Paper SAS142-2014

# Security Scenario for SAS® Visual Analytics

Dawn Schrader, SAS Institute Inc., Cary, NC

## ABSTRACT

Even if you are familiar with security considerations for SAS® BI deployments, such as metadata and file system permissions, there are additional security aspects to consider when securing any environment that includes SAS® Visual Analytics. These include files and permissions to the grid machines in a distributed environment, permissions on the SAS® LASR™ Analytic Servers, and interactions with existing metadata types. We approach these security aspects from the perspective of an administrator who is securing the environment for himself, a data builder, and a report consumer.

## INTRODUCTION

The Customer Experience Testing (CET) team tests pre-release SAS software in ways that mimic the experience of SAS customers. This testing includes downloading, installing, configuring, customizing, and performing usage testing with different, orderable combinations of SAS software. From this testing we have learned several important factors to consider when securing content in SAS Visual Analytics software, both alone and in combination with other software. The three main discussion points are considerations for designing the metadata folder and library setup, securing SAS LASR Analytics Server system files, and using common identities.

## TESTING OBJECTIVES

### PERSONA-BASED TESTING

Part of the focus of this particular CET testing experience is persona-based testing, where different users are defined within an environment with different identities, tasks, and capabilities. These personas include an administrator, a super-user, and several end-users. This paper will focus on the administrator, one super-user, and one end-user. The administrator is attempting to systematically define an organized approach for securing an environment that includes SAS Visual Analytics.

### DEPARTMENTALIZED SETUP

This testing experience also enforces departmentalized testing, where end-users are members of different departments. Additionally, there is a “shared” location for consumption by all departments that is managed by the administrators. End-users see the shared content and the content for their own departments. Only the administrator can see and administer content in the shared location and across all departments.

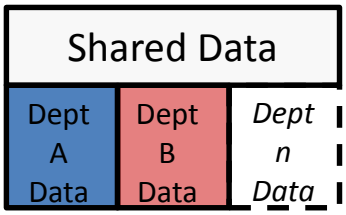



**Figure 1. Departmental Data**

For this paper, there exists one power-user in the same department as the administrator and one end-user in a different department. The power-user is tasked with creating data queries to load some of the data to SAS LASR Analytics Servers and creating some of the reports for end-users in the shared location or in his own department. The administrator alone can manage all the servers and see all the data. He loads data directly, but he has delegated the creation of data queries to the power-user. The end-user is primarily a consumer, but he may want to load data through self-service capabilities. These personas are listed in Table 1.

| Persona | Identity | Department | Role |
|---|---|---|---|
| Administrator | Violet | Blue | Control SAS LASR Analytic Servers; load data, general administrative duties |
| Power-User | Bluebell | Blue | Create data queries, reporting |
| End-user | Rose | Red | Viewing, self-service data-loading |

**Table 1. Personas, Identities, Departments, and Roles**

## METADATA SETUP

### FOLDERS AND TABLES

In this scenario, raw data on the system is stored in secure folders. The administrator will begin with basic data and metadata folder setup for this data. To make it easier to apply security, he positions the metadata library definitions inside the same metadata folders where the associated data is registered.

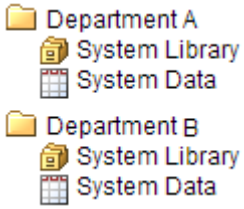



**Figure 2. Initial Departmental Folder Structure in Metadata**

This type of setup is exactly the same as in his SAS® Enterprise Business Intelligence configuration. However, an additional feature of SAS Visual Analytics is in-memory data, which is loaded on the SAS LASR Analytics Server. In order for the SAS Visual Analytics web applications and some other products to use the data, it must be loaded into memory on a SAS LASR Analytics Server. Traditional web applications, such as SAS® Web Report Studio, will only use system data. Therefore, users may need access to two metadata definitions for the same data, depending on whether the data is in-memory or not. The administrator and power-user, who load the system data to the SAS LASR Analytics Servers, need access to both data types as well.

In-memory data has the same metadata type as system data: they are both tables. If the SAS LASR Analytics Server library and in-memory data were placed in the same metadata folder, the two types of tables would be indistinguishable.

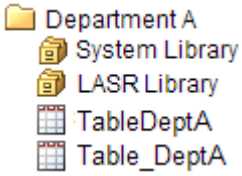
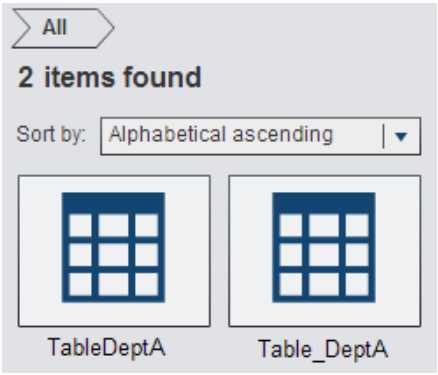



**Figure 3. Indistinguishable Table Types in Metadata, Shown in SAS® Management Console**

The same is true in the SAS® Visual Analytics Hub search feature; both types of data are listed as tables.




**Display 1. Indistinguishable Table Types in Search Results in SAS Visual Analytics Hub**

To make finding the right data easier, the administrator can recommend that a naming convention be used to distinguish the types of data. However, there are no software controls to enforce such rules. The only software restriction is that the tables cannot have exactly the same name in the same folder. Placing similarly named tables in the same location can cause confusion and result in many calls to the administrator.

Instead, the administrator creates separate locations for system data and in-memory data beneath the departmental metadata folders. This configuration also gives the administer the ability to secure the data differently if, for example, some users only need access to system data and not in-memory data or if power-users only need write permission to in-memory data to perform uploads.

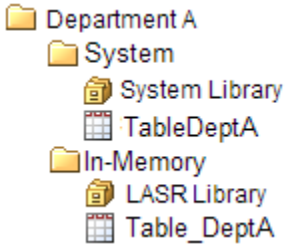



**Figure 4. Indistinguishable Table Types in Distinct Metadata Folders Shown in SAS Management Console**

In a distributed environment, data may also be loaded to the co-located data provider. For that, a third set of library and table definitions would be required in metadata, so the administrator could also create a separate location for the co-located data.

In this way, even if the table names are identical, either for system data and in-memory data in the same department or for tables in different departments, the end-user should be able to distinguish them by their folder locations.

### SAS LASR ANALYTICS SERVERS, LIBRARIES, AND DATA

For our scenario, the administrator has now created folders, libraries, and servers for each department. The metadata folders and the objects beneath them have been secured so that each department can only see their content and the shared content. It is possible to assign multiple libraries to the same SAS LASR Analytics Server, but, at the moment, for each department's data, there is one library 'in' and one library 'up' for each SAS LASR Analytics Server.

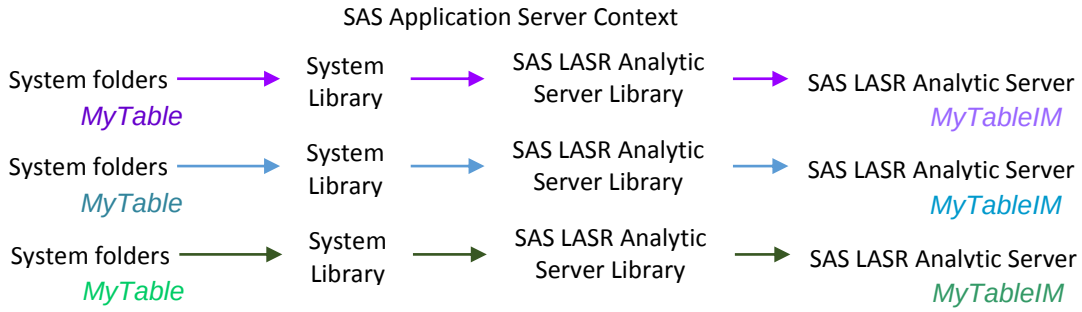



**Figure 5. Illustration of Departmental Tables and Servers**

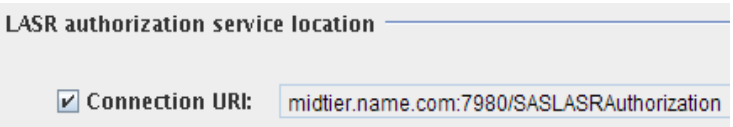
When data are loaded to the SAS LASR Analytic Servers, one workspace server session is used to read in and write out the data, as represented by the application server context in the diagram here. If there are multiple application server contexts defined in the configuration, make sure that those that are licensed for LASR will have access to the data as well as the proper license to read that type of input data.

Each element in the diagram is also represented in metadata. Metadata permissions are used to restrict access to all elements in the diagram when they are referenced by the SAS Visual Analytics web applications. To control other access, the folders on the system that contain data are secured. Similarly, system permissions must be considered to secure access to the SAS LASR Analytic Servers themselves.

## AUTHORIZATION

### SAS LASR AUTHORIZATION SERVICE AND SIGNER

Metadata permissions on in-memory data are enforced by the SAS LASR authorization service on the middle tier. Each SAS LASR Analytic Server connection in metadata includes a link to this authorization service.




**Display 2. SAS LASR Authorization Service Enabled in Metadata**

This dependency on the middle tier has a few implications for securing in-memory data. First, metadata security can only be enforced when the SAS LASR authorization service is available, meaning that the SAS® Web Application Server is running and reachable. Typically, the SAS Visual Analytics web applications are on the same web application server as the LASR authorization service, so they would be available at the same time. But other

applications that use in-memory data may be deployed on other SAS Web Application Servers, or there may be batch jobs that are scheduled to load data that rely on this web server as well.

Second, metadata security can only be enforced when the SAS LASR authorization service is specified. For the SAS LASR Analytic Servers, the option in metadata that was shown earlier is enabled by default. In batch code, the SIGNER option is required in the LIBNAME statement to enforce metadata security on in-memory data:

```
LIBNAME inmem SASIOLA TAG=Shared
        PORT=10010 HOST="gridhost.lax.com"
        SIGNER="midtier.name.com:7980/SASLASRAuthorization";
```

Third, without the SIGNER option enabled, permissions to perform some actions are affected by system file permissions. These system files, called *signature files*, can affect permissions for starting and stopping servers, as well as for loading and unloading data.

In other words, the security that is applied to SAS LASR Analytic Servers and in-memory data is a combination of the permissions set in metadata and on these files on the file system. In the same way that system data should be protected to prevent unwanted access, it is important to restrict system access to the SAS LASR Analytic Server signature files.

## PASSWORDLESS SSH, SIGNATURE FILES, SIGNER, AND UMASK

A SAS LASR Analytic Server consists of a cooperation of processes across a grid of systems. Each of these processes must be started by the same identity in order to act as a single SAS LASR Analytic Server. Communication between the grid machines, to start the different processes and communication between them, is authenticated and established via passwordless ssh. Only a user with passwordless ssh credentials configured properly across the grid can start a SAS LASR Analytic Server and load data.

In addition to passwordless ssh, users may need write access to the system. At startup and when loading data, the SAS LASR Analytic Server creates its signature files in a directory specified in the metadata for that server. This location only exists on the head node in a distributed environment, but it is also required on the workspace server host for non-distributed SAS LASR Analytic Servers. Because the SAS LASR Analytic Server runs under the identity that starts it, that identity needs write permission to the signature file location. Without write access to this location, a user cannot start a SAS LASR Analytic Server.

Signature files are important for restricting actions on SAS LASR Analytic Servers and in-memory data when metadata permissions are not enforced. As discussed here, that includes any requests that are not mediated by the SAS LASR authorization service. When metadata permissions are bypassed, only the signature files are available to protect the SAS LASR Analytic Server and the in-memory data. The administrator will want to secure those locations to prevent incidental or unwanted access. In our departmentalized example, each SAS LASR Analytic Server uses a different path for signature files. Only the administrator has write access to each location; individual power-users may have write access to their departmental locations so that they can load data, as discussed here.

The most important, top-level protection is the signature file folder itself. Without write and execute access to this location, administrators and power-users cannot start the servers because the signature files cannot be created.

The signature files for a SAS LASR Analytic Server are stored in a temporary subfolder of the signature file location. When the SAS LASR Analytic Server starts, the subfolder is created and named in the format `_T_hexvalue_hexvalues`. The permissions on this subfolder are 777 on UNIX systems and inherited from the parent folder on Windows. Specifying UNIX `setgid` permissions on the parent folder will have no effect on the permissions of this subfolder. The `_T_*` subfolder is deleted when the SAS LASR Analytic Server is stopped.

There are two types of signature files: server signature files and table signature files. Each type of file is created in sets of three: read, write, and execute. Actions are permitted based on the settings for each set of permissions.

The three server signature files are created in the signature file subfolder at startup, such as in the following example:

```
-rwxr--r-- violet blu  LASR.HEXVALUE1.HEXVALUE.saslasr
-rwx------ violet blu  LASR.HEXVALUE2.HEXVALUE.saslasr
-rwxr--r-- violet blu  LASR.HEXVALUE3.HEXVALUE.saslasr
```

The three files summarize read, write, and execute permissions for different groups of users. The ‘r’ permission for each identity on each file affects permissions given to that server and its data. For example, in the files here, the permissions assigned to the server equate to 755, as follows:

- The owner has ‘r’ for all files, so he can read, write, and execute (7).
- The owner’s group has ‘r’ for the read and execute key files, so he can read and execute (5).
- The same permissions (5) are set for other.

```
             Owner   Group   Other
Read (4)     rwx     r--     r—
Write (2)    rwx     ---     ---
Execute (1)  rwx     r--     r--
             7       5       5
```

Those permissions are determined by the UMASK. In a distributed environment, the UMASK is specified when the SAS® High-Performance Analytics environment, the TKGrid files, were installed. In a non-distributed environment, the UMASK settings for the identity that starts the SAS LASR Analytic Server are applied. In code, the UMASK can be overridden by the PERMISSION data set option when used with the LIBNAME statement or with the PERMISSIONS option in a PROC LASR statement.

The three table signature files are created when a table is loaded to the SAS LASR Analytic Server. The table signature files have names in the form of

```
-rwxr--r-- blubel blu  LIBNAME_TABLE.HEXVALUE1.HEXVALUE.saslasr
-rwxr--r-- blubel blu  LIBNAME_TABLE.HEXVALUE2.HEXVALUE.saslasr
-rwxr--r-- blubel blu  LIBNAME_TABLE.HEXVALUE3.HEXVALUE.saslasr
```

Again, permissions are enforced based on the system read permission, ‘r’. The required permissions for each file for each action are summarized in the following table.

| | | **Without SAS LASR Authorization Service** |
|---|---|---|
| **Server signature files** | Write signature file | Add a table (direct, from co-located provider, as a star schema) |
| | Execute signature file | Stop SAS LASR Analytic Servers |
| **Table signature files** | Read signature file | List data<br>Append data |
| | Write signature file | Append data<br>Unload tables |
| | Execute signature file | Unload tables |

**Table 2. Required Signature Files Permissions When Metadata Permissions Are Not Applied**

In SAS Visual Analytics 6.3 and higher, metadata permissions can completely override system file permissions on signature files, so the permissions in this table only apply when the SAS LASR Authorization Service is not enforcing metadata permissions. Permission to access the signature file parent directory is always required. For example, if a user is denied Administrator privileges on the SAS LASR Analytic Server in metadata, he cannot stop a SAS LASR Analytic Server using SAS Visual Analytics Administrator. However, if he has ‘r’ permission on the execute signature file, then he could run code directly, without the SIGNER option, to stop the server.

For this scenario, the administrator has defined multiple SAS LASR Analytic Servers in metadata, each with a separate, secured location to write their signature files. Both the administrator and power-user need passwordless ssh in order to load tables to the SAS LASR Analytic Servers. Group controls enforce access to the signature file locations, although the administrator owns each location to retain his own permissions to it. Only the Public folder is open to all identities.

```
drwxrwx--- violet blu  Blue
drwxrwx--- violet red  Red
drwxrwxrwx violet blu  Public
drwxrwx--- violet blu  Shared
```

**Display 3 – Example Security Settings on Signature File Locations**

The administrator has both passwordless ssh and execute permissions on the signature files in order to start and stop the servers and control them when the middle-tier is unavailable. At installation, the UMASK for the SAS High-Performance Environment was set to 007, which enforces 770 controls on the signature files. The identity that starts the server, and members of that system group, have all permissions to signature file locations and the files themselves. The administrator has prevented direct access to the servers except to himself and members of the group that uses them.

```
drwxrwx--- violet blu  Blue
    drwxrwxrwx violet blu  _T_hexvalue_hexvalues
           -rwxr----- violet blu  LASR.HEXVALUE1.HEXVALUE.saslasr
           -rwxr----- violet blu  LASR.HEXVALUE2.HEXVALUE.saslasr
           -rwxr----- violet blu  LASR.HEXVALUE3.HEXVALUE.saslasr
           -rwxr----- blubel blu  LIBNAME_TABLEA.HEXVALUE1.HEXVALUE.saslasr
           -rwxr----- blubel blu  LIBNAME_TABLEA.HEXVALUE2.HEXVALUE.saslasr
           -rwxr----- blubel blu  LIBNAME_TABLEA.HEXVALUE3.HEXVALUE.saslasr
```

**Display 4 – Example Signature Files for a LASR Server and an In-Memory Table**

In order to read data from within the SAS Visual Analytics web applications, the end-user requires neither passwordless ssh nor access to the signature files, because metadata permissions are always enforced by the SAS LASR Authorization Service. This setup makes the end-user dependent upon others to start servers and load the data he needs. He can become more self-sufficient if he is given a location where he can load data for himself. Instead of configuring passwordless ssh for each end-user, the administrator can define a SAS LASR Analytic Server to run as a common, shared identity instead, and also take advantage of the new autoload feature of SAS Visual Analytics 6.2.

## SHARED IDENTITIES

### COMMON IDENTITIES, TOKEN AUTHENTICATION, AND AUTOLOAD

An example of a common identity is the sassrv identity that is used to execute a pooled workspace server or a stored process server. If a user has metadata permissions to access these servers, then any code the user runs will execute on a server as that shared identity. The log files that the servers generate will be owned by the common identity, and permissions to system resources are granted based on this common identity.

Most actions performed through the SAS Visual Analytics web applications use a standard workspace server. This server executes under the identity that started it. When the administrator starts a SAS LASR Analytic Server from the SAS Visual Analytics administrator, the workspace server runs as the administrator and uses the administrator's passwordless ssh credentials to start the SAS LASR Analytic Server. When the power-user runs a query, the workspace server runs as the power-user and uses his passwordless ssh credentials to load the output table to the SAS LASR Analytic Server.

When the end-user performs actions from within the SAS Visual Analytics web applications, the workspace server starts under his identity, but access to the SAS LASR Analytic Server is controlled by the LASR authorization service. Actions are performed by the SAS LASR Analytic Servers, such as producing a forecast analysis, and returned to the web client. However, users may want to load their own data to the SAS LASR Analytic Servers, which requires both passwordless ssh and system write permissions. Rather than providing every user with passwordless ssh credentials to have access to the entire grid, the administrator can designate one common identity to act on behalf of a set of users by configuring token authentication.

When token authentication is enabled, one outbound identity is configured for the workspace server. When an end-user makes a request of this workspace server, his credentials are authenticated in metadata. Then the outbound identity, whose credentials are stored in metadata, is passed along to perform the actuals steps. In this scenario, only the common outbound identity needs passwordless ssh credentials and permissions to the signature file location.

While it is convenient, using a common identity also poses some restrictions. First, it requires that the common identity be created on the system that has passwordless ssh and other system permissions and that this identity's credentials (ID and password) be stored in metadata. The identity is generic, but some real person must be tasked with maintain its password in metadata as well as assigning appropriate system permissions. The files that are generated by user actions will be owned by the common identity, not by the specific users.

Second, configuring a common identity might require a restart of the middle-tier servers. For an end-user to access a workspace server from within the SAS Visual Analytics applications, it must be registered with the Web Infrastructure Platform (WIP) Job Execution Service (JES). Whenever security changes are made to these workspace servers, it is strongly recommended that the SAS Web Application Servers be restarted to help insure that JES, and therefore the SAS Visual Analytics applications, pick up the change.

Third, the convenience features that load data into the applications are currently designed to work with one common server. SAS Visual Analytics 6.2 introduced a new, default SAS LASR Analytic Server called the Public LASR server to help end-users upload their own data. While it is possible to pattern new, departmental servers after this common server, there are restrictions for both the interactive and batch convenience features.

"Import Data" is a new interactive convenience feature of SAS® Visual Analytics Explorer, SAS® Visual Analytics Designer, and SAS® Visual Data Builder. It is meant to help end-users become more self-sufficient. When importing the data, power-users who have access to SAS Visual Data Builder will be able to select which metadata folder and in-memory data library to use in all three applications, and the data will be written to the SAS LASR Analytic Server associated with that library. However, end-users who do not have access to SAS Visual Data Builder, who are denied

the “Build data” capability in metadata, may only import table metadata to the Public LASR library or to their My Folder personal location and may only load the table to the Public LASR server. One global setting, `va.defaultWorkspaceServer`, indicates which application server context will be used for this feature for all users. It is not possible to specify different application server contexts for each department.

“Autoload” is a batch convenience feature of SAS Visual Analytics. By default, the Public LASR server and its associated libraries are configured to read data from local system files and upload them at regular intervals, usually every fifteen minutes. End-users may copy their data to the autoload, append, or unload folders, depending on what action they want to perform. The Public LASR and autoload folders are configured automatically. They grant full access to all SAS Visual Analytics end-users by default.

To departmentalize the data, the administrator can manually create additional autoload configurations. After defining a new application server context, if needed, the administrator must create the SAS LASR Analytic Server, the library with its extended attributes, and the metadata folders using SAS Management Console. He must also create and secure the appropriate system folders as well as the script files. Each of these steps is documented in the *SAS® Visual Analytics Administration Guide*. End-users who do not have the capability to load data from within SAS Visual Data Builder applications could still write the data to these folders and have it uploaded within a scheduled interval. As long as the data persists in these locations, it can be reloaded whenever the SAS LASR Analytic Server restarts.

If the department has a workspace server configured for token authentication, the same common identity can be used to run the autoload batch job for that department. That configuration helps simplify metadata security, but it has an additional caveat. If that departmental workspace server has registered with the JES so that it can be used in SAS Visual Analytics web applications, the autoload batch job needs the Trusted User credentials to successfully make a connection as that common identity, and the SAS Trusted User or the SAS General Servers group must be granted permissions to departmental folders, libraries, and tables in metadata to perform uploads.

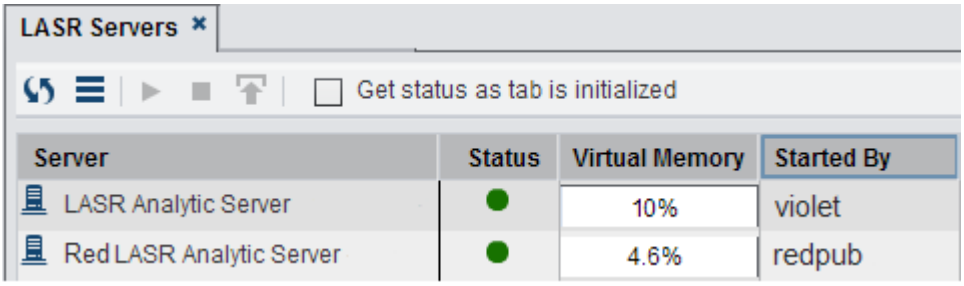
```
options METASERVER="metadata.host.com"
    METAPORT=8561
    METAREPOSITORY="Foundation"
    metauser="sastrust@saspw"
    metapass="{SAS002}ENCODEDPASSWORD";
```

**Display 5. Specifying SAS Trusted User Credentials in the autoload.sas Code**

Because of these restrictions, in this scenario the power-user has been given the “Build data” capability, and he is a valid user of the SAS Visual Data Builder. He also has passwordless ssh credentials and write permission to the signature file location for his department. He is barred from becoming the SAS Visual Analytics administrator, but while he cannot start SAS LASR Analytic Servers with that application, he can load and unload data. If the in-memory data library he uploads to is enabled for autostart, then when he loads data to it, the associated SAS LASR Analytic Server will start if it is not already running. The administrator can see the signature files that are created and owned by this power-user.

For our end-user, a new application server context was created with token authentication, as well as the supporting libraries, folders, and SAS LASR Analytic Server definition, to create a departmental autoload location. This end-user does not have passwordless ssh credentials, and he is denied access to the SAS Visual Data Builder and the SAS Visual Analytics administrator. He has permission to create and view reports only. He cannot import local data from the web applications; instead, he is allowed to upload data by placing it in the departmental autoload folder for his department. That data will be visible to any members of his department. The administrator can always determine who loaded the data by looking at the owner of the data sets in the autoload location.

The administrator has the ability to start any SAS LASR Analytic Server using the SAS Visual Analytics administrator. Because he uses a workspace server that is not configured for token authentication, he will start each server as himself. If a batch autoload job starts a server as a common identity or is started by the power-user, the administrator can see that clearly in the owner of the server signature files as well as in the SAS Visual Analytics administrator interface.




**Display 6. SAS Visual Analytics Administrator Shows Who Started Each LASR Server**

### JOBS AND RELOAD

There are two distinct ways in which tables that are autoloaded are different from those that are manually loaded. First, in-memory data that is loaded manually must be created from existing system tables that are registered in metadata. When data is uploaded by autoload, the source system data is not registered in metadata.

Second, when a query is run or data is loaded from within the SAS Visual Analytics administrator application, a corresponding job is created in the same location in metadata. That job enables the 'reload' option for the data in the SAS Visual Analytics administrator. Data that is uploaded via the autoload mechanism has no associated job. The data can only be reloaded by its persistence in the autoload folders.

These distinctions are important to keep in mind when designing end-user self-service. It may not be possible for the administrator to discern which raw data is missing, nor be able to reload it, when an end-user runs into trouble.

### HOW TO LIST ALL TABLES ON A SAS LASR ANALYTIC SERVER

In addition to specifying the SIGNER when loading data to LASR in batch mode, the table should be registered in metadata using the METALIB procedure. Otherwise, this table will be consuming resources on the SAS LASR Analytic Server, but it will not be visible to the SAS Visual Analytics applications.

```
proc metalib;
 omr(repname="Foundation" library="metadata-name-of-library");
select (tablename);
run;quit;
```

To see if any tables were loaded but not registered, use the LASR, VASMP, or DATASETS procedures:

**Distributed LASR Servers**

```
proc lasr details port=10010;
performance host="the.host.com";
run;
```

**Non-Distributed LASR Servers**

```
proc vasmp;
tableinfo / port=10010;
run;quit;
```

**Both Distributed and Non-Distributed LASR Servers**

```
libname lasrlib sasiola PORT=10010 HOST="grid.host.com" tag=tag;
proc datasets lib=lasrlib;
run;quit;
```

## CONCLUSION

From our experiences in testing SAS Visual Analytics, CET has several recommendations for making the administration of the environment easier. First, create distinct metadata locations for table registrations so that users do not confuse system and in-memory data. Second, apply system settings as well as metadata permissions to protect SAS LASR Analytic Servers and in-memory data. Third, configuring departmentalized, self-service uploads using common identities has some restrictions, but it can make restricted end-users more self-sufficient.

## REFERENCES


SAS Institute Inc. 2013. *SAS® 9.4 Intelligence Platform: Security Administration Guide, Second Edition*. "Mediated Access", page 84. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/cdl/en/bisecag/67045/PDF/default/bisecag.pdf

SAS Institute Inc. 2013. *SAS® 9.4 Intelligence Platform: Security Administration Guide, Second Edition*. "SAS Token Authentication", page 136. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/cdl/en/bisecag/67045/PDF/default/bisecag.pdf

SAS Institute Inc. 2013. *SAS® LASR™ Analytic Server 2.1: Administration Guide*. "Signature Files", page 5. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/solutions/lasrserver/inmsag21.pdf.

SAS Institute Inc. 2013. *SAS® Visual Analytics 6.3: Administration Guide*. "How to Add an Implementation [of Autoload]", page 18. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/solutions/va/6.3/vaag.pdf

SAS Institute Inc. 2013. *SAS® Visual Analytics 6.3: Administration Guide*. "Permissions by Task", page 27. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/solutions/va/6.3/vaag.pdf

SAS Institute Inc. 2013. *SAS® Visual Analytics 6.3: Administration Guide*. “Signature Files”, page 50. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/solutions/va/6.3/vaag.pdf

SAS Institute Inc. 2013. *SAS® Visual Analytics 6.3: Administration Guide*. “Scenario: Multiple Levels of Host Access”, page 56. Cary, NC: SAS Institute Inc. Available at http://support.sas.com/documentation/solutions/va/6.3/vaag.pdf

## ACKNOWLEDGMENTS

The author gratefully acknowledges Steve Clark of SAS Institute for reviewing the technical content of this paper. Thanks.

## RECOMMENDED READING

Several of these documents are only available if you have purchased the products:

- *SAS® 9.4 Intelligence Platform: Security Administration Guide, Second Edition*. Available at http://support.sas.com/documentation/cdl/en/bisecag/67045/PDF/default/bisecag.pdf
- *SAS® Visual Analytics 6.3: Administration Guide*. Available at http://support.sas.com/documentation/solutions/va/6.3/SAS Visual Analytics Administratorg.pdf
- *SAS® High-Performance Analytics Infrastructure 2.4: Installation and Configuration Guide.* Available at http://support.sas.com/documentation/solutions/hpainfrastructure/24/hpaicg24.pdf
- *SAS® High-Performance Analytics Server 12.2: User’s Guide*. Available at http://support.sas.com/documentation/solutions/hpa/122/hpaug.pdf
- *SAS® LASR™ Analytic Server 2.1: Administration Guide*. Available at http://support.sas.com/documentation/solutions/lasrserver/inmsag21.pdf.
- *SAS® LASR™ Analytic Server 2.2: Reference Guide*. Available at http://support.sas.com/documentation/cdl/en/inmsref/67213/PDF/default/inmsref.pdf
- *SAS® Visual Analytics 6.3: Installation and Configuration Guide*. Available at http://support.sas.com/documentation/solutions/va/6.3/vaicg.pdf
- *SAS® Visual Analytics 6.3: User's Guide*. Available at http://support.sas.com/documentation/cdl/en/vaug/66720/PDF/default/vaug.pdf

## CONTACT INFORMATION

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

Dawn Schrader
100 SAS Campus Drive
Cary, NC 27513
SAS Institute Inc.
Dawn.Schrader@sas.com
http://www.sas.com