



Best Practices with SAS[®] 9 Metadata Security

Paul Homes

SAS Forum ANZ (12Aug2010)

productivity through metadata visibility



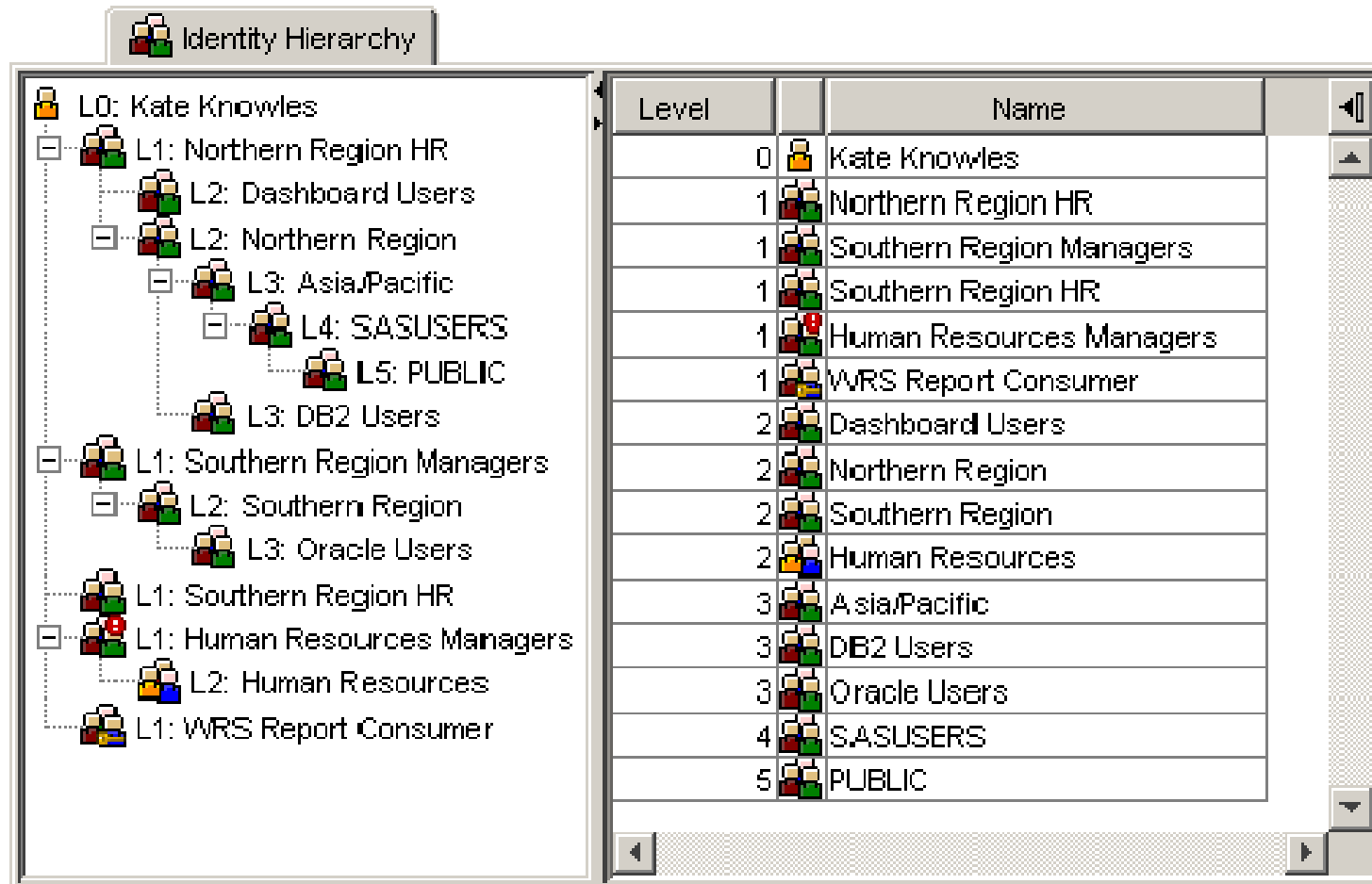
- Introduction to Best Practices with SAS9 Metadata Security
 - High level overview
 - Procedural
 - Implementation
 - Information sources

Best Practices

- Collected wisdoms from the community
- Methods with significant advantages
- Best practices help us avoid:
 - Many per-user, per-object based access controls resulting from individual email/phone requests
 - Chaos / 'unpredictable' access controls
 - Undocumented implementation
 - Large effort required to deal with change

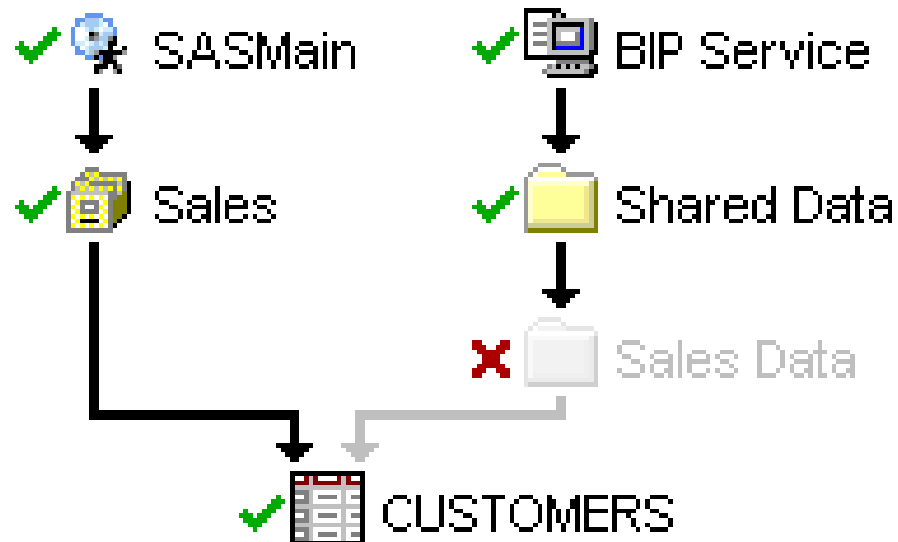
- Learn from people with prior experience...
- SAS Education
 - What's New in 9.2 Platform Administration
 - SAS 9.2 Platform Administration Fast Track
- SAS Certified Platform Administrator for SAS 9
- Documentation/Conferences/Papers/Communities
 - SAS Global Forum, SAS Forum ANZ
 - QUEST, SNUG, SMUG etc.
 - SAS discussions forums, sasprofessionals.net, sascommunity.org
- Knowledge of 3rd Party Software

- Identity Hierarchy

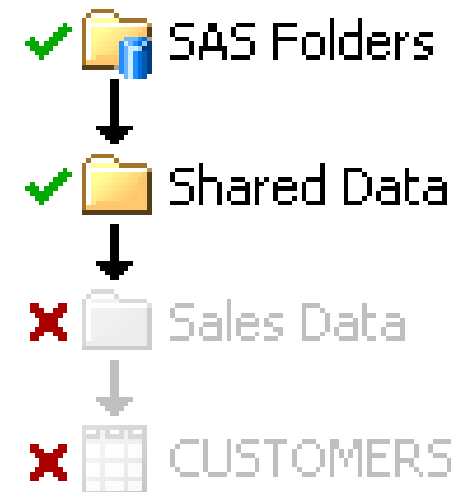


- Inheritance Paths

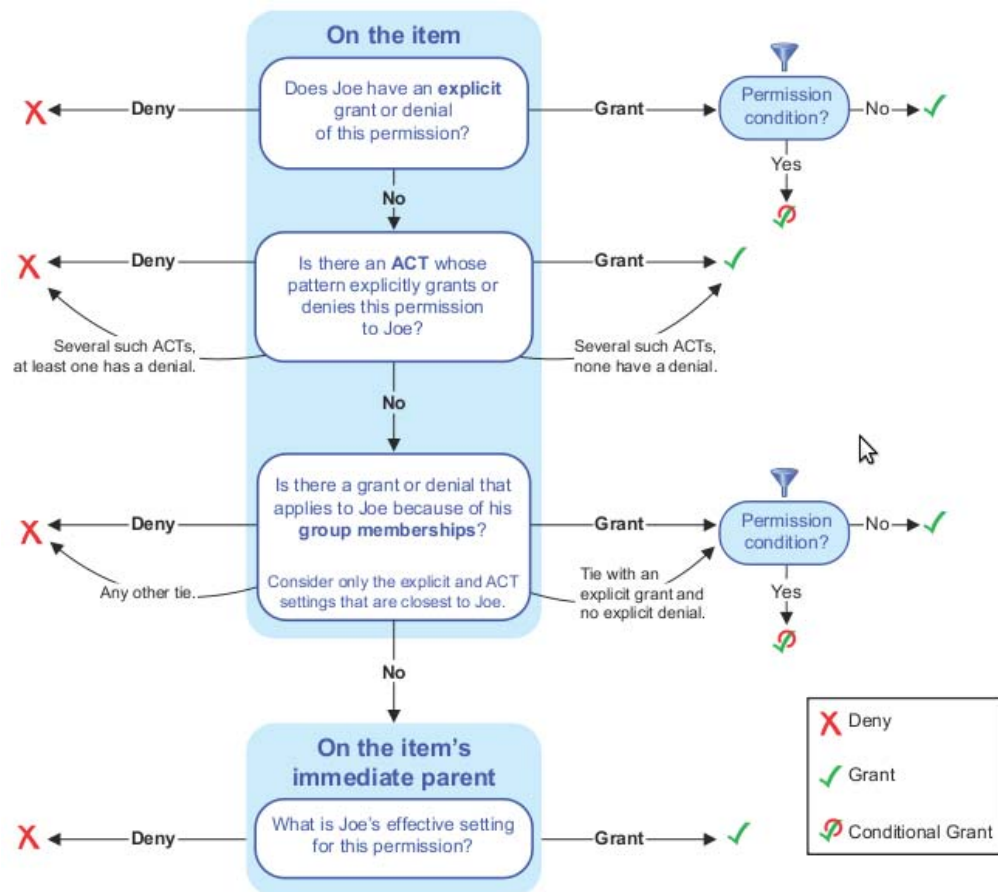
SAS 9.1.3
Multiple Inheritance



SAS 9.2
Single Inheritance



- Access Decision Flow *



* Diagram reproduced from SAS® 9.2 Intelligence Platform Security Administration Guide

Plan Well

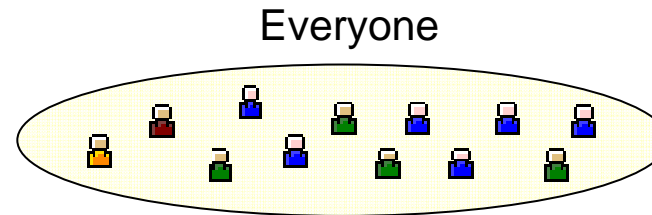
- Plan well ... before implementation
- Collaborate with other departments
- Integrate with Enterprise Directories (AD, LDAP)
 - Synchronize with SAS metadata
- Prepare for evolving requirements
- Identify Job Roles and Software Access
 - Roles & Capabilities in SAS 9.2

Plan Well

- Partition content using tree folders
 - Organizational, Job Role
- Secure tree folders
- Secure non-tree folder content
 - Servers, Groups, ACTs etc.
- Document then implement
- Allow sufficient time for testing

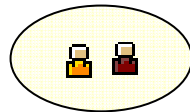
Develop a Security Plan

“Open” Security Model

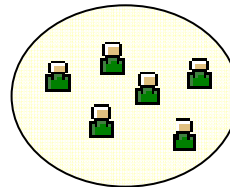


Basic Security Model

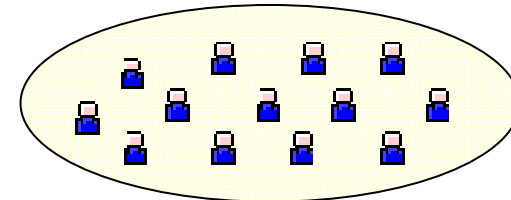
Administrator/Developer



Authors

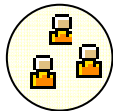


Consumers

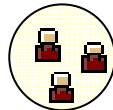


Complex Security Model

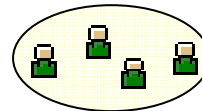
Administrators



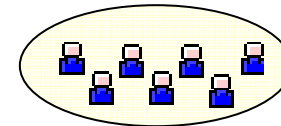
HR Developers



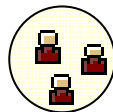
HR Authors



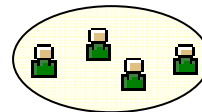
HR Consumers



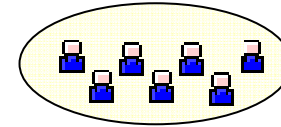
Sales Developers



Sales Authors



Sales Consumers

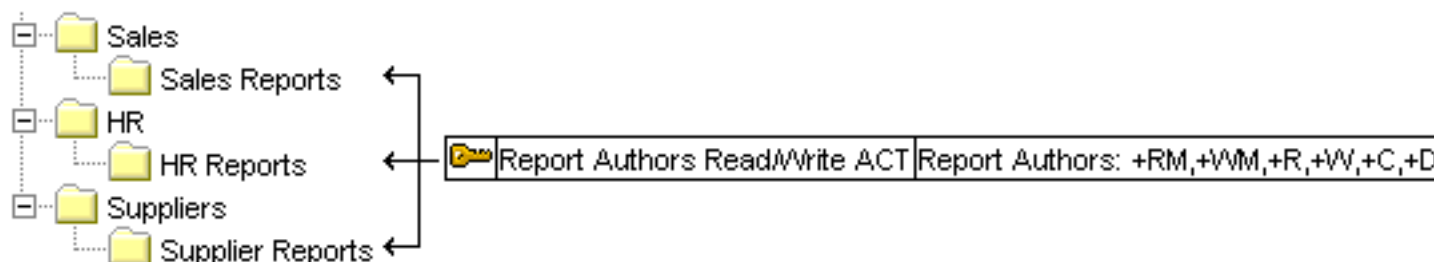


Prefer ACTs over ACEs

- ACEs: single-use permissions



- ACTs: reusable package of permissions





Prefer ACTs over ACEs










- ACTs easier to manage/change
- Skip SAS application managed ACEs
- Work towards replacing ACEs with ACTs

The screenshot shows the SAS Management Console interface with a table of Access Control Entries (ACEs) and Access Control Templates (ACTs). The table has columns for Protected Type, Protected Object Name, Protected Object Folder, Identities, User Ref., and various permission flags (RM, VM, CM, R, W, C, D, A). The Permission Condition column contains complex expressions like {{d_geo].[All Countries], [d_geo].[All Countries].[U.S.A.]}. The status bar at the bottom indicates 'Found 15 Access Control Entries (ACEs) in 0.48 seconds.' and the user is 'sasadm as Unrestricted' on 'localhost : 8562'.

Protected Type	Protected Object Name	Protected Object Folder	Identities	User Ref.	RM	VM	CM	R	W	C	D	A	Permission Condition
Access Control Template	Default ACT		Wendy Williams (Person)	Yes	✓	✓							
Column	CustomerName		SAS Demo User (Person)	Yes	✗	✗	✗						
Cube	ProductSalesCube		SAS Demo User (Person)	Yes	✓								
Dimension	d_time		SAS Demo User (Person)	Yes	✓			✓					
Dimension	d_geo		SASUSERS	No				✓					{{d_geo].[All Countries], [d_geo].[All Countries].[U.S.A.]}
Dimension	d_geo		SAS Demo User (Person)	Yes	✓			✓					{{d_geo].[All Countries]}
Hierarchy	d_time		SAS Demo User (Person)	Yes	✓								
Level	MONTH		SAS Demo User (Person)	Yes	✓								
Measure	ACTUALSUM		SAS Demo User (Person)	Yes	✓	✓							
SAS Library	ODBC Library	/Shared Data/ODBC Library	Wendy Williams (Person)	Yes	✓	✓							
SAS Table	TRANSACTIONS	/Shared Data/Sales Data	SAS Demo User (Person)	Yes	✗			✗					
SAS Table	CUSTOMERS	/Shared Data/Sales Data	SAS Demo User (Person)	Yes	✓								
Stored Process	Sample: Year to Date Bu...	/Samples/Stored Process...	PUBLIC	No	✓	✓		✓					
Stored Process	Sample: European Demo...	/Samples/Stored Process...	SAS Demo User (Person),P...	Yes	✓	✓							
User	SAS Guest		Wendy Williams (Person),Po...	Yes	✓	✓							

Prefer Groups over Users

- Users change, Groups are relatively static
- Goal: Manage access by group membership
- Improve ACTs or ACEs referring to users

	Name	User Ref.	Permissions
	Default ACT	No	PUBLIC: -RM,-WM,-CM,-R,-W,-C,-D,-A; Metadata Admin
	SASUSERS Read Only	No	SASUSERS: +RM,-WM; Metadata Administrators: +RM,+
	SASUSERS No Access	No	Metadata Administrators: +RM,+WM; SASUSERS: -RM,-
	ACT Securing Groups	No	PUBLIC: +RM,-WM; Metadata Administrators: +RM,+WM
	ACT Securing ACTs	No	PUBLIC: +RM,-WM; Metadata Administrators: +RM,+WM
	HR Read	No	
	HR Read/Write	No	Human Resources: +RM,+WM,+R,+W,+C,+D
	Managers Read	Yes 	Northern Region Managers,Alice Adams (Person): +RM



Secure Folders over Objects

- Objects inherit from folders
- Secure folders with ACTs
- Ignore objects within folders
- Align folders with access requirements
 - Folders for projects
 - Folders for organizational units
 - Folders for job roles
- WriteMemberMetadata (WMM) in SAS 9.2
 - Manage folder contents but not the folder itself

Wide Denials, Narrow Grants

- An Identity Hierarchy Conflict ...

Australia folder denies access to Asia/Pacific and grants to Australia

Folder		/Shared Data/Australia		
ACEs (2)		ACTs (0)		
	Identities	User Ref.	RM	WM
	Asia/Pacific	No	✗	
	Australia	No	✓	

Sam and Tara both members of Asia/Pacific and Australia
... but by different mechanisms



Sam sees the folder ✓



... but Tara doesn't ✗



Wide Denials, Narrow Grants

- To minimize identity hierarchy conflicts ...
- Only deny PUBLIC / SASUSERS
- Grant back to groups that require access:
 - Metadata Administrators
 - BI Developers
 - Human Resources
 - SASUSERS

Thorough Testing

- Test various classes of users:
 - PUBLIC identity (not registered in metadata)
 - SASUSERS identity (registered in metadata but in no groups)
 - Single and Multi-Group Memberships (identity hierarchy conflicts)
- Test various actions: Read, Update, Rename, Move, Delete etc.
- Impersonate real users (using your own login)
- Consider testing in dedicated/private admin environment (Lev9)
 - Disruptive/Destructive testing

Regular Reviews

- Security plan & implementation evolves
- Update documentation



Table of Contents

- Access Control Templates (ACTs)
- Access Control Entries (ACEs)
- Users
- User Groups
- Endpoint Objects
- Users

Access Control Templates (ACTs)

Access Control Template (ACT) Summary

Row	Name	Description	Protected	Is Active	Redundant	User Set	Permissions Summary
1	SASUSERS Read Only	An ACT that restricts all SAS users who are non-administrators to read-only access	Yes	Yes	No	No	SASUSERS: +RM,-WM; Metadata Administrators: +RM,+WM
2	SASUSERS No Access	An ACT that prohibits access by all SAS users who are non-administrators	Yes	Yes	No	No	Metadata Administrators: +RM,+WM; SASUSERS: -RM,-WM
3	Managers Read	An ACT that grants managers read access	Yes	Yes	No	Yes	Southern Region Managers, Alice Adams (Person): +RM,+R; Southern Region Managers: +RM
4	HR Read/Write	An ACT that grants HR users read and write access	Yes	Yes	No	No	Human Resources: +RM,+WM,+R,+C,+D
5	HR Read	An ACT that grants HR users read access	Yes	Yes	Yes	No	
6	Default ACT	Default ACT for Foundation	Yes	Yes	No	No	PUBLIC: -RM,-WM,-CR,-E,-W,-C,-D,-A; Metadata Administrators: +RM,+WM,+CR,+R,+C,+D,+A; SAS System Services: +RM,+R; SASUSERS: +RM,+WM,+CR,+R
7	ACT Security Groups	An ACT used to protect user groups from being modified by non-administrators	Yes	Yes	No	No	PUBLIC: +RM,-WM; Metadata Administrators: +RM,+WM
8	ACT Security ACTs	An ACT used to protect ACTs from being modified by non-administrators	Yes	Yes	No	No	PUBLIC: +RM,-WM; Metadata Administrators: +RM,+WM

Detail for ACT: SASUSERS Read Only

Permissions (2)

Row	Identity	Is Inherited	RM	WM	R	C	D	A
1	SASUSERS	No	✓	✗				
2	Metadata Administrators	No	✓	✓				

Objects (15)

Row	Type	Name	Description	Table
1	Folder	Integration Technologies		
2	Folder	SAS Data Integration Studio Custom Tree	Root tree object for Custom Tree	
3	Folder	Samples	Root folder for SAS samples.	
4	Folder	Support Files		

- Keep learning
- Plan well
- Secure with:
 - ACTs not ACEs
 - Groups not users
 - Folders not objects
- Take care with denials
- Test thoroughly
- Review regularly

Resources (SAS 9.2)

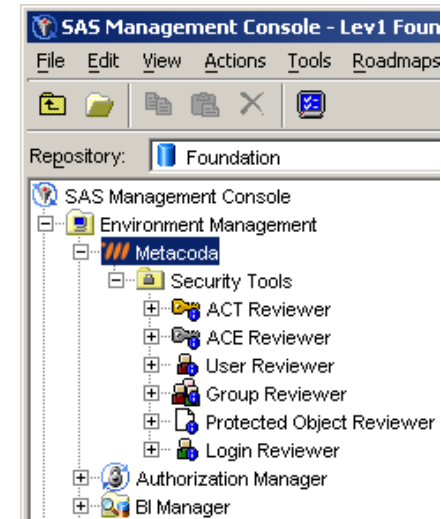
- SAS® 9.2 Intelligence Platform Security Administration Guide
 - <http://support.sas.com/documentation/cdl/en/bisecag/61133/PDF/default/bisecag.pdf>
- SAS® 9.2 Management Console: Guide to Users and Permissions
 - <http://support.sas.com/documentation/cdl/en/mcsecug/61708/PDF/default/mcsecug.pdf>
- SAS Global Forum 2010 Paper 324-2010: Be All That You Can Be: Best Practices in Using Roles to Control Functionality in SAS® 9.2, Kathy Wisniewski
 - <http://support.sas.com/resources/papers/proceedings10/324-2010.pdf>
- SAS Global Forum 2010 Paper 311-2010: A Practical Approach to Securing a SAS® 9.2 Intelligence Platform Deployment, Jim Fenton & Robert Ladd
 - <http://support.sas.com/resources/papers/proceedings10/311-2010.pdf>
- Others: see <http://platformadmin.com/>

- SAS® 9.1.3 Intelligence Platform: Security Administration Guide, Second Edition
 - <http://support.sas.com/documentation/configuration/bisecag.pdf>
- Best Practices for SAS®9 Metadata Server Change Control
 - <http://support.sas.com/resources/papers/MetadataServerchngmgmt.pdf>
- TS-760 Metadata Security and the DefaultACT in SAS®9
 - <http://support.sas.com/techsup/technote/ts760.pdf>
- TS-750 Securing SAS®9 Business Intelligence Content Managed in Metadata
 - <http://support.sas.com/techsup/technote/ts750.pdf>
- Others: see <http://platformadmin.com/>



About Metacoda

- SAS Alliance Silver Member
- Specialise in the development of plug-ins to SAS software
 - Metacoda Security Plug-ins
- Goals:
 - Improve your productivity through enhanced metadata visibility
- Web: <http://www.metacoda.com/>
- Twitter: <http://twitter.com/metacoda>



- Contact Details
 - Email: paul.homes@metacoda.com
 - Web: <http://www.metacoda.com/>
 - Blog: <http://platformadmin.com/>
 - Twitter:
 - <http://twitter.com/PaulAtMetacoda>
 - <http://twitter.com/metacoda>