Paper 786-2017

SAS® Metadata Security 301: Auditing your SAS Environment

Charyn Faenza, F.N.B Corporation; Michelle Homes, Metacoda

ABSTRACT

You've got your SAS environments installed, configured, and running smoothly. Time to relax and put your feet up, right? Not so fast! There is still one more leg to go on your security journey. After the deployment of your initial security plan the security audit process provides active and regular monitoring and ensures your environment remains secure. There are many reasons to carry out security audits: for regulatory compliance, for business confidence, and to keeping your SAS platform as per the design specifications. This paper will at look some of the available ways to regularly review your environment to ensure protected resources are not at risk; to comply with security auditing requirements; and to answer quickly and easily the question "Who has access to what?" through efficient SAS metadata security management using Metacoda software.

INTRODUCTION

The SAS administrator role has evolved over the years, and so has one of their key responsibilities: security auditing. Once you've set up an initial security plan, how do you ensure that the environment remains secure? Can you just "set it and forget it"? Probably not. Especially if you want to ensure regulatory compliance, maintain business confidence, and keep your SAS platform in line with its design specifications as your business grows and the SAS environment evolves.

Thinking about your own SAS platform:

- What would happen in your organization if someone accessed data they shouldn't?
- When was your last SAS platform security project?
- When was it last tested? How extensive was it? How long did it take?
- Have there been any changes since it was last tested? Whether they are deliberate, accidental, expected or unexpected.
- How do you know if it's still secure today?

SECURITY JOURNEY

If security is important to you and your organization, please join our journey as we discuss SAS® Metadata Security 301: Auditing Your SAS Environment. Hold your horses… "301?", I hear you say… "what about 101 and 201"? Glad your curious mind asked… At the last two SAS Global Forum events, Charyn presented SAS Metadata Security 101 and 201 papers that step through the fundamentals on Authentication and Authorization. If you haven't read them, take the side path, and check them out (we'll wait) before we continue the journey with this 301 paper.

- SAS® Metadata Security 101: A Primer for SAS Administrators and Users Not Familiar with SAS
- SAS® Metadata Security 201: Security Basics for a New SAS Administrator

Thanks for rejoining the path… This 301 paper will focus on auditing to complete the three 'A's: Authentication, Authorization and Auditing. As outlined in the 101 paper:

- Authentication answers the question, "Who are you?"
- Authorization answers the question "What are you allowed to do?" and
- Auditing answers the questions "What can you access and What did you do?"

We will also discuss how you can use Metacoda software to regularly review your environment, so you can protect your resources, comply with security auditing requirements, and quickly and easily answer the question "Who has access to what?"

Whether you're a new SAS administrator or an experienced one, you'll know that security is a journey rather than a destination so join us as we take you through the SAS Metadata Security Auditing ride.

AUDIT – FRIEND OR FOE?

Generally, administrators and managers find their internal and external audits to be unpleasant; or at the least, not pleasant. There is often a feeling of Us versus Them between the audit groups and the departments they are auditing. After all, who doesn't get a bit anxious when someone is evaluating their work? For some it feels like waiting for marks at the end of the school term and, just as students question whether they will ever use the quadratic equation again, it is not unusual for administrators to question the usefulness of the multiple, and often redundant audits they must participate in. The answer is, in fact, for a security conscious organization, audit processes are powerful tools in the administrator's arsenal that can be used to mitigate risks, expose threats, aid in development, all while ensuring regulatory compliance.

REGULATORY COMPLIANCE

Of all the reasons to perform an audit, compliance is the one most commonly recognized. All businesses, regardless of their industry, geographic location, or size, are subject to any number of laws, with certain industries, such as healthcare and financial services, far more regulated than others. Additionally, the number and complexity of the laws governing a business tends to grow with the size and complexity of the business. Some of the most comprehensive and recognizable regulations are shown in table below.

Gramm-Leach-Bliley Act (USA)	The Safeguards Rule requires financial institutions to protect the consumer information they collect.	• Designate responsible party. • Identify applications hosting or transacting customer information. • Assess risks to customer information. • Design, monitor and test assessment program. • Hold service providers to same standards. • Continue to evaluate and adjust programs.
Sarbanes-Oxley Act (USA)	To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes	• Sections 302 and 404 indirectly charge information systems to support accounting and oversight for the accuracy of reporting.
Dodd-Frank Wall Street Reform (USA)	Intended to promote financial stability by improving accountability and transparency in the financial system	• Sets the baseline for what is "reasonable and appropriate" security around consumer financial data. • Institutions must be ready to prove their security controls and document them. • Controls must include time to detect, respond and report breaches impacting sensitive data. • Considers the size and maturity of the organization
General Data Protection Regulation (EU)	Intended to strengthen and unify data protection for individuals within the European Union	• Designate a data protection officer. • Process personal data only for specific purposes. • Allow customers to take their data with them. • Delete personal data once it's purpose is fulfilled. • Recognize an individual's 'Right to be Forgotten'.
Payment Card Industry Data Security Standards	Industry standards for self-regulation of security	• Protect cardholder data • Manage vulnerabilities • Provide strong access controls • Monitor and test • Maintain policy

Rulemakers, when creating laws, must establish mechanisms to monitor whether companies are complying with them. Each law will have its own unique requirements, so it is not uncommon for each to have their own set of audit standards. It is important to note, however, that regulatory compliance, which focuses on ensuring that reasonable controls, policies, and procedures are in place to mitigate risks, does not necessarily equate to better security. A system with a lackluster security implementation that is mitigated by hundreds of hours of manual oversight and processing may be compliant, even though the system is not secured as well as it could be.

RESPONDING TO AUDIT REQUESTS

Answering internal and external compliance audit requests in a timely manner demonstrates a well maintained and organized environment, bolstering the auditor's confidence that the platform is secure and well managed. Below are some typical audit scenarios.

Scenario 1: Testing a Specific Users Access

The auditors would like a report on what Hannah, HR director has access too. If using the SAS Management Console Plug-in, the administrator can select each folder and to visually check the authorization tab for every folder in the SAS folder tree as shown in Figure 1: Effective Permissions and Access Levels for Hannah Hanes on the Data folder.

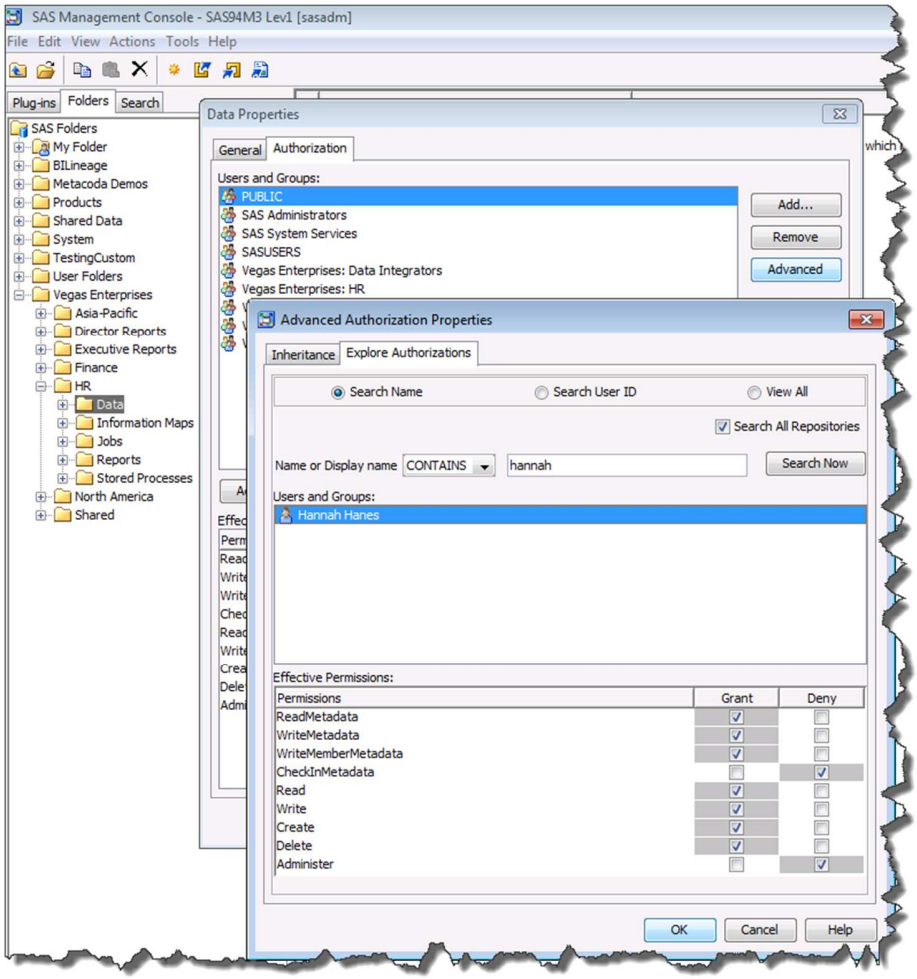


Figure 1: Effective Permissions and Access Levels for Hannah Hanes on the Data folder

In an organization where there are many folders, this can be a time-consuming task. Using Metacoda Identity Permissions Explorer Plug-in the report can be generated for the auditors with just a few clicks. The Metacoda Plug-in quickly calculates the net effect of all applicable permission settings (derived from all Access Control Templates (ACTs) and Access Control Entries (ACEs) inherited from the folder tree) across all folders. See Figure 2: Effective Permissions and Access Levels for Hannah Hanes.

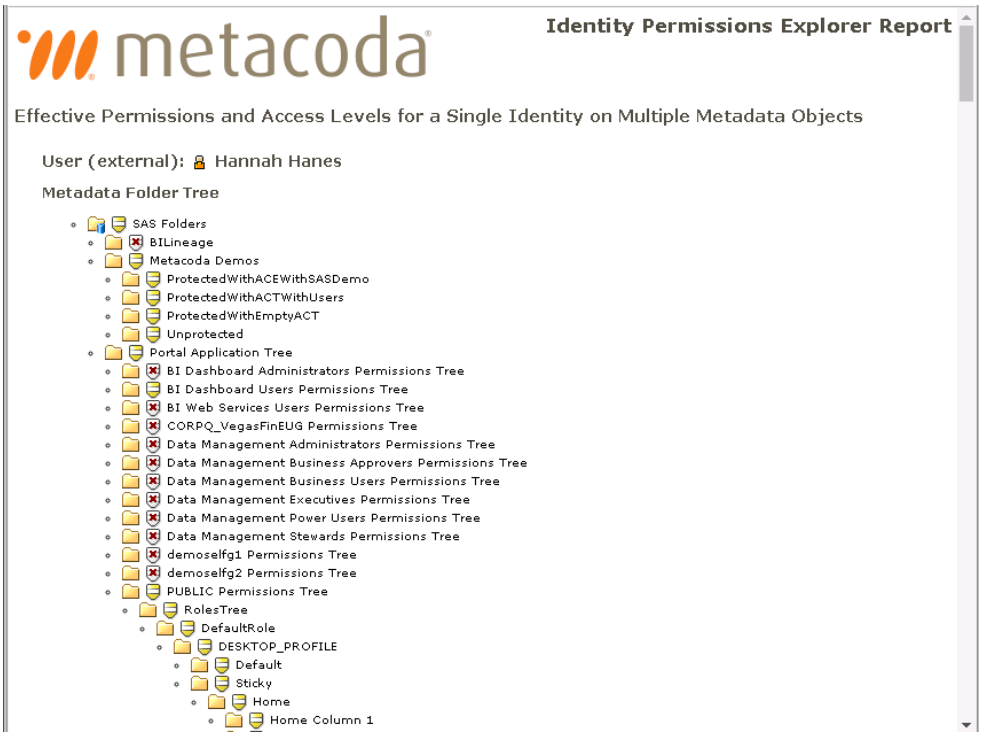


Figure 2: Effective Permissions and Access Levels for Hannah Hanes across all folders

The SAS administrator can also ensure Hannah's group membership, both direct and indirect, is as expected, using Metacoda User Reviewer. In Figure 3: Reviewing Hannah Hanes' identity hierarchy and group membership, it's clear she is a direct member of three groups: HR, Directors and Finance / AU (Global).

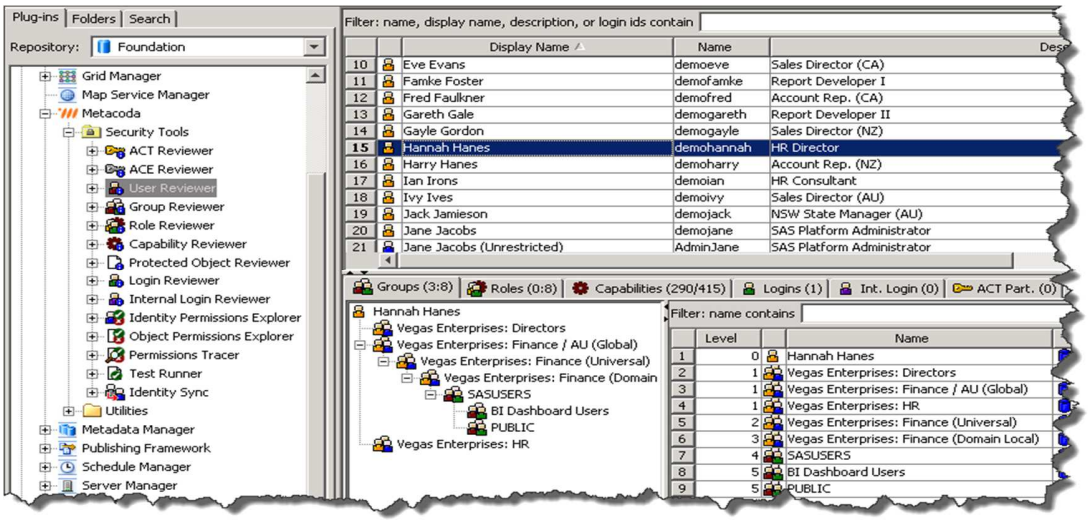


Figure 3: Reviewing Hannah Hanes' identity hierarchy and group membership

Through the batch reporting facility within Metacoda Security Plug-ins, further reports can also be made available to auditors and management who don't have access to SAS Management Console, which will allow them to review users' identity hierarchy and group membership as needed.

Scenario 2: Reviewing Administrative Privilege Assignments

When the auditors ask to see who has administrator privileges, it is natural to look at the administrative related groups in Management Console however, it is possible that someone may have put a non-administrative group or user into an administrative role. The way to check this is to use Metacoda Role Reviewer to verify the members of the related administrative roles. Searching for "metadata" within the Metacoda Role Reviewer finds that there are three metadata types of roles as in Figure 4: Searching for metadata related roles:

- Metadata Server: Unrestricted - people who can do anything! A role that should be closely monitored as unrestricted users can create other unrestricted users, have access to all metadata and can provide all capabilities in SAS Management Console.
- Metadata Server: User Administration - administrators that can change and create users, groups and roles but not unrestricted.
- Metadata Server: Operation - the ability to manipulate repositories and metadata servers.

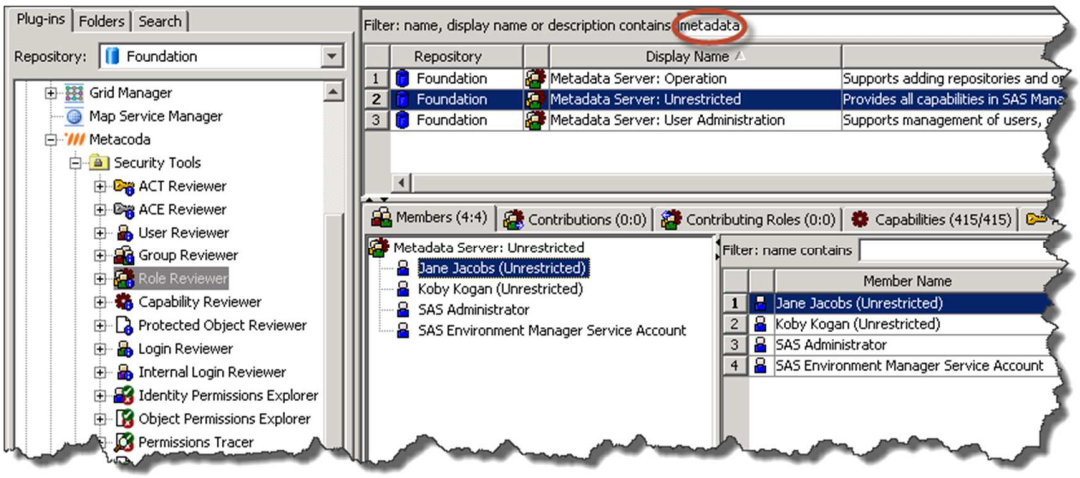


Figure 4: Searching for metadata related roles

It is a good approach to use internal accounts if you don't have multiple AD logins. As an example, in Figure 5: "Metadata Server: User Administration" role members Jane and Koby have dual identities where they have internal accounts for unrestricted access in addition to their domain accounts for general administration access. Barbara and the SAS demo user account also have user administration access but not unrestricted.

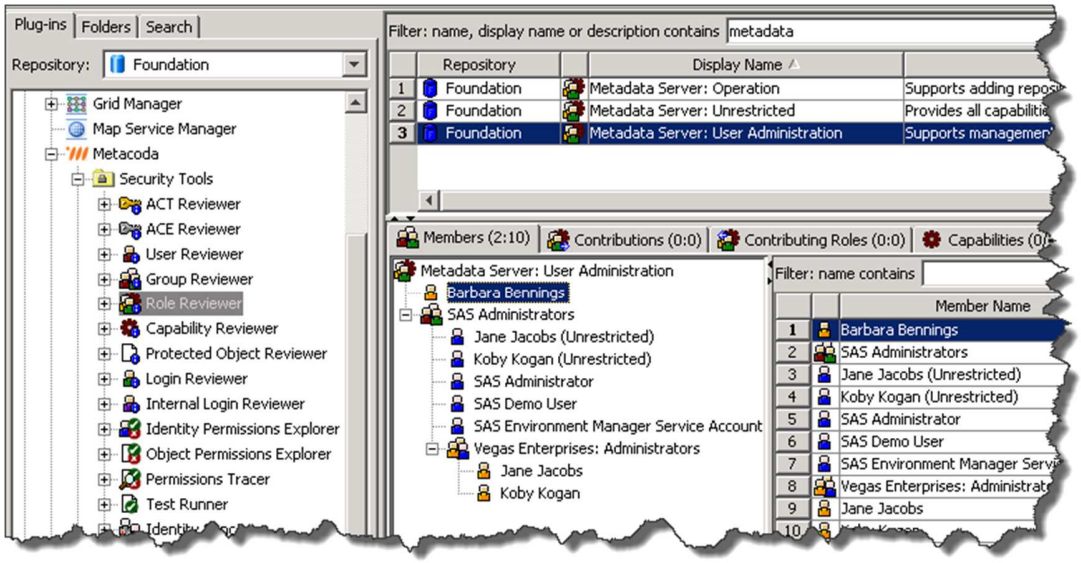


Figure 5: "Metadata Server: User Administration" role members

It is also important to check that the appropriate users have access to file system files such as adminUsers.txt as otherwise they could add themselves to the file and be granted admin access.

Scenario 3: Reviewing Changes to User Security

An auditor would also be interested in knowing what changes have been made to user security. There are stored process reports within the SAS Environment Manager Report Center that can assist with providing information on user account history. The log file data is gathered from the SAS logging facility which can be used by programmers to create custom reports for auditors. In this scenario, the default reports provided within SAS Environment Manager Report Center are used; and as described earlier it is possible to create custom reports from the log files as Gerry Nelson describes in his blog post *Auditing data access: who did what and when?* (Nelson, 2015).

The Audit Report Group_Changes report lists the changes made to the three Metadata Server administration roles mentioned above. The report in Figure 6: Audit Report Group_Changes shows that Barbara was added to the “META: User and Group Administrators Role” on the 23rd January 2017 with other members added at the same time.

The report also shows that Koby and Jane’s (unrestricted) accounts were added to the Unrestricted Users Role on 22rd January 2017.

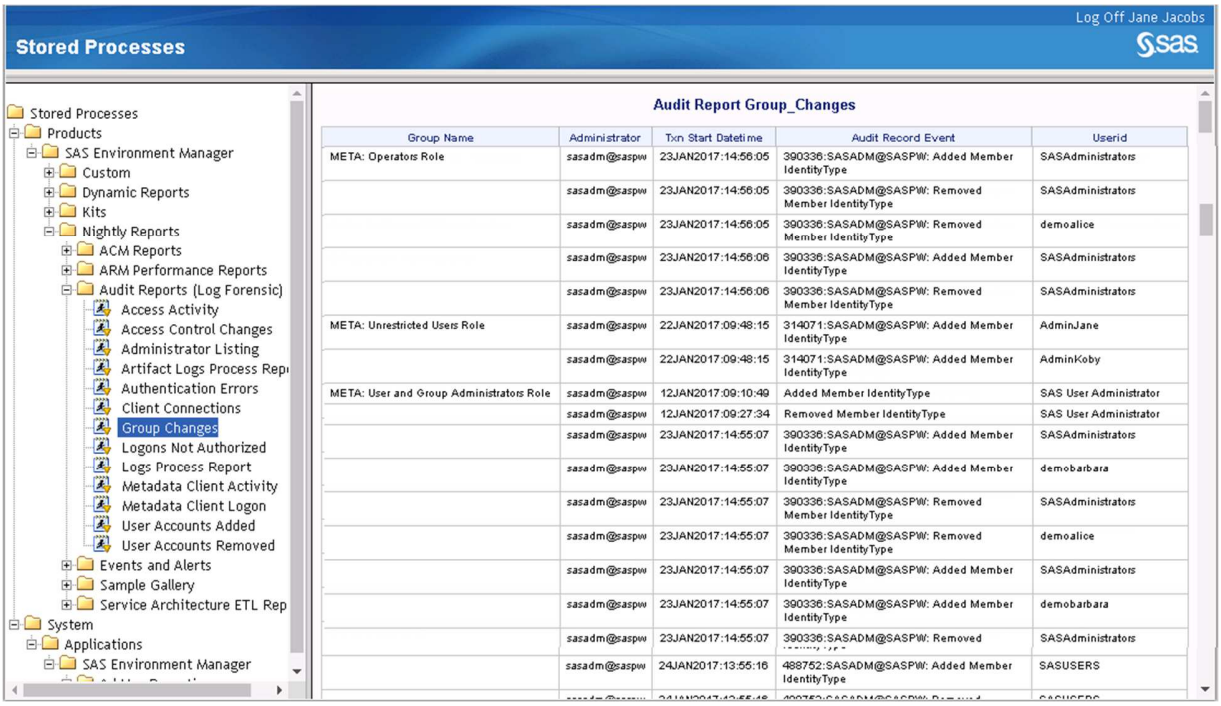


Figure 6: Audit Report Group_Changes

Scenario 4: Change Control & Testing Process for Security Changes

The HR folder contains sensitive data and reports, therefore, the administrator needs to ensure the resources are continuously protected and only the appropriate people have access to it. As such they will want to be notified when there are any changes to the HR group. Using the Metacoda Metadata Security Testing Framework changes can be tested for in batch, weekly, daily, hourly or more frequently. From the Group Reviewer, we can export a XML test script as seen in Figure 7: Export metadata security test script.

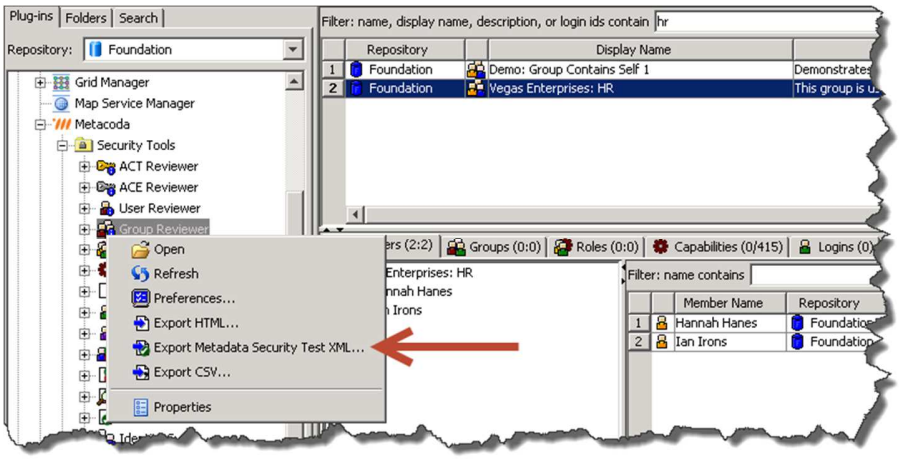


Figure 7: Export metadata security test script

As an XML starter test script, the file can be modified if not all areas are required for testing. Using the Metacoda Test Runner plug-in the test is run interactively and admin can see immediately that all the tests pass (see Figure 8: Metadata security test on HR group). The test can also be set to run daily in

batch so the administration team is notified when there are any non-compliant changes to metadata security, for instance if David Doyle, an account representative, who is not part of the HR team or management, was accidentally added to the Vegas Enterprises: HR group.

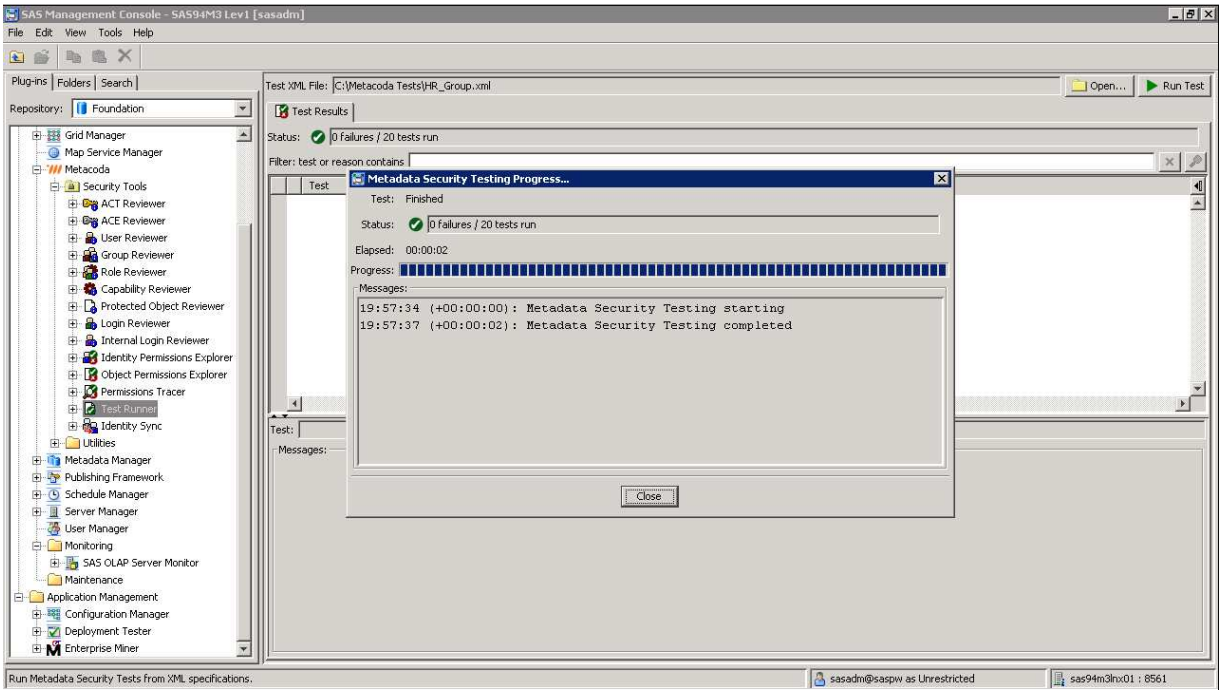


Figure 8: Metadata security test on HR group

The distinction between compliance and security efficacy is important because one often overlooked benefit to a well secured system is a reduction of risks to the company's technology and data assets and the resulting reduction in the costs associated to manage those risks. A strong audit program provides the necessary level of assurance to a company through two primary methods: (1) Assessment & Remediation and (2) Secure Development.

ASSESSMENT & REMEDIATION OF RISKS

In today's environment, where it seems like there is a new security breach announcement every week, the security conscious administrator needs to take security auditing beyond basic compliance. A program of robust periodic reviews not only ensures a smooth audit, it strengthens the overall security program. In additional to monitoring compliance, administrators should review how well their security programs are adhering to established best practices when performing the periodic security audit.

For example, for compliance purposes, the auditor will only require that sensitive data (for example, customer data) is secured. The administrator could simply add each individual user to the Customer Data folder and explicitly secure them. Best practice, however, would be to place an ACT on the folder that contains a group with all the users who should be granted access to the folder. While both processes will accomplish the goal, the second is a stronger security methodology due to the consistency and ease of maintenance associated with using ACTs and groups.

EVALUATING THE SECURITY OF THE SAS ENVIRONMENT

The administrator's periodic review should provide them with an overview of the state of the secured objects in the system. Using that data, they can prioritize the issues that require remediation based upon the business risk. If an issue cannot be corrected, appropriate processes can be put in place to mitigate the risk. As an example, we will look at two reports that support this type of assessment.

Report 1: The Administration Report

Who has administrative access to the system? As described above there are various levels of administrative access within a SAS platform. Administrators can use the Metacoda Group Reviewer to see who the members are in the administrative related groups. Searching for admin as shown in Figure 9: Group Reviewer - search for "admin" groups provides a list of groups from which the admin can easily generate reports for the auditor to show who the members are of the SAS Administrators group.

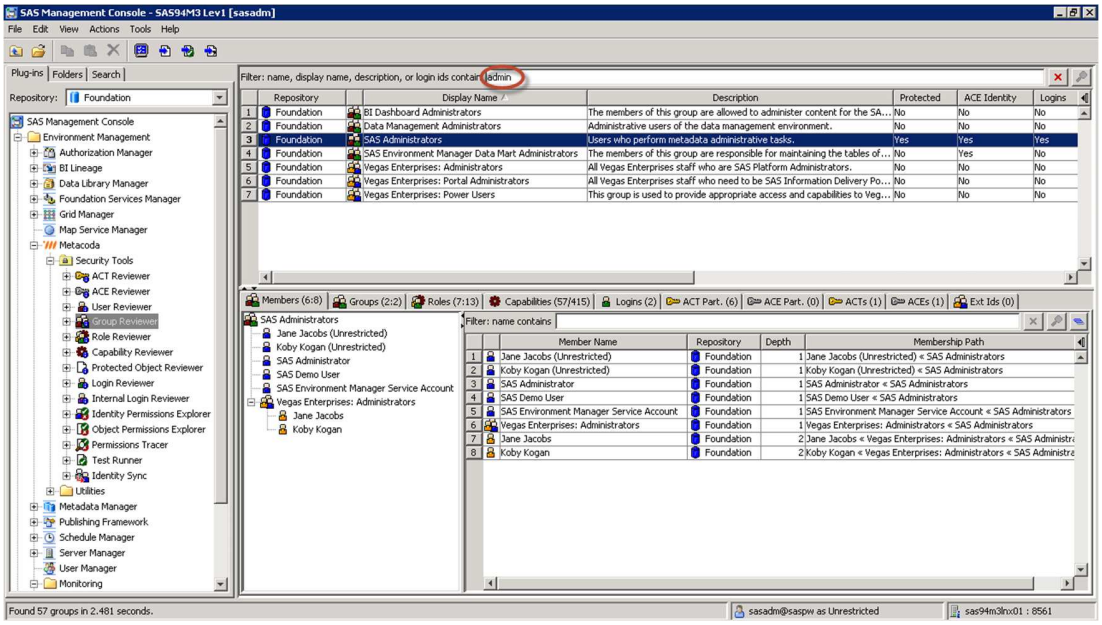


Figure 9: Group Reviewer - search for "admin" groups

Additionally, using SAS Environment Manager, the admin related group “SAS Environment Manager: Super Users”, which also exposes administrative privileges, is reviewed to verify only the expected users are members as shown in Figure 10.

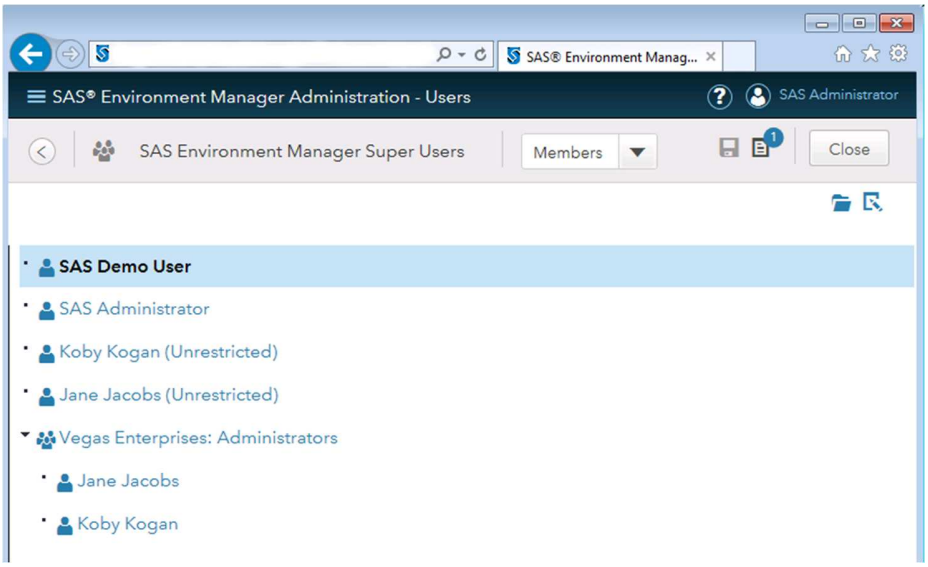


Figure 10: SAS Environment Manager showing the SAS Environment Manager Super Users

As noted in “Scenario 2: Reviewing Administrative Privilege Assignments”, checking groups demonstrates who are members in the administrative related groups; however, it is possible that someone may have put a non-administrative group or user into an administrative role.

Reviewing the “Metadata Server: Unrestricted” role, will verify the Metadata Server related roles are as expected. In examining the “Metadata Server: User Administration” role (see Figure 11: Members of the Metadata Server: User Administration role) it’s clear that Barbara has been directly added to the role.

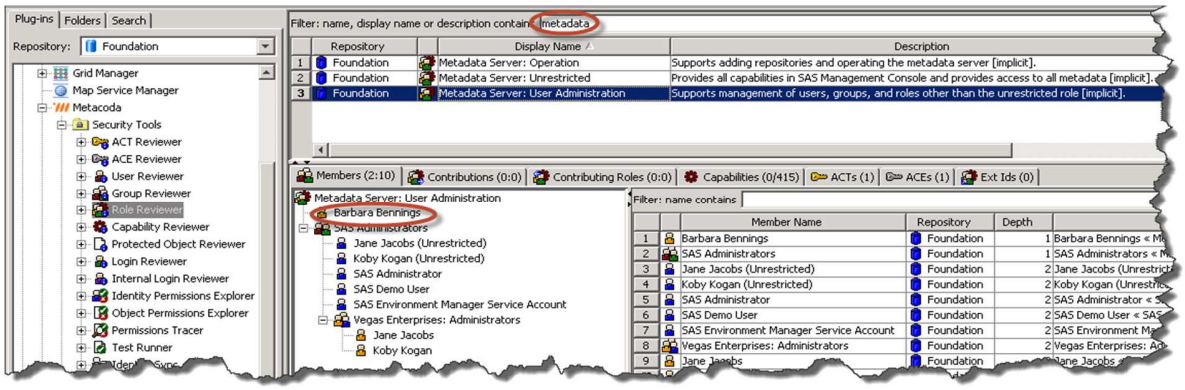


Figure 11: Members of the Metadata Server: User Administration role

This means Barbara has permission to make changes to users, groups and roles but is not unrestricted. This is a potential issue an administrator can investigate further, using the Metacoda User Reviewer to look at Barbara from another perspective. In Figure 12: Examining Barbara's role membership shows that Barbara has been granted the role directly (see the Roles tab where it is numbered 1:10 - this means she has one role directly and 10 roles indirectly).

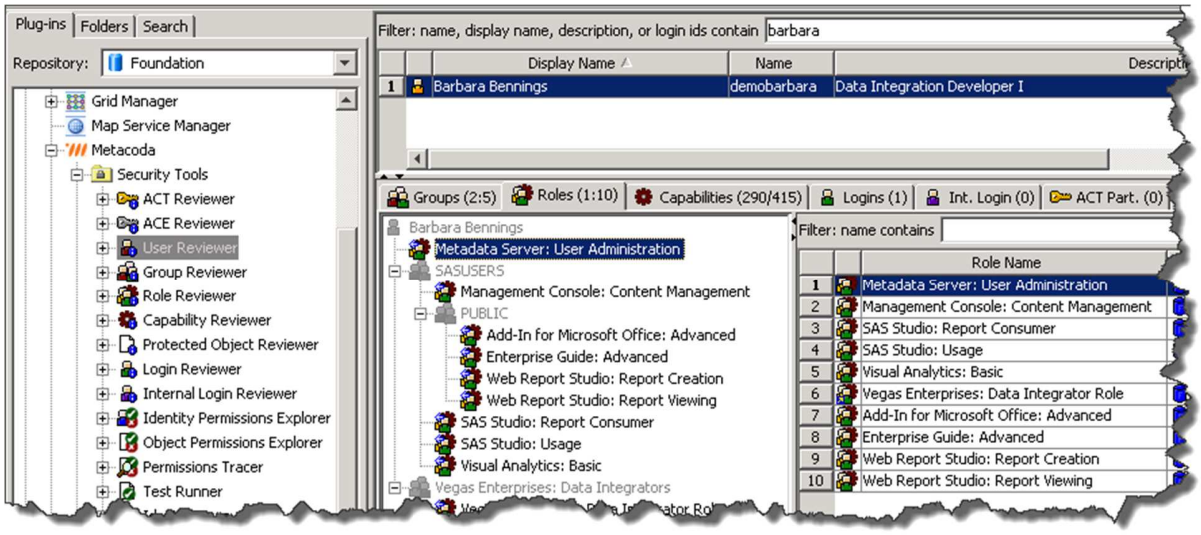


Figure 12: Examining Barbara's role membership

Barbara’s roles give her the capability to access the SAS Management Console User Manager Plug-in and to make changes to users, groups and roles. In other words, if Barbara is given access to SAS Management Console, she can make administrative changes.

As a final check on who has administrative access, a quick look at the “Metadata Server: Operation” role confirms only the expected members are there.

Report 2: The Departmental Access Report

Who has access to the HR department data?

The initial question is who are the members within the HR group. In this example, using Metacoda Group Reviewer, the admin searches for HR and finds Ian and Hannah are the only direct members.

In the design of the SAS metadata security model, each department has a SAS folder and the associated department group is granted access and any other group as approved by management. So, who has access to the HR resources can be determined by using the Metacoda Object Permissions Explorer. The output in Figure 13: Access level to HR folder shows that there are more users than expected that have access.

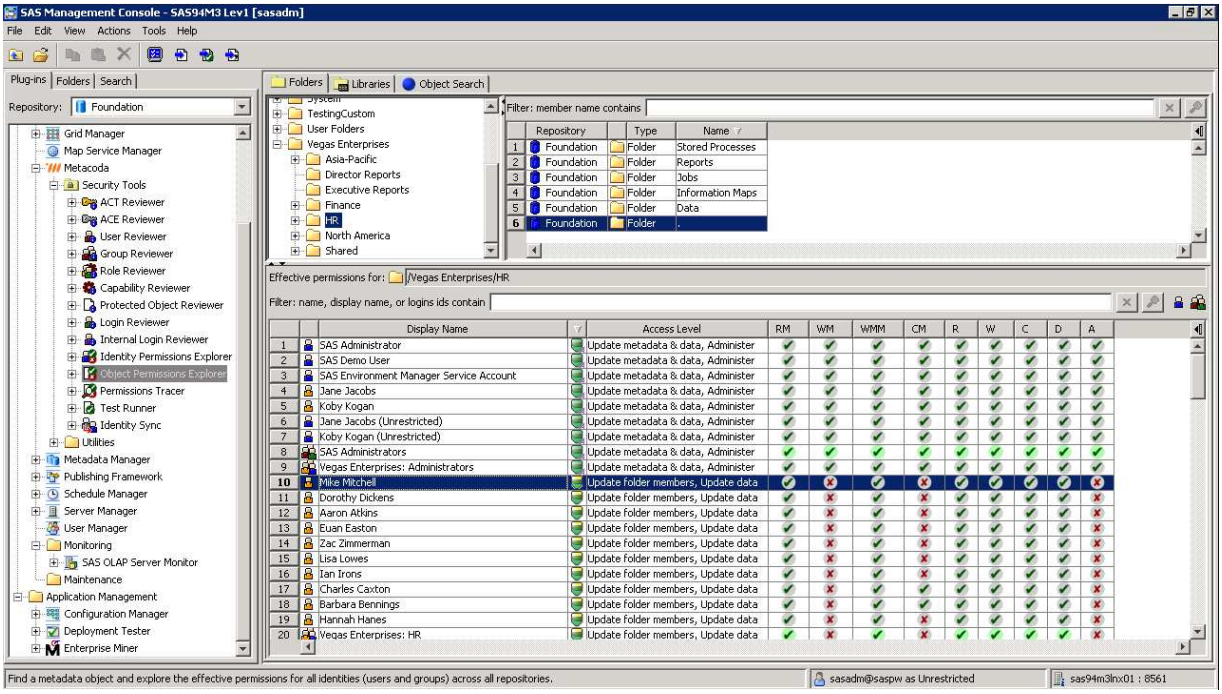


Figure 13: Access level to HR folder

Unexpected results will typically result in a series of follow-up questions, such as how unexpected access was granted. In this case the administrator wants to know how Mike and Aaron got access to the HR folder. A logical forensic question to ask! By right-mouse clicking over Mike, they can select Permissions Tracer to answer this question. In Figure 14: How does Mike Mitchell get access to the HR folder? - Permission Tracing the orange definitive squares indicate that Mike has been granted access due to the Data Scientist group membership. The only remaining question that the admin will need to ask is… Is this appropriate? Should this group be given access?

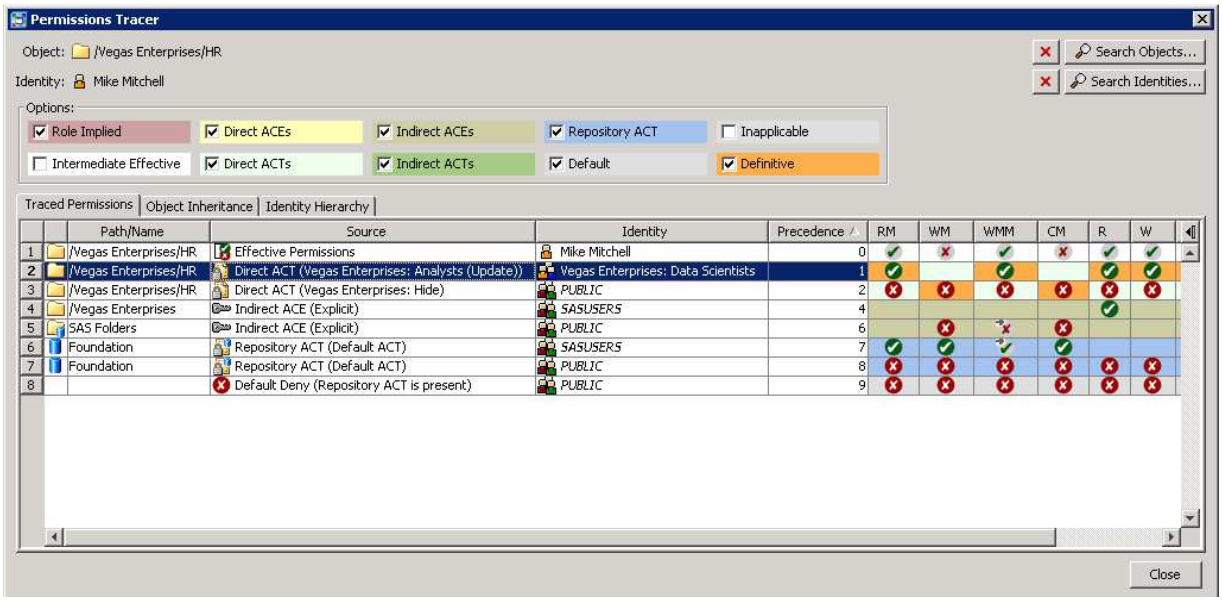


Figure 14: How does Mike Mitchell get access to the HR folder? - Permission Tracing

The same steps carried out for Aaron finds that Aaron's access is through membership of the Vegas Enterprises: Business Analysts group which has been granted access. Both sets of permissions can now be further investigated and determined why and when they were granted access and whether the access is appropriate.

SECURE DEVELOPMENT

It is easy to place the burden of security on the system administrators; however, it is just as important for the development team to apply the same security best practices during the development life cycle. From the audit perspective, this means testing. As projects are generated and moved through the development, testing and production phases, administrators and developers should work together to test for both intended and unintended security implications.

VERIFYING SECURITY INTEGRITY

Hannah, a HR director, created a SAS Visual Analytics bonus report for country managers. To allow for expansion to new countries, without increasing the number of reports that she would need to maintain, she created one report and used row level security (conditional grants) to manage access to the data. This security model will allow the executives to see all the country data, while restricting the country managers to only their own country data. Due to the sensitivity of the data, she wanted assurances the security conditions set on the report are correctly configured and will not change. In environments where there is manual human intervention it can be difficult to provide 100% assurances; however, using the Metacoda metadata security testing framework, she can configure non-compliant alerts via machine-testing conditions to ensure the security integrity of a SAS platform remains as expected.

In the example environment, there is a "Vegas Enterprises: Directors" group for the country managers. Carol is the country manager for U.S.A., Eve is the country manager for Canada, Gayle is the country manager for New Zealand and Ivy is the country manager for Australia.

There is row-level security defined on the reports' underlying data source whereby the conditional grants were individually configured using the SAS Visual Analytics Administrator tool ensures that each of the country managers can only see the data for the country they manage. See Figure 15: SAS Visual Analytics Administrator showing Permission Condition for Eve Evans.

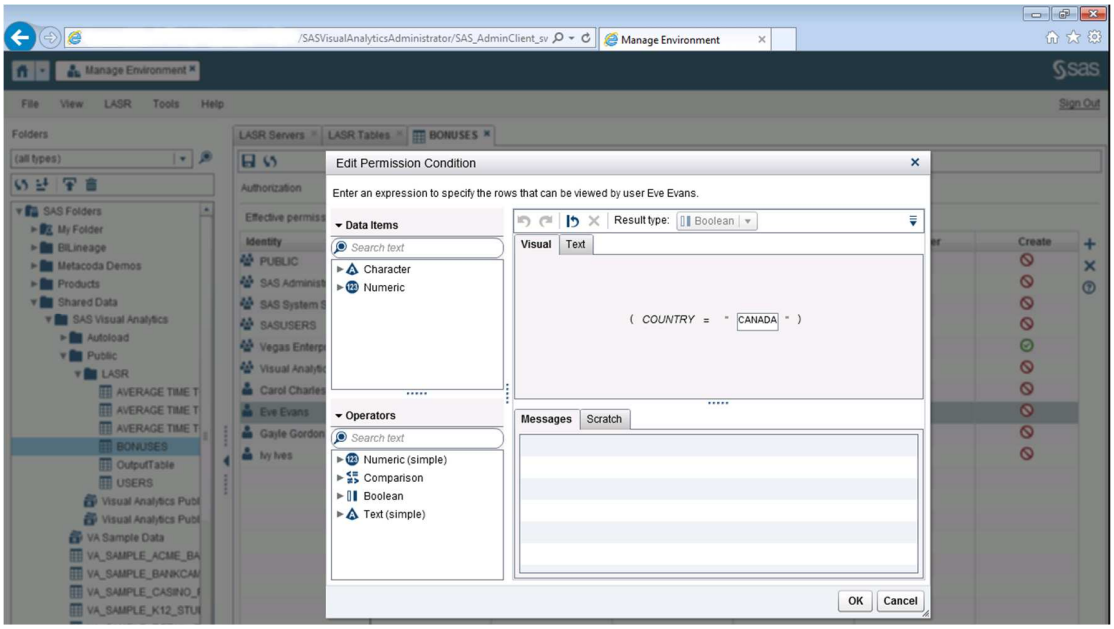


Figure 15: SAS Visual Analytics Administrator showing Permission Condition for Eve Evans

The Metacoda Protected Object Reviewer allows the developer to review all the permission conditions and the underlying XML at a glance as seen in Figure 16: Reviewing the SAS Visual Analytics table row level security.

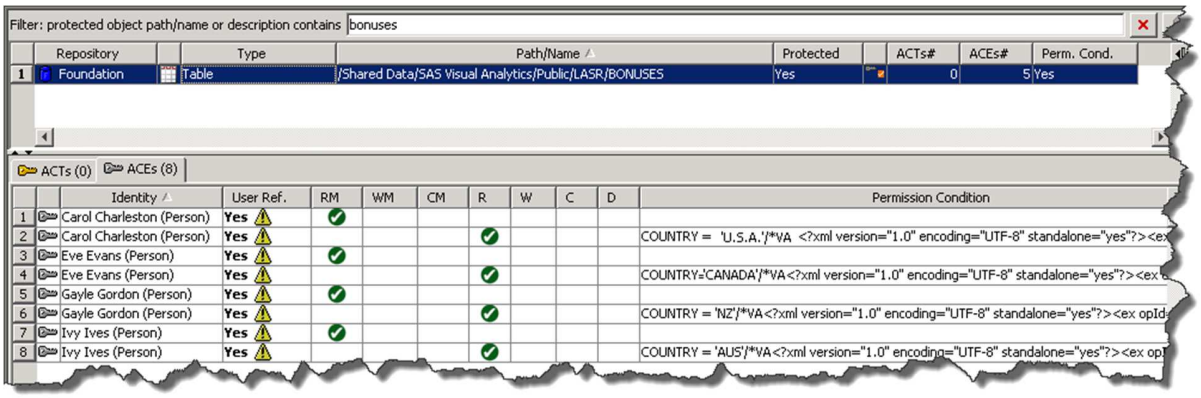


Figure 16: Reviewing the SAS Visual Analytics table row level security

While there is row-level access for the country managers ensuring they can only see their own reports, additional review is needed to confirm that users who shouldn't see the data are not given access to see the report, which is governed by the ACTs set at the folder level. General good practice is to use groups rather than identities when designing row-level access to avoid any gaps in security and the User Ref column in Figure 16 helps administrators identify when this has occurred.

The SAS Visual Analytics report, Country Bonus Report that uses the BONUSES table, also has security inherited from its parent Director Reports folder and the access levels can be identified and sorted using the Metacoda Object Permissions Explorer. Developers can see what access has been assigned – from administrator access to hide access. The list of users who have access to the report can be verified as directors and above, and the confirmed as only those who are expected to see it. See Figure 17: Effective permissions and access level on Country Bonus Report.

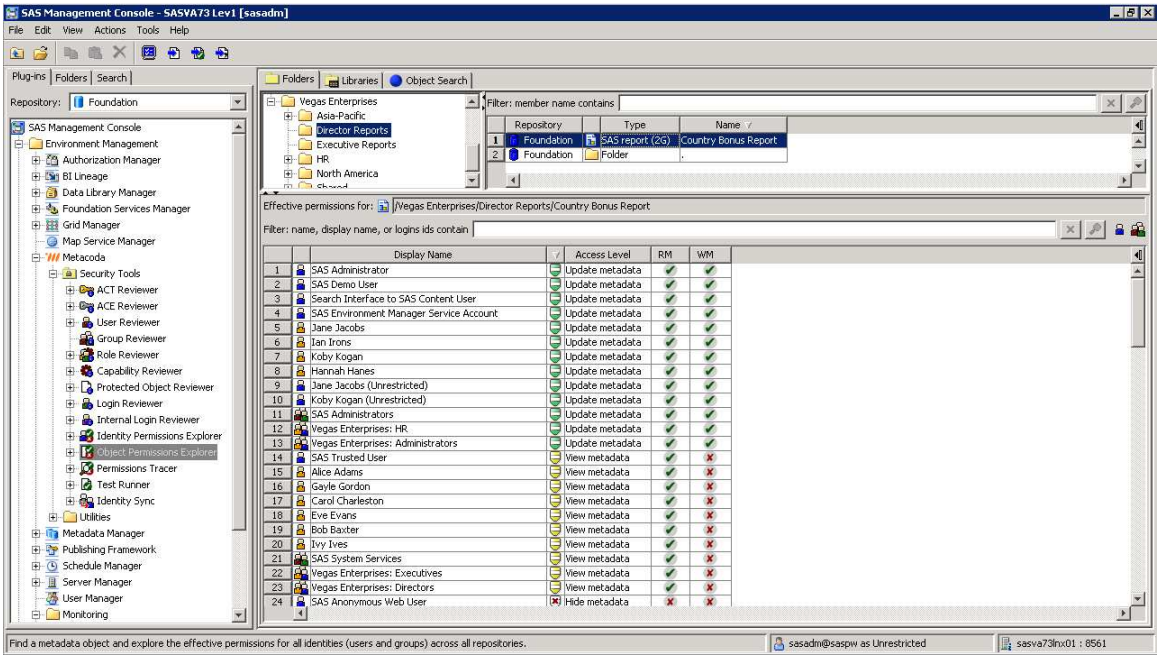


Figure 17: Effective permissions and access level on Country Bonus Report

When setting up access controls, it is recommended practice to deny access to all/most and grant back as required. To accomplish this, there is a “Vegas Enterprises: Hide” custom ACT that hides metadata from all but administrator’s and system services. Update access is then granted to the HR team and read access to executives and directors via custom ACTs. To ensure the SAS metadata security integrity on the Director Reports folder a Metacoda metadata security test script (see Figure 18: Verifying security integrity through test scripts) on the current access controls is put in place to be tested each night.

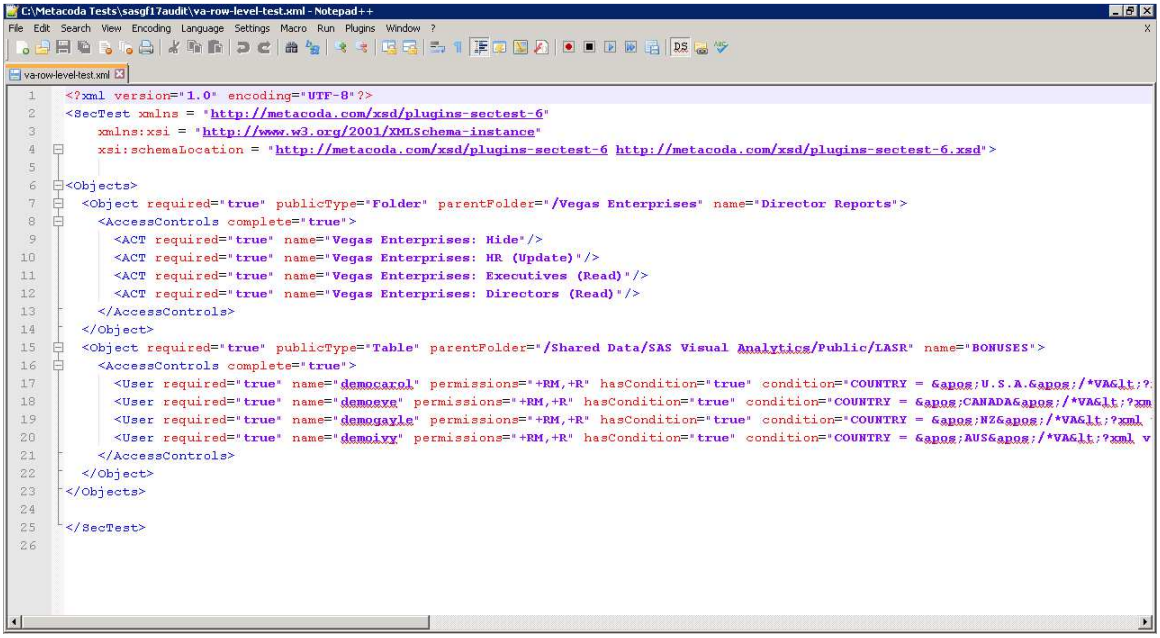


Figure 18: Verifying security integrity through test scripts

Whilst this example shows permission conditions for individual users, as a best practice you would use appropriate groups. This approach highlights some of the best practices discussed in other papers such

as the “6 golden rules” as described by Hoffritz and Jørgensen in their *Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark* paper where everyone’s access is taken away and added back the groups that should have access. In the preceding example, this is demonstrated through the use of ACTs and the row-level security. If there is any variation to the security access controls, or if the conditional grants are removed/altered, the alert distribution list, which includes Hannah and the HR team, will be notified. This helps to ensure the security integrity of the Country Bonus Report and underlying SAS Visual Analytics LASR table.

OPERATIONAL REQUESTS

On a day to day basis, knowing how to audit the security in your SAS environment is a critical function for a SAS administrator. While periodic reviews of the system help to reduce the number of calls due to incorrect security settings, questions from users on why they can’t (or can) see certain data or perform certain functions is commonplace, turning administrators into detectives. Here we will show how to solve some of the most common requests.

COMPARING DIFFERENCES BETWEEN USERS

Situations can occur where an ad-hoc security change is made to a SAS environment, causing confusion as to why users with the same role are configured differently. While it is useful to know how it happened to prevent it from happening again in the future, a SAS administrator needs to be able to resolve the differences in a timely manner to ensure business continuity. For example, the Finance department runs a monthly SAS stored process report, Monthly Product Income Report, that was created by a developer. Susan can run the report successfully; however, her co-worker, Maria, in the same department, is not able to run the report. Maria has logged a request for immediate rectification.

Where to start? In this environment users have been synchronized with Active Directory (AD) so their group membership should be the same. Who can see and run the stored process can be determined using the Metacoda Object Permissions Explorer by examining the effective access level. Sorting by the Access Level badge, as in Figure 19, we can see that both Maria and Susan have the same level of access (Read Metadata and Write Metadata) to the stored process.

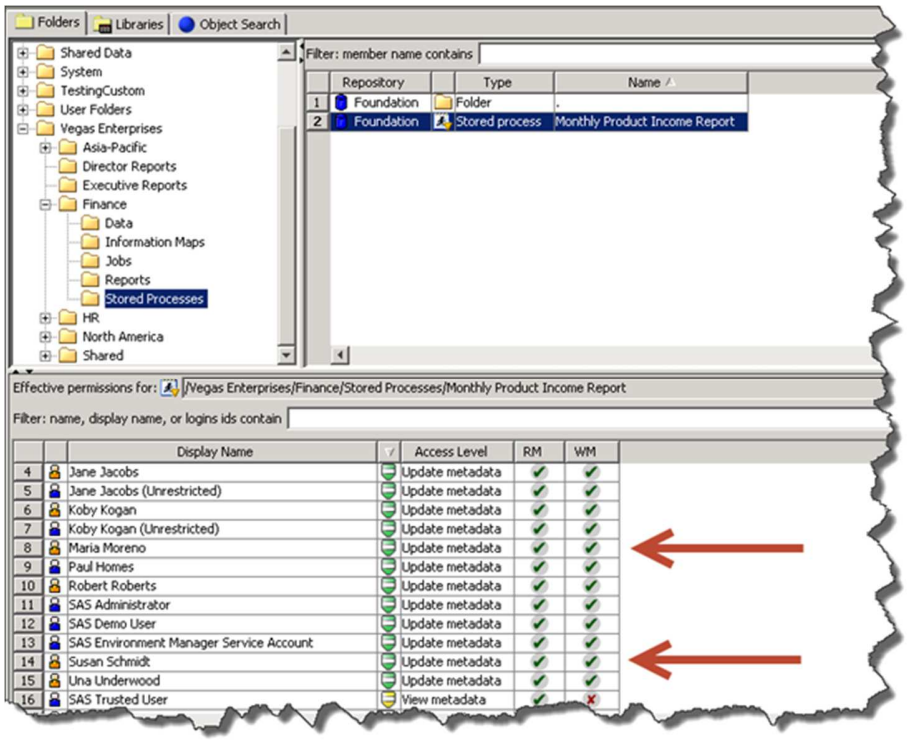


Figure 19: Reviewing Maria and Susan's access level to the stored process

As Maria and Susan have the same level of access to the stored process, the next step is to check their access to any underlying tables and libraries the SAS stored process references. This stored process uses the PRODUCT table and Maria and Susan again have the same level of access to the table and the library.

Where to look next? After verifying that their level of access to the SAS stored process, table, and library are the same the next step is to determine if there are any differences in their user profiles as was assume earlier. The Metacoda User Reviewer tool allows the administrator to compare two users and their associated attributes very quickly. Searching first for 'accountant' subsets the users so Maria and Susan can be quickly accessed side-by-side. Figure 20: Maria's group membership shows Maria's memberships. Using the tabs in the lower pane the administrator can see that she is a member of one group directly and five groups indirectly, she has eight her role memberships, capabilities are 251 from 415 available in the environment, and there is login.

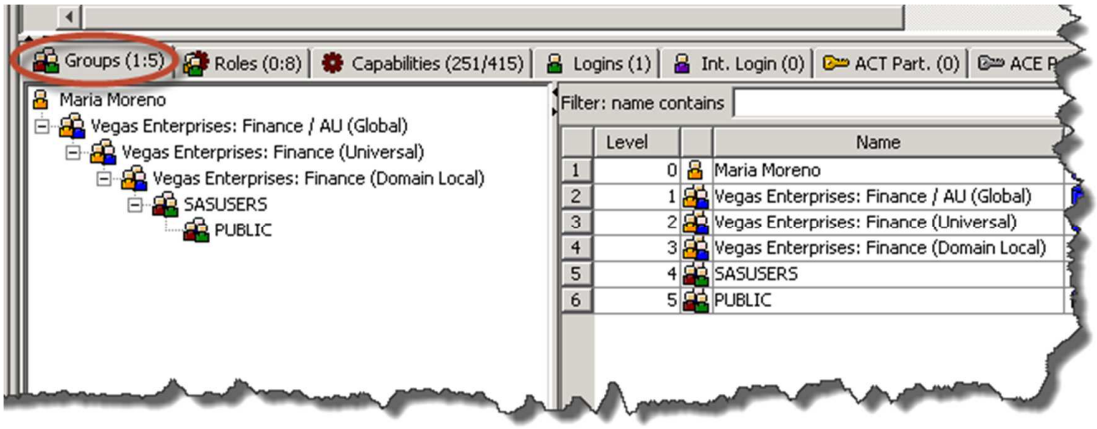


Figure 20: Maria's group membership

Looking at Susan's profile in Figure 21: Susan's group membership the administrator can see she is a member of two groups directly and six groups indirectly. Aha! They can furthermore see that Susan is a member of "Vegas Enterprises: Oracle Users" group and has two logins

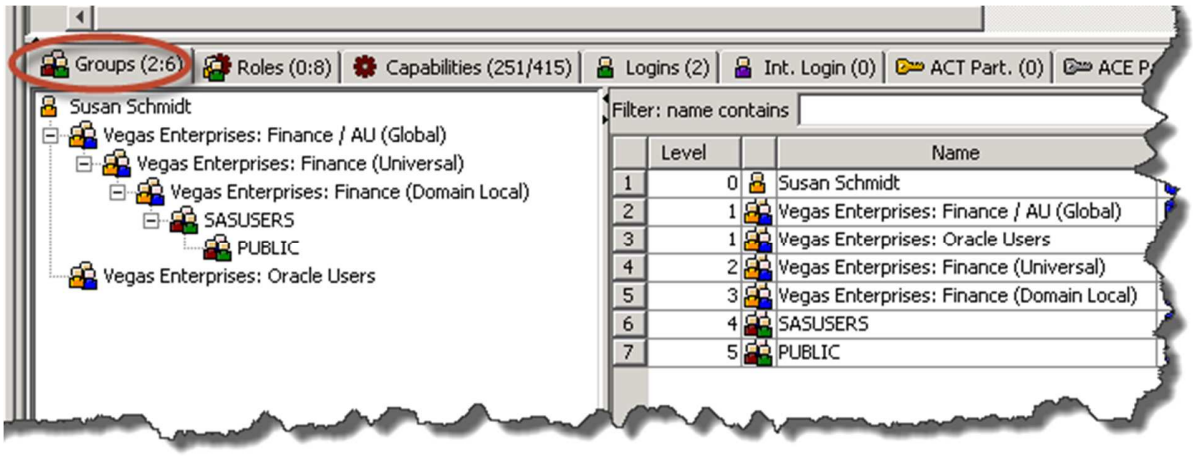


Figure 21: Susan's group membership

The detective work has uncovered that Maria was not able to run the SAS stored process because she did not have access to the underlying Oracle database the SAS metadata table, PRODUCT was referring to. For Maria to successfully run the report, the administrator simply needs to make Maria a member of

the “Vegas Enterprises: Oracle Users” group via the User Manager plug-in. Investigating the group finds that Susan has been directly added as a member. As there may be other individuals in Finance who need access, and because groups are less fluid than users, it is best to use a group rather than adding users directly, so we add the “Vegas Enterprises: Finance (Universal)” group to the “Vegas Enterprises: Oracle Users” group as in Figure 22: Adding the finance group to the Oracle Users group. This now means both Maria and Susan (and other members of the group) now have the Oracle database shared login.

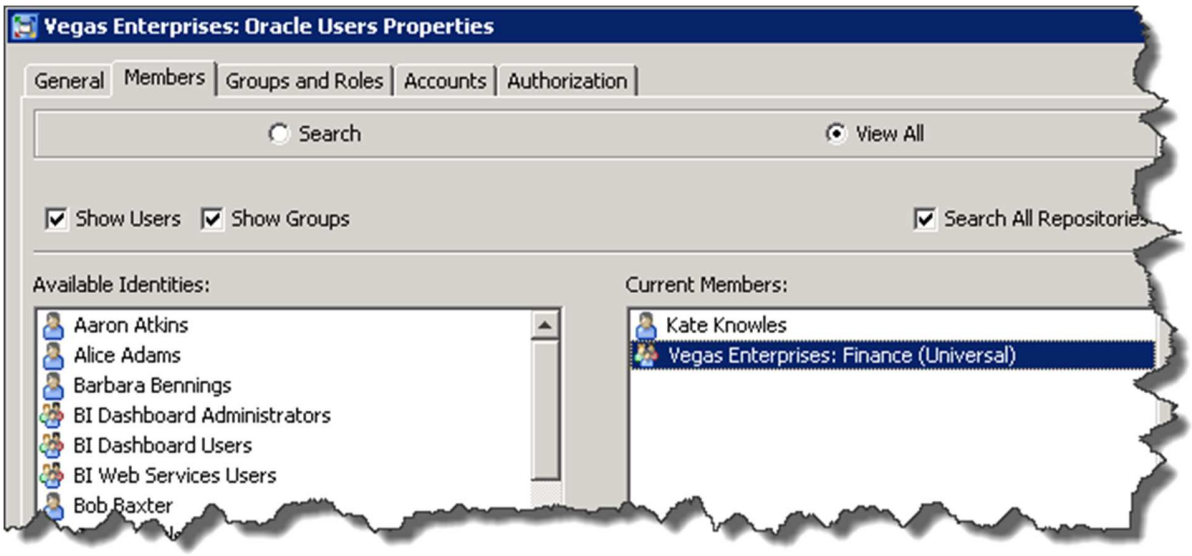


Figure 22: Adding the finance group to the Oracle Users group

Additionally, from the Metacoda Group Reviewer, a difference perspective verifies that Maria is now a member as well as all the other users that now have access via the “Vegas Enterprises: Finance (Universal)” group as shown in Figure 23: Members of the Oracle Users group.

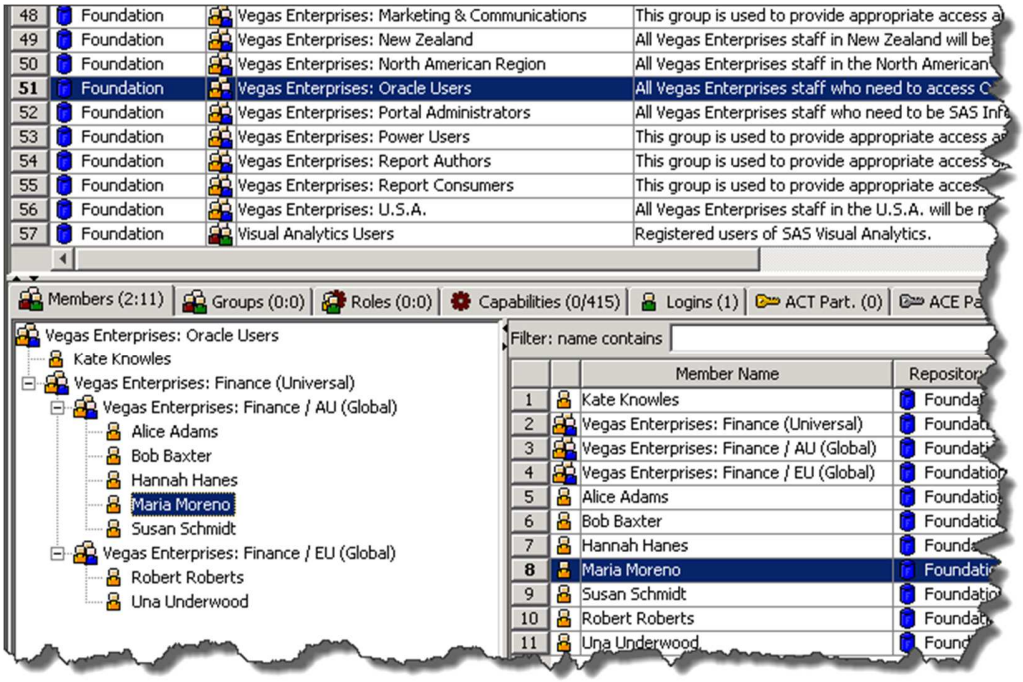


Figure 23: Members of the Oracle Users group

DIAGNOSING SAS APPLICATION FEATURE ACCESS

Zac, an analyst, launches SAS Enterprise Guide to run some SAS code provided by a consultant. He could start SAS Enterprise Guide however when he chooses to open a SAS program he discovers the menu open is not there (Figure 24: No SAS program option in SAS Enterprise Guide).

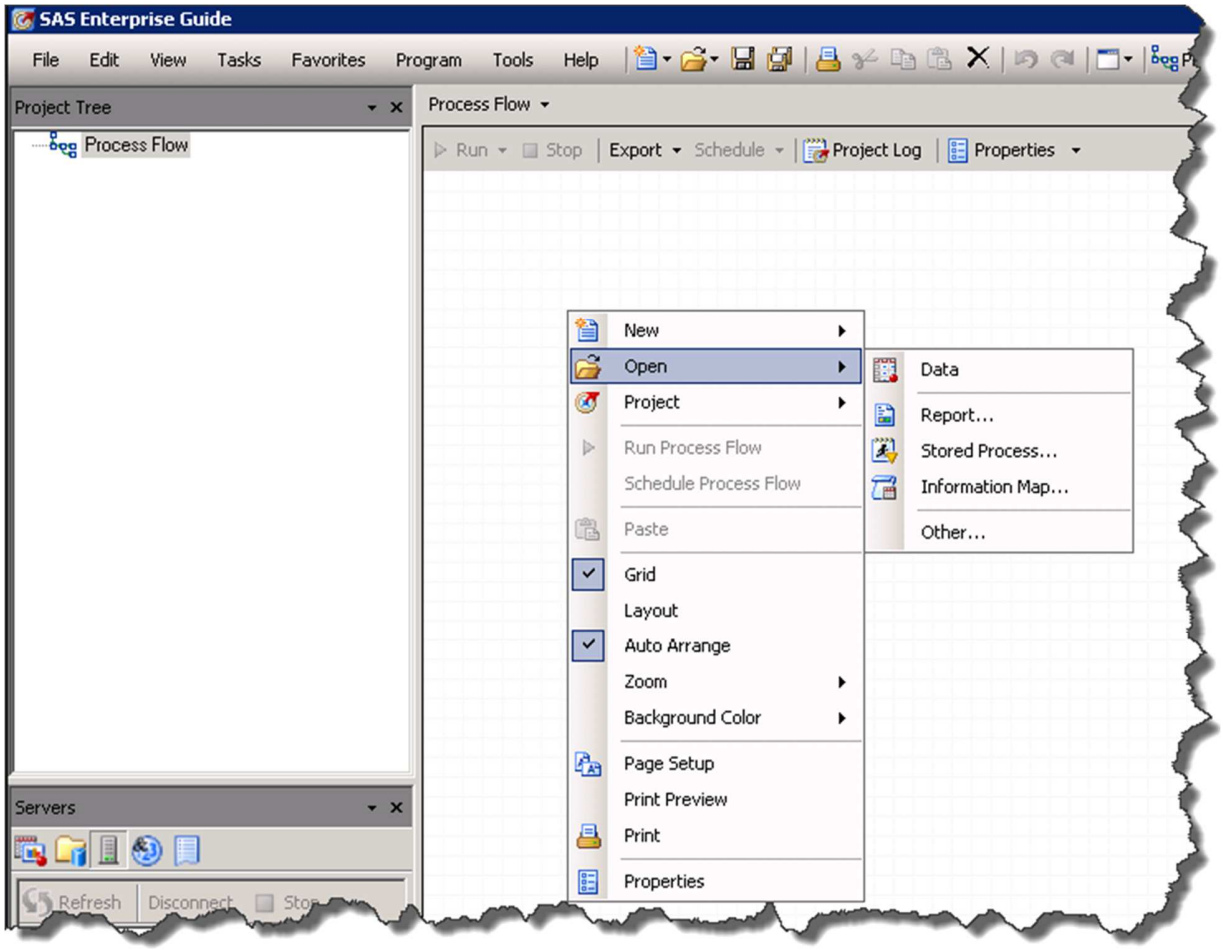


Figure 24: No SAS program option in SAS Enterprise Guide

Being an inquisitive analyst, Zac notices in the lower right corner there is a Functions: Restricted message 

which he hadn't noticed before so he clicks on the Functions hyperlink and discovers there are a list of Function Settings that he doesn't have access to. Unsure what needs to be done Zac contacts his administration team to resolve.

The administrators, upon receiving the call, thank him for his diagnosis and explain Function Settings (Capabilities or Application Action) to him. A quick look at his profile using the Metacoda User Reviewer and the capabilities tab, confirms he doesn't have access.

As there is a large community of SAS Enterprise Guide users, the question becomes, who does have the "Create and Modify SAS Program" capability and how? This is difficult and time-consuming to answer using the standard SAS Management Console plug-ins as the admins would have to select every user, and check their capabilities individually. Instead, this investigation can be performed using the Metacoda Capability Reviewer. Filtering on program, and selecting the "Create and Modify SAS Program" capability, quickly displays the groups and members that have this functionality. For Zac to have this capability he needs to be a member of the "Vegas Enterprises: Power Users" group as shown in Figure 25.

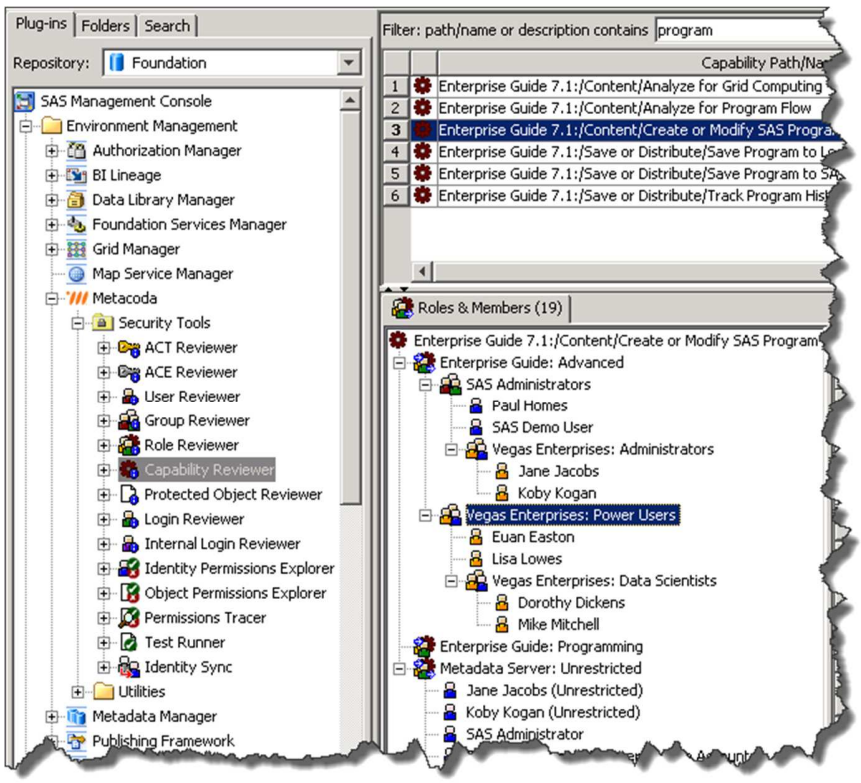


Figure 25: Answering the question "Who has the Create or Modify SAS Program?" capability

To resolve this, assuming Zac is approved to use this functionality, the administrator temporarily adds Zac as a member to the “Vegas Enterprises: Power Users” group and notifies the IT AD administrators to make the change in AD so his group membership is correct in AD for synchronization in the batch job overnight. Zac reconnects to SAS Enterprise Guide and is pleased to see (Figure 26) that he no longer has restricted access and can open and run SAS programs.

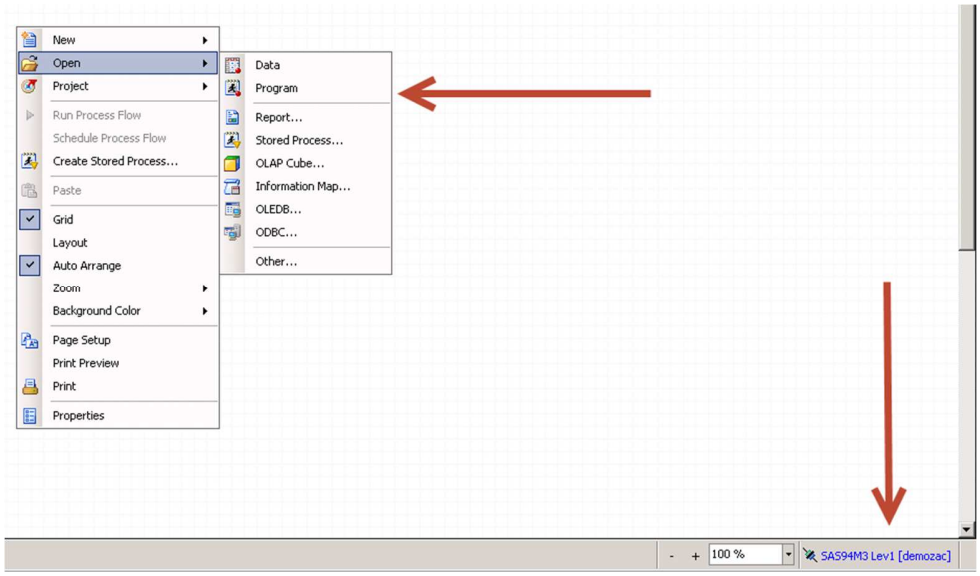
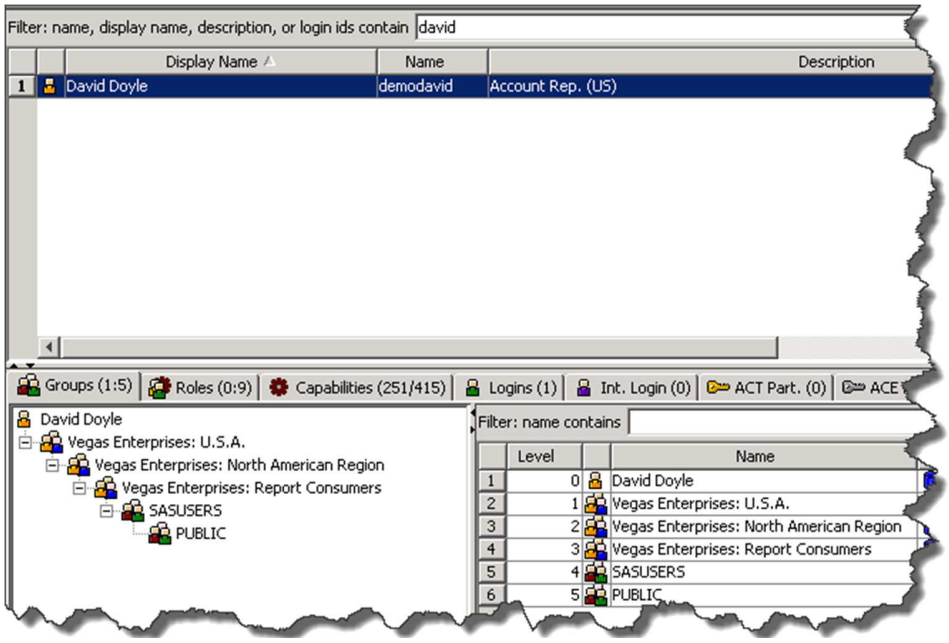


Figure 26: No restricted access and can create and modify SAS programs

CONFIRMING USERS ONLY HAVE ACCESS TO WHAT THEY'RE SUPPOSE TO HAVE ACCESS TO



Eve, a sales director in Canada is concerned that David, an account representative who previously worked for her and is now an account representative in U.S.A. still has access to her department records. She has requested confirmation that he only has access to his new department related data.

Figure 27: David's group membership

To provide Eve the ad-hoc request and confidence in the SAS platform security, the admins first verify that David is no longer a member of any Canadian group and is only in the U.S.A. groups.

Using the Metacoda User Reviewer, filtering for "David", and viewing his group membership in the lower pane confirms this (Figure 27: David's group membership).

Eve would also like confirmation that David does not have access to the Canada folder. Using the Metacoda Object Explorer and filtering on "David" quickly confirms that he does not have SAS metadata access. See access level is Hide metadata in Figure 28.

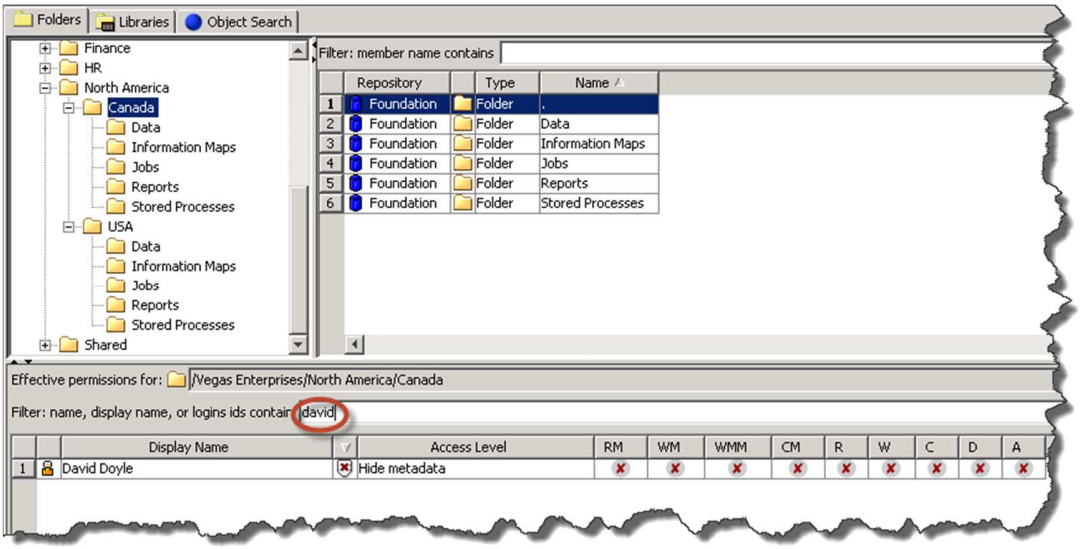
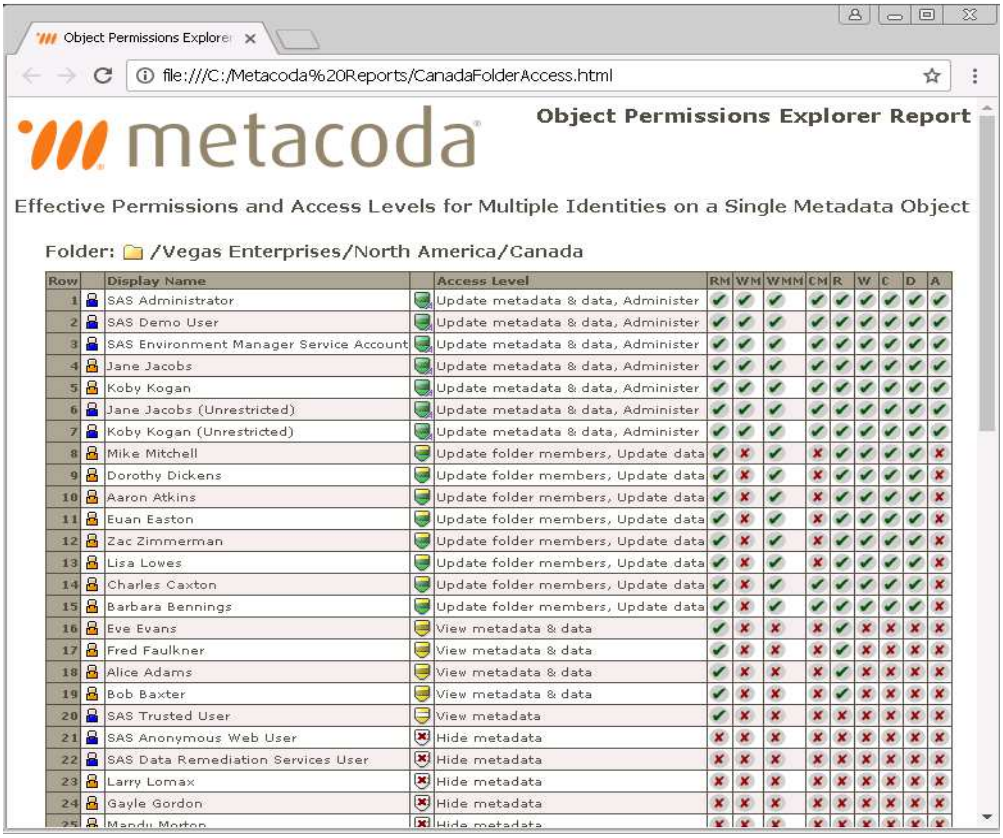


Figure 28: Access level on the Canada folder

While a verbal confirmation assures Eve, she would like a report on who has access, which the administrators can immediately provide by exporting an HTML report on who has access to the folder and emailing it to her (see Figure 29). Customer Service A+!



Row	Display Name	Access Level	RM	WM	WMM	CM	R	W	C	D	A
1	SAS Administrator	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
2	SAS Demo User	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
3	SAS Environment Manager Service Account	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
4	Jane Jacobs	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
5	Koby Kogan	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
6	Jane Jacobs (Unrestricted)	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
7	Koby Kogan (Unrestricted)	Update metadata & data, Administer	✔	✔	✔	✔	✔	✔	✔	✔	✔
8	Mike Mitchell	Update folder members, Update data	✔	✘	✔	✘	✔	✔	✔	✔	✘
9	Dorothy Dickens	Update folder members, Update data	✔	✘	✔	✘	✔	✔	✔	✔	✘
10	Aaron Atkins	Update folder members, Update data	✔	✘	✔	✘	✔	✔	✔	✔	✘
11	Euan Easton	Update folder members, Update data	✔	✘	✔	✘	✔	✔	✔	✔	✘
12	Zac Zimmerman	Update folder members, Update data	✔	✘	✔	✘	✔	✔	✔	✔	✘
13	Lisa Lowes	Update folder members, Update data	✔	✘	✔	✘	✔	✔	✔	✔	✘
14	Charles Caxton	Update folder members, Update data	✔	✘	✔	✔	✔	✔	✔	✔	✘
15	Barbara Bennings	Update folder members, Update data	✔	✘	✔	✔	✔	✔	✔	✔	✘
16	Eve Evans	View metadata & data	✔	✘	✘	✘	✔	✘	✘	✘	✘
17	Fred Faulkner	View metadata & data	✔	✘	✘	✘	✔	✘	✘	✘	✘
18	Alice Adams	View metadata & data	✔	✘	✘	✘	✔	✘	✘	✘	✘
19	Bob Baxter	View metadata & data	✔	✘	✘	✘	✔	✘	✘	✘	✘
20	SAS Trusted User	View metadata	✔	✘	✘	✘	✘	✘	✘	✘	✘
21	SAS Anonymous Web User	Hide metadata	✘	✘	✘	✘	✘	✘	✘	✘	✘
22	SAS Data Remediation Services User	Hide metadata	✘	✘	✘	✘	✘	✘	✘	✘	✘
23	Larry Lomax	Hide metadata	✘	✘	✘	✘	✘	✘	✘	✘	✘
24	Gayle Gordon	Hide metadata	✘	✘	✘	✘	✘	✘	✘	✘	✘
25	Mandy Morton	Hide metadata	✘	✘	✘	✘	✘	✘	✘	✘	✘

Figure 29: Effective Permissions and Access Levels report on Canada folder

Appreciative of the prompt verification, Eve requests the security audit report on the Canada folder on an ongoing basis. Her report, can be added to a regular batch audit report process that provides ongoing reporting to departments, auditors, administrators, and developers.

CONCLUSION

This paper discussed multiple ways in which a SAS Administrator can do internal and external audit requirements, facilitate secure development, review the environment to ensure protected resources are not at risk, and trouble shoot user security issues. By using the SAS Management Console, SAS Environment Manager, and Metacoda software we demonstrated how to test specific user access with the Metacoda Identity Permissions Explorer and the Metacoda User and Group Reviewer plug-ins; specific user capabilities with the Metacoda Role Reviewer; changes to users with the default reports provided within SAS Environment Manager Report Center. We also discussed setting up a testing framework using the Metacoda Metadata Security Testing Framework and XML in both interactive and batch mode. Lastly, we looked at testing the security of individual metadata objects using the Metacoda Protected Object Reviewer.

While audit requirements are at an all-time high for administrators in all industries, using both SAS and Metacoda tools allows the administrator to leverage their audit processes to mitigate risks, expose threats, and aid in development, all while maintaining regulatory compliance in their systems. Just as the analyst can reassure skeptical students that the quadratic equation is used in lots of ways, for example business optimization, the administrator can rest assured that their audits provide business value far beyond regulatory compliance.

REFERENCES

Faenza, Charyn. “SAS® Metadata Security 101: A Primer for SAS Administrators and Users Not Familiar with SAS” SAS Global Forum 2015. Available at https://support.sas.com/resources/papers/proceedings15/3479-2015.pdf

Faenza, Charyn. “SAS® Metadata Security 201: Security Basics for a New SAS Administrator” SAS Global Forum 2016. Available at http://support.sas.com/resources/papers/proceedings16/10962-2016.pdf

Cecily Hoffritz and Johannes Jørgensen “Best Practice Implementation of SAS® Metadata Security at Customer Sites in Denmark.” SAS Global Forum 2011. Available at http://support.sas.com/resources/papers/proceedings11/376-2011.pdf

Nelson, Gerry. “Auditing data access: Who did what and when?”. SAS blog post 30SEP2015. Available at http://blogs.sas.com/content/sgf/2015/09/30/part-1-auditing-data-access-who-did-what-and-when/

RECOMMENDED READING

Dodd-Frank Wall Street Reform and Consumer Protection Act, Titles X and XIV. Federal Trade Commission. (2010, July). Available at: https://www.ftc.gov/enforcement/statutes/dodd-frank-wall-street-reform-and-consumer-protection-act-titles-x-and-xiv

Financial Institutions and Customer Information: Complying with the Safeguards Rule. Federal Trade Commission. (2006, April). Available at: https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

platformadmin.com blog Reading List - https://platformadmin.com/blogs/paul/reading-list/

Sarbanes – Oaxley Act of 2002. Available at: https://www.sec.gov/about/laws/soa2002.pdf

U.S. companies spending millions to satisfy Europe's GDPR. CSOOnline (2017, January) Available at: http://www.csoonline.com/article/3162106/privacy/article.html

Verify PCI Compliance, Download Data Security and Credit Card Security Standards. PCI Security Standards Council. Available at: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

ACKNOWLEDGMENTS

Thanks to Nicole DeCenso and Paul Homes for their support, guidance, and expertise. Any errors or omissions may be credited to the authors.

CONTACT INFORMATION

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

Charyn Faenza
F.N.B Corporation
+1 (724) 983-2474
FaenzaS@fnb-corp.com
www.fnbcorporation.com

Michelle Homes
Metacoda
+ 61 7 3103 0964
Michelle.Homes@metacoda.com
www.metacoda.com