tenant] – [Dept1] LASR Server

Table 6 - GEL Recommended 'VA'LASR Servers

When creating each LASR server in metadata, you will need to provide values for many other settings, such as LASR server type (SMP/Non-distributed or MMP/Distributed), the High Performance Analytics Environment install location, the name of the LASR server root node, a path to a filesystem location in which signature files should be stored, a port number for the LASR server to listen on, and others. You will need to determine the values of each setting as appropriate for your SAS deployment: existing LASR servers may provide some help as to what these values could be, or you can ask an architect or read the installation documentation for help with these values.

6.3 LASR Libraries

For SAS deployments that include Visual Analytics, create one of each of the following LASR Libraries for each 'tenant' organisation in your SAS deployment. In this table:

- The placeholder string [TEN] should be replaced with a maximum 5-letter abbreviation for the tenant organisation name in the libref.
- The placeholder string [Tenant] should be replaced with the longer name of the tenant organisation.
- Create one copy of each of the LASR library containing the placeholder string [Dept1] for each department (etc.) that a given tenant has.

Library Name	Libref	LASR Server	BASE Library Name	Metadata Folder for LASR Library	AutoLoad Metadata Folder (same folder as ←)	AutoLoad Filesystem Path
[Tenant] Global LASR Data_[TEN] LG0	[TEN]LG0	[Tenant] – Global LASR Server	[Tenant] Global Source Data_[TEN] VG0	/[Tenant]/Global/Data/ LASR Data	/[Tenant]/Global/Data/ LASR Data	…\sasfolders\[tenant]\global\data\source_data
[Tenant] [Dept1] LASR Data_[TEN] L10	[TEN]L10	[Tenant] – [Dept1] LASR Server	[Tenant] [Dept1] Source Data_[TEN] V10	/[Tenant]/[Dept1]/Data/ LASR Data	/[Tenant]/[Dept1]/Data/ LASR Data	…\sasfolders\[tenant]\[dept1]\data\source_data

Table 7 - GEL Recommended 'VA' LASR Libraries

When creating each LASR library in metadata, you will need to provide values for several other settings. Determine the values of each setting as appropriate for your SAS deployment: existing LASR servers may provide some help as to what these values could be, or you can ask an architect or read the installation documentation for help with these values.

6.4 SASHDAT Libraries

For SAS deployments that include Visual Analytics, create one of each of the following SASHDAT Libraries for each department in each 'tenant' organisation in your SAS deployment. In this table:

- The placeholder string [TEN] should be replaced with a maximum 5-letter abbreviation for the tenant organisation name in the libref.
- The placeholder string [Tenant] should be replaced with the longer name of the tenant organisation.
- Create one copy of each of the SASHDAT library containing the placeholder string [Dept1] for each department (etc.) that a given tenant has.

Library Name	Libref	LASR Server	Metadata Folder for LASR Library	Hadoop Path
[Tenant] [Dept1] SASHDAT Data_[TEN]H10	[TEN]H10	[Tenant] – Global LASR Server	/[Tenant]/[Dept1]/Data	/[HadoopDir]/[Tenant]

Table 8 - GEL Recommended 'VA' SASHDAT Libraries

When creating each SASHDAT library in metadata, you will need to provide values for several other settings, especially the name and connection of the Hadoop Server, and a path at which the data in the library will be stored in HDFS (shown as the Hadoop Path in the table above). The values show above – and even the suggestion that you create one SASHDAT library per department is more of a suggestion than a recommendation, since customer organization may not use Hadoop, and may or may not require SASHDAT libraries. If you do create these SASDHDAT libraries, determine the values of each setting as appropriate for your SAS deployment: existing LASR servers may provide some help as to what these values could be, or you can ask an architect or read the installation documentation for help with these values.

7 Modifications to AppServer Config Files

In this section, example entries in the main sasv9_usermods.cfg file, and in supplemental configuration files, are shown with placeholder strings as follows:

Placeholder string	Substitute this with
`[tenant]`	The tenant's name written without spaces
`sasfolders_dir`	The full path to that tenant's sasfolders directory

Following the suggested template for each set of configuration lines, examples are shown in which the placeholder strings have been substituted for a tenant called "Rigel" whose sasfolders directory is at D:\sasfolders on Windows, or /opt/sas/data/sasfolders on Unix.

7.1 SASApp/sasv9_usermods.cfg

For each VA tenant using the SAS deployment, add one copy of a set of lines similar to those in the following examples to the sasv9_usermods.cfg file in each AppServer Context which users belonging to that tenant will use.

Note that the GEL Recommended SAS 9.4 Security Model Design: **Core Artefacts** paper explains how an alias for `![tenant]_sasfolders` is defined in the sasv9_usermods.cfg file.

Notice also how the last '-config' line added to the SASApp/sasv9_usermods.cfg file causes SAS to also read the tenant-specific VA config file in the tenant's sasfolders directory. That file is described in section 7.2 below.

Take care when editing sasv9_usermods.cfg to not specify invalid values: an error reading the config file can prevent SAS from starting a workspace, batch or other SAS session.

7.1.1 Windows

Note that on Windows the filesystem paths must be in double quotes, even when there are no spaces in the path.

```
-SET [tenant]_vafolders "sasfolders_dir\[tenant]"

-config ![tenant]_sasfolders/[tenant]_va_usermods.cfg
```

Here is what this might look like with the placeholder strings replaced with example values:

```
-SET Rigel_vafolders "D:\sasfolders\Rigel"

-config "!Rigel_sasfolders/Rigel_va_usermods.cfg"
```

7.1.2 Unix and Linux

Note that on Unix and Linux, the filesystem paths do not need to be quoted unless they contains spaces.

```
-SET [tenant]_vafolders sasfolders_dir/[tenant]

-config ![tenant]_sasfolders/[tenant]_va_usermods.cfg
```

Here is what this might look like with the placeholder strings replaced with example values:

```
-SET Rigel_vafolders /opt/sas/data/sasfolders/Rigel

-config !Rigel_sasfolders/Rigel_va_usermods.cfg
```

7.2 …/sasfolders/[tenant]_va_usermods.cfg

For each DI tenant using the SAS deployment, create a separate SAS config file in the tenant's sasfolders directory, named [tenant]_di_usermods.cfg, containing the lines below. These define the libref filepath aliases listed in section 6 above.

7.2.1 Windows

Note that on Windows the filesystem paths must be in double quotes, even when there are no spaces in the path.

Notice how on Windows, you can use another filesystem alias (such as !Rigel_vafolders) in the second argument to a –SET line.

The template content to put in this file is:

```
-SET [tenant]_gbl_0    "![tenant]_vafolders/global/data/source_data"
-SET [tenant]_dept1_0  "![tenant]_vafolders/dept1/data/source_data"
-SET [tenant]_gblfmt   "![tenant]_vafolders/global/data/formats"
-SET [tenant]_dept1fmt "![tenant]_vafolders/dept1/data/formats"

-insert fmtsearch [tenant]_gblfmt
-insert fmtsearch [tenant]_dept1fmt
```

Here is what this might look like with the placeholder strings replaced with example values:

```
-SET Rigel_gbl_0    "!Rigel_vafolders/global/data/source_data"
-SET Rigel_dept1_0  "!Rigel_vafolders/dept1/data/source_data"
-SET Rigel_gblfmt   "!Rigel_vafolders/global/data/formats"
-SET Rigel_dept1fmt "!Rigel_vafolders/dept1/data/formats"

-insert fmtsearch Rigel_gblfmt
-insert fmtsearch Rigel_dept1fmt
```

7.2.2 Unix and Linux

Note that on Unix and Linux, the filesystem paths do not need to be quoted unless they contains spaces.

Notice now on Unix, you cannot use another filesystem alias in the second argument to a –SET line. You have to give the target directory in full.

The template content to put in this file is:

```
-SET [tenant]_gbl_0    sasfolders_dir/[tenant]/global/data/source_data
-SET [tenant]_dept1_0  sasfolders_dir/[tenant]/dept1/data/source_data
-SET [tenant]_gblfmt   sasfolders_dir/[tenant]/global/data/formats
-SET [tenant]_dept1fmt sasfolders_dir/[tenant]/dept1/data/formats

-insert fmtsearch [tenant]_gblfmt
-insert fmtsearch [tenant]_dept1fmt
```

Here is what this might look like with the placeholder strings replaced with example values:

```
-SET Rigel_gbl_0    /opt/sas/data/sasfolders/Rigel/global/data/source_data
-SET Rigel_dept1_0  /opt/sas/data/sasfolders/Rigel/dept1/data/source_data
-SET Rigel_gblfmt   /opt/sas/data/sasfolders/Rigel/global/data/formats
-SET Rigel_dept1fmt /opt/sas/data/sasfolders/Rigel/dept1/data/formats

-insert fmtsearch Rigel_gblfmt
-insert fmtsearch Rigel_dept1fmt
```

8 Access Control Templates

In this section, the permissions set in access control templates are given using abbreviations, which are explained in the section titled "Abbreviations of Permissions in Access Control Templates" in the Recommended SAS® 9.4 Security Model Design: Core Principles paper.

For SAS deployments that include Visual Analytics, create one of each of the following Access Control Templates for each 'tenant' organisation in your SAS deployment. These should be created *in addition* to the ACTs described in the Recommended SAS® 9.4 Security Model Design: Core Principles paper.

Create or Modify: ACT Name	Group	Permissions Granted (G) or Denied (D)
Create: [Tenant] All Users ACT	[Tenant] All Users	G: RM R
Create: [Tenant] All Report Developers ACT	[Tenant] All Report Developers	G: RM WMM R
Create: [Tenant] All Analysts ACT	[Tenant] All Analysts	G: RM WMM R
Create: [Tenant] All LASR Administrators ACT	[Tenant] All LASR Administrators	G: RM WM WMM R W C D A
Create: [Tenant] All Consumers ACT	[Tenant] All Consumers	G: RM R
Create: [Tenant] All [Dept1] ACT	[Tenant] All [Dept1]	G: RM R
Create: [Tenant] [Dept1] Report Developers ACT	[Tenant] [Dept1] Report Developers	G: RM WMM R
Create: [Tenant] [Dept1] Analysts ACT	[Tenant] [Dept1] Analysts	G: RM WMM R
Create: [Tenant] [Dept1] Analysts Server ACT	[Tenant] [Dept1] Analysts	G: RM WM

Create: [Tenant] [Dept1] LASR Administrators ACT	[Tenant] [Dept1] LASR Administrators	G: RM WM WMM R W C D A
Create: [Tenant] [Dept1] Consumers ACT	[Tenant] [Dept1] Consumers	G: RM R

Table 9 – GEL Recommended 'VA' Access Control Templates to include in security model designs for deployments which include SAS Visual Analytics

9 Apply Access Control Templates

9.1.1 Apply ACTs to Metadata Folders

Table 10 shows which VA ACTs to apply to which metadata folders.

Location in Folders Tab	**VA ACTs to apply**
SAS Folders	
[Tenant, if this folder exists]	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] All Users ACT
Reason: If there is only one tenant in this SAS deployment, this folder should not exist. Or if it exists for some other reason, such as acting as the top level folder for DI content, it should not contain any of the VA content described in this paper, and none of these VA-specific ACTs should be applied to it. *But if there* are *multiple tenants in this SAS deployment, their content should be kept separate so that one tenant cannot see other tenants' folder structures. In that case, this folder should exist, and you should apply these ACTs so that only SAS Administrators and members of one of the groups belonging to this tenant can see it and its contents.*	
[Dept1]	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT [Tenant] All [Dept1] ACT
Reason: Users belonging to other tenants should be denied access to each [Dept1] folder for each tenant. SAS Administrators retain their usual full access. LASR Administrators for Dept1 specifically get Read Write access to this folder and its contents, and all members of any of the [Dept1] groups get read-only access to it, so that they can navigate to its subfolders.	
Analyses	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT [Tenant] [Dept1] Analysts ACT
Reason: Most users should be denied access to a department/project/team etc. Analyses folder, even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators and Analysts for that specific department/project/team in that tenant organisation have (read-write) access to this folder, so that they can save finished global data explorations in it.	
Data	
Formats (if present)	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT

Reason: Most users should be denied access to a department/project/team etc. Formats folder (if it is present), even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators for that specific department/project/team in that tenant organisation have (read-write) access to this folder, so that they can manage the tables in this folder used for creating formats, and apply formats to data they load from Source tables into LASR.	
LASR Data	SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT
Reason: Most SASUSERS inherit read-only permissions for this folder from the parent Global folder. Apart from SAS Administrators, only LASR Administrators for the relevant tenant organisation have read-write access to this folder, so that they can create/delete/update LASR tables within it.	
Source Data	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT
Reason: Most users should be denied access to a department/project/team etc. Source Data folder. Apart from SAS Administrators, only LASR Administrators for that specific department/project/team in that specific tenant organisation have (read-write) access to this folder, so that they can manage the Source library and tables in this folder, and load data from Source tables into LASR.	
Reports	SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT [Tenant] [Dept1] Report Developers ACT [Tenant] [Dept1] Consumers ACT
Reason: Most users who are members of any of the [Dept1] groups belonging to a tenant inherit read-only access to the corresponding department/project/team etc. Reports folder. Apart from SAS Administrators, LASR Administrators and department/project/team Report Developers have read-write access to this folder, so that they can publish completed reports to their departmental audience. Consumers belonging to the specific department within this tenant organisation should also have access to read (and run) the reports in this department/project/team etc. Reports folder.	
Work In Progress	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] [Dept1] LASR Administrators ACT [Tenant] [Dept1] Analysts ACT [Tenant] [Dept1] Report Developers ACT
Reason: Most users should be denied access to a department/project/team etc. Work In Progress folder, even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators, Analysts and Report Developers for that specific department/project/team in that tenant organisation have (read-write) access to this folder, so that they can work on unfinished global data explorations and reports in it.	
Global	[Tenant] SASUSERS Read Only ACT SAS Administrator Settings [Tenant] All LASR Administrators ACT
Reason: All users (who belong to the tenant organisation that owns this Global folder) should have read-only access to this folder and its contents. SAS Administrators retain their usual full access to this folder. LASR Administrators belonging to any of the Departments, Projects, Teams, Subject Areas, Data Topics, or Organisations within this tenant organisation should also have access to create and remove LASR tables within this folder, and any of its subfolders.	
Analyses	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] All LASR Administrators ACT

	[Tenant] All Analysts ACT
Reason: Most users should be denied access to the Global Analyses folder, even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators and Analysts for that tenant organisation have (read-write) access to this folder, so that they can save finished global data explorations in it.	
Data	
Formats (if present)	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] All LASR Administrators ACT
Reason: Most users should be denied access to the Global Formats folder (if it is present), even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators for that tenant organisation have (read-write) access to this folder, so that they can manage the formats in this folder, and apply formats to data they load from Source tables into LASR.	
LASR Data	SAS Administrator Settings [Tenant] All LASR Administrators ACT
Reason: Most SASUSERS inherit read-only permissions for this folder from the parent Global folder. Apart from SAS Administrators, only LASR Administrators for the relevant tenant organisation have read-write access to this folder, so that they can create/delete/update LASR tables within it.	
Source Data	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] All LASR Administrators ACT
Reason: Most users should be denied access to the Global Source Data folder, even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators for that tenant organisation have (read-write) access to this folder, so that they can manage the Source library and tables in this folder, and load data from Source tables into LASR.	
Reports	SAS Administrator Settings [Tenant] All LASR Administrators ACT [Tenant] All Report Developers ACT [Tenant] All Consumers ACT
Reason: Most users inherit read-only access to the Global Reports folder. Apart from SAS Administrators, LASR Administrators and Report Developers have read-write access to this folder, so that they can publish completed reports to a global (tenant-wide) audience. All consumers belonging to any of the Departments, Projects, Teams, Subject Areas, Data Topics, or Organisations within this tenant organisation should also have access to read (and run) the reports in this Global Reports folder.	
Work In Progress	[Tenant] PUBLIC and SASUSERS Denied ACT SAS Administrator Settings [Tenant] All LASR Administrators ACT [Tenant] All Analysts ACT
Reason: Most users should be denied access to the Global Work In Progress folder, even when they are a member of a group belonging to the relevant tenant organisation. Apart from SAS Administrators, only LASR Administrators and Analysts for that tenant organisation have (read-write) access to this folder, so that they can work on unfinished global data explorations in it.	

Table 10 – Metadata folders which should have GEL recommended 'VA' ACTs applied to them

9.1.2 Apply ACTs to the VA ACTs and to SASApp

Table 11 below shows how you should apply ACTs so that only SAS Administrators can modify the ACTs.

Objects and their location in the Plug-in Tab	**VA ACTs to apply**
SAS Management Console	
Environment Management	
Authorization Manager	
Access Control Templates	
[Tenant] All Users ACT [Tenant] All Report Developers ACT [Tenant] All Analysts ACT [Tenant] All LASR Administrators ACT [Tenant] All Consumers ACT [Tenant] All [Dept1] ACT [Tenant] [Dept1] Report Developers ACT [Tenant] [Dept1] Analysts ACT [Tenant] [Dept1] Analysts Server ACT [Tenant] [Dept1] LASR Administrators ACT [Tenant] [Dept1] Consumers ACT	*To* each one *of these ACTs, apply:* SAS Administrator Settings [Tenant] SASUSERS Read Only ACT
Reason: Only SAS Administrators should have permission to modify ACTs in your security model. Everyone (i.e. SASUSERS) has RM on every ACT: anyone can see the design of any ACTs, but read-only.	
SAS Management Console	
Environment Management	
Server Manager	
SASApp	*Already recommended in the **Core Artefacts** paper:* SAS Administrator Settings [Tenant] SASUSERS Read Only ACT *In addition to those, for VA, you may also **optionally** apply:* [Tenant] All LASR Administrators ACT
Reason: As already recommended in the Core Artefacts paper, only SAS Administrators should have permission to modify Application Server Contexts. Everyone (i.e. SASUSERS) needs RM for the default AppServer Contexts. Also, optionally add [Tenant] All LASR Administrators ACT to SASApp, to allow them to create libraries on any server that is part of the SASApp server context.	

Table 11 – Metadata objects which should have GEL recommended 'VA' ACTs applied to them

10 Filesystem folder permissions and ownership

10.1.1 Windows Security

On Windows, three levels of permission are used in security windows directories:

Abbreviation	Permission	Controls
F	Full Control	Users with this permission can do anything with the object
C	Change	Read-write. Users with Change permission can edit the object, but cannot change *permissions* on the object.
R	Read	Read only.

Secure the VA-specific directories on the filesystem like this:

Folder	Windows Security Settings
…\sasfolders\[Tenant]	(Set on "This folder, subfolders and files") SYSTEM: F Administrators: F SAS [Tenant] All Users: C

10.1.2 Unix and Linux Security

Unix has basic posix filesystem security capabilities, and file mounts can optionally be configured to use a more advanced capability called Access Control Lists (ACLs). These recommendations use only the basic posix capabilities. More advanced filesystem security designs are only possible with ACLs.

The general principle for filesystem access **in this very simple design** is that if a user is going to have access to a directory, they will have write access to it.

Only one group can be set as the owner of a directory, which means that we create groups differently in Unix than we do in Windows. The following are examples only: you will need to design these as required for your specific needs.

Unix Group	Members
sas	SAS Installation User (sas or sasinst) SAS General Servers user (sassrv)
[tenant]allusers	SAS [Tenant] all users
[tenant][dept1]users	SAS [Tenant] all Dept1 users

Then secure the sasfolders directory on the filesystem like this:

Folder	Unix Security Settings	
	Owner (user:group)	Permission pattern
...\sasfolders	sas:sas	2770
[Tenant]	sas:[tenant]allusers	2750
[dept1]	sas:[tenant][dept1]users	2750
analyses	sas:[tenant][dept1]users	2770
data	sas:[tenant][dept1]users	2770
formats	sas:[tenant][dept1]users	2770
lasr_data	sas:[tenant][dept1]users	2770
source_data	sas:[tenant][dept1]users	2770
reports	sas:[tenant][dept1]users	2770
work_in_progress	sas:[tenant][dept1]users	2770
global	sas:[tenant]allusers	2770
analyses	sas:[tenant]allusers	2770
data	sas:[tenant]allusers	2770
formats	sas:[tenant]allusers	2770
lasr_data	sas:[tenant]allusers	2770
source_data	sas:[tenant]allusers	2770
reports	sas:[tenant]allusers	2770
work_in_progress	sas:[tenant]allusers	2770

SAS INSTITUTE INC. WORLD HEADQUARTERS SAS CAMPUS DRIVE CARY, NC 27513
TEL: 919 677 8000 FAX: 919 677 4444 U.S. SALES: 800 727 0025 WWW.SAS.COM