User and security setup in SAS Viya

A best practice guideline

Jonas Lie-Nielsen, Advisory Pre-Sales Solutions Architect , Customer Advisory Technology Northern Europe
Email: Jonas.Lie-Nielsen@sas.com

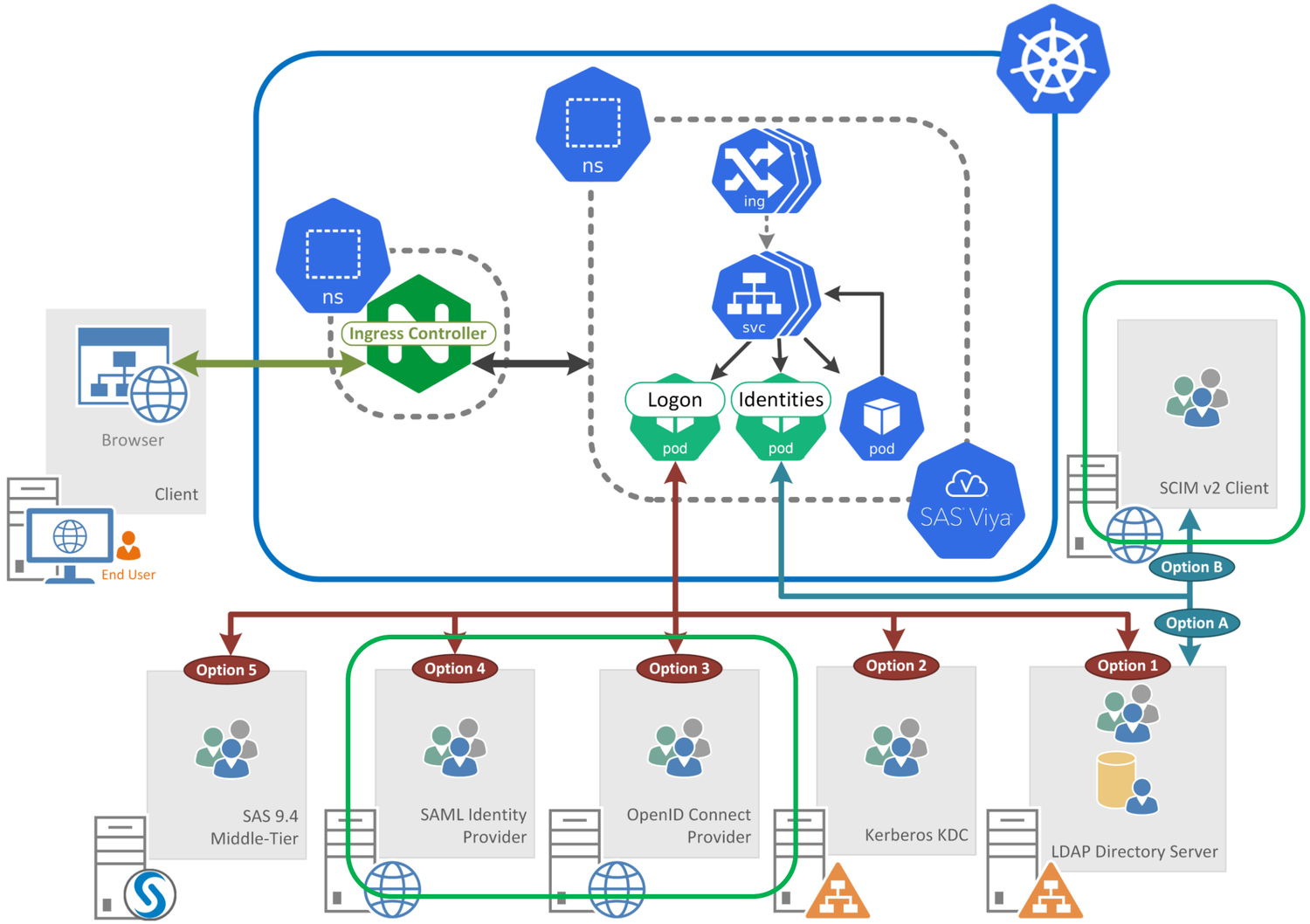
Introduction

Why this?

- A good overview on how to implement the user security setup has been missing on Viya
- Different projects have been doing different things
- They have quite good control on the caslibs, folders and content folders, but how to create groups from a functionality perspective has not been the key focus in most projects.
- This presentation covers all the dimensions, but with a focus on the functional groups
- It is combined with a demo on a viya race image

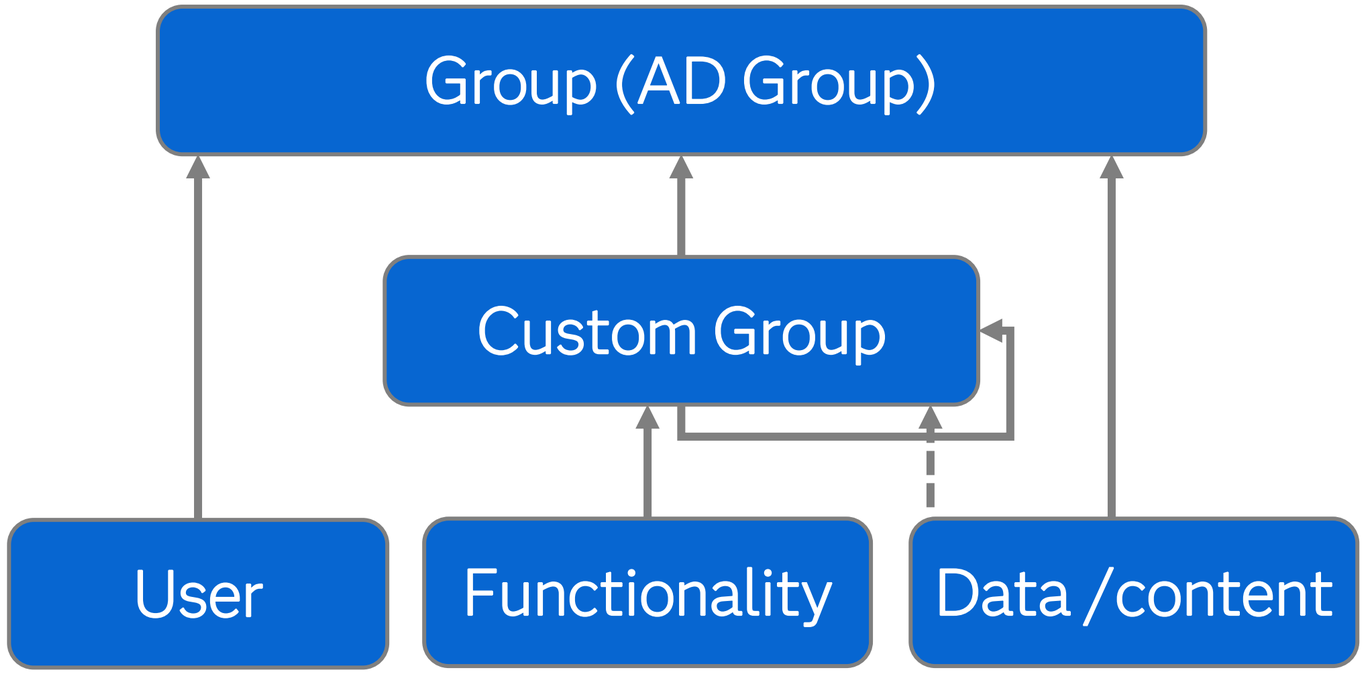
Authentication and Provisioning of users

OIDC/SAML + SCIM



User groups in Viya

How to use users / groups / custom groups?



- The relationship above is not absolute, but a best practise to keep the administration as simple as possible
- Viya lack the term role, custom group is used instead, not exactly the same

General best practises

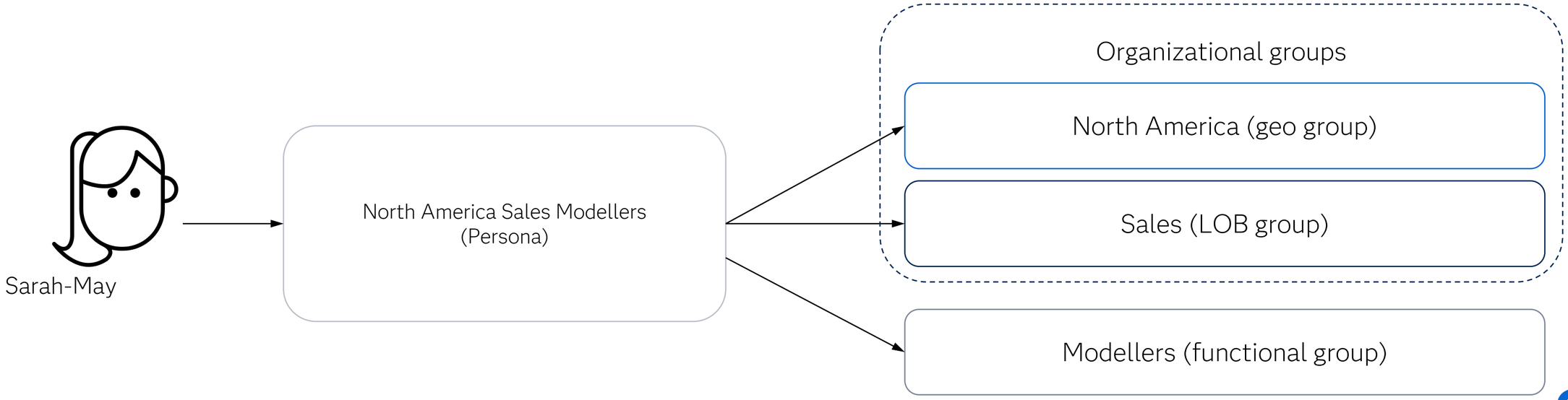
- Always Grant access on group/custom group level and not user level
- Only manage one mapping between groups and content/data. If multiple AD groups need the same access, make a custom group in Viya and put the rules in that. Then add the custom group into all AD Groups that needs the access
- Don’t mix the definition of data/content access with functional access in the same group
- Don’t make the security model more complex than nessesary

Functional groups

- Customers expect a *simple* way to enable *selected* groups of users to use or not use entire **applications**, or **application capabilities**:
- Define **functional groups** representing job roles, like report author, modeller, content administrator etc.
- Different from organizational groups: the same job role might be performed by users in many different parts of the organization

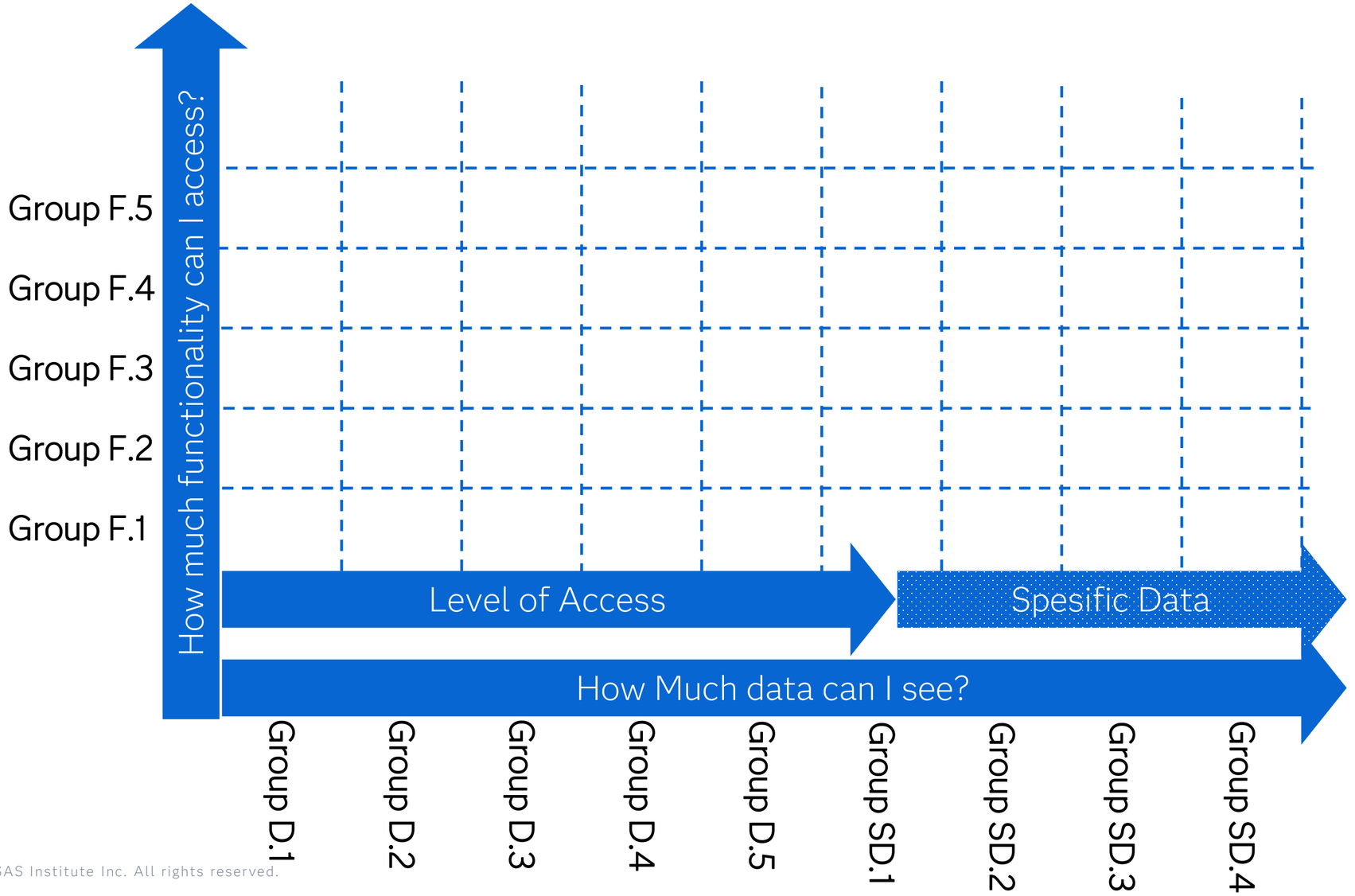
Personas

- The term **persona** does not have a single widely-accepted definition in authorization model design, but a **persona** in Viya is implemented as:
- A specific combination of:
  - **Organizational groups**, used to manage access to content and data
  - **Functional groups** used to manage access to applications and features



Access Management

See it from two perspectives – Functionality and Data/content



The common user groups

Controlling functionality

Group	Inherits	Description
Report Viewer		Can only use reports in VA
Report Creator	Report Viewer	Use and create reports Use VA for data exploration Use standard version of SAS Studio Data explorer (load data) Information catalog viewer
Data Analyst	Report Creator	Can use all studio analyst functionality
Data Engineer	Data Analyst	Adds all SAS Studio Engineer objects Create libnames and caslibs
Data Stuart	Data Analyst	
Batch Admin	Data Engineer	Can see and modify scheduled jobs Can schedule using all batch users
Data Scientist	Data Analyst	Have full access to VML + model manager + other analytical modules
Content Admin	Data Analyst	Can admin all sas content, folders, reports, data,flows, models,
SAS Administrator (std group)		Full sas admin rights – member of SAS Administrator
Decision Developer	Data Scientist	Developer in Intelligent decisioning
ESP Developer	Data Scientist	Develop in Event Stream Processing

The mapping between licensing and user groups

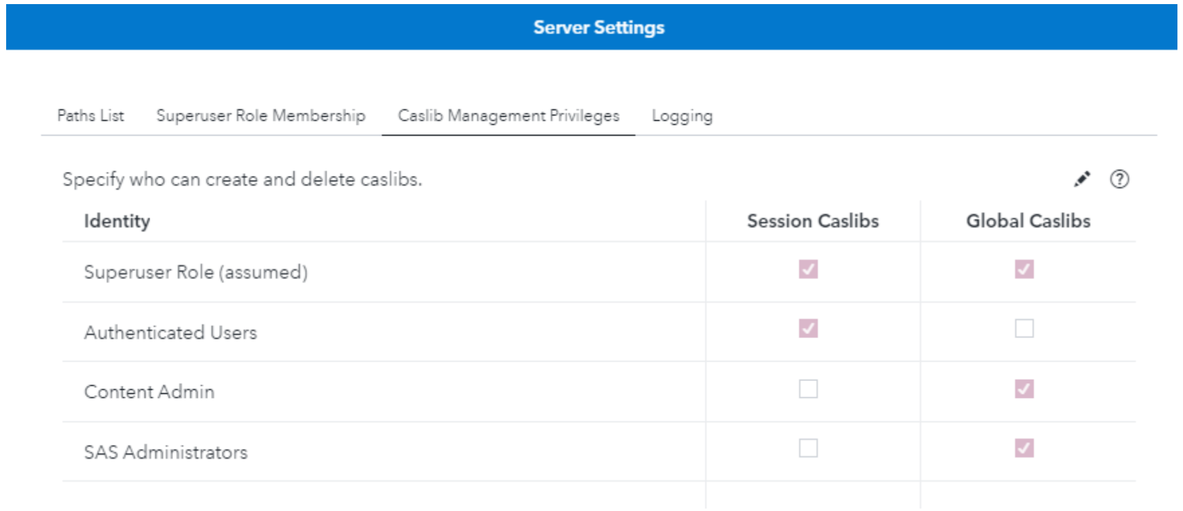
Offering	User group	Tool in Viya	Comment
SAS Visual Analytics	Report Creator	Visual Analytics editor Can view information catalog	Gives also basic access to Studio and data prep No of users for the viewer is unlimited
SAS Visual Statistics	Business Analyst	Access to predictive and descriptive analytics through Visual Analytics + code	Gives access to all VS procedures to all Studio Analyst users
SAS Viya	Data Scientist	Visual Analytics Studio Analyst Information Governance Visual Statistics Model Studio Model Manager	Gives access to all ML procedures and the model studio and model manager tools independet of interface (sas code, python or visual)
SAS Studio Analyst	Data Analyst	Studio Analyst	Requires SAS Visual Analytics license
SAS Information Governance	Data Stuart	Information Catalog	Requires SAS Visual Analytics license users that can analyze data and edit in the tool
SAS Studio Engineer	Data Engineer	Sas Studio with all transformations objects	Maps to DI users today Requires both Studio Analyst and Information Goverance license
SAS Viya Advanced	Data Scientist Advanced	VML + optimization, visual forecasting, IML, visual text analytics, ecnometrics, SAS/QC,	Access to all analytics tools in SAS
SAS Intelligent Decisioning	Decision Developer	SAS Intelligent Decisioning	Separate group to control access
SAS ESP	ESP Developer	SAS Event Stream Processing	Separate group to control access

Global Caslib rights

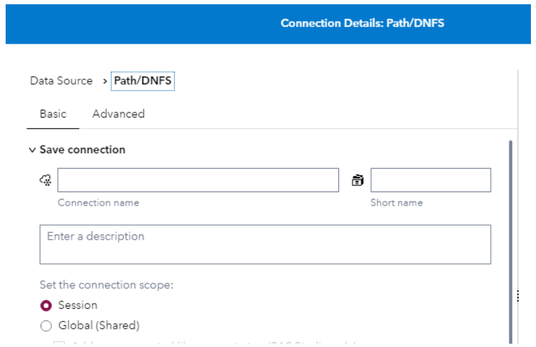
How to control who can create global caslibs?

Steps:

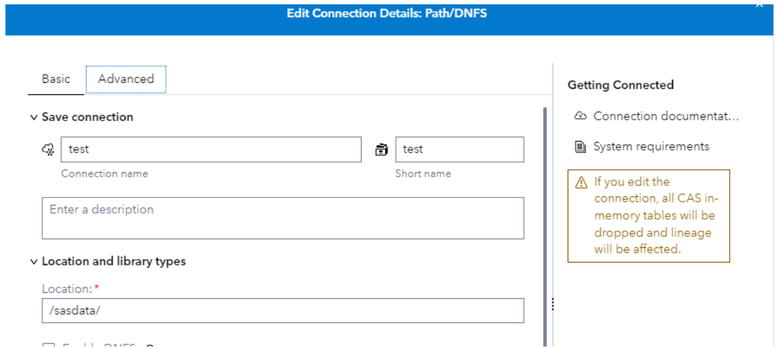
1. Select servers in EVM
2. Assume superuser role
3. Roght click on the cas server and select «settings»
4. Select the «CAS Management Privileges»
5. Select the groups that can make global and session caslibs
6. Users with only session caslibs rights miss the global checkbox in Data Explorer



With Global caslibs rights



Without Global caslibs rights



Implementation rules per tool

Product / Capability	Rule	
View in Visual Analytics	/SASVisualAnalytics/**	Feature-level access is supported.
Edit in Visual Analytics	/SASVisualAnalytics_capabilities/edit	
SAS Data Explorer	/SASDataExplorer/**	Feature-level access is supported.
SAS Data Studio	/SASDataStudio/**	Initially granted to Data Builders. (Legacy disabled)
SAS Drive	/SASDrive/**	Feature-level access is supported.
SAS Environment Manager	/SASEnvironmentManager/	Page-level access is supported.
SAS Graph Builder	/SASGraphBuilder/**	
SAS Information Catalog	/SASInformationCatalog/	Feature-level access is supported.
SAS Lineage Viewer	/SASLineage/**	
SAS Model Manager	/SASModelManager/	
SAS Model Studio	/SASModelStudio/**	
SAS Studio	/SASStudio/**	
SAS Theme Designer	/SASThemeDesigner/**	Initially granted to Application Administrators.
SAS Visual Analytics App	/SASMobileBI/**	Feature-level access is supported.
SAS Workflow Manager	/SASWorkflowManager/**	
SAS Studio	/SASEventStreamProcessingStudio/** /SASEventStreamProcessingStudio/esp-project/**	
ESP Manager	/SASEventStreamManager/**	
ESP Viewer	/SASEventStreamProcessingStreamviewer/**	
Intelligent decisioning	/SASDecisionManager/**	

Implementation

Group	Rule	Rights	comment
Report Viewer	/SASVisualAnalytics/**	Read	Gives view access
	/SASInformationCatalog/	Read	Feature-level access is supported.
Report Creator	/SASVisualAnalytics_capabilities/edit	Read	Gives edit access
	/SASGraphBuilder/**	Read	
	/SASDataExplorer/**	Read/Remove/Create/Add/Update/Delete	Feature-level access is supported.
Content Admin	/SASThemeDesigner/**	Read	Initially granted to Application Administrators.
Content Admin	/casManagement/servers/*/caslibs	Create	Create global caslibs
None - hidden	/SASDataStudio/**	Everyone - prohibit	Initially granted to Data Builders. (Legacy disabled)
Authenticated user	/SASDrive/**	Default	Feature-level access is supported.
	/SASEnvironmentManager/		Page-level access is supported.
	/SASLineage/**	default	
Data Stuart	See next page		
Data Scientist	/SASModelManager/	R/W/U/D	
	/SASModelStudio/** /SASModelManager/ /ModelStudio/** SASVisualAnalytics_capabilities/buildAnalyticalModel	R	
	/SASWorkflowManager/**	R/W//U/D	
Data Analyst	/SASStudio/**		

Information catalog admin

Discovery agents

Object URI	Principal	Setting	Permissions
/catalog/bots/**	your_custom_group	Grant	Update, Read, Delete, Create
/catalogTableBot/jobs/**	your_custom_group	Grant	Update, Read, Delete, Create
/catalogTableBot/bots/**	your_custom_group	Grant	Update, Read, Delete, Create
/catalog/instances/*	your_custom_group	Grant	Update, Read, Delete, Create
/catalog/definitions/*/instances/**	your_custom_group	Grant	Update, Read, Delete, Create
/catalog/instances	your_custom_group	Grant	Read, Create
/catalog/deletions	your_custom_group	Grant	Create

Semantic type remediation

Object URI	Principal	Setting	Permissions	Notes
/catalog/instances	your_custom_group	Grant	Create	Create instances
/catalog/instances/*	your_custom_group	Grant	Delete	Delete instances
/catalog/deletions	your_custom_group	Grant	Create	Create bulk deletions
/catalog/definitions/63e3d825-8906-4f37-a970-685ee1fa91a8/instances/*	your_custom_group	Grant	Read, Create, Delete	Read, Create, and Delete semantic relationships

Rebuild indexes

Object URI	Principal	Setting	Permissions	Notes
/catalog/jobs	your_custom_group	Grant	Read, Create	Not applicable
/catalog/search/indices	your_custom_group	Grant	Create	Specify the content type as *application/vnd.sas.select-ion+json*.This setting allows the user to rebuild existing indexes, and denies the user the ability to create new indexes.
/catalog/search/indices/*	your_custom_group	Grant	Read, Update	Adding /* to the path enables the user to rebuild all indexes. The user can also specify an index ID to rebuild only the specified index.

Content Admin

Define your of content admin

- Add capabilities in environment manager for type of content you want to get access to, default open to everyone as read

Object URI	Principal	Setting	Permissions
/SASEnvironmentManager/pwa/*	Authenticated Users	Grant	Read
/SASEnvironmentManager/**	SASAdministrators	Grant	Read
/SASEnvironmentManager/content	Authenticated Users	Grant	Read
/SASEnvironmentManager/qkbs	Authenticated Users	Grant	Read
/SASEnvironmentManager/servers	Authenticated Users	Grant	Read
/SASEnvironmentManager/	Authenticated Users	Grant	Read
/SASEnvironmentManager/import	Authenticated Users	Grant	Read
/SASEnvironmentManager/data	Authenticated Users	Grant	Read
/SASEnvironmentManager/*	Authenticated Users	Conditional Grant	Read
/SASEnvironmentManager/resources/**	Authenticated Users	Grant	Read
/SASEnvironmentManager/domains	ScheduleServiceAccountUsers	Grant	Read
/SASEnvironmentManager/credentials	Authenticated Users	Grant	Read
/SASEnvironmentManager/jobs	Authenticated Users	Grant	Read
/SASEnvironmentManager/workload	Authenticated Users	Grant	Read

What about the SAS Viya Advanced?

The access to the cas actions can be controlled

- Access to actionssets can be controlled using the **Access Control Action Set**
  - https://go.documentation.sas.com/doc/en/pgmsascdc/v_047/caspg/cas-accesscontrol-TblOfActions.htm
  - This is a topic for a later session
- Graphical tools like Visual Forecasting and Visual Text Analytics can be controlled using rules

Design of caslib access

Make a design up front

			Custom Groups						
CAS library	Organization	Path	Orion Users (=Authenticated Users)	Orion Marketing Readers	Orion Marketing Writers	Orion Sales Readers	Orion Sales Writers	Orion Classified Sales Readers	Orion Classified Sales Writers
Public	Orion	/cas/data/caslibs/public/	Read + Write						
CASMrktg	Marketing	/orn/warehouse/cas/cas_marketing		Read	Write				
CASSales	Sales	/orn/warehouse/cas/cas_sales				Read	Write		
CASClSls	Classified Sales	/orn/warehouse/cas/cas_classified_sales						Read	Write

Access to folders /content folders

Same principels, but controled in EVM / linux rights

	Groups										
SAS Contents	Orion	Marketing			Sales			Classified Sales			
Folder	Orion Users	Orion Marketing Users	Orion Marketing Writers	Orion Marketing Super Users	Orion Sales Users	Orion Sales Writers	Orion Sales Super Users	Orion Classified Sales User	Orion Classified Sales Write	Orion Classified Sales Super Users	CAS Data Library
SAS Content											
SAS Content/Orion	R	[R]	[R]	[R]	[R]	[R]	[R]	[R]	[R]	[R]	
SAS Content/Orion/Orion Shared	RC, EC	[RC, EC]	[RC, EC]	CA	[RC, EC]	[RC, EC]	CA	[RC, EC]	[RC, EC]	CA	Public
SAS Content/Orion/Orion Marketing		RC	[RC]	CA							
SAS Content/Orion/Orion Marketing/Shared		(RC)	EC	(CA)							CASMrktg
SAS Content/Orion/Orion Marketing/Project M001		(RC)	EC	(CA)							CASMrktg
SAS Content/Orion/Orion Marketing/Project M002		(RC)	EC	(CA)							CASMrktg
SAS Content/Orion/Orion Sales					R	[R]	[R]	[R]	[R]	[R]	
SAS Content/Orion/Orion Sales/Shared					RC	EC	CA	[RC]	[EC]	[CA]	CASSales
SAS Content/Orion/Orion Sales/Project S001					RC	EC	CA	[RC]	[EC]	[CA]	CASSales
SAS Content/Orion/Orion Sales/Project S002					RC	EC	CA	[RC]	[EC]	[CA]	CASSales
SAS Content/Orion/Orion Sales/Orion Classified Sales								RC	[RC]	CA	
SAS Content/Orion/Orion Sales/Orion Classified Sales/Shared								(RC)	EC	(CA)	CASClSls
SAS Content/Orion/Orion Sales/Orion Classified Sales/Project CS001								(RC)	EC	(CA)	CASClSls
SAS Content/Orion/Orion Sales/Orion Classified Sales/Project CS002								(RC)	EC	(CA)	CASClSls

How to control the data

Some general guidelines

- Split between read vs write access to data as most users don’t need write access to a lot of the caslibs/libnames
- Keep the same rules on caslibs and libnames
- Keep the data access rules as simple as possible, especially don’t limit access to data that don’t has any restrictions related to them
- Try to keep data access on libname level and not table or column