Gain Greater Insight into Your SAS® Software with SAS Books.

Discover all that you need on your journey to knowledge and empowerment.

support.sas.com/bookstore for additional books and resources.
## Contents

*Using This Book* ......................................................... vii  
*What's New* ................................................................. ix  
*Accessibility* ................................................................. xi

### PART 1  Fundamentals  1

**Chapter 1 / Getting Started** ........................................ 3
  Orientation ................................................................. 3
  Adding Users .............................................................. 5

**Chapter 2 / Loading Data** ........................................... 9
  About Loading Data .................................................... 10
  Self-Service Import ................................................... 11
  Reload-on-Start .......................................................... 15
  Interactive Load .......................................................... 17
  Autoload ........................................................................ 20

**Chapter 3 / Managing Access** ....................................... 29
  Setting Permissions ........................................................ 29
  Assigning Capabilities .................................................. 35

**Chapter 4 / Managing Servers** ...................................... 37
  Operate a SAS LASR Analytic Server .............................. 37
  Monitor a SAS LASR Analytic Server .............................. 38
  Add a SAS LASR Analytic Server .................................... 41
  Add a SAS LASR Analytic Library ................................... 43
  Manage Other Servers .................................................... 44

**Chapter 5 / Managing Devices** ..................................... 45
  About Managing Mobile Devices ..................................... 45
  How to Manage Mobile Devices ...................................... 45
  Change How Devices Are Managed ................................... 47
  About the Mobile Devices Tab ......................................... 47

### PART 2  Special Topics  49

**Chapter 6 / Security** .................................................. 51
  Data Security ............................................................... 51
  Row-Level Security ....................................................... 55
  Locked-Down Servers .................................................... 58
  Authentication and Encryption ......................................... 59
  Protections for Mobile Content ....................................... 61
# Contents

Passwordless SSH .................................................. 62

**Chapter 7 / Fine-Tuning** ........................................ 65
Supporting Guest Access ....................................... 66
Customizing Appearances .................................. 69
Customizing the Home Page .................................. 70
Managing Alerts and Notifications ...................... 72
Supporting Stored Processes .................................. 73
Supporting the Search Features ................................. 74
Supporting the Geo Map Features ................................. 75
Supporting User-Defined Formats ................................. 77
Supporting the Monitoring Features ...................... 77
Adjusting the Logging Configuration ................... 79
Thresholds for High-Cardinality Data .................. 81
User Preferences in the Administrator .................... 85
Designating a SAS Application Server .................... 86
Configuration Properties: SAS Mobile BI .................. 87
Configuration Properties: SAS Visual Analytics ....... 90

**Chapter 8 / Troubleshooting** .................................. 95
Troubleshooting: SAS Visual Analytics .................. 95
Troubleshooting: SAS Mobile BI ............................. 101
Permission Origins ............................................. 101

**Chapter 9 / SAS LASR Analytic Server** .................. 105
About SAS LASR Analytic Server ...................... 105
Depictions of Data Loading .................................. 106
Memory Usage: A Closer Look .................................. 110
LASR-Related Metadata Objects ............................... 110
How In-Memory Tables Are Identified .................. 112
Advanced Options: SAS LASR Analytic Server ........ 113
Extended Attributes: SAS LASR Analytic Server .......... 115
Reference: Predefined LASR Libraries ................. 115

**PART 3 Appendixes** ........................................ 119

**Appendix 1 / Reference: Roles and Capabilities** ........ 121
Predefined Roles ............................................. 121
Capability Descriptions .................................. 124

**Appendix 2 / Reference: Co-Located Data Providers** ...... 127
Co-Located Data Providers .................................. 127
Co-Located Hadoop ............................................. 127
Alternate Providers of Co-Located Data ................. 133

Glossary ................................................................. 135
Index ................................................................. 137
Using This Book

Audience

This book documents administrative tasks that are specific to SAS Visual Analytics. For additional technical resources for SAS Visual Analytics, see the SAS Visual Analytics page on the SAS support site.

Documentation Conventions

Short Forms of Selected Phrases

This book uses short forms of the following phrases:

<table>
<thead>
<tr>
<th>Long Form</th>
<th>Short Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Visual Analytics Administrator</td>
<td>the administrator</td>
</tr>
<tr>
<td>SAS Visual Analytics Explorer</td>
<td>the explorer</td>
</tr>
<tr>
<td>SAS Visual Analytics Designer</td>
<td>the designer</td>
</tr>
<tr>
<td>SAS Visual Analytics Graph Builder</td>
<td>the graph builder</td>
</tr>
<tr>
<td>SAS Visual Analytics Viewer</td>
<td>the web viewer</td>
</tr>
<tr>
<td>SAS Visual Data Builder</td>
<td>the data builder</td>
</tr>
<tr>
<td>distributed SAS LASR Analytic Server</td>
<td>distributed server</td>
</tr>
<tr>
<td>non-distributed SAS LASR Analytic Server</td>
<td>non-distributed server</td>
</tr>
<tr>
<td>SAS LASR Analytic Server library</td>
<td>LASR library</td>
</tr>
<tr>
<td>SAS LASR Analytic Server table</td>
<td>LASR table</td>
</tr>
<tr>
<td>library of the type SAS Data in HDFS</td>
<td>HDFS library</td>
</tr>
</tbody>
</table>
Host Paths and File Extensions

In general, this book presents host operating system information in UNIX style. Where applicable, you can substitute the Windows equivalent directory paths and file extensions.

In documentation of host paths, the phrase "SAS configuration directory" refers to a configuration name and level (for example, C:\sas\Config\Lev1 or /opt/sas/config/Lev1). For more information, see Overview of the Configuration Directory Structure in the SAS Intelligence Platform: System Administration Guide.

Secure Documentation

Some of the administrative and deployment documentation for SAS Visual Analytics is password protected and available to only licensed customers. To request access, see the instructions on the SAS Visual Analytics page on the SAS support site.
What’s New

SAS Visual Analytics 6.4 Administration

- On the LASR Tables tab, you can filter the display by user ID. See “About the Loaded By Column” on page 19.
- The metadata option that enables logging for a SAS LASR Analytic Server is supported for a non-distributed server (as well as for a distributed server). See “Advanced Options: SAS LASR Analytic Server” on page 113.
- On the Authorization page, the icon for an explicit setting is a yellow diamond (instead of a yellow star). See “About the Authorization Page” on page 34.
- New capabilities enable you to more granularly manage the availability of the self-service import functionality. See “Capability Descriptions” on page 124.
- A new configuration property enables you to specify how frequently the system verifies that alerts are running. See “va.Alert.EvaluationCycleMilliseconds” on page 73.
- New configuration properties enable you to limit the size of self-service imports. See “How to Limit Import Size” on page 14.
What's New
For information about the accessibility of any of the products mentioned in this document, see the usage documentation for that product.
Part 1

Fundamentals

Chapter 1
Getting Started ......................................................... 3

Chapter 2
Loading Data ................................................................. 9

Chapter 3
Managing Access ......................................................... 29

Chapter 4
Managing Servers ......................................................... 37

Chapter 5
Managing Devices ......................................................... 45
Getting Started

Orientation

Administrative Tasks

Administration of SAS Visual Analytics involves the following activities:

- Adding and managing users.
- Loading enterprise data to memory.
- Supporting users’ self-service imports.
- Managing the SAS LASR Analytic Server.
- Managing mobile devices by maintaining a blacklist or whitelist.
- Fine-tuning the configuration and troubleshooting any problems.

Note: For documentation about platform-level functionality, see the SAS Intelligence Platform page on the SAS support site.

SAS Visual Analytics

On the surface, SAS Visual Analytics is an integrated suite of web applications. The suite offers intuitive, drag-and-drop interactions; rapid, highly visual responses; and role-based access to functionality. See the SAS Visual Analytics: User’s Guide.
Behind the scenes, SAS LASR Analytic Server applies analytics to any amount of data. The server provides speedy, secure, multi-user access to in-memory data. See Chapter 9, “SAS LASR Analytic Server,” on page 105.

At the foundation, SAS Visual Analytics is built on the SAS Intelligence Platform, which provides a robust, metadata-centric environment for a wide range of business intelligence and analytic activities.

Software Components

Here is a simplified view of the architecture and process flows:

*Figure 1.1  Architecture and Process Flows*

Here is an introduction to selected components:

- **mobile viewers**
  - support native viewing and interacting with reports and dashboards on mobile devices.

- **web applications**
  - provide role-based access to an integrated suite of functionality.

- **SAS LASR Authorization Service**
  - enforces metadata-layer permissions before allowing access to data and server operations.

- **SAS Visual Analytics Transport Service**
  - enables communication from mobile devices.

- **SAS Information Retrieval Studio**
  - creates a searchable index.

- **Search Interface to SAS Content**
  - provides efficient, robust searching for certain types of objects.

- **SAS LASR Analytic Server**
  - provides secure, multi-user, concurrent access to in-memory data.
SAS LASR Analytic Server Monitor supports monitoring (for distributed servers) and HDFS browsing (for deployments that use co-located Hadoop).

SAS High-Performance Computing Management Console (not depicted) supports configuration of accounts for passwordless secure shell (SSH). This application runs on the root node of a distributed SAS LASR Analytic Server.

SAS Content Server stores digital content in the middle tier. SAS Visual Analytics reports are stored in the content server, explorations are not.

Here are some examples of how SAS Visual Analytics uses platform servers:

- The metadata server provides metadata management and authorization decisions.
- The pooled workspace server and the stored process server support geographic visualizations. The pooled workspace server also supports remote file system browsing (for the SAS Application Server) and viewing the results of a data query.
- The workspace server supports tasks such as registering tables, importing data, loading data, and starting or stopping the SAS LASR Analytic Server.
- The SAS DATA Step Batch Server (not depicted) supports scheduling queries in the data builder.

About SAS Visual Analytics Administrator

The main administrative tool, SAS Visual Analytics Administrator, supports tasks such as loading data, managing mobile devices, setting metadata-layer permissions, adding data to a co-located data provider, and managing SAS LASR Analytic Servers.

To open SAS Visual Analytics Administrator, click Manage Environment on the SAS Visual Analytics home page.

TIP For the direct URL, go to your equivalent of SAS-configuration-directory/Documents/Instructions.html on the middle-tier machine.

Note: The navigation pane provides a filtered view of your site’s metadata. Only certain object types are visible.

Note: In the workspace, each tab represents either an object that you opened (for example, a table) or a specialized function that you launched (for example, Mobile Devices).

Adding Users

Summary

To enable users to access SAS Visual Analytics, create metadata identities for them and assign them to groups as follows:
Assign administrators to the Visual Analytics Data Administrators group and (for user administrators) to the SAS Administrators group.

Assign data builders to the Visual Data Builder Administrators group.

Assign other users to the Visual Analytics Users group.

**TIP** Users who connect to only guest access URLs do not need metadata identities. See “Supporting Guest Access” on page 66.

### Membership Structure

The following figure depicts selected group and role relationships in the standard membership structure. Here are some details about the figure:

- Containers indicate nested group memberships. For example, the Visual Analytics Data Administrators group is a direct member of the Visual Analytics Users group.
- Bracketed text indicates role assignments. For example, the SASUSERS group is a direct member of the **Visual Analytics: Basic** role.

*Figure 1.2 Standard Membership Structure*

---

### How to Add a User

Here is one way to add a new user:

1. Identify or create an account that can access the metadata server.

   **Note:** In the simplest case, accounts are in the metadata server’s host. For example, a metadata server on Windows usually authenticates users against Active Directory.
2 On the **Plug-ins** tab in SAS Management Console, right-click **User Manager**, and select **New ▶ User**.

**Note:** If you do not yet have your own administrative account, log on as the initial unrestricted user (for example, sasadm@saspw).

3 On the **General** tab, enter a name.

4 On the **Groups and Roles** tab, add direct memberships for the new user:
   - If the user performs administrative tasks, move one or more of the following groups to the **Member of** list:
     - Visual Data Builder Administrators
       a group for users who perform data preparation tasks.
     - Visual Analytics Data Administrators
       a group for users who perform suite-level administrative tasks, such as starting the SAS LASR Analytic Server, loading data, and blacklisting mobile devices.
     - SAS Administrators
       a group for users who perform platform-level administrative tasks, such as user management.
   - If the user does not perform administrative tasks, move the Visual Analytics Users group to the **Member of** list.

5 On the **Accounts** tab, click **New** to add a login.
   a Enter the user ID for the account from step 1.
     - **Windows Specifics:** In the login, enter the user ID in a fully qualified format (**userID@domain.extension, domain\userID, or machine\userID**).
   b Do not store a password.
   c Select the **DefaultAuth** authentication domain.
     - **Note:** If web authentication is configured, see “Web Authentication” on page 59.
   d Click **OK**.

6 In the New User Properties window, click **OK** to save the new user.

7 If the user imports data, loads data, or starts and stops a SAS LASR Analytic Server, make sure that the requirements that are described in the following section are met.

---

**TIP** To facilitate integration with your environment, SAS supports alternate authentication mechanisms and provides a bulk-loading method for adding identity information to metadata. See the **SAS Intelligence Platform: Security Administration Guide**.

---

**Host Account Privileges**

Accounts that load data, import data, or start or stop a SAS LASR Analytic Server must meet the following requirements:

- The account must be able to authenticate to the server’s host.
Windows Specifics: The **Log on as a batch job** privilege on the computer that hosts the SAS object spawner is required. This privilege is a Windows local security policy. If you have an operating system group (such as SAS Server Users) that has this privilege, you can simply add the user’s account to that group.

UNIX Specifics: For a distributed server, the ability to authenticate to all of the machines in the cluster (using passwordless SSH) is required. See “Passwordless SSH” on page 62.

- The account must have Write access to the `va.monitoringPath/PIDs` directory (in order to start a server). See “va.monitoringPath” on page 92.
- The account must have Write access to the signature files directory. See “Signature Files” on page 53.
# Loading Data

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>About Loading Data</strong></td>
<td>10</td>
</tr>
<tr>
<td>Introduction</td>
<td>10</td>
</tr>
<tr>
<td>Convenience Features</td>
<td>10</td>
</tr>
<tr>
<td>Features by Data Type</td>
<td>10</td>
</tr>
<tr>
<td>Table and Column Names</td>
<td>11</td>
</tr>
<tr>
<td><strong>Self-Service Import</strong></td>
<td>11</td>
</tr>
<tr>
<td>Introduction</td>
<td>11</td>
</tr>
<tr>
<td>Requirement: User Privileges</td>
<td>11</td>
</tr>
<tr>
<td>Requirement: SAS/ACCESS</td>
<td>12</td>
</tr>
<tr>
<td>Optimization: Parallel Loading</td>
<td>12</td>
</tr>
<tr>
<td>How to Protect Imported Data</td>
<td>13</td>
</tr>
<tr>
<td>How to Hide an Import Action</td>
<td>14</td>
</tr>
<tr>
<td>How to Limit Import Size</td>
<td>14</td>
</tr>
<tr>
<td>Additional Considerations</td>
<td>14</td>
</tr>
<tr>
<td><strong>Reload-on-Start</strong></td>
<td>15</td>
</tr>
<tr>
<td>How Reload-on-Start Works</td>
<td>15</td>
</tr>
<tr>
<td>How to Enable Reload-on-Start</td>
<td>15</td>
</tr>
<tr>
<td>Additional Considerations</td>
<td>16</td>
</tr>
<tr>
<td>Reference</td>
<td>16</td>
</tr>
<tr>
<td><strong>Interactive Load</strong></td>
<td>17</td>
</tr>
<tr>
<td>Preparing for Interactive Load</td>
<td>17</td>
</tr>
<tr>
<td>How to Load Data Interactively</td>
<td>18</td>
</tr>
<tr>
<td><strong>Autoload</strong></td>
<td>20</td>
</tr>
<tr>
<td>How Autoload Works</td>
<td>20</td>
</tr>
<tr>
<td>The Autoload Directories</td>
<td>20</td>
</tr>
<tr>
<td>Timing of Autoload</td>
<td>21</td>
</tr>
<tr>
<td>How to Schedule Autoload</td>
<td>21</td>
</tr>
<tr>
<td>How to Unschedule Autoload</td>
<td>22</td>
</tr>
<tr>
<td>How to Add an Implementation</td>
<td>22</td>
</tr>
<tr>
<td>Additional Considerations</td>
<td>25</td>
</tr>
<tr>
<td>Reference</td>
<td>26</td>
</tr>
</tbody>
</table>
About Loading Data

Introduction

SAS Visual Analytics uses data that is loaded to memory in a SAS LASR Analytic Server. Any table that SAS can access (either directly or through a SAS/ACCESS engine) can be loaded. After a table is loaded, it remains in memory until the server stops or the table is explicitly unloaded.

To load data in the administrator using a simple point-and-click interface, see “Interactive Load” on page 17.

Convenience Features

The following convenience features can streamline the process of loading data:

- **Autostart** starts a server on demand as needed for data load and import requests. See “Autostart” on page 38.
- **Reload-on-start** reloads certain tables each time a server is started interactively. See “Reload-on-Start” on page 15.
- **Autoload** periodically synchronizes in-memory tables against a designated source directory. See “Autoload” on page 20.

Note: In the standard configuration, all of the convenience features are enabled for the general purpose (public) LASR library.

Features by Data Type

For each load method, the following table documents supported data types and explains how you can reload data.

Table 2.1 Features Matrix

<table>
<thead>
<tr>
<th>Load Method</th>
<th>SAS Data Set</th>
<th>Co-located Table</th>
<th>CSV, XLS, XLSX</th>
<th>DBMS</th>
<th>How to Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interactive load*</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Interactive reload.*</td>
</tr>
<tr>
<td>Data query</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Rerun the data query.**</td>
</tr>
<tr>
<td>Autoload</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Unload. Wait for the task to run.</td>
</tr>
<tr>
<td>Local import</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Reload-on-start or repeat the import.</td>
</tr>
<tr>
<td>Server import</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Repeat the import.</td>
</tr>
</tbody>
</table>

* Using the point-and-click interface in SAS Visual Analytics Administrator. See “How to Load Data Interactively” on page 18.
** As an alternative, you can schedule the data query in the data builder.

Here are some details about the preceding table:
The "Server import" row represents importing a SAS data set from a server, importing from Twitter, and importing from a supported third-party DBMS.

The "Co-Located Table" column represents data in a co-located data provider.

The "DBMS" column represents data in a remote (not co-located) data provider.

For information about importing data, creating data queries, and scheduling data queries, see the *SAS Visual Analytics: User’s Guide*.

Table and Column Names

In general, names can include spaces and special characters. Exceptions include the following:

- **SAS name limitations apply.** When data is imported as a local file or autoloaded, any character that is not supported by SAS is replaced with an underscore.

- **For interactions with third-party data sources and operating systems, third-party name limitations apply.**

- **For LASR table names, the period character (.) is not supported.** If you load a SAS data set that has a period in its name, the period is replaced with an underscore (_).

Self-Service Import

Introduction

Data imports that are performed in the designer, the explorer, or the data builder are referred to as self-service imports. This topic provides information to help an administrator support self-service imports. For user instructions, see the *SAS Visual Analytics: User’s Guide*.

Requirement: User Privileges

- Individual data source-specific capabilities affect the availability of all self-service import actions. In the designer and the explorer, the Import and Load Data capability is a prerequisite for all self-service imports. For example, users who perform self-service imports from Oracle should have both of the following capabilities:
  - Import and Load Data
  - Import from Oracle

- Self-service import actions load data to memory, so users must have appropriate metadata-layer access to the target LASR library, server, and folder. See *Table 3.2 on page 31*.

- Self-service import actions use a workspace server, so users must have appropriate host-layer access. See “Host Account Privileges” on page 7.
Requirement: SAS/ACCESS

For most data sources, self-service import requires a SAS/ACCESS engine.

- For importing local files, importing SAS data sets from a server, or importing from Twitter, no SAS/ACCESS engine is required.
- For other data sources, a SAS/ACCESS engine is required. On the workspace server machine, the corresponding SAS/ACCESS engine must be licensed, installed, and configured. For example, to perform a self-service import from Oracle, SAS/ACCESS Interface to Oracle is required.

Note: Imports from Salesforce use SAS/ACCESS Interface to ODBC and the Salesforce driver.

Optimization: Parallel Loading

Introduction

This topic addresses parallel loading for self-service import actions from data providers that support massively parallel processing (MPP) to distributed servers.

Parallel loading for self-service import actions is a specialized feature that requires advanced configuration. This feature is intended for sites that have already configured the SAS High-Performance Analytics Environment to support parallel data transfer from a remote data provider.

For a depiction, see "Distributed Server: Parallel I/O: Remote Data Provider" on page 108.

Software Prerequisites

Parallel loading for self-service import actions requires the SAS High-Performance Analytics infrastructure, configured for parallel loads from your remote data provider.

See the SAS High-Performance Analytics Infrastructure: Installation and Configuration Guide.

Metadata Configuration

1 Verify that the distributed server’s definition references the appropriate remote embedded process path. The path is created as part of setting up the SAS High-Performance Analytics infrastructure.

   a In SAS Management Console, right-click a distributed server, and select Properties. For example, on the Plug-ins tab, expand Server Manager, and right-click LASR Analytic Server.

   b On the Options tab, make sure that the High-Performance Analytics environment install location references a remote embedded process path (for example, /opt/TKGrid_REP).

Note: If you need to change the path, stop the server, make the change, and then start the server. See “Operate a SAS LASR Analytic Server” on page 37.
2 Configure a LASR library to perform parallel loading for self-service import actions from one or more remote data providers.

a Identify or create a LASR library. Assign the library to the distributed server from step 1. See “Add a SAS LASR Analytic Library” on page 43.

b On the library’s **Extended Attributes** tab, set one or more `VA.EP.Capable.engine-name` attributes to **Yes**. Here are the supported attributes:

- `VA.EP.Capable.Hadoop`
- `VA.EP.Capable.Greenplm`
- `VA.EP.Capable.Oracle`
- `VA.EP.Capable.Teradata`

**Note:** These extended attributes affect only self-service import actions from remote data providers that support parallel loading. These extended attributes do not affect the availability of parallel data transfer for other types of load actions.

3 If the remote data provider is Hadoop, make sure that required metadata about your files exists.

**Note:** Parallel loads from Hadoop rely on SAS metadata about your files. In general, you use the HDMD procedure to generate the metadata. If data is written to Hadoop by SAS, and the HDFS_METADIR= option is used, the Hadoop engine generates the required metadata. See **SAS/ACCESS Interface to Hadoop** and **HDMD Procedure** in **SAS/ACCESS for Relational Databases: Reference**.

4 Instruct users to specify the parallel load enabled library when they perform self-service imports from participating data providers.

**TIP** In the standard configuration, self-service import actions load data to the general purpose (public) library. Only users who have the Build Data capability can select another library.

---

**How to Protect Imported Data**

User access to each data source is controlled by that data source’s authorization system.

Each self-service import action loads a source table to memory. The in-memory copy of the data is not subject to access controls from the original data source’s authorization system. Instead, access to in-memory data is controlled by metadata-layer permissions. Unless permissions are set directly on a LASR table, permissions on the LASR table’s parent folder determine access.

The following guidelines apply:

- Users who have privileged access to source data should import that data to only a location that has appropriate metadata-layer protections.

- Users who have fine-grained, individual, identity-based access to source data should import that data to only a private location. For example, if UserA imports a source table that has salary information, and the source table has...
row-level controls that enable UserA to see only his salary, the in-memory version of the imported table contains only information about UserA.

If your deployment supports self-service import of sensitive data, use the following measures:

- Give self-service import capabilities to only users who understand and can conform to the preceding guidelines.
- Set up an appropriately protected output location (metadata folder) for each distinct level of access. Ensure that users who have self-service import capabilities load data to the appropriate location.

**TIP** In the initial configuration, self-service import actions load data to a general-purpose location. Users can instead select a private location (My Folder). Only users who have the Build Data capability can select other locations.

**How to Hide an Import Action**

In the initial configuration, all self-service import actions are visible to all members of the Visual Analytics Users group.

You can hide the self-service import actions that your deployment doesn’t support. For example, if your deployment does not include a SAS/ACCESS engine for Oracle, you might not want the self-service import action for importing from Oracle to be visible to users. To hide that action from all restricted users, remove the Import from Oracle capability from all roles.

**TIP** To remove a capability from a role, clear the capability’s check box on the role’s Capabilities tab in SAS Management Console. For a summary of which roles have which capabilities in the initial configuration, see Table A1.1 on page 122.

**How to Limit Import Size**

To prevent users from importing extremely large tables, you can set a maximum number of rows for self-service import actions. If the number of rows in a source table exceeds the limit, no data is imported. In the initial configuration, no limit is imposed. See “va.SelfService.ImportRowsHardCap” on page 91.

You can set a warning threshold for self-service import actions. If a user attempts to import source data that exceeds a specified number of rows (and does not exceed the maximum number of rows that can be imported), a warning message informs the user that the import might take a long time. The user can either continue the import or cancel the action. In the initial configuration, no limit is imposed. See “va.SelfService.ImportRowsSoftCap” on page 91.

**Additional Considerations**

- For self-service import actions from a DBMS, the server tag of the output LASR library must be valid as a libref. You cannot import to a LASR library that has a server tag with more than eight characters or more than one level.
For example, you cannot import to a LASR library that has a server tag of MyServerTag or user.sasdemo. See “Server Tags” on page 54.

- Self-service imports require a workspace server that supports the job execution service. See “Designating a SAS Application Server” on page 86.
- A library that supports parallel loads for a remote data provider cannot also support serial loads from that data provider.

### Reload-on-Start

#### How Reload-on-Start Works

Here is an example of how reload-on-start works:

1. In the explorer, a user initiates an import of a Microsoft Excel spreadsheet.
2. SAS places a copy of the source data in the data provider library that is the designated backing store for the target LASR library.
3. SAS loads the data to memory and creates a corresponding LASR table object in metadata.
4. If the server stops, all of the server's in-memory data is unloaded.
5. If the server is interactively restarted, the data is reloaded to memory from the designated backing store.

**Note:** The reload is driven by the LASR table object’s association to a LASR library that supports reload-on-start. That LASR library must be associated with a data provider library that contains a backing store copy of the original source data.

#### How to Enable Reload-on-Start

To automatically reload participating tables each time a server starts, enable reload-on-start as follows:

1. In SAS Management Console, right-click on a LASR library, and select Properties.
2. On the Options tab, in the Data provider library field, specify a Base SAS library. The specified library functions as the backing store for data that users import from their computers (self-service imports of local files).
3. On the Extended Attributes tab, set properties as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA.ReloadOnStart.Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>VA.ReloadOnStart.TableDefault</td>
<td>Yes</td>
</tr>
<tr>
<td>VA.ReloadOnStart.Method</td>
<td>Selective</td>
</tr>
</tbody>
</table>
4 (Optional) To selectively exclude a LASR table from participation, set the VA.ReloadOnStart.Enabled property to No on that table’s Extended Attributes tab.

Additional Considerations

- A table that is enabled for reload-on-start is reloaded only if all of the following additional requirements are met:
  - The table is eligible to participate in reload-on-start. See "Features by Data Type" on page 10.
  - The table is not in a My Folder metadata location. Or, the table is in the My Folder metadata location that belongs to the identity who starts the server.
    Note: Even an administrator who has access to another user’s My Folder metadata location cannot reload a table to that location using reload-on-start.
  - The identity that starts the server has metadata-layer access to the table, its parent folder, and its parent library. See “Permissions by Task” on page 31.
  - The identity that starts the server has host access to the table (in the associated data provider library).

- Reload-on-start occurs only when the SAS LASR Analytic Server is started interactively (by an explicit start request in the administrator or by a user action that triggers autostart).

- Only a Base SAS library can be used as a designated backing store for reload-on-start.

- If you enable reload-on-start for a library that contains sensitive data, you must protect the corresponding data provider library against unauthorized access.

Reference

Logging for Reload-on-Start

A log of reload actions is captured to the directory that is specified by the va.monitoringPath property. See "va.monitoringPath" on page 92.

Beneath the monitoring directory, the Logs directory contains a SAS log file (named reload_on_start_short-hostname_port.log) that documents submitted code and results.

Beneath the monitoring directory, the PIDs directory contains files that document process IDs.

Library-Level Attributes for Reload-on-Start

VA.ReloadOnStart.Enabled (No | Yes) specifies whether a LASR library supports reload-on-start. A No value for a library prevents participation by all of the library’s tables, regardless of any Yes values on the tables. For a new library, the value is No.
VA.ReloadOnStart.TableDefault (No | Yes)  
specifies whether tables that neither explicitly enable nor explicitly disable 
reload-on-start participate. For a new library, the value is No. Therefore, a 
table for which the extended attribute VA.ReloadOnStart.Enabled is not 
specified does not participate.

VA.ReloadOnStart.Method (All | Selective)  
affects table participation in reload-on-start.

All  causes all eligible tables to participate, regardless of any 
contradictory table-level settings.

Selective  causes any table-level settings (of 
VA.ReloadOnStart.Enabled) to be honored.

For a new library, the value is All.

Table-Level Attributes for Reload-on-Start

VA.ReloadOnStart.Enabled (No | Yes)  
affects whether the table participates in reload-on-start. For a new table, this 
attribute does not exist. Instead, table participation is determined by the 
library-level setting for VA.ReloadOnStart.TableDefault. If necessary, you 
can manually add the VA.ReloadOnStart.Enabled attribute to a table object. 
This table-level setting is effective only if both of the following conditions are 
met:

- reload-on-start is enabled for the parent library
- the parent library’s VA.ReloadOnStart.Method is set to Selective

Interactive Load

Preparing for Interactive Load

Register Tables

Note: Source tables must be registered in metadata before they can be 
interactively loaded in SAS Visual Analytics Administrator. The administrator’s 
interactive loading process relies on table and column information that is stored 
in the metadata.

1 In the Folders pane in SAS Visual Analytics Administrator, right-click on a 
library, and select Register and Update Tables.

Note: To register a new library, use SAS Management Console’s Data 
Library Manager plug-in.

2 In the Select Tables window, select the tables that you want to register. Click 
OK.

3 In the Register Tables window, make any necessary adjustments. Click OK.

Note: If you register a table that already exists in the specified metadata 
folder, that table’s metadata is updated.
Stage Tables

Note: In the context of SAS Visual Analytics Administrator, staging a table means adding the table to a co-located data provider. Not all deployments use a co-located data provider. The following example is for co-located Hadoop.

1. In the Folders pane in SAS Visual Analytics Administrator, locate the source table.

2. Right-click on the table, and select Add to HDFS.

3. In the Add Table window, make any necessary adjustments.
   
   Note: The Co-located Table section specifies output information. Select a library of the type SAS Data in HDFS.

4. Click OK.

How to Load Data Interactively

Load a New Table

1. In the main menu in SAS Visual Analytics Administrator, select LASR ▶ Manage Tables.

2. In the tab toolbar, click.

3. In the Load a Table window:
   
   a. Select the source table that you want to load to memory.
   
   b. In the LASR Table section, specify output information.
      
      Note: The metadata location that you select determines access to the loaded table. Each table inherits permissions from its parent folder.
   
   c. Click OK.
      
      Note: The table is loaded and remains in memory until the associated server stops or the table is explicitly unloaded.

      Note: A job object (named source-table-Load Job) is created to support reloading of the table. To deploy a job for scheduling, see the book Scheduling in SAS. If you edit a job, SAS Visual Analytics might not be able to use the job. In this circumstance, a new job is created when you reload the table.

   TIP You can also load a table from the Folders pane (right-click on a source table) or from the LASR Servers tab (right-click on a server).

Unload, Reload, or Delete Tables

1. In the main menu in SAS Visual Analytics Administrator, select LASR ▶ Manage Tables.

2. On the LASR Tables tab, select a table, right-click, and select the appropriate action.
Here are some details:

- Not all tables can be interactively reloaded. See "Features by Data Type" on page 10.
- An action is available only if it is applicable to the selected table. For example, only a table that is not currently loaded can be reloaded or deleted.
- The Unload action removes a table from memory, but it does not delete the corresponding metadata object.
- The Delete action deletes the metadata object that represents an in-memory table.
- The LASR Name column shows table names in the in-memory format server-tag.table-name. See Figure 9.7 on page 112.

Use a Different Source Table

Note: You might perform this specialized task if the original source table is missing.

1. In the main menu in SAS Visual Analytics Administrator, select LASR ▶ Manage Tables.
2. On the LASR Tables tab, select a table.
3. Right-click, and select Change Source.
4. Click Yes to dismiss the warning message.
   
   Note: If the replacement table differs from the original table in a way that affects a permission condition, data access problems can occur. To provide access, remove the permission condition from the LASR table. See “Set a Row-Level Permission Condition” on page 33.
5. In the Load a Table window, select the replacement table. Click OK.

Get Table Status

1. In the main menu in SAS Visual Analytics Administrator, select LASR ▶ Manage Tables.
2. Click on a table. The status indicator for the table is displayed.

   TIP  To populate the entire Status column, click in the tab’s toolbar.

About the Loaded By Column

On the LASR Tables tab in SAS Visual Analytics Administrator, you can filter the display by user ID. The Loaded by filter returns results for only tables for which the loaded status icon ( ) is displayed. Similarly, the Loaded By column contains user IDs for only tables for which the loaded status icon is displayed.

UNIX Specifics: The Loaded By column displays the user ID that loaded each table.

Windows Specifics: The Loaded By column displays the user ID that started each server instance.
Autoload

How Autoload Works

Autoload periodically synchronizes in-memory data against tables in a designated directory. Here is a summary of how autoload works:

1. A SAS program periodically scans the contents of a designated directory, which is referred to as the autoload data directory. The directory functions as a drop box for source tables.

2. After each scan, the SAS program synchronizes in-memory data against source tables in the autoload data directory as follows:
   - For each delimited file or spreadsheet, a corresponding source table (SAS data set) is created.
   - Source tables that are not already in memory are loaded.
   - Source tables that are newer than their corresponding in-memory tables are refreshed (unloaded and then reloaded).
   - Source tables that are in the Unload subdirectory and in memory when a run of autoload begins are unloaded in that run.
   - Source tables that are in the Append subdirectory and newer than their corresponding in-memory tables are appended to their corresponding in-memory tables. If a table in the Append subdirectory has no corresponding in-memory table, it is loaded as a new table.
     - Each Append table is also appended to its corresponding table in the autoload data directory. If no corresponding table exists, a new table is added to the autoload data directory.
     - To prevent redundant append actions, data in the Append subdirectory is compared to corresponding data in the autoload data directory. The append action is performed on only data in the Append subdirectory that is newer than its corresponding data in the autoload data directory.

Note: To ensure that refresh and append actions occur for only source tables that are newer than their corresponding in-memory tables, autoload compares file timestamps of source tables to load timestamps of corresponding in-memory tables.

The Autoload Directories

Autoload Data

In the standard configuration, autoload data directories are in the AppData branch of the SAS configuration directory:

/AppData/SASVisualAnalytics/VisualAnalyticsAdministrator/Autoload
Each autoload data directory has three required subdirectories (Append, Logs, and Unload).

Note: The scheduler account and anyone who places tables in these directories must have Read and Write access to these directories.

Autoload Scripts

In the standard configuration, autoload scripts directories are in the Applications branch of the SAS configuration directory:

/Applications/SASVisualAnalyticsVersion/VisualAnalyticsAdministrator/

Note: The scheduler account must have Read and Write access to the autoload scripts directory and its contents.

Timing of Autoload

The SAS program that performs autoload runs as a periodic scheduled task.

In the standard configuration, a new run of autoload is started every 15 minutes. The timing is controlled by a setting in the schedule script (schedule.sh or schedule.bat in the autoload scripts directory).

Here are some additional details:

- A new run of autoload starts only after the previous run is complete.
- Starting the associated SAS LASR Analytic Server does not trigger an immediate run of autoload.
- Stopping the associated SAS LASR Analytic Server does not stop autoload activity. If the server is down when a run of autoload begins, autoload starts the server.

UNIX Specifics: The interval clock starts on the hour. For example, if the interval is 15 minutes, then autoload runs on the hour and at 15, 30, and 45 minutes after the hour.

Windows Specifics: The interval clock starts when autoload is scheduled. For example, if the interval is 15 minutes, then autoload runs 15 minutes after the schedule script is invoked, and every 15 minutes thereafter.

How to Schedule Autoload

To start scheduled runs of autoload:

1. Identify or create a scheduler account.

   - The account must have the host privileges that are required to start a server, load data, and run a scheduled task. See “Host Account Privileges” on page 7.

   UNIX Specifics: The ability to run cron jobs is also required.

   - The account must have Read and Write access to the following directories and their contents:

     - the autoload data directory and its subdirectories (so that logs can be written and source tables can be read, appended, and deleted)
the autoload scripts directory and its subdirectories (so that logs and process IDs can be written)

- The account must have an individual metadata identity. See “Adding Users” on page 5.
  
  **Note:** This requirement reflects the standard configuration in which the account that schedules autoload is also used to run autoload.

- The account’s metadata identity must have sufficient metadata-layer access to load data to start the server and load data. See “Permissions by Task” on page 31.

2 Log on as the scheduler, and invoke schedule.sh (or schedule.bat).

  **TIP** You can reduce the schedule interval by editing the schedule script. For the purpose of validation, an interval of 2 minutes is suggested.

3 Verify that the scheduled task is running.

**Windows Specifics:** Access the **Task Scheduler** (for example, select **Start** ➤ **Control Panel** ➤ **Administrative Tools** ➤ **Task Scheduler**). Locate the task in the **Task Scheduler Library** (for example, **Visual Analyt Hi-Perf Cfg - Auto Load Scheduler**).

**UNIX Specifics:** Run the command: `crontab -l`

4 If you reduced the schedule interval, edit the schedule script again to reset the interval. The standard interval is 15 minutes.

### How to Unschedule Autoload

To stop the scheduled task, use the scheduler account to invoke unschedule.sh or unschedule.bat. Stopping autoload does not stop the associated SAS LASR Analytic Server.

### How to Add an Implementation

Each LASR library that supports autoload must have its own implementation of autoload. The standard configuration has two predefined implementations. See “Reference: Predefined LASR Libraries” on page 115.

The following example sets up an additional implementation of autoload for sales data.

1 Create a new autoload data directory as follows:

   ```
   autoload-data-branch/VASALES
   autoload-data-branch/VASALES/Append
   autoload-data-branch/VASALES/Logs
   autoload-data-branch/VASALES/Unload
   ```

2 Create a new autoload scripts directory.

   a Make a sibling copy of an existing autoload scripts directory. For this example, copy `autoload-scripts-branch/VALIBLA` (or your equivalent of that predefined existing scripts directory) to a new directory named `autoload-scripts-branch/VASALES`. 
In the new `autoload-scripts-branch/VAALES/Logs` directory, delete any copied files.

3 In the new `autoload-scripts-branch/VAALES` directory, edit the copied files as follows:

AutoLoad.sas

Change the `%LET AL_META_LASRLIB=` value to the metadata name of the new implementation’s LASR library. For example:

```sas
%LET AL_META_LASRLIB=SalesAutoload;
```

runsas.sh (or runsas.bat)

Beneath the `# Source level_env` comment, adjust the location of the environment script, if necessary. For example:

```
. /sas94/config/Lev1/level_env.sh
```

Edit the `FILENAME=`, `LOG_FILE=`, `LST_FILE=`, and `PID_FILE=` values to reference the new autoload scripts directory. For example:

```bash
FILENAME="autoload-scripts-branch/VAALES/AutoLoad.sas"
LOG_FILE="autoload-scripts-branch/VAALES/Logs/AutoLoad_#Y.#M.#D_#H.#M.#S.log"
LST_FILE="autoload-scripts-branch/VAALES/Logs/AutoLoad.lst"
PID_FILE="autoload-scripts-branch/VAALES/autoload.pid"
```

schedule.sh (or schedule.bat) and unschedule.sh (or unschedule.bat)

Edit the `RUNSAS_PATH=` value to reference the new implementation’s autoload scripts directory. For example:

```bash
RUNSAS_PATH="autoload-scripts-branch/VAALES/runsas.sh"
```

Windows Specifics: Change the name of the scheduled task. On Windows, each implementation must explicitly specify a unique name for its scheduled task. (For example, in one of the predefined implementations, the task name is "Visual Analyt Hi-Perf Cfg - Auto Load Scheduler".)

4 In SAS Management Console, identify or create a metadata folder for generated LASR table objects (in this example, `/Shared Data/SAS Visual Analytics/Autoload/SALES`).

5 In SAS Management Console, identify or create a LASR library that supports autoload. See “Add a SAS LASR Analytic Library” on page 43.

- The library’s name must exactly match the value that you entered in the AutoLoad.sas file in step 3 (in this example, SalesAutoload).
- The library must be in a metadata folder that has appropriate permission settings (in this example, `/Shared Data/SAS Visual Analytics/Autoload/SALES`).
- The library’s extended attributes must enable autoload. The following table depicts example values. See “Library-Level Attributes for Autoload” on page 26.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA.AutoLoad.AutoStart</td>
<td>Yes</td>
</tr>
<tr>
<td>VA.AutoLoad.Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>VA.AutoLoad.Location</td>
<td><code>autoload-data-branch/VAALES</code></td>
</tr>
</tbody>
</table>
TIP  A new library’s extended attributes are visible only after you save and then reopen the library.

6 Invoke the new scheduled task.

The following image depicts the new autoload directories. The new autoload data directory is above the new autoload scripts directory.

Display 2.1  Example: VASALES Implementation of Autoload
Note: For clarity, the preceding image omits directories that are not related to autoload.

Additional Considerations

- Not all tables can participate in autoload. See “Features by Data Type” on page 10.
- Autoload is supported for both distributed and non-distributed servers. However, you cannot autoload data from a co-located data provider.
- Autoload is not a simple mirroring of content from a physical directory to memory. Instead, autoload synchronization is driven by directory-based rules.
- A new log file is generated for each run. The autoloader-scripts/Logs directory must be periodically emptied.
- You cannot interactively reload an autoloaded table. You can instead interactively unload the table, and then wait for the next run of the autoload scheduled task, which refreshes (unloads and then reloads) the table.
- You cannot autoload multiple tables that have the same base name. For example, if the files abc.xls and abc.xlsx are placed in an autoload data directory, only one data set (abc.sas7bdat) is loaded.
- In a multi-machine deployment, autoload-related files are on the machine that hosts the workspace server.
- If you move a delimited file or spreadsheet from the autoload data directory to the Unload subdirectory, remember to also delete the file’s corresponding SAS data set (from the autoload data directory and, if applicable, from the Append subdirectory).
- A table that exists in both the autoload data directory and the Unload subdirectory is repeatedly loaded and unloaded by alternating runs of autoload.
- If the metadata name of a LASR library that supports autoload includes UTF-8 characters, the corresponding AutoLoad.sas program must be saved in UTF-8 encoding. (In the AutoLoad.sas program, the %LET AL_META_LASRLIB= parameter specifies the library’s metadata name.)
- All synchronization actions create and update corresponding LASR table objects as needed. However, autoload does not delete LASR table objects.
- Autoload runs a SAS session directly from SAS Foundation. To modify session behavior for autoload, set SAS options (such as SSLCALISTLOC or MEMSIZE) in an appropriate location. For the narrowest effect, set options in the runsas script (which is located in the autoload scripts directory).
Reference

Logging for Autoload

Table 2.2 Log Files

<table>
<thead>
<tr>
<th>Directory or File</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>autoload-data/Logs/autoload.sas7bdat</code></td>
<td>A data set that contains most of the messages from the SAS log. Each message has a timestamp.</td>
</tr>
<tr>
<td><code>autoload-scripts/Logs/autoload.log</code></td>
<td>The complete SAS log.</td>
</tr>
<tr>
<td><code>autoload-scripts/Logs/autoload.lst</code></td>
<td>Any list output that the autoload process generates.</td>
</tr>
<tr>
<td><code>autoload-scripts/Logs/autoload.dbg</code></td>
<td>The debug log (which exists only if debugging is enabled).</td>
</tr>
<tr>
<td><code>va.monitoringPath/Logs</code>**</td>
<td>The directory where server logs (for non-distributed servers that are started by autoload) are written.</td>
</tr>
</tbody>
</table>

* When a non-distributed server is started, the filename is in the format `smp_machine_port`.

** See “va.monitoringPath” on page 92.

The following process ID (PID) files are written to the `va.monitoringPath/PIDs/` directory. To view a process ID, use a text editor to open a process ID file.

- The PID file for the autoload process includes the name of the target library (for example, `autoload_VisualAnalyticsPublicLASR.pid`).
- The PID file for a non-distributed server autoload includes the prefix `smp_`, the machine name, and the host (for example, `smp_myhost_12345.pid`).

Note: An additional PID file (`autoload.pid`) represents an implementation’s runsas script. That PID file is written to the autoload scripts directory to prevent that implementation’s runsas script from starting again if it is already running.

Library-Level Attributes for Autoload

The following attributes support autoload:

`VA.AutoLoad.Location`

sets the autoload data directory. If you change the location, make sure you create the three required subdirectories (Append, Logs, and Unload). For a new library, the suggested value is `autoload-data-branch/LIBNAME`.

`VA.Default.MetadataFolder`

sets the metadata location for the LASR table objects that autoload generates. For a new library, the initial value is your equivalent of `/Shared Data/SAS Visual Analytics/Autoload`.

`VA.AutoLoad.Enabled (No | Yes)`

specifies whether the library supports any autoload features. For a new library, the value is `No`.

Note: Setting this attribute to `Yes` does not disable interactive loading. You can interactively load data to a library that supports autoload.
VA.AutoLoad.Sync.Enabled (No | Yes)  
specifies whether synchronization actions are enabled. This is a parent  
setting (and a prerequisite) for other "Sync." attributes. For a new library, 
the value is No.

To preview synchronization actions, set this value to No, run autoload, and 
then examine the autoload log file.

VA.AutoLoad.Sync.Import (No | Yes)  
specifies whether the import action is enabled. For a new library, the value is  
No.

VA.AutoLoad.Sync.Load (No | Yes)  
specifies whether the load action is enabled. For a new library, the value is 
No.

VA.AutoLoad.Sync.Refresh (No | Yes)  
specifies whether the refresh action is enabled. For a new library, the value is 
No.

VA.AutoLoad.Sync.Append (No | Yes)  
specifies whether the append action is enabled. For a new library, the value 
is No.

VA.AutoLoad.Sync.Unload (No | Yes)  
specifies whether the unload action is enabled. For a new library, the value is 
No.

VA.AutoLoad.Debug.Enabled (No | Yes)  
specifies whether debugging is enabled for autoload. For a new library, the 
value is No.

The following attribute is used by autoload (but is not exclusive to autoload):

VA.AutoLoad.AutoStart (No | Yes)  
specifies whether the associated SAS LASR Analytic Server starts on 
demand for load requests against this library. For a new library, the value is  
No.

To set these extended attributes, access a LASR library’s Properties dialog box 
in SAS Management Console. Changes take effect on the next run of autoload.

### Processing of Delimited Files and Spreadsheets

In general, autoload processes delimited files and spreadsheets in the same 
way that these files are processed during a self-service import in the data 
builder, explorer, or designer. For information such as supported file types, 
missing values, and valid names, see the SAS Visual Analytics: User’s 
Guide.

The following list documents differences:

- File size limitations for interactive import are not applicable to autoload.
- Autoload always reads column names from the first row and begins data 
  import on the second row.
- When you autoload a spreadsheet that has multiple worksheets, only the first 
  worksheet is loaded.
- Up to the first 500 rows are used to estimate the data format and length of 
  each column.
- For append actions, column data types and lengths in both files must match.
Setting Permissions

About Permissions

**Key Points**

Here are the key points about permissions:

- SAS Visual Analytics uses the platform’s metadata authorization layer to manage access to objects such as reports, explorations, tables, libraries, servers, and folders.

  **Note:** Some tasks, such as importing data, loading data, and operating servers require host access. See “Host Account Privileges” on page 7.

- Access to each object is displayed as part of the object’s properties. Not all permissions are relevant for all objects.

- In SAS Visual Analytics Administrator, you can set folder, library, table, and row-level permissions.

- The current release of SAS Visual Analytics does not support column-level permissions.

  **Note:** If a table is loaded by a user who lacks access to one or more columns, duplicate metadata entries are created for the unavailable columns. Do not set denials of the ReadMetadata permission on individual columns within a table.

- For simplicity, set permissions on folders, not on individual objects. Most objects (including tables) inherit permissions from their parent folders.
Note: To learn how to customize the metadata folder structure, see Working with SAS Folders in the SAS Intelligence Platform: System Administration Guide.

- For simplicity, assign permissions to groups, not to individual users. The broadest group is called PUBLIC. The SASUSERS group includes all registered users.

Note: To learn how to manage permissions systematically using access control templates, see Access to Metadata Folders in the SAS Intelligence Platform: Security Administration Guide.

- Do not block ReadMetadata access for the SAS Trusted User. The standard method of preserving access for that service identity is to grant the ReadMetadata permission to one of its direct parent groups, SAS System Services.

Permission Definitions

The following table documents the permissions that are relevant for SAS Visual Analytics:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Affected Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReadMetadata (RM)</td>
<td>View an object or folder. For example, to see an exploration, report, table, or library, you need the ReadMetadata permission for that object.</td>
</tr>
<tr>
<td>Read (R)</td>
<td>Read data. For example, to see any data within a LASR table, you need the Read permission for that table.</td>
</tr>
<tr>
<td>WriteMetadata (WM)</td>
<td>Edit, rename, set permissions for, or delete an object. To delete an object, you also need the WriteMemberMetadata permission for the object’s folder. The WriteMetadata permission affects the ability to create certain associations among objects.</td>
</tr>
<tr>
<td>WriteMemberMetadata (WMM)</td>
<td>Add or remove objects from a folder. To enable a user to interact with a folder’s contents, but not with the folder itself, grant the WriteMemberMetadata permission and deny the WriteMetadata permission.</td>
</tr>
<tr>
<td>Write (W)</td>
<td>Load, unload, and reload existing tables; append and delete rows; and edit computed columns.</td>
</tr>
<tr>
<td>Administer (A)</td>
<td>Stop a SAS LASR Analytic Server, and load new tables to a LASR library.</td>
</tr>
</tbody>
</table>
Permissions by Task

LASR Tables and Servers
The following table documents metadata-layer permissions for working with LASR tables and SAS LASR Analytic Servers.

Table 3.2 Permissions for Working with LASR Tables and Servers

<table>
<thead>
<tr>
<th>Task</th>
<th>Server</th>
<th>Library</th>
<th>Folder</th>
<th>Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read data</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, R</td>
</tr>
<tr>
<td>Append rows</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, R, W</td>
</tr>
<tr>
<td>Delete rows</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, R, W</td>
</tr>
<tr>
<td>Edit computed columns</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, R, W</td>
</tr>
<tr>
<td>Load or import a table*</td>
<td>RM</td>
<td>RM, R, WM, A</td>
<td>RM, R, WMM, W</td>
<td>-</td>
</tr>
<tr>
<td>Reload a table</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, R, WM, W</td>
</tr>
<tr>
<td>Unload a table</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, R, W</td>
</tr>
<tr>
<td>Start a server</td>
<td>RM</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Stop a server</td>
<td>RM, A</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Assign a library to a server</td>
<td>RM, WM</td>
<td>RM, WM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Register a table in metadata</td>
<td>-</td>
<td>RM, WM</td>
<td>RM, WMM</td>
<td>-</td>
</tr>
<tr>
<td>Update a table’s metadata</td>
<td>-</td>
<td>RM</td>
<td>RM</td>
<td>RM, WM</td>
</tr>
<tr>
<td>Delete a table from metadata</td>
<td>-</td>
<td>RM, WM</td>
<td>RM, WMM</td>
<td>RM, WM</td>
</tr>
</tbody>
</table>

* An initial load (or import) creates a new LASR table object. Read and Write permissions on the folder support actions against the new table.

Explorations and Reports
The following table documents metadata-layer permissions for working with reports and explorations.

Table 3.3 Permissions for Working with Reports and Explorations

<table>
<thead>
<tr>
<th>Task</th>
<th>Server</th>
<th>Table</th>
<th>Folder</th>
<th>Report</th>
<th>Exploration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a report or exploration</td>
<td>RM</td>
<td>RM, R</td>
<td>-</td>
<td>RM</td>
<td>RM</td>
</tr>
<tr>
<td>Print a report or exploration</td>
<td>RM</td>
<td>RM, R</td>
<td>-</td>
<td>RM</td>
<td>RM</td>
</tr>
<tr>
<td>Export a report or exploration</td>
<td>RM</td>
<td>RM, R</td>
<td>-</td>
<td>RM</td>
<td>RM</td>
</tr>
<tr>
<td>Modify a report or exploration</td>
<td>RM</td>
<td>RM, R</td>
<td>-</td>
<td>RM, WM</td>
<td>RM, WM</td>
</tr>
</tbody>
</table>
To create, update, or delete a report, access to the SAS Content Server is also required. See the SAS Intelligence Platform: Middle-Tier Administration Guide.

### Data Queries and LASR Star Schemas

The following table documents metadata-layer permissions for working with data queries and LASR star schemas.

**Table 3.4 Permissions for Working with Data Queries and LASR Star Schemas**

<table>
<thead>
<tr>
<th>Task</th>
<th>Server</th>
<th>Table</th>
<th>Folder</th>
<th>Report</th>
<th>Exploration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save a new query or schema</td>
<td>RM</td>
<td>RM</td>
<td>RM, WMM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Save a new query or schema</strong></td>
<td>RM</td>
<td>RM</td>
<td>RM, WMM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Run a query or schema</td>
<td>RM</td>
<td>RM</td>
<td>-</td>
<td>RM</td>
<td></td>
</tr>
<tr>
<td>Edit and save a query or schema</td>
<td>RM</td>
<td>RM</td>
<td>RM</td>
<td>RM, WM</td>
<td></td>
</tr>
<tr>
<td>Delete or rename a query or schema</td>
<td>RM</td>
<td>-</td>
<td>RM, WMM</td>
<td>RM, WM</td>
<td></td>
</tr>
</tbody>
</table>

* These tasks create new LASR tables, so the permission requirements for loading a LASR table must also be met. See Table 3.2 on page 31.

** This column refers to any source tables that are represented in metadata. To run a query or schema against a LASR table, Read permission for the LASR table is also required.

Read access to data in a LASR star schema is not affected by permissions for input tables. Instead, Read access to data in a LASR star schema is affected by the Read and ReadMetadata permissions for the output table or view. ReadMetadata permission for the associated server, library, and folder is also required. See the first row in Table 3.2 on page 31.

**Note:** You can set explicit access controls (including permission conditions) on the output table or view for a LASR star schema. Any explicit access controls persist when you rerun the LASR star schema.

### Set an Explicit Grant or Denial

To set an explicit grant or denial in SAS Visual Analytics Administrator:

1. Right-click on an object in the **Folders** pane, and select **Authorization**.

2. In the **Effective Permissions** table, locate the identity to which you want to assign an explicit control. If the identity is not listed, click **+** to open the Add Identities window.

**Note:** In the Add Identities window, only user administrators can successfully search by user ID. Regular users cannot see other users’ IDs.

**Note:** An explicit grant of the ReadMetadata permission is automatically set for each identity that you add.
Double-click on a cell. From the cell’s drop-down list, select either **Deny** or **Grant**. Notice that the cell contains an explicit control indicator ◆.

**Note:** If the selected identity is an unrestricted user, all permissions are granted and you cannot make changes.

If you changed a group’s access, review the impact on the other listed identities. Controls that you add for a group can affect access for all members of that group.

In the toolbar at the top of the tab, click ✨.

**TIP** For alternate methods for setting permissions, see the *SAS Intelligence Platform: Security Administration Guide*.

---

**Set a Row-Level Permission Condition**

To limit Read access to rows in a LASR table:

1. In the **Folders** pane in SAS Visual Analytics Administrator, right-click on a LASR table, and select **Authorization**.

2. In the **Read** column, double-click on the cell for the identity whose row-level access you want to constrain. (Or, if the identity is not listed, click ✨ at the right edge of the table.)

   **Note:** An explicit grant of the ReadMetadata permission is automatically set for each identity that you add.

3. From the cell’s drop-down list, select **Conditional grant**.

   **Note:** If **Conditional grant** is not in the drop-down list, the table doesn’t support row-level security. Only LASR tables support row-level security.

   **Note:** If **Conditional grant** is already selected, select **Conditional grant** again to view or edit the existing condition.

4. In the New Permission Condition window, create a condition that specifies which rows the identity can see.

   - Conditions from releases prior to 6.2 or from batch tools use a basic editor. In the basic editor, syntax is not validated. See “Syntax (Basic Editor, Batch)” on page 56.

   - Other conditions use an enhanced editor.

     - On the **Visual** tab, you can drag and drop operators and data items from the left panes.

       **Note:** When you enter values, do not enclose them in quotation marks. The editor adds any necessary quotation marks for you.

     - On the **Text** tab, only the syntax and operators that are available on the **Visual** tab are supported.

5. Click **OK**. Notice that the cell contains the conditional grant icon ✨ with an explicit control indicator ◆.
6 If you set a permission for a group, review the impact on the other listed identities. Constraints that you add for a group can affect access for all members of that group.

7 In the toolbar at the top of the tab, click 📂.

**TIP** When you test conditions in another SAS Visual Analytics application (such as the explorer), refresh the data source in that application (so that your changes are reflected). See “Caching” on page 53.

A permission condition constrains Read access to rows within a LASR table. For more information, see “Row-Level Security” on page 55.

### About the Authorization Page

Here are some details about the **Authorization** page:

- Each object’s **Authorization** page describes access to that object. The displayed effective permissions are a calculation of the net effect of all applicable metadata-layer permission settings. To identify the source of an effective permission, double-click on its cell, and select **Show Origins** from the drop-down list. See “Permission Origins” on page 101.

- Icons indicate grants ☑️, conditional (row-level) grants 🟥, and denials ✗.

- The explicit indicator icon ☑️ indicates an access control that is explicitly set on the current object and explicitly assigned to the selected identity.

- The ACT indicator icon ■ indicates an access control that comes from an applied ACT whose pattern assigns the grant or denial to the selected identity.

- In combination, icons provide information as follows:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑️</td>
<td>Grant from an explicit control</td>
</tr>
<tr>
<td>☑️■</td>
<td>Grant from a directly applied ACT</td>
</tr>
<tr>
<td>☑️</td>
<td>Grant from an indirect source (such as a parent group or parent object)</td>
</tr>
<tr>
<td>🟥</td>
<td>Conditional grant from an explicit control</td>
</tr>
<tr>
<td>🟥■</td>
<td>Conditional grant from an indirect source (a parent group)</td>
</tr>
<tr>
<td>✗■</td>
<td>Denial from a directly applied ACT</td>
</tr>
<tr>
<td>✗</td>
<td>Denial from an indirect source (such as a parent group or parent object)</td>
</tr>
</tbody>
</table>
To compare permissions for two tables, open them both, and then select View \(\rightarrow\) Tab Layout \(\rightarrow\) Stacked from the main menu bar.

### Assigning Capabilities

#### About Capabilities

Here are the key points about capabilities:

- Unlike permissions, which affect access to data, content, and metadata, capabilities affect access to application functionality.
- Capabilities are assigned to roles. Users get their capabilities through their memberships. See "Membership Structure" on page 6.
- You can’t deny a capability to a user. Instead, make sure that user is not a member of any role that provides the capability. See the SAS Management Console: Guide to Users and Permissions.

#### Create a Custom Role

If the predefined distribution of capabilities is not optimal for your environment, consider creating custom roles. Here are some tips:

- If you create a specialized administrative role, remember to provide the Manage Environment capability in addition to any specific functional capabilities.
- If you create a global administrative role, make the Visual Analytics: Administration role a contributing role for the new custom role. In addition, add the Build Data capability to the custom role.
Managing Servers

**Operate a SAS LASR Analytic Server**
- Get Server Status .................................................. 37
- Start a Server Interactively .................................. 37
- Autostart ............................................................... 38
- Stop a Server .......................................................... 38
- Set Server Properties .............................................. 38

**Monitor a SAS LASR Analytic Server**
- Memory Gauges ...................................................... 38
- Resource Monitor ..................................................... 39
- Process Monitor ....................................................... 40

**Add a SAS LASR Analytic Server**
- Introduction .......................................................... 41
- Instructions .............................................................. 42

**Add a SAS LASR Analytic Library**
- Introduction .......................................................... 43
- Instructions .............................................................. 43

**Manage Other Servers** .............................................. 44

---

**Operate a SAS LASR Analytic Server**

**Get Server Status**

1. In the main menu bar in SAS Visual Analytics Administrator, select LASR ▶ Manage Servers.

2. Click on a server. The status indicator for the server is displayed.

**TIP** To populate the entire Status column, click ⬤.

**Start a Server Interactively**

To start a server interactively:

1. In the main menu bar in SAS Visual Analytics Administrator, select LASR ▶ Manage Servers.
2 Select a server, right-click, and select Start.

Autostart

To start a SAS LASR Analytic Server on demand, enable autostart on one or more of the server’s associated LASR libraries. Requests to load or import data to an autostart-enabled LASR library cause the associated server to start.

Note: The requesting identity must have the required privileges. The server must not be already running. Running a query in the data builder does not trigger autostart.

To enable autostart for a server:

1 In SAS Management Console, right-click on an associated LASR library, and select Properties.
2 On the Extended Attributes tab, set the value of the VA.AutoLoad.AutoStart property to Yes.

Note: One of the uses of autostart is to facilitate autoload. You can use autostart independently of autoload.

Stop a Server

By default, a SAS LASR Analytic Server runs forever. See “Server lifetime” on page 114.

To stop a server, right-click on the server on the LASR Servers tab, and select Stop.

When you stop a server, any in-memory tables for that instance are unloaded. Restarting the server reloads only tables that participate in reload-on-start. See “Reload-on-Start” on page 15.

Set Server Properties

To set properties for a SAS LASR Analytic Server, use SAS Management Console. Right-click on the server, and select Properties.

TIP The properties that enable autostart, reload-on-start, autoload, and parallel import are library-level properties, not server-level properties.

Monitor a SAS LASR Analytic Server

Memory Gauges

For a distributed server, an overall memory gauge is displayed in the main menu bar in SAS Visual Analytics Administrator. The overall gauge indicates how much of the server host’s total physical memory is currently in use. The overall gauge is refreshed every minute.
Here are some details:

- If a specified percentage of memory is used, the server rejects requests to load tables or append rows. See “Memory Limits” on page 113.

- The gauge provides information for only the distributed SAS LASR Analytic Server that is referenced in the service.properties file in the SAS configuration directory (at /Applications/SASVisualAnalyticsVersion/HighPerformanceConfiguration).

  Note: This constraint also applies to memory usage information on the Monitor tabs and the LASR Servers tab.

- Individual memory gauges are displayed in the Memory column on the LASR Servers tab. Each individual gauge indicates how much of the cluster’s total virtual memory is being used by a particular server instance (process). The individual gauges are refreshed every minute after the LASR Servers tab is opened.

- The calculation behind the overall memory gauge differs from the calculation behind the individual memory gauges. For details, see “Memory Usage: A Closer Look” on page 110.

**Resource Monitor**

For a distributed server, you can monitor resource utilization by selecting LASR Monitor Resources in the main menu bar in SAS Visual Analytics Administrator.

In the upper half of the Resource Monitor tab, the Utilization History graph plots utilization against time as follows:

- CPU and memory utilization are plotted as percentages of capacity. Under high demand, the upper bound can reach 100%. Under low demand, the upper bound can drop below 10%.

- Network input and output utilization is displayed as two line plots. The plots show the transfer rate in megabytes per second.

To view resource utilization for a particular sampling period, place your pointer over a line. To select that sampling period in the entire display, click a line. You can then place your pointer over the sampling period on each line to view details.

In the lower half of the Resource Monitor tab, the Real-Time View heat map contains a column for each machine in the cluster. To view the host name and details, place your pointer over a cell.

- The top and middle sections show CPU utilization and memory utilization, respectively. The color reflects the workload (more saturated color indicates heavier use).

- The bottom section shows network output transfer rate (in the first row) and network input transfer rate (in the last row). The color reflects the transfer rate between 0 and 25 megabytes per second. If the transfer rate exceeds 25 MBps, the color is purple.
Process Monitor

For a distributed server, you can monitor per-process utilization by selecting LASR » Monitor Processes in the main menu bar in SAS Visual Analytics Administrator.

At the top of the Process Monitor tab, the Selection and Filter controls enable you to specify which server instances to display.

The Process Monitor tab displays two graphs:

- **Memory Utilization versus CPU Utilization**
  Each server instance is represented by a bubble. The size of the bubble represents the number of processes for that instance. The location of the bubble indicates the resource utilization for that instance. Ideally, an instance has one process for each machine in the cluster.

- **CPU and Memory Utilization by Instance**
  Each bar shows CPU and memory utilization for a server instance. If a bar is vertically divided, CPU utilization is shown in the lower section, and memory utilization is shown in the upper section.

To view details, place your pointer over a bubble or a bar. For machine-level information, click on a bubble or bar. A window lists host names, ranks the hosts (by the column that you most recently sorted), and shows used memory and
CPU. For table-level information, click **Show tables** within the window. The window lists loaded tables, the user ID of the person who loaded them, and the number of rows and columns in each table.

**Note:** The per-process utilization is calculated from the traditional systems perspective. See “Memory Usage: A Closer Look” on page 110.

---

**Add a SAS LASR Analytic Server**

**Introduction**

This topic explains how to define an additional instance of a SAS LASR Analytic Server in metadata. Adding a server instance facilitates separation for management and ease-of-use purposes.

- Each server instance has a unique, multi-user connection to the hardware on which the SAS LASR Analytic Server process runs.
- Each server instance has a distinct set of associated LASR libraries and provides access to only those tables that are in an associated LASR library.
Instructions


3. Enter a name for the server. Click Next.

4. Set properties as follows:

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single machine server</td>
<td>For a distributed server, select No. For a non-distributed server, select Yes.</td>
</tr>
<tr>
<td>High-Performance Analytics environment install location</td>
<td>Specify the host path where files that define the cluster are located (for example, /opt/TKGrid). This field is applicable to a distributed server only.</td>
</tr>
<tr>
<td>Number of machines to use</td>
<td>Accept the default value (ALL). This field is applicable to a distributed server only.</td>
</tr>
</tbody>
</table>

Click the Advanced Options button.

5. In the Advanced Options window, select the Additional Options tab. Make sure that Signature files location on server field references a directory that has appropriate host protection. See “Signature Files” on page 53.

Note: For information about the other advanced options, see “Advanced Options: SAS LASR Analytic Server” on page 113.

When you are finished setting advanced options, click OK in the Advanced Options window. In the wizard, click Next.

6. Enter connection properties as follows. Click Next.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>Enter a unique port number. See “How In-Memory Tables Are Identified” on page 112.</td>
</tr>
<tr>
<td>High-Performance Analytics environment host</td>
<td>Enter the fully qualified machine name of the host (for example, va.abc.com).</td>
</tr>
<tr>
<td>Use LASR authorization service</td>
<td>Leave this check box selected. See “SAS LASR Authorization Service” on page 51.</td>
</tr>
</tbody>
</table>

7. If you want to adjust the default grants of the Administer permission that the wizard applies to the server, move identities from one list to the other. Click Next.
Add a SAS LASR Analytic Library

Introduction

Here are the main reasons for creating a new LASR library:

- You want additional separation for management or ease-of-use purposes.
- You use co-located Hadoop, and you added a new directory within that provider. You already created the new library for your co-located data provider. Now, you need to create the corresponding LASR library.

Instructions

To create a new LASR library:


2. In the New Library wizard, select High-Performance Analytics ▶ SAS LASR Analytic Server Library. Click Next.

3. Enter a name (for example, Sales LASR). If necessary, adjust the location. Click Next.

4. It is not necessary to assign the library to a SAS Application Server. Click Next.

   Note: In SAS Visual Analytics, user preferences and a configuration property determine which SAS Application Server is used for interactions with LASR libraries. See “Designating a SAS Application Server” on page 86.

5. Set library properties as follows. Click Next.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Libref</td>
<td>Enter an identifier of your choice (for example, SALESLIB).</td>
</tr>
<tr>
<td>Engine</td>
<td>This field is not editable. The value (SASIOLA) is the engine name for LASR libraries.</td>
</tr>
<tr>
<td>Server tag</td>
<td>See “Server Tags” on page 54.</td>
</tr>
</tbody>
</table>
Data provider library

If you want locally imported files to be reloaded when the associated server starts, specify a Base library to function as the backing store for this LASR library. See “Reload-on-Start” on page 15.

6 Assign the library to a SAS LASR Analytic Server by entering settings as follows. Click Next.

<table>
<thead>
<tr>
<th>Database Server</th>
<th>Select a server from the drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>Use the pre-selected value (which prepends the selected server name with the string Connection:).</td>
</tr>
<tr>
<td>Default Login</td>
<td>This field is not editable. The value is None.</td>
</tr>
</tbody>
</table>

7 If you want to adjust the default grants of the Administer permission that the wizard applies to the library, move identities from one list to the other. Click Next.

Note: Only users who have the Administer permission for the library can load new tables to memory. The library inherits settings from its parent folder, so it might not be essential to add any explicit grants.

8 Click Finish.

9 (Optional) If you want the associated server to start on demand for data load and import requests against the new library, enable autostart for the library. See “Autostart” on page 38.

10 (Optional) If you want locally imported files to reload each time the associated server restarts, enable reload-on-start for the library. See “Reload-on-Start” on page 15.

11 (Optional) If you want to automatically synchronize the library’s in-memory data against source tables in a host directory, set up a corresponding implementation of autoload. See “Autoload” on page 20.

Manage Other Servers

In addition to the SAS LASR Analytic Server, SAS Visual Analytics uses middle-tier, metadata, and compute servers that are provided by the underlying platform. For an overview, see “Software Components” on page 4.

For instructions, see Operating Your Servers in the SAS Intelligence Platform: System Administration Guide.
Managing Devices

About Managing Mobile Devices

How to Manage Mobile Devices

Blacklist a Device

Whitelist a Device

Determine Which List Is Enforced

Determine When a Device Was Blacklisted

Change How Devices Are Managed

About the Mobile Devices Tab

About Managing Mobile Devices

Here are the key points:

- To manage devices that use SAS Mobile BI, select Tools » Manage Devices from the main menu in SAS Visual Analytics Administrator. You can manage devices either by exclusion or by inclusion.

- If you manage by exclusion, all devices can use SAS Mobile BI, except those that are on the blacklist.

- If you manage by inclusion, only devices that are on the whitelist can use SAS Mobile BI.

- A deployment enforces only one list (either the blacklist or the whitelist). In a new deployment the blacklist is enforced, so there are no device-level barriers to participation.

- You can modify both lists. Making changes to a list that is not currently enforced can help accommodate a future change.

- These lists affect devices, not users. To manage what a particular user can see or do in SAS Mobile BI, use permissions and capabilities.

How to Manage Mobile Devices

Blacklist a Device

Note: These instructions have an effect only if the blacklist is enforced.
To prevent a mobile device from using SAS Mobile BI:

1. In the main menu bar, select **Tools > Manage Devices**.
2. On the **Mobile Devices** tab, select the **Blacklist** tab.
3. At the right edge of the tab, click **+**.
4. In the **Add Device To Blacklist** window, enter the ID of the device that you want to exclude from using SAS Mobile BI. (Or, to add multiple device IDs, click **Add List**.) Click **OK**.

   **Note:** The information that you supply is not validated by the software.

   **TIP** For a device that has already connected (or attempted to connect), you can initiate this task from the **Logon History** tab. Select the device, right-click, and select **Add to Blacklist**.

To remove a device from the blacklist, select it on the **Blacklist** tab, right-click, and select **Move to Whitelist**.

### Whitelist a Device

Note: These instructions have an effect only if the whitelist is enforced.

To enable a mobile device to use SAS Mobile BI:

1. In the main menu bar, select **Tools > Manage Devices**.
2. On the **Mobile Devices** tab, select the **Whitelist** tab.
3. At the right edge of the tab, click **+**.
4. In the **Add Device To Whitelist** window, enter the ID of the device that you want to enable to use SAS Mobile BI. (Or, to add multiple device IDs, click **Add List**.) Click **OK**.

   **Note:** The information that you supply is not validated by the software.

   **TIP** For a device that has already connected (or attempted to connect), you can initiate this task from the **Logon History** tab. Select the device, right-click, and select **Add to Whitelist**.

To remove a device from the whitelist, select it on the **Whitelist** tab, right-click, and select **Move to Blacklist**.

### Determine Which List Is Enforced

In the toolbar at the top of the **Mobile Devices** tab, the **Enforced** drop-down list indicates which list is enforced.

In addition, text at the top of either the **Blacklist** tab or the **Whitelist** tab indicates the list that is not currently enforced.

**TIP** You can also verify the current configuration in SAS Management Console. The blacklist is enforced unless the
Determine When a Device Was Blacklisted

Here is one way to determine when a device was blacklisted:

1. On the **Blacklist** tab, right-click on the device, and select **Copy Device ID**.
2. On the **Management History** tab, select **Device ID** from the **Filter** drop-down list.
3. Click in the text field, and enter Ctrl+V from the keyboard. (You cannot perform the paste action from the pop-up menu.)
4. Click **Apply**.

**TIP** You can also copy a device ID from the **Whitelist** tab. You can also paste a device ID into the **Device ID** filter on the **Logon History** tab.

Change How Devices Are Managed

**CAUTION!** These are deployment-level instructions that affect all access to SAS Mobile BI.

To switch from enforcing one list to enforcing the other:

1. Select **Tools** > **Manage Devices** from the main menu.
2. Verify that the list that you intend to enforce is appropriately populated.
   - If you enforce the whitelist, the whitelist should contain all eligible devices. The blacklist is ignored.
   - If you enforce the blacklist, the blacklist should contain all excluded devices. The whitelist is ignored.
3. In the toolbar at the top of the **Mobile Devices** tab, make a selection from the **Enforced** drop-down list. In the confirmation window, click **Yes**.

About the Mobile Devices Tab

Here are some details about the **Mobile Devices** tab:

- On the **History** tabs, you can filter by selecting an item from a **Filter** drop-down list, specifying a value, and clicking **Apply**.
- The **Logon History** tab displays logon events. By default, only one logon event for each device is displayed. To view previous logon events, select the **Include device history** check box. The following occurrences are logon events:
- A connection attempt that comes from a new source (a unique combination of device ID and user ID).

- A connection attempt that is accompanied by a device change (such as a new operating system version or application version).

- On the Logon History tab, the Status column provides information about a logon event. The Status column does not indicate the current status of a device connection.

- When you right-click on a device on the Logon History tab, remember that only one list is in use. Adding a device to the list that is not in use has no immediate effect. For example, if your deployment uses the blacklist, adding a device to the whitelist has no immediate effect.

- On the Blacklist and Whitelist tabs, each cell in the User ID column contains the user ID that connected (or attempted to connect) to SAS Mobile BI from the associated device. The user ID is provided for the purpose of helping you identify a device. If no user has attempted to connect from a particular device, no user ID is listed for that device. If multiple users have attempted to connect from a particular device, all of those user IDs are listed.

- On the Manage tabs, you can right-click on a device ID, and select Copy Device ID. On the History tabs, you can paste a device ID into the text field next to the Filter drop-down list.

  Note: A device ID is a unique identifier (usually a hardware device number) that is determined and communicated by the connecting mobile application.

- The Management History tab displays device management events, such as adding a device to a list or removing a device from a list. The Admin ID column provides the user ID of the administrator who performed each action.

- When you right-click on a device in the blacklist or whitelist, you can choose either a move action or a remove action. In terms of immediate effect, there is no difference between these two actions.
Part 2

Special Topics

Chapter 6
  Security .............................................................. 51

Chapter 7
  Fine-Tuning ....................................................... 65

Chapter 8
  Troubleshooting .................................................. 95

Chapter 9
  SAS LASR Analytic Server ................................. 105
## Security

### Data Security

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS LASR Authorization Service</td>
<td>51</td>
</tr>
<tr>
<td>Signature Files</td>
<td>53</td>
</tr>
<tr>
<td>Server Tags</td>
<td>54</td>
</tr>
</tbody>
</table>

### Row-Level Security

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>55</td>
</tr>
<tr>
<td>Permission Precedence</td>
<td>55</td>
</tr>
<tr>
<td>Syntax (Enhanced Editor)</td>
<td>56</td>
</tr>
<tr>
<td>Syntax (Basic Editor, Batch)</td>
<td>56</td>
</tr>
</tbody>
</table>

### Locked-Down Servers

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Encryption</td>
<td>59</td>
</tr>
<tr>
<td>Introduction</td>
<td>59</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>59</td>
</tr>
<tr>
<td>SAS Token Authentication</td>
<td>59</td>
</tr>
<tr>
<td>Policy.ConcurrentUserLogins</td>
<td>61</td>
</tr>
<tr>
<td>Transport Layer Security (TLS)</td>
<td>61</td>
</tr>
</tbody>
</table>

### Protections for Mobile Content

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwordless SSH</td>
<td>62</td>
</tr>
<tr>
<td>What Is Passwordless SSH?</td>
<td>62</td>
</tr>
<tr>
<td>Who Needs Passwordless SSH?</td>
<td>62</td>
</tr>
<tr>
<td>How to Set Up Passwordless SSH</td>
<td>62</td>
</tr>
<tr>
<td>Generate SSH Keys Manually</td>
<td>63</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>63</td>
</tr>
</tbody>
</table>

---

### Data Security

#### SAS LASR Authorization Service

**Overview**

The SAS LASR Authorization Service is a middle-tier component that collaborates with the metadata authorization layer to manage user access to in-memory data.
The following figure depicts the authorization process:

**Figure 6.1 Authorization Process**

1. In a SAS Visual Analytics client, a user performs an action that uses a SAS LASR Analytic Server. In this example, the request is to read data. The client sends the request to the authorization service.

   **Note:** Other examples of actions include requesting analysis of data, loading tables, appending rows, and stopping the server.

2. The authorization service requests the following information from the metadata server:
   - authorization decisions that indicate whether the requesting user has the effective metadata-layer permissions that are required to perform the requested action. See “Permissions by Task” on page 31.
   - the security key for the target SAS LASR Analytic Server

3. The authorization service receives the authorization decisions and security key from the metadata server. If the requesting user has a conditional grant of the Read permission, the authorization service also receives a clause (or set of clauses) that specifies which rows the user can access.

4. If the requesting user has effective grants of all permissions that are required for the requested action, the authorization service provides a signed grant to the client.

   **Note:** The authorization service uses the security key to create the signed grant. The signed grant includes the table name, the type of action (for example, Table Info, Summary Statistics, or Regression), and any applicable row-level security conditions.

5. The client submits the signed grant to the SAS LASR Analytic Server.

6. The SAS LASR Analytic Server uses its knowledge of the security key to validate the signed grant that the client supplies. If the signed grant is valid, the server provides access to the requested in-memory table (conforming to any row-level security conditions in the signed grant).

**Security Keys**

A LASR security key is a unique, shared secret between a SAS LASR Analytic Server and the metadata server. LASR security keys are created and stored as follows:
When a SAS LASR Analytic Server is started, a key is generated. In the SAS LASR Analytic Server, the key is stored in memory. The key is also stored in metadata in the password field of a login object that is associated with the server’s connection object.

If a SAS LASR Analytic Server is stopped, the associated key remains in the metadata. If the server connection is restarted, a new key is generated. The new key replaces the existing key in the metadata.

Note: A LASR security key is a SAS internal construct.

Caching
To avoid making repeated queries to the metadata server for a security key, the authorization service caches the key. When the cache interval has expired, the authorization service removes the key from the middle-tier cache. When the next request is made for in-memory data, the authorization service again obtains the key from the metadata server and repopulates the cache.

To enhance performance, the authorization service caches information about users and permissions. When a SAS Visual Analytics user accesses a data source in the SAS LASR Analytic Server, a user object is created and cached. A permission object is also created and cached for the data source. These are middle-tier, session-based caches.

The duration of each cache is set by the las.caching.* properties. See “Configuration Properties: SAS Visual Analytics” on page 90.

Access Denials
If a user does not have sufficient metadata-layer access to perform a requested action, the displayed error includes a statement such as the following:

- Metadata Server denied access to operation.
- You do not have permission to access the selected data source.
- The requested data source is not available.

For definitive information about which permission to which object is needed, examine the appropriate log. See “Logging of Access Denials” on page 80.

Signature Files
Signature files are small files that are created when a SAS LASR Analytic Server is started (server signature files) and when a table is loaded to memory (table signature files). The location for each server’s signature files is specified by a setting in its metadata definition. See “Signature files location on server” on page 114.

Manage access to the signature files directory as follows:

- Administrators must have Write access to the directory. Without this access, they cannot perform tasks that generate signature files.
- Any service accounts that perform tasks that generate signature files must have Write access to the directory. For example, if you use automated data loading, the account under which the scheduled task runs must have this access.
Nobody else needs access to signature files. (Access from SAS Visual Analytics clients to the SAS LASR Analytic Server and its in-memory data is controlled by metadata permissions.)

Host-layer access controls on signature files determine access for any requests that are not mediated by the SAS LASR Authorization Service. For this reason, it is important to restrict access to signature files.

For greater security, host-protect the signature files directory as follows:

1. In SAS Management Console, right-click on a SAS LASR Analytic Server, and select **Properties**.

2. On the **Options** tab, click the **Advanced Options** button.

3. In the Advanced Options window, select the **Additional Options** tab. Note the path that is specified in the **Signature files location on server** field.

4. Host-protect the directory, using the following guidelines:
   - **Windows Specifics:** Limit Read and Write access as described above.
   - **UNIX Specifics:** For a distributed server, the UMASK value of the TKGrid determines the permissions on signature files. Set the TKGrid UMASK to 077. For a non-distributed server, set the personal UMASK to 077. These settings prevent any user other than the file owner (creator) from gaining access to signature files.

### Server Tags

Server tags are identifiers that help the SAS LASR Authorization Service map each in-memory table to a corresponding metadata object. See “How In-Memory Tables Are Identified” on page 112.

Each LASR library's server tag should be defined as follows:

- If the LASR library’s data is from co-located Hadoop, the server tag must be the source HDFS path in dot-delimited format. Here are some examples:

<table>
<thead>
<tr>
<th>HDFS Directory</th>
<th>Corresponding Server Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>/hps</td>
<td>hps</td>
</tr>
<tr>
<td>/hps/special</td>
<td>hps.special</td>
</tr>
<tr>
<td>/sales</td>
<td>sales</td>
</tr>
</tbody>
</table>

- If the LASR library’s data is loaded directly, the server tag can be any unique string. If you do not supply a server tag in a LASR library’s metadata definition, the tag **WORK** is used.

- If the LASR library is used for self-service import actions from a DBMS, see “Additional Considerations” on page 14.

**CAUTION!** Within a server instance (a host-port combination), each server tag must be unique.
Row-Level Security

Introduction

Row-level security enables you to control who can access particular rows within a LASR table, and it is defined by data filter expressions. Row-level access distinctions can be based on a simple attribute (such as security clearance level) or on a more complex expression that consists of multiple criteria.

Row-level security affects access to subsets of data within a resource. To establish row-level security, you add constraints called permission conditions to explicit grants of the Read permission. Each permission condition filters a particular LASR table for a particular user or group. Each permission condition constrains an explicit grant of the Read permission so that the associated user or group can see only those rows that meet the specified condition.

When row-level security is used, there are three possible authorization decision outcomes for a user request to view data:

- **Grant**
  - The requesting user can see all rows.

- **Conditional grant**
  - The requesting user can see only those rows that meet the specified filtering conditions.

- **Denial**
  - The requesting user cannot see any rows.

TIP When you test conditions in a SAS Visual Analytics application (such as the explorer), refresh the data source in that application (so that the results reflect your saved changes to permission conditions). See “Caching” on page 53.

Permission Precedence

Here are some key points about how permission conditions are incorporated into the metadata-layer access control evaluation process:

- A permission condition is applied only if it is on the setting that is closest to the requesting user. Other permission conditions that are relevant because of further-removed group memberships do not provide additional, cumulative access.

- If there is an identity precedence tie between multiple groups at the highest level of identity precedence, those tied conditions are combined in a Boolean OR expression. If the identity precedence tie includes an unconditional grant, access is not limited by any conditions.

The following table provides examples:
### Table 6.1 Precedence for Permission Conditions

<table>
<thead>
<tr>
<th>Principle</th>
<th>Scenario</th>
<th>Outcome and Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>If there are multiple permission conditions that apply to a user because of the user's group memberships, then the identity that has the highest precedence controls the outcome.</td>
<td>A condition on TableA limits Read permission for GroupA. Another condition on TableA limits Read permission for the SASUSERS group. The user is a member of both GroupA and SASUSERS.</td>
<td>The user can see only the rows that GroupA is permitted to see. GroupA has a higher level of identity precedence than SASUSERS, so the filters that are assigned to GroupA define the user's access.</td>
</tr>
<tr>
<td>If there are multiple permission conditions at the highest level of identity precedence, then any data that is allowed by any of the tied conditions is returned.</td>
<td>A condition on TableA limits Read permission for GroupA. Another condition on TableA limits Read permission for GroupB. The user is a first level member of both GroupA and GroupB.</td>
<td>The user can see any row that is permitted for either GroupA or GroupB.</td>
</tr>
</tbody>
</table>

### Syntax (Enhanced Editor)

**TIP** To access the enhanced editor, see “Set a Row-Level Permission Condition” on page 33.

This topic is applicable to permission conditions created in SAS Visual Analytics Administrator 6.2 and later.

In the enhanced editor for permission conditions, a **Text** tab supports entering text directly.

Here are some key points about the **Text** tab:
- The **Text** tab supports only those operators that are available on the **Visual** tab.
- The **Text** tab does not use the same syntax as the basic editor and the batch tools. For hints, select the **Text** tab, and then click in the window toolbar.

### Syntax (Basic Editor, Batch)

#### Introduction

This topic is applicable to permission conditions created in the following contexts:
- In SAS Visual Analytics Administrator 6.1 and earlier.
- In the batch tools for metadata authorization. See **Batch Tools for Metadata Authorization** in the *SAS Intelligence Platform: Security Administration Guide*.

#### General Guidelines

- Enclose non-numerical character values within quotation marks.
The symbol | | is not supported. Instead, use the keyword OR.

Expressions with months or dates are not supported.

Do not include the WHERE keyword in any expression.

### Supported Syntax

**Table 6.2  Supported Syntax**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND, OR, NOT</td>
<td>Toy_Type='cars' AND Toy_Type='dolls'</td>
</tr>
<tr>
<td>IN, NOTIN</td>
<td>Toy_Type IN ('dolls' 'cars' 'animals')</td>
</tr>
<tr>
<td>CONTAINS, ?</td>
<td>Toy_Type CONTAINS 'cars'</td>
</tr>
<tr>
<td>BETWEEN, NOT BETWEEN</td>
<td>Toy_Price BETWEEN 20 AND 30</td>
</tr>
<tr>
<td>LIKE</td>
<td>Toy_Type LIKE 'dolls'</td>
</tr>
<tr>
<td>=, &gt;, &lt;, &gt;=, &lt;=, &lt;&gt;</td>
<td>Toy_Price=25</td>
</tr>
<tr>
<td>^=, NE</td>
<td>Toy_Price^=30</td>
</tr>
</tbody>
</table>

### Identity-Driven Properties

The following table introduces properties that you can use to create identity-driven permission conditions. When you use these properties in a permission condition, values are dynamically substituted into the condition at run time, based on the metadata identity of each requesting user.

**Table 6.3  Identity-Driven Properties**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUB::SAS_UserId</td>
<td>returns the requesting user’s authenticated ID, normalized to the uppercase format USERID or USERID@DOMAIN. Here is an example for use in the batch tools: -condition &quot;empID='SUB::SAS_UserId'&quot;</td>
</tr>
<tr>
<td>SUB::SAS_IdentityGroups</td>
<td>returns the requesting user’s group and role memberships (direct, indirect, and implicit). The returned list contains group and role names (not display names). Here is an example for use in the batch tools: -condition &quot;FacilityRegion IN {‘SUB::SAS_IdentityGroups’}&quot;</td>
</tr>
<tr>
<td>SUB::SAS_PersonName</td>
<td>returns the requesting user’s name (as specified in the Name field on the General tab of the user’s metadata definition).</td>
</tr>
<tr>
<td>SUB::SAS_ExternalIdentity</td>
<td>returns a site-specific identifier for the requesting user. External identity values are populated by the platform’s user import macros (if you bulk load user information into metadata).</td>
</tr>
</tbody>
</table>
For example, if a LASR table has an empID column with values that match the user IDs with which users authenticate, you might use the condition `empID='SUB::SAS.Userid'`. Each affected user’s ID is substituted into the right side of the condition. In a request from the sasdemo user, the condition resolves as `empID='sasdemo'`, so only those rows where the value in the empID column is `sasdemo` are returned to the sasdemo user. If you assign the condition to a group, each member’s access is restricted to those rows where the empID value matches his or her authenticated user ID. Here is an example of the full command for the use in batch tools:

```
sas-set-metadata-access -profile Admin */Shared Data/LASRtableA(Table)
-grant sasusers:Read -condition "empID='SUB::SAS.Userid'"
```

Note: Two additional properties (SAS.IdentityName and SAS.IdentityGroupName) are not documented here because they are less frequently useful. See About Identity-Driven Properties in the SAS Intelligence Platform: Security Administration Guide.

---

### Locked-Down Servers

You can limit the reach and activities of certain SAS servers. For more information, see Locked-Down Servers in the SAS Intelligence Platform: Security Administration Guide.

If you choose to lock down a server that is used by SAS Visual Analytics, make sure that the following directories are accessible to that server:

- **SAS-configuration-directory/Applications/**
  - For a non-distributed server, the signature files directory. See “Signature files location on server” on page 114.
  - For a distributed server, each user’s home directory (~) to provide access to SSH keys. See “Passwordless SSH” on page 62.
  - The directory where process IDs are written. See “va.monitoringPath” on page 92.
  - The directory that contains geographic data sets. See “Geographic Data Sets” on page 76.
  - The directory that contains the SAS linguistic files for text analytics. See “Extended Attributes: SAS LASR Analytic Server” on page 115.
  - Any directory to which users export code. See “Record actions as SAS statements” on page 86.
  - Any directory that serves as a data provider for reload-on-start. See “Reload-on-Start” on page 15.
  - Any directory from which users import non-local data. See “Self-Service Import” on page 11.
  - The directory where scheduled jobs for SAS Visual Data Builder are written. (The standard location is in the SAS configuration directory at your equivalent of **SAS-application-server\SASEnvironment\SASCode\Jobs**.)
Note: You can apply lockdown to autoload by adding the LOCKDOWN system option to the SAS command (in the runsas.bat or runsas.sh file). The associated autoload source and script directories must be made accessible to the locked-down SAS session. See Lockdown System Option in the SAS Intelligence Platform: Application Server Administration Guide.

Authentication and Encryption

Introduction

SAS Visual Analytics uses platform-level functionality for authentication and encryption. This topic provides details that are specific to SAS Visual Analytics.

Web Authentication

Note: For background information, see Web Authentication in the SAS Intelligence Platform: Security Administration Guide.

In a deployment that uses web authentication, specialized configuration might be necessary to enable users to perform actions that require a standard workspace server and access to the SAS LASR Analytic Server’s host.

Here are some methods for facilitating access:

- Create individual accounts that are valid for the SAS LASR Analytic Server’s host. Use one of the following approaches to make the account credentials available:
  - Behind web authentication, use Integrated Windows authentication with user delegation. See SAS Intelligence Platform: Middle-Tier Administration Guide.
  - Store the credentials in metadata (on each user’s Accounts tab in SAS Management Console). For example, a user might have the following logins:

```
web           | sue       | (no password)
DefaultAuth   | sue       | (password)
```

- Create shared service accounts and use SAS token authentication (after reviewing the information in the following topic).

SAS Token Authentication

Introduction

CAUTION! Before you configure SAS token authentication for a standard workspace server, make sure you understand the security implications. See SAS Token Authentication in the SAS Intelligence Platform: Security Administration Guide.
Scenario: One Level of Public Access

If you want to enable designers and explorers to import data to a public area under a generic, shared host identity, consider configuring the workspace server to use SAS token authentication.

For instructions, see How to Configure SAS Token Authentication in the SAS Intelligence Platform: Security Administration Guide.

Note: Any sensitive data should be accessed through an additional SAS Application Server, whose standard workspace server uses host authentication, not SAS token authentication.

Scenario: Multiple Levels of Host Access

To give different groups of users distinct host-layer access and allow each group to share one back-end account, set up multiple SAS Application Servers. Within each application server, configure a standard workspace server for SAS token authentication using a distinct launch credential.

Note: This is an advanced configuration that requires in-depth knowledge of platform-level servers, metadata permissions, and host permissions.

Note: Only the data builder and the administrator enable different users to use different SAS Application Servers. See “Which Server is Used?” on page 86.

Here is an overview of the setup tasks with links to detailed instructions in the platform administration guides:

1 For each distinct set of secured resources, create a service account that can authenticate to the SAS LASR Analytic Server. Make sure the account has the privileges that are required to operate the server and load data. See “Host Account Privileges” on page 7.

2 For each service account, create a SAS Application Server that contains a standard workspace server. See Managing SAS Application Servers in the SAS Intelligence Platform: Application Server Administration Guide.

Note: Configure the application server to support the job execution service. See “How to Configure the Job Execution Service” on page 87.

Note: If data builders schedule queries, include a SAS DATA Step Batch Server within the SAS Application Server.

Note: If users import remote SAS data sets (Import SAS Data Sets from a Server), and those data sets must be secured, include a pooled workspace server within the SAS Application Server. Use a unique service account as the launch credential.

3 For each standard workspace server, configure SAS token authentication using a unique service account as the launch credential. See How to Configure SAS Token Authentication in the SAS Intelligence Platform: Security Administration Guide.

Note: Within each SAS Application Server, if applicable, you can use the same service account as the launch credential for both the pooled workspace server and the standard workspace server.

4 For each SAS Application Server, create a corresponding SAS LASR Analytic Server instance. Assign a unique signature files directory to each instance. Give each service account exclusive host access to the signature files directory for its server instance. (Also, give each launch credential host...
access to the appropriate source data.) See “Add a SAS LASR Analytic Server” on page 41.

5 For each SAS LASR Analytic Server instance, create one or more LASR libraries. See “Add a SAS LASR Analytic Library” on page 43.


**Policy.ConcurrentUserLogins**

SAS Visual Analytics does not support deny or logoff values for the Policy.ConcurrentUserLogins property. For successful interactions with the SAS LASR Analytic Server, make sure this property is set to allow.

The Policy.ConcurrentUserLogins property is documented in Disabling Concurrent Sign In Sessions in the SAS Intelligence Platform: Middle-Tier Administration Guide.

**Transport Layer Security (TLS)**

To use transport layer security (TLS) between the browsers that access the SAS Visual Analytics web applications and SAS Web Server, you can configure SAS Web Server for HTTPS. The preferred approach is to acquire certificates before installation and use the SAS Deployment Wizard to perform the configuration. If you need to configure HTTPS after installation, see Configuring SAS Web Server Manually for HTTPS in the SAS Intelligence Platform: Middle-Tier Administration Guide.

**Protections for Mobile Content**

Protections for mobile content include the following:

- Users must authenticate to establish a connection.
- SAS metadata security is enforced on all reports and data.
- You can manage device eligibility by exclusion or inclusion. See “Managing Devices” on page 45.
- To minimize persistence of mobile data, assign users or groups to a role that has the Purge Mobile Report Data capability. See “Purge Mobile Report Data” on page 125.
- To require knowledge of an application passcode, assign users or groups to a role that has the Require Passcode on Mobile Devices capability. See “Require Passcode on Mobile Devices” on page 125.
- Content on a mobile device is encrypted by the device’s operating system.
- You can encrypt communication between mobile devices and SAS servers. See Configuring SAS Web Server Manually for HTTPS in the SAS Intelligence Platform: Middle-Tier Administration Guide.
Passwordless SSH

What Is Passwordless SSH?

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. Passwordless SSH enables an identity to connect from one device to another without specifying a password. The identity can log on without a credential challenge, or it can invoke commands on the other device without a credential challenge.

Who Needs Passwordless SSH?

For a non-distributed server, passwordless SSH is not applicable.

For a distributed server, the requirements for passwordless SSH are as follows:

- Each data administrator must have an account that is configured for passwordless SSH (on each machine in the cluster). This is necessary to perform tasks such as starting and stopping the server and loading and unloading tables.

- If you use automated loading, the service account under which the scheduled task runs must be configured for passwordless SSH (on each machine in the cluster). This is necessary to perform tasks such as starting and stopping the server and loading and unloading tables.

- The service account for SAS LASR Analytic Server Monitor must be configured for passwordless SSH (on each machine in the cluster). This is necessary to monitor hardware resources and processes for a distributed SAS LASR Analytic Server. This service account can be the same as the SAS installer account.

How to Set Up Passwordless SSH

You can use a point-and-click interface to generate SSH keys and configure them for passwordless SSH automatically for administrator accounts. See the SAS High-Performance Computing Management Console: User’s Guide.

Here are some tips:

- In the SAS High-Performance Computing Management Console, be sure to select the Generate and Propagate SSH Keys option on the Create User page. This ensures that passwordless SSH is configured correctly for the account.

- After you add user or group accounts to the machines in the cluster, you must restart SAS High-Performance Deployment of Hadoop. An error message such as the following indicates that a user is not recognized:

  ```
  ERROR: host02.example.com (192.168.1.240) User does not belong to .
  ```

- You can use SAS High-Performance Computing Management Console to perform an SSH lockout.
Generate SSH Keys Manually

The recommended method is to use the SAS High-Performance Computing Management Console to generate SSH keys (as described in the preceding topic).

If you must generate SSH keys manually (for example, for existing user IDs), use the following steps:

1. Generate a private/public key pair on a Linux system. Enter the following command to generate the keys and avoid using a passphrase:

   `ssh-keygen -t rsa -P ""`

2. After the keys are generated, if passwordless SSH is required, then add the public key to the list of authorized keys by entering this command on the command line:

   `cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys`

3. Check permissions on the `.ssh` directory and the files in your `.ssh` directory. The directory must be readable and writable by you only. The `id_rsa` file must be readable by you only. To verify access, enter the following command, and check the results:

   `ls -asl ~/.ssh`

   ```
   drwx------ 2 datamgr datamgr 4096 Jan 23 10:27 .
   drwx------ 4 datamgr datamgr 4096 Jan 12 19:09 ..
   -rw-r--r-- 1 datamgr datamgr  397 Jan 23 10:27 authorized_keys
   -rw------- 1 datamgr datamgr  1675 Jan 23 10:00 id_rsa
   -rw-r--r-- 1 datamgr datamgr  397 Jan 13 10:00 id_rsa.pub
   -rw-r--r-- 1 datamgr datamgr 1705 Jan 23 10:27 known_hosts
   ```

   a. The directory permissions for the `.ssh` directory indicate that access is denied for all users other than the directory owner.

   b. The `id_rsa` file is the private key. Read access and Write access are available to the file owner only.

   Note: If the machines in the cluster are not configured to access the home directories for the users, create local home directories for the users. Copy the `.ssh` directory for each user to his or her local home directory. Make sure that the permissions are preserved.

Troubleshooting

If access problems occur, use the following steps to help diagnose any SSH configuration errors:

1. Impersonate the user or ask the user to perform the following command that requires passwordless SSH:

   `/opt/webmin/utilbin/simsh hostname`

   If each of the machines in the cluster responds with a host name, then no passwordless SSH configuration error exists.
2 As root, log on to one of the machines in the cluster and monitor the logon access:

```
    tail -f /var/log/secure
```

3 Review the messages in the `/var/log/secure` file. The following example shows that the file system access permissions for `/home/sas` are not set correctly:

```
Mar 14 22:12:36 hostname sshd[11235]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar 14 22:12:57 hostname sshd[11266]: Authentication refused: bad ownership or modes for directory /home/sas
```
Fine-Tuning

Supporting Guest Access .................................................. 66
  About Guest Access .................................................. 66
  Limit Content for Guest Access .................................. 67
  Limit Functionality for Guest Access ......................... 68
  Customize Guest Access ............................................. 68
  Enable or Disable Guest Access .................................. 69

Customizing Appearances ............................................... 69
  Application Themes .................................................. 69
  Report Styles .......................................................... 70

Customizing the Home Page ............................................. 70
  Populate "Other Content" .......................................... 70
  Make Global Changes to the Right Pane ..................... 71

Managing Alerts and Notifications .................................... 72
  Introduction .......................................................... 72
  Requirements .......................................................... 72
  How to Delete Other Users’ Alerts ......................... 72
  Configuration Properties for Alerts ..................... 72

Supporting Stored Processes ........................................... 73

Supporting the Search Features ....................................... 74
  About the Search Interface to SAS Content .................. 74
  How the Search Index Is Created ............................. 74
  How the Search Index Is Loaded ............................... 75

Supporting the Geo Map Features ..................................... 75
  Introduction .......................................................... 75
  OpenStreetMap Server .............................................. 75
  Esri Server ........................................................... 76
  Geographic Data Sets .............................................. 76

Supporting User-Defined Formats .................................... 77
  About User-Defined Formats .................................... 77
  Basic Instructions ................................................... 77
  Considerations ........................................................ 77

Supporting the Monitoring Features ................................ 77
  Introduction .......................................................... 77
  Network Name Resolution ....................................... 78
  Managing the Monitoring Server ............................. 78
  Logging for the Monitoring Server ......................... 79

Adjusting the Logging Configuration ................................ 79
Supporting Guest Access

About Guest Access

Guest access is an optional feature that provides anonymous access to a subset of SAS Visual Analytics resources and functionality. In guest access, there is no individualized authentication of the requesting user, so there are no requirements for individual user accounts or metadata identities. Instead, all users who connect to a guest access URL are authenticated as the same service account (the SAS Anonymous Web User). That service account functions as the single surrogate identity for all connecting users.

Here are some key points:

- In a deployment where guest access is enabled, the following guest access URLs are available:

  http://host/SASVisualAnalyticsHub/guest.jsp
  provides guest access to the home page (the hub)

  http://host/SASVisualAnalyticsViewer/guest.jsp
  provides guest access to the web viewer

Because everyone connects to the guest access URLs as the same shared, surrogate identity (the SAS Anonymous Web User), everyone’s experience at those URLs is identical. At the guest access URLs, everyone can see what the SAS Anonymous Web User can see, and everyone can do what the SAS Anonymous Web User can do. Even the My Content section of the home page is the same for all connecting users.

To provide guest access within an intranet only, place the applications behind a firewall. See Best Practices for Configuring Your Middle Tier in the SAS Intelligence Platform: Middle-Tier Administration Guide.

Guest access is not compatible with web authentication. In other words, if your deployment authenticates users in the middle tier (for example, to provide single sign-on for initial connections to SAS Visual Analytics), your deployment cannot support guest access.

**Limit Content for Guest Access**

At the guest access URLs, any content that the SAS Anonymous Web User can access is available to all connecting users.

**CAUTION!** Grants to the SASUSERS and PUBLIC groups can introduce additional content at the guest access URLs. If your deployment supports guest access, it is important to review access that is granted to the SASUSERS and PUBLIC groups. The SAS Anonymous Web User is an implicit member of those groups, so any content that you make available to those groups is potentially available at the guest access URLs.

Here are some guidelines for managing access:

- Periodically connect to the guest access URLs to verify that the available content is as intended.
- Do not expect user or group-based access distinctions (such as row-level security) to be reflected at the guest access URLs. The guest access URLs provide only generic, lowest-common-denominator access to content.
- Review the metadata-layer permissions that are granted to the SASUSERS and PUBLIC groups. You can use either of the following approaches to exclude content from the guest access URLs:
  - Where access is granted to SASUSERS or PUBLIC, add denials for the SAS Anonymous Web User.
  - Replace grants to SASUSERS or PUBLIC with grants to the Visual Analytics Users group and the SAS System Services group.

See “Setting Permissions” on page 29.

- Do not revoke the SAS Anonymous Web User’s ReadMetadata access to the /System folder.
Limit Functionality for Guest Access

Guest access functionality corresponds to the capabilities of the SAS Anonymous Web User. The Visual Analytics: Basic role provides an appropriate set of capabilities for guest access. See “Predefined Roles” on page 121.

CAUTION! Any capabilities that SASUSERS or PUBLIC has can expand guest access functionality. This expansion of functionality can cause unintended results. If your deployment supports guest access, it is essential to limit the capabilities of the SASUSERS and PUBLIC groups. The SAS Anonymous Web User is an implicit member of those groups, so any capabilities that you give to those groups are potentially available at the guest access URLs.

Here are some additional guidelines:

- Periodically connect to the guest access URLs to verify that the available functionality is as intended.
- Do not give the Personalization capability to the Visual Analytics: Basic role. Failure to conform to this guideline causes each user’s experience to reflect the activities of the prior user.

Customize Guest Access

To change the personalization settings that apply to all users at the guest access URLs:

1. Temporarily make the Personalization capability available at the guest access URLs.
   - Log on to SAS Management Console as someone who has user administration capabilities (for example, sasadm@saspw).
   - On the Plug-ins tab, select User Manager.
   - In the right pane, right-click the Visual Analytics: Basic role, and select Properties.
   - On the Capabilities tab, expand the Visual Analytics node, and select the check box for the Personalization capability. Click OK.

2. Connect to the guest access URL for the home page. As soon as your session is established, remove the Personalization capability from the Visual Analytics: Basic role.

   Note: Minimizing the period of time in which the Personalization capability is granted to the Visual Analytics: Basic role reduces the risk of another user inadvertently affecting the guest access configuration.

3. Make changes as needed. Here are some examples:
   - To change the applications’ colors, select File ▶ Preferences from the main menu. In the Preferences window, make a selection from the Theme drop-down list. Click OK.
   - To make certain objects easily visible, click the Manage link in the My Content section of the home page. In the Manage My Content window, add favorites or collections, and then click OK.
4 In the main menu bar, click **Log Off**. Then, log on to the guest access URLs again.

a Verify that the results are as expected.

b Verify that further personalization is not available. For example, the Manage link should not be available in the My Content section of the home page.

### Enable or Disable Guest Access

#### How to Enable Guest Access

The preferred method for configuring guest access is to make the following choices during installation:

- create a SAS Anonymous Web User
- enable guest access for SAS Visual Analytics

To enable guest access after installation is completed:

1 Create a SAS Anonymous Web User if that service identity does not already exist in your deployment. See *Using the SAS Anonymous Web User with SAS Authentication* in the *SAS Intelligence Platform: Middle-Tier Administration Guide*.

2 Set the App.AllowGuest property to **True**. See “How to Set Advanced Properties for SAS Visual Analytics” on page 90.

#### How to Disable Guest Access

In a deployment that supports guest access, you can disable guest access by setting the App.AllowGuest property to **False**.

### Customizing Appearances

#### Application Themes

**About Application Themes**

The appearance of SAS Visual Analytics applications can be modified as follows:

- Each user can select a standard theme that defines colors, graphics, and fonts for the SAS Visual Analytics web applications. This theme setting is a suite-level, per-user preference. Users can access the theme setting by selecting **File ▶ Preferences** in any of the web applications.

  **Note:** In SAS Visual Analytics Designer, the workspace for building reports uses a fixed style that is not affected by application themes.
A site can use the SAS Theme Designer for Flex to create and deploy custom themes. See the [SAS Theme Designer for Flex: User’s Guide](#).

**TIP** If you are authorized to use SAS Theme Designer for Flex, you can launch it from the SAS Visual Analytics home page (also known as the hub). To use SAS Theme Designer for Flex, you must have the Customize Themes capability (Theme Designer for Flex ▶ Basic ▶ Customize Themes). In the initial configuration, the Theme Designer for Flex:Administration role provides this capability.

A site can customize the SAS Mobile BI banner. See “Configuration Properties: SAS Mobile BI” on page 87.

### Promotion of Custom Themes

Custom themes are not promoted with the reports that use them. To make custom themes available in a new environment:

1. In the source environment, use SAS Theme Designer for Flex to export all custom themes.
2. In the target environment, use SAS Theme Designer for Flex to import the .tdf file that the export generated.
3. In the target environment, use SAS Theme Designer for Flex to deploy the custom themes that you want to make available.

### Report Styles

Reports are affected by report styles, not by application themes. The appearance of reports can be modified as follows:

- In the preferences for SAS Visual Analytics Designer, a user can specify a default theme for reports. This specification is independent from the application theme, but one of the choices is to use the same theme as the application uses.
- In the report building process in SAS Visual Analytics Designer, a user can specify styles for individual tables, graphs, and gauges. See the [SAS Visual Analytics: User’s Guide](#).

### Customizing the Home Page

#### Populate "Other Content"

If you have the Administer Hub capability, you can add and remove shared, folder-level shortcuts in the Other Content section of the SAS Visual Analytics home page.

To add a folder-level shortcut:

1. On the home page, next to the Other Content section, click Manage.
2 In the Manage Other Content Lists window:
   a  Click.
   b  Enter a name for the list (shortcut).
   c  Click Browse, and select the metadata folder to which you want to provide a shortcut. Click OK.

   **TIP** You can drag and drop lists to change their display order. To facilitate reordering, any lists for which you lack the ReadMetadata permission are represented by placeholder labels (for example, <list 1>).

   **TIP** You can temporarily hide a list by selecting its Hide check box in the Manage Other Content Lists window. Hiding a list excludes it from the Other Content section on the home page.

3 On the home page, verify the results.
   - If there is only one list, eligible objects that are within the corresponding folder are displayed.
   - If there are multiple lists, they are displayed horizontally below the Other Content heading. Eligible objects that are within the folder that corresponds to the selected list are displayed.

Here are some details:
   - The Other Content section is not a personalization feature. Any lists that you create are displayed for all users, except where access is constrained by the ReadMetadata permission.
   - Users who have the Administer Hub capability can always see and populate the Other Content section. Other users see the Other Content section only if it references lists (folders) for which they have the ReadMetadata permission.
   - Only objects that are of a type that the home page supports are displayed.
   - Only objects for which the requesting user has ReadMetadata permission are displayed.
   - A user sees a list only if he or she has ReadMetadata permission for the corresponding metadata folder.

**Make Global Changes to the Right Pane**

If you have the Administer Hub capability, you can hide sections and shared links in the right pane of the SAS Visual Analytics home page.

1 From the Views drop-down list in the main menu bar ( ), select Manage Shared View of Right Pane.

2 In the Manage Shared View of the Right Pane window, make changes, and then click OK.

   **Note:** Changes that you make in this window affect all users. If a user has the Personalization capability, he or she can make further, individualized changes.
Managing Alerts and Notifications

Introduction

This topic provides information to help administrators support the alerts that users can create in the designer. For user instructions, see Working with Alerts for Report Objects in the SAS Visual Analytics: User's Guide.

Requirements

Evaluation of data-driven alerts requires the following conditions:

- The associated SAS LASR Analytic Server is running.
- The target LASR table is loaded.
- The SAS Trusted User (for example, sastrust@saspw) has metadata-layer access to the target LASR table. The standard method for providing the necessary access is to grant the ReadMetadata and Read permissions to the SAS System Services group.

TIP Alert evaluations are performed by SAS Visual Analytics Hyperlink Services, so any errors are reported in your equivalent of /Web/Logs/server/SASVisualAnalyticsHyperlinkVersion.log.

Delivery of alert notifications to a subscriber requires that the subscriber’s metadata user definition includes a valid e-mail address. The SAS Web Infrastructure Platform handles delivery. See SAS Web Infrastructure Platform in the SAS Intelligence Platform: Middle-Tier Administration Guide.

How to Delete Other Users’ Alerts

To delete other users’ alerts:

1. From the main menu in SAS Visual Analytics Administrator, select Tools ➤ Manage Alerts.
2. On the Alerts tab, select one or more alerts, right-click, and select Delete.

Here are some details:

- Anyone who has the Manage Environment capability can access the Alerts tab.
- Alerts are stored in the SharedServices database in the middle tier.

Configuration Properties for Alerts

va.Alert.DefaultEvaluationIntervalMilliseconds specifies the evaluation interval (how frequently the system makes a determination about whether the alert’s conditions have been met). The default is 600000 milliseconds (10 minutes).
Note: This property affects only alerts that do not use a custom interval. In the designer’s Edit Alert window, the Use the system default setting causes the value for this property to be used.

Note: Long intervals increase the risk of a missed incident (where the alert’s conditions are met intermittently between one evaluation and the next). Short intervals consume more resources and can negatively impact the performance of the entire SAS Visual Analytics suite of applications.

va.Alert.DefaultMaxEvaluationTimeMilliseconds
    specifies how long an individual evaluation can run before it terminates and restarts. The default is 1800000 milliseconds (30 minutes).

va.Alert.EvaluationCycleMilliseconds
    specifies how frequently the system verifies that alerts are running. The default is 30000 milliseconds (30 seconds). If a large number of alerts are registered, consider increasing the value to reduce the use of resources.

va.AlertThreadPool.CoreSize
    specifies the number of threads that are available in normal circumstances (for concurrent evaluation of alerts). The default is 3.

va.AlertThreadPool.MaxSize
    specifies the maximum number of threads that can be used (for concurrent evaluation of alerts). If the load is heavy, additional threads are temporarily added to the CoreSize (up to the value that is set for this property). The default is 3.

va.AlertThreadPool.QueueSize
    specifies the maximum number of tasks that can be queued. The default is 100000.

va.AlertThreadPool.IdleTimeoutSeconds
    specifies how long excess threads can be idle before they are terminated. The purpose of terminating idle excess threads is to reduce the number of threads to the specified CoreSize. The default is 1800 seconds (30 minutes).

Note: This property is applicable only if the MaxSize is greater than the core size.

va.Alert.Eventgen.disabled
    specifies whether alerts generate notifications. The default is false. To disable notifications, set this property to true.

Note: To add or set these properties in SAS Management Console, select the Plug-ins tab, and expand the Application Management ➤ Configuration Manager ➤ SAS Application Infrastructure ➤ Visual Analytics Version ➤ Visual Analytics Services Version node. Right-click Visual Analytics Hyperlink Service Version, select Properties, and then select the Advanced tab.

Supporting Stored Processes

A stored process is a SAS program that is stored on a server and defined in metadata. The following considerations are specific to the administration of stored processes for SAS Visual Analytics:
 Stored processes can use any available data source (not only LASR tables). However, running stored processes against large LASR tables is not a high-performance operation. Any referenced LASR tables must be read from the SAS LASR Analytic Server into a SAS session in the stored process server. Using a stored process to read large tables from memory is not a high-performance operation.

 Most SAS procedures are available to only sites that license additional software (such as Base SAS). For a site that licenses only SAS Visual Analytics, most stored processes do not run.

For information about how stored processes are incorporated in SAS Visual Analytics, see the *SAS Visual Analytics: User’s Guide*.

For information about how to create and register a stored process, see *Managing Stored Process Metadata* in the *SAS Stored Processes: Developer's Guide*.

---

**Supporting the Search Features**

**About the Search Interface to SAS Content**


Administrative details about the Search Interface to SAS Content are as follows:

- Searches are performed against an index that is periodically generated and loaded.
- A specialized service identity, the Search Interface to SAS Content User, makes SAS content available to the indexing process.

*Note:* The Search Interface to SAS Content User is unrestricted in metadata and in ROLE_ADMIN in the middle tier. These privileges are required for successful indexing.

**How the Search Index Is Created**

The search index is created by the SAS Information Retrieval Studio server.

**UNIX Specifics:** The IRStudio.sh script is in the SAS configuration directory under `/Applications/SASInformationRetrievalStudioforSAS`. To operate the server, use the following commands:

```
IRStudio.sh start | stop | status | restart
```

**Windows Specifics:** The server runs as a local service (for example, *SAS [Config-Lev1] Information Retrieval Studio*).

Generated log files are in the `/logs` subdirectory.
How the Search Index Is Loaded

The search index is loaded by a script (loadindex) that runs as a scheduled task (scheduler). These .sh (or .bat) files are in the SAS configuration directory under /Web/Applications/SearchInterfacetoSASContent.

Logging for the loadindex script uses log4j.
- The log configuration file, SASSearchServiceClient-log4j.xml, is in the same directory as the loadindex and scheduler scripts.
- The generated log is in the /Logs directory (below the directory that contains the log configuration file).

If there is a failure in loading the index, an e-mail is sent to the address that is designated for administrative messages for your deployment. To modify e-mail notifications, use the following properties:

searchsas.notification.email.is_active
  controls whether notifications are sent. To disable notifications, set this property to false.

searchsas.notification.email.sender.address
  specifies the sender’s e-mail address

searchsas.notification.email.to.address
  specifies the recipient’s e-mail address. To assign multiple recipients, provide a comma-separated list of addresses.

Note: To set the preceding properties in SAS Management Console, select the Plug-ins tab, and expand the Application Management > Configuration Manager node. Right-click Search Interface to SAS Content Version, select Properties, and then select the Advanced tab.

Supporting the Geo Map Features

Introduction

Use of geo maps introduces two specialized requirements:
- A connection to one of the following geographic information servers:
  - An OpenStreetMap server, which is available for all deployments.
  - An esri server (ArcGIS for Server, version 10.1 or later).
- A data source that contains geographic information, including longitude and latitude values.

OpenStreetMap Server

Hosted by SAS

In the default configuration, SAS Visual Analytics retrieves mapping tiles from an OpenStreetMap server that is hosted by SAS. All sites that have deployed SAS
Visual Analytics can access an OpenStreetMap server that SAS hosts. These hosted servers support replication and failover, providing reliable and dependable access.

The only information that is sent to an OpenStreetMap server is a request for a tile number (in a URL format). The only information that is returned from an OpenStreetMap server is the map image. No other information is exchanged between SAS and the OpenStreetMap server. The rendering of the map images occurs internally within SAS Visual Analytics Explorer.

For greater security, you can choose to use a Secure Sockets Layer (SSL) connection from your site to the OpenStreetMap server that SAS hosts. During installation, you select a protocol (https or http).

To change the protocol that SAS Visual Analytics uses to connect to the OpenStreetMap server that SAS hosts, set the appropriate property. See "va.SASGeomapCommunicationProtocol" on page 91.

**Hosted Elsewhere**

As an alternative to using a server that is hosted at SAS, you can choose to install, configure, host, and maintain an OpenStreetMap server at your site. This is a complex task that should be attempted only after you have carefully evaluated the requirements, needs, benefits, and maintenance responsibilities at your site. For information about OpenStreetMap servers, see [www.openstreetmap.org](http://www.openstreetmap.org).

To configure SAS Visual Analytics to use an OpenStreetMap server that is not hosted by SAS, set the appropriate property. See "va.GeoMapServerUrl" on page 92.

**Esri Server**

As an alternative to using an OpenStreetMap server, you can choose to install, configure, host, and maintain an Esri server at your site.

To register an Esri server for use in SAS Visual Analytics, set the appropriate property. See "va.SASGeomapEsriURL" on page 91.

**Note:** For deployments that include an Esri server, the explorer and the designer provide user preferences and per-object settings that determine which geographic information server is used.

**Geographic Data Sets**

SAS provides data sets that contain geographic information for several geographic domains (for example, states in the United States and ZIP codes for cities in the United States). The data sets (ATTRLOOKUP and CENTLOOKUP) are in the SAS configuration directory at your equivalent of `/SASApp/Data/valib/`. A corresponding library (for example, `SASApp - valib`) is registered in metadata.

**Note:** In addition to the predefined geographical roles that use the SAS geographic data sets, you can define custom geographical roles for your data. If your data contains latitude and longitude values, then you can assign custom geographical roles using those values.
Supporting User-Defined Formats

About User-Defined Formats

A format is an instruction that SAS uses to write data values. Formats are used to control the written appearance of data values, or, in some cases, to group data values together for analysis. An informat is an instruction that SAS uses to read nonstandard data values, such as dates, currency values, or hexadecimal values.

User-defined formats are specialized formats that are stored in a custom format library.

User-defined formats are supported by the designer, the explorer, the data builder, and any stored process that is executed in the SAS Visual Analytics environment.

Note: Associations between columns and user-defined formats must exist in the table metadata when the table is loaded to memory. You cannot make a new association from within the SAS Visual Analytics suite.

Basic Instructions

The preferred method for making user-defined formats available to a SAS Application Server is to use a standard name and location for the custom format catalog as follows:

1. Name the format catalog formats.sas7bcat.

2. On each machine that hosts a workspace server, place the format catalog in the SAS configuration directory under `/SAS-application-server/SASEnvironment/SASFormats`.

Considerations

To use a nonstandard name or location or to make multiple custom format catalogs available, see Create a User-Defined Formats Configuration File in the SAS Intelligence Platform: Data Administration Guide.

If you use load-balanced workspace servers, see Managing Data and Catalogs for Servers on Multiple Machines in the SAS Intelligence Platform: Application Server Administration Guide.

Supporting the Monitoring Features

Introduction

Note: This topic is not applicable to non-distributed servers.
Some of the features in SAS Visual Analytics Administrator depend on the monitoring server (SAS LASR Analytic Server Monitor). Examples include table details on the Process Monitor tab, per-instance memory gauges on the LASR Servers tab, and certain information on the HDFS tab.

**Network Name Resolution**

For successful functioning of the monitoring server, network name resolution might need to be modified. Make any necessary adjustments on the middle-tier machine.

With co-located Hadoop, the middle-tier machine typically has network name resolution without modification. However, if the machines in the cluster use multiple network interfaces, then verify that name resolution works.

If the middle-tier machine does not have the necessary network name resolution, the following results can occur:

- the user gets an error message
- in the bihpgrdc.monitor.console.log file, a log entry such as the following is recorded:
  
  ```
  Exception caught in LASRClient (lasr=null, host=hostname, port=nnnn)
  java.net.UnknownHostException: hostname
  action=TableInfo
  ```

  **Note:** The file is in the SAS configuration directory at `/Applications/SASVisualAnalyticsVersion/HighPerformanceConfiguration/Logs`.

  The host name that the log entry references requires name resolution on the middle-tier machine. You can alias the host name to the IP address for the grid host that is used for the SAS LASR Analytic Server.

**Managing the Monitoring Server**

The following table provides commands for managing the server process that monitors the SAS LASR Analytic Server:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start’</td>
<td><code>LASRMonitor.sh start</code></td>
</tr>
<tr>
<td>Stop</td>
<td><code>LASRMonitor.sh stop</code></td>
</tr>
<tr>
<td>Restart</td>
<td><code>LASRMonitor.sh restart</code></td>
</tr>
<tr>
<td>Display status</td>
<td><code>LASRMonitor.sh status</code></td>
</tr>
</tbody>
</table>

* You must have passwordless SSH access. See “Passwordless SSH” on page 62.

The `LASRMonitor.sh` script is in the SAS configuration directory under `/Applications/SASVisualAnalyticsVersion/HighPerformanceConfiguration`. 
Note: The LASRMonitor.sh script’s console option is not intended for use by administrators. It is used in development environments.

Logging for the Monitoring Server

Note: Changes to logging should be made only if you are advised to do so by SAS Technical Support.

Generated log files are in the SAS configuration directory under /Applications/SASVisualAnalyticsVersion/HighPerformanceConfiguration/Logs.

The following log excerpt contains a message about being unable to enumerate the grid. This message indicates that the user account that attempted to start the monitoring server is not configured correctly for passwordless SSH:

```
NOTE: SAS Grid Broker initialization is complete.

NOTE: ServerSocket open on 42088
NOTE: Executing [/opt/SASHome/SASFoundation/9.3/utilities/bin/tkgridmon, -showranks, -quiet, -guiport, 42088]
NOTE: Unable to enumerate grid.
```

Adjusting the Logging Configuration

Log Directories

In the standard configuration, SAS Visual Analytics logs are in the SAS configuration directory as follows:

- Generated logs are in /Web/Logs/server.
- Log configuration files are in /Web/Common/LogConfig.

How to Change Log Levels

**CAUTION! Excessive logging can degrade performance.** Do not use the TRACE and DEBUG logging levels unless you are directed to do so by SAS Technical Support.

The preferred method for changing a logging level is to make a temporary, dynamic change in SAS Web Administration Console.

As an alternative to making a dynamic change, you can directly edit the appropriate log configuration file. The following example demonstrates how to change the log level to debug the explorer.
1 In the SASVisualAnalyticsExplorer-log4j.xml file, change the log level to DEBUG:

```
<category additivity="false" name="com.sas.biv">
<level value="DEBUG"/>
<appender-ref ref="SAS_CONSOLE"/>
<appender-ref ref="SAS_INFO_FILE"/>
</category>
```

2 Restart the web application server.

See Administering Logging for SAS Web Applications in the SAS Intelligence Platform: Middle-Tier Administration Guide.

**How to Log Submitted Code**

To include SAS logs in the data builder and administrator logs:

1 In the SASVisualDataBuilder-log4j.xml file and the SASVisualAnalyticsAdministrator-log4j.xml file, remove the comments that enclose the SAS Job submission section.

2 Restart the SAS Web Application Server.

**TIP** Related functionality is provided by a user preference. See “Record actions as SAS statements” on page 86.

**How to Log LASR Requests**

To log commands that are issued to a SAS LASR Analytic Server from the designer or the web viewer:

1 In the logging contexts section of the SASVisualAnalyticsDesigner-log4j.xml file and the SASVisualAnalyticsViewer-log4j.xml file, remove the comments that enclose the tags for the com.sas.lasr.command category.

2 Restart the SAS Web Application Server.

**Logging of Access Denials**

Metadata-layer access denials are logged as follows:

- For requests from the administrator and the data builder, access denials are logged in the LASR authorization log (SASLASRAuthorizationVersion.log).
- For requests from other SAS Visual Analytics applications, access denials are logged in the application’s log file (for example, SASVisualAnalyticsExplorerVersion.log).

Log entries provide details about the cause of the access denial, indicating which user lacks which permissions for which metadata object. Here is an extracted example:

```
** Access Denied **
Action: 2
Table: HPS.CARS
```
Logging for SAS Mobile BI

The logging configuration for SAS Mobile BI is defined in the SASVisualAnalyticsTransport-log4j.xml file.

You can use the viewerservices.validate.schema.* properties to increase logging for the rendering of reports on mobile devices. See “Configuration Properties: SAS Mobile BI” on page 87.

Logging for Platform Servers

See Administering Logging for SAS Servers in the SAS Intelligence Platform: System Administration Guide.

Thresholds for High-Cardinality Data

Introduction

High-cardinality data has one or more columns that contain a very large number of unique values. For example, user names, e-mail addresses, and bank account numbers can be high-cardinality data items.

SAS Visual Analytics supports billions of values that are aggregated to thousands of values. If the billions of values in a table have millions of unique identifiers, then a column that contains those identifiers is a high-cardinality data item.

To help ensure that users get meaningful results in a timely fashion, the number of unique values that can be returned for certain visualizations and report objects is constrained. When a user selects a high-cardinality data item, the outcome is determined by any applicable thresholds, the number of unique values in the data, and the user’s selections.

The following topics provide information about two distinct levels of thresholds: client-side thresholds and middle-tier thresholds.

Client-Side Thresholds for High-Cardinality Data

Client-side thresholds are specific to an individual application (such as the explorer), or to a group of applications (such as the designer and the web viewer). For some requests that exceed a client-side threshold, an error is displayed, and no results are returned. For some requests that exceed a client-side threshold, but do not exceed a middle-tier threshold, adapted results are returned.
Note: In general, client-side thresholds are fixed. An exception is that a user can select a low, medium, or high threshold level as a user preference in the explorer. On a computer that has low memory availability, setting the client-side threshold to Low can help prevent events such as system crashes.

Client-side thresholds for visualizations and report objects are documented in the Data Limits appendix in the SAS Visual Analytics: User’s Guide. The appendix explains the adapted responses that clients provide for certain requests that exceed a client-side threshold (but do not exceed a middle-tier threshold).

**Middle-Tier Thresholds for High-Cardinality Data**

Middle-tier thresholds have a wider scope, affecting all instances of the specified visualization or report object. Compared to client-side thresholds, middle-tier thresholds are less granular and less restrictive. For requests that exceed a middle-tier threshold, an error message is displayed, and no results are returned. The default thresholds work in almost all environments. In general, users filter or group any high-cardinality data items, so requests rarely exceed a middle-tier threshold.

The following table documents the middle-tier thresholds. The second column indicates the maximum number of unique values (not the maximum volume of data).

<table>
<thead>
<tr>
<th>Visualization or Report Object</th>
<th>Rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decision trees*</td>
<td>10,000</td>
</tr>
<tr>
<td>Crosstabs</td>
<td>50,000</td>
</tr>
<tr>
<td>Tables (in the designer and the viewers)</td>
<td>50,000</td>
</tr>
<tr>
<td>Box plots: at least one measure, no categories**</td>
<td>50,000</td>
</tr>
<tr>
<td>Bar charts: single category</td>
<td>50,000</td>
</tr>
<tr>
<td>Heat maps: single category</td>
<td>50,000</td>
</tr>
<tr>
<td>Line charts: at least one measure, single category (numeric, date, time, or string)</td>
<td>50,000</td>
</tr>
<tr>
<td>Bubble plots: three measures, grouped</td>
<td>50,000</td>
</tr>
<tr>
<td>Bubble plots: three measures, grouped with animation category</td>
<td>50,000</td>
</tr>
<tr>
<td>Bubble plots: three measures, not grouped, horizontal or vertical series (or both)</td>
<td>50,000</td>
</tr>
<tr>
<td>Bubble plots: three measures, no categories</td>
<td>100,000</td>
</tr>
<tr>
<td>Scatter plots</td>
<td>100,000</td>
</tr>
</tbody>
</table>
Visualization or Report Object | Rows
---|---
Tables (in the explorer) | 100,000

* There is also a time-out period for decision tree calls. See "vae.DecisionTreeTimeout" on page 92.
** If there is no category, one box is applied for each measure, up to 400 measures.

**Properties That Affect Middle-Tier Thresholds**

**CAUTION! Increasing a middle-tier threshold can affect performance and stability.** The default settings are appropriate in most environments. Do not set excessively high thresholds. If you have questions about adjusting the following properties, contact SAS Technical Support.

The following properties affect middle-tier thresholds:

- **va.DistinctCountServerLimit**
  - sets the distinct count limit for graphs. By default, there is no distinct count limit for graphs. The default is -1.
  - Scope: Entire suite

- **va.DistinctCountDataPanelLimit**
  - sets the distinct count limit for data that is displayed in a data panel. This property affects only the data panel, not the distinct count limits within graphs. The default is 5,000.
  - Scope: Entire suite

- **va.SortResultServerLimit**
  - sets the maximum number of values that can be returned for detail queries that are run with sorting. This property affects only results in list tables for which details are turned on.
  - Scope: Entire suite, except for the explorer

- **va.CategoryCardinalityServerLimit**
  - sets the maximum number of values for category crossings. Only a fixed (and finite) number of category crossings are supported. For example, if you drag and drop "First name" and "Last name" onto the population of the United States, the server might generate 200 million different values. This property determines how high the cardinality can be and still allow the server to process and return results to the client. If the number of values for category crossings exceeds this limit, the query is not run.
  - Scope: Entire suite, except for the explorer

- **va.SummaryServerRowLimit**
  - sets the maximum number of values that can be returned to the middle tier for further processing. For example, for high-cardinality data that is sorted by first name, the number of values computed could be very large.
  - Scope: Entire suite, except for the explorer (which uses vae.SummaryServerLimit)

- **va.MidtierCellLimit**
  - sets the maximum size of a crosstab.
  - Scope: Entire suite, except for the explorer
va.maxPeriodCalculations
specifies the maximum number of calculated columns that are constructed for period calculations. If this limit is exceeded for a particular period measure, excess calculations are excluded, and existing calculations (for that particular period measure) are replaced with missing values. The user is prompted to apply a filter to reduce the number of calculations. The default is 800.

Note: Software optimizations reduce the number of calculations before this limit is applied, so this limit is rarely exceeded. An example of the effect of this property is a distinct count calculation with cumulative periods (the number of unique date values that are visible cannot exceed the specified limit).

Scope: designer, web viewer, transport services

va.MaxSparkTables
sets the maximum number of spark tables. The default is 300.

Scope: Entire suite, except for the explorer

va.CheckCardinalityBeforeQuery
controls whether cardinality pre-checks occur. The default value is -1 (which disables this constraint). By default, pre-checks do not occur.

Scope: Entire suite, except for the explorer

va.CheckCardinalityWithinQuery
controls whether SAS LASR Analytic Server enforces cardinality limits. By default, these checks do occur.

Scope: Entire suite, except for the explorer

va.BoxPlotServerLimit
sets middle-tier thresholds for box plots that have at least one measure and no more than one category.

Scope: Explorer only

va.DecisionTreeServerLimit
sets the middle-tier threshold for decision trees.

Scope: Explorer only

va.FetchRowsServerLimit
sets middle-tier thresholds for tables.

Scope: Explorer only

va.FrequencyServerLimit
sets middle-tier thresholds for bar charts that have a single category. This constraint is applied before a selection list of values is displayed.

Scope: Explorer only

va.RealScatterServerLimit
sets middle-tier thresholds for scatter plots and bubble plots that have three measures and no categories.

Scope: Explorer only

va.ScatterPlotServerLimit
sets middle-tier thresholds for heat maps that have exactly one category.

Scope: Explorer only
vae.SummaryServerLimit
sets middle-tier thresholds for the following visualization types:

- crosstabs
- line charts that have at least one measure and a single category (numeric, date, time, or string)
- bubble plots that are grouped with no series, grouped with animation, or with series and not grouped

Scope: Explorer only (other applications use va.SummaryServerRowLimit)

---

**User Preferences in the Administrator**

**Introduction**

This topic documents individual user preferences that are specific to SAS Visual Analytics Administrator. For information about global preferences, see *Specifying Your Preferences* in the *SAS Visual Analytics: User’s Guide*.

To review or set preferences, select **File ➤ Preferences** from the main menu bar in SAS Visual Analytics Administrator.

**Server Preference**

In the Preferences window, under **SAS Visual Analytics Administrator ➤ Application Server**, the **Default application server** specifies which SAS Application Server (server context) is used to run code that is submitted in the administrator.

*Note:* Only application servers that are configured to use the job execution service are listed.

**Other Preferences**

In the Preferences window, under **SAS Visual Analytics Administrator ➤ Manage Environment**, the following settings are available:

**Resource monitor sample rate (ms)**

Specifies, in milliseconds, the sampling rate that the resource monitor uses for polling the machines in the cluster. This setting is not applicable to a non-distributed server.

**Process monitor sample rate (ms)**

Specifies, in milliseconds, the sampling rate that the performance monitor uses for polling application instances. This setting is not applicable to a non-distributed server.

**Show the processes that measure performance**

Controls whether processes that measure performance are included in the process-monitoring graphs. To include performance measurement processes in the graphs, select the check box. If several instances of performance measurement processes are running, they can negatively impact performance. This setting is not applicable to a non-distributed server.
Record actions as SAS statements
Saves the SAS code that SAS Visual Analytics Administrator generates when you perform certain tasks. You can save all recorded code in a single file or you can save the recorded code for each task in its own file.

If you enable recording, SAS code for the following actions is saved:

- Starting and stopping a SAS LASR Analytic Server.
- Loading, reloading, and unloading data.
- Adding data to a co-located data provider.
- Deleting HDFS tables.

Note: You can modify and schedule recorded statements. However, metadata server connection information is not recorded. For information about the metadata server connection options, see SAS Language Interfaces to Metadata.

Designating a SAS Application Server

Which Server is Used?

The administrator and the data builder have a user preference that determines which SAS Application Server is used to run all submitted SAS code. See “User Preferences in the Administrator” on page 85.

The designer and the explorer do not have a corresponding user preference. Instead, they use a suite-level configuration property to determine which server to use. See “va.defaultWorkspaceServer” on page 92.

Note: For the designer and the explorer, the server designation affects actions such as importing data. To support import actions, the designated server must support the job execution service.

How to Add a New SAS Application Server

Adding a new SAS Application Server is an advanced platform-level task. See Managing SAS Application Servers in the SAS Intelligence Platform: Application Server Administration Guide.

The following details are specific to SAS Visual Analytics:

- If the server is used by the administrator or the data builder or to import data, configure support for the job execution service.
- If the server is used by the administrator or data builder, instruct users to select the server in their application preferences. For example, see “User Preferences in the Administrator” on page 85.
- If the server is used for importing data in the designer or explorer, specify the server in a suite-level configuration property. See “va.defaultWorkspaceServer” on page 92.
How to Configure the Job Execution Service

To enable the job execution service for a SAS Application Server:


2. Right-click JobExecutionService, and select Properties.

3. On the Settings tab, move the SAS Application Server from the Available list to the Selected list. Click OK.

Changes take effect when the SAS Web Application Server is restarted. For details and alternatives, see Job Execution Service in the SAS Intelligence Platform: Middle-Tier Administration Guide.

---

Configuration Properties: SAS Mobile BI

How to Set Advanced Properties for SAS Mobile BI


3. On the Advanced tab of the Properties dialog box, add or set values.

   **TIP** The lock icons indicate which settings can be changed in child components. The lock icons do not indicate which changes you can make to the current component.

4. Restart the web application server.

---

Reference for Selected Properties

**Printing.Timeout**

sets a maximum wait time (in milliseconds) that affects printing reports from applications such as the designer and the web viewer. The default is 900000 milliseconds (15 minutes). To disable this property, set its value to 0.

**Note:** This setting does not affect the first phase of a print request, which generates a report package. This setting affects only the second phase of a print request, which uses a stored process call to execute the print routine.

**Note:** In the current release, printing is a preproduction feature.
viewerservices.company.banner.logoUrl
provides the URL for an alternate logo in the SAS Mobile BI banner. The URL must be accessible to the mobile device.

viewerservices.company.banner.message
provides a custom message for the SAS Mobile BI banner.

viewerservices.company.banner.title
provides a custom title for the SAS Mobile BI banner.

viewerservices.data.default.interactive.drill.depth
determines how much data is sent to a mobile device for offline drilling. This property is applicable to visualizations that reference a hierarchy. The default is 3 (users can drill down three levels). If certain reports require users to have the ability to drill down more than three levels into a hierarchy, modify the value.

viewerservices.default.max.cells.produced
sets the maximum number of data cells that can be delivered to a mobile device for a single data query. The default is 250000 data cells, which is sufficient for most environments and does not cause the web application server to crash. In very rare scenarios, you might need to modify the value.

Note: If the number of data cells in a query exceeds the value specified for this property, the data that is returned to SAS Mobile BI is truncated. Data in the displayed report is not complete.

viewerservices.enable.whitelist.support
controls which approach is used to manage mobile devices. Valid values are:

- false: causes the blacklist to be enforced and the whitelist to be ignored. With this setting, all mobile devices can use SAS Mobile BI except for those devices that are on the blacklist. This is the default.
- true: causes the whitelist to be enforced and the blacklist to be ignored. With this setting, only mobile devices that are on the whitelist can use SAS Mobile BI.

CAUTION! Enabling the whitelist can disrupt existing users. Make sure that all valid mobile devices are on the whitelist before you make the change.

TIP As an alternative to setting this property explicitly, you can set it from within SAS Visual Analytics Administrator. See “Change How Devices Are Managed” on page 47.

viewerservices.image.default.max.bytes
sets the maximum size of images (PNG, BMP, JPEG, or GIF) that can be delivered to a mobile device. Larger images are resized on the server side before delivery. The default is 300 KB, which is sufficient for most environments. In very rare scenarios when you want to change this constraint, consider modifying the value. To entirely disable resizing of images in the middle tier, set the value to 0. However, to ensure faster download times and smaller memory footprints on the mobile device, do not increase the value of this property or set the value to 0.

Note: Users can customize image resizing on their devices by setting the Scale type option (under Insert ▶ Other ▶ Image). If the option is set to None, the user’s device is exempt from middle-tier resizing.
viewerservices.lasr.socketTimeout.milliseconds.interactions
sets the maximum wait time for when SAS Mobile BI attempts to contact SAS LASR Analytic Server. This property is applicable to live requests from a mobile device for tasks such as filtering, brushing, and drilling. The default is 30000 milliseconds (30 seconds), which is sufficient for most environments. If sessions between SAS Mobile BI and SAS LASR Analytic Server are timing out, consider modifying the value.

viewerservices.lasr.socketTimeout.milliseconds.subscribe
sets the maximum wait time for a response to a query in a subscribed report when SAS Mobile BI contacts the SAS LASR Analytic Server. The default is 300000 milliseconds (5 minutes), which is sufficient for most environments. If the queries within some reports take an excessive amount of time for completion, consider modifying the value.

viewerservices.passcode.attempts
limits the number of sequential failed attempts to enter a passcode. The default is 5. If a user reaches the limit, the user is locked out of the app for 15 minutes. After the lockout interval, the user can again attempt to enter his or her passcode. If the user reaches the limit again, all custom content (data, reports, settings, and connection information) is removed from the mobile device.

Note: This property is applicable to only those users who are subject to the capability “Require Passcode on Mobile Devices”.

viewerservices.passcode.timeout
specifies, in minutes, how frequently a user must re-enter his or her passcode. The default is 15.

viewerservices.validate.schema.write
enables XML schema validation when reports are rendered in SAS Mobile BI. When this property is set to true, all actions that apply to the writing of reports are captured in the transport log. See “Adjusting the Logging Configuration” on page 79. The default is false. Set this property only if SAS Technical Support instructs you to do so.

viewerservices.validate.schema.create
enables XML schema validation when reports are rendered in SAS Mobile BI. When this property is set to true, all actions that apply to the creation of reports are captured in the transport log. The default is false. Set this property only if SAS Technical Support instructs you to do so.

viewerservices.validate.schema.read
enables XML schema validation when reports are rendered in SAS Mobile BI. Also, this property checks for schema validation errors when reports are created in the mobile viewer. When this property is set to true, all actions that apply to opening and viewing reports are captured in the transport log. The default is false. Set this property only if SAS Technical Support instructs you to do so.
Configuration Properties: SAS Visual Analytics

How to Set Advanced Properties for SAS Visual Analytics

   - For suite-level properties, right-click Visual Analytics Version, and select Properties.
   - For component-specific properties, expand the Visual Analytics Version node, right-click on the component, and select Properties. For example, to set properties that begin with vae., right-click Visual Analytics Explorer Version.

2. On the Advanced tab of the Properties dialog box, add or set values.

   **TIP** The lock icons indicate which settings can be changed in child components. The lock icons do not indicate which changes you can make to the current component.

3. Restart the web application server.

Reference for Selected Properties

To adjust any of the following properties, make changes on the Advanced tab for the Visual Analytics node.

App.AllowGuest
   Enables or disables guest access. Valid values are true and false. See “Supporting Guest Access” on page 66.

las.caching.key.lifetime
   Sets the duration of time (in seconds) for which a LASR security key is cached in the middle tier. The default is 180 seconds (3 minutes). Do not set a custom value unless you are directed to do so by SAS Technical Support.

las.caching.permission.lifetime
   Sets the duration of time (in seconds) for which permission information is cached by the LASR authorization service. The default is 900 seconds (15 minutes). Do not set a custom value unless you are directed to do so by SAS Technical Support.

las.caching.user.lifetime
   Sets the duration of time (in seconds) for which user information is cached by the LASR authorization service. The default is -1 (the cache does not have a time-based expiration period). With the default setting, user objects remain in the cache until the requesting user’s session ends. Do not set a custom value unless you are directed to do so by SAS Technical Support.
va.Alert.*
properties that enable and affect alerts and notifications for report objects.
See “Configuration Properties for Alerts” on page 72.

va.ComparisonEpsilon
specifies a small number to be used to account for floating-point rounding
error in the following numeric comparisons: equals, not equals, less than,
greater than, less than or equals, greater than or equals. Valid values are
doubles. The default is \(1e-12\). In the unusual circumstance in which users
find that some values are being compared as equal when they should not be
(or vice versa), consider changing this value. The epsilon comparison is
relative to the size of the numbers that are being compared (it is not
absolute). When the following expression is true, a and b are considered to
be equal:

\[
\text{ABS}(a-b) \leq \epsilon \times \text{MAX}(\text{ABS}(a), \text{ABS}(b))
\]

va.MaxTiesToIncludeOnRank
sets the maximum number of identically ranked values that can be returned
in a rank operation. Valid values are integers. The default is 100.

va.SASGeomapCommunicationProtocol
sets the protocol for connections between SAS Visual Analytics and an
OpenStreetMap server that SAS hosts. Valid values are http and https.

va.SASGeomapEsriURL
specifies a URL that references an Esri map server. The full URL includes
protocol, host name, and REST endpoint of the map server (for example,
http://services.arcgisonline.com/ArcGIS/rest/services). This
property enables a site to use an alternate Esri map server.

va.SelfServe.MaxUploadSizeInMegabytes
sets the maximum file size (in megabytes) that a user can import. This
property affects importing local files in the data builder, the explorer, and the
designer. The default, 4096, corresponds to browser-based constraints. To
further constrain import activities, set a lower value for this property. You
cannot use this property to circumvent browser-based constraints.

va.SelfService.ImportRowsHardCap
sets a maximum number of rows for a self-service import action. If this value
is exceeded, no data is imported. No initial value is set (initially, no limit is
imposed).

Note: Enforcing a threshold requires a query to the data provider for each
import action, so setting a value for this property can negatively impact
performance.

va.SelfService.ImportRowsSoftCap
sets the number of rows that triggers a warning message for a user who is
performing a self-service import action. The message indicates that the
import action might take a long time. No initial value is set (initially, no limit is
imposed).

Note: Enforcing a threshold requires a query to the data provider for each
import action, so setting a value for this property can negatively impact
performance.

va.GeoMapMaxResolution
sets the maximum resolution that can be applied when rendering a geo map.
This property is applicable only if you are also using the
va.GeoMapServerUrl property. The default is 156543.0339.
va.GeoMapNumResolutions
sets the number of levels of rendered details about the server. This value
determines the number of increments by which a user can zoom in to a geo
map. This property is applicable only if you are also using the
va.GeoMapServerUrl property. The default is 18.

va.GeoMapServerUrl
specifies a comma-delimited list of URL addresses that reference map
servers (for example, http://serverA.org, http://serverB.org,

va.dataServer.PublicLibrary
identifies the standard co-located data provider library (for example, Visual
Analytics Public HDFS). The window for adding data to a co-located
data provider is initially prepopulated with this value. If you change the name
of the referenced library, you must also update this property.

va.defaultPublicFolder
identifies the standard metadata location for LASR tables that are generated
by data import and load activities (for example, /Shared Data/SAS Visual
Analytics/Public/LASR). If you change the name of the referenced
folder, you must also update this property.

va.defaultWorkspaceServer
identifies the SAS Application Server that contains the workspace server that
runs submitted code. If you change the name of the referenced server (for
example, SASApp), you must also update this property. See “Designating a
SAS Application Server” on page 86.

va.monitoringPath
specifies the host location for monitoring information for autoload and reload-
on-start. In a multi-machine deployment, this location is on the workspace
server host. The standard location is within the SAS configuration directory
at /Applications/SASVisualAnalyticsVersion/
VisualAnalyticsAdministrator/Monitoring.

va.publicLASRLibrary
identifies the general purpose library for data import and load activities (for
example, Visual Analytics Public LASR). If you change the name of the
referenced library, you must also update this property.

va.publicLASRServer
identifies the server that is associated with the va.publicLASRLibrary (for
example, Public LASR Analytic Server).

va.supportSharedThumbnails
determines whether the home page shows specific preview images. Valid
values are true and false. The default is false. (By default, generalized
images are used instead of specific images.)

CAUTION! Shared thumbnails reflect the most recently rendered version
of an object and are not subject to each requesting user’s data access
permissions. Before you enable shared thumbnails, consider the security
implications.

To set any of the following properties, add them to the Advanced tab for the
Visual Analytics Explorer node.

vaец.DecisionTreeTimeout
affects how long (in seconds) the explorer waits for a response after the
explorer makes a decision tree request. The default is 300.
vae.PageRowCount
limits the amount of data that can be returned for a table visualization. If table sorting is enabled, the vae.PageRowCount limit is applicable only if its value exceeds the value that is specified for the vae.SortResultLimit property. The default is 10000.

Note: For example, if the value is 10000, then 10000 rows of data are returned to the client. If the user scrolls through the data, and passes the row that is numbered 10001, the client prompts the SAS LASR Analytic Server for the next 10000 rows.

vae.SortResultLimit
limits the number of rows that can be returned after sorting is performed. Because sorting on large data that is distributed across several machines can take a long time, the number of rows that are returned after a sorting process ends is limited. The remainder of the data is truncated. The default is 5000.

vae.TableSortingEnabled
specifies whether users in the explorer can click on a column heading to sort the items. Valid values are true and false. The default is true.
Troubleshooting

Troubleshooting: SAS Visual Analytics .................................................. 95
Access to Resources and Functionality ................................................. 95
Server Operation and Monitoring ......................................................... 97
Data Load and Import ........................................................................... 99
Search, Themes ..................................................................................... 100

Troubleshooting: SAS Mobile BI .......................................................... 101

Permission Origins ................................................................................ 101
Introduction .......................................................................................... 101
Simple Permission Origins .................................................................. 101
Inherited Permission Origins ............................................................... 102

Troubleshooting: SAS Visual Analytics

Access to Resources and Functionality

Issue: Users get a "Public access denied" error when they attempt to log on.

Resolution:
- Make sure that each user has a well-formed definition in metadata. On a user's Accounts tab, this problem can be caused by a user ID that is not in a qualified format. This problem is not caused by passwords or authentication domain assignments on a user's Accounts tab. See “Adding Users” on page 5.

Issue: Users cannot connect to the guest access URLs.

Resolution:
- Make sure that guest access is enabled. See “Supporting Guest Access” on page 66.
- Make sure that the SAS Anonymous Web User exists in metadata and is appropriately configured. See Using the SAS Anonymous Web User with SAS Authentication in the SAS Intelligence Platform: Middle-Tier Administration Guide.
- Make sure that the SAS Anonymous Web User has ReadMetadata access to the /System folder.

Issue: Users cannot access any LASR tables in the explorer or the designer.
Resolution:

- Make sure that the SAS LASR Analytic Server is running and that tables are loaded.

- In SAS Management Console, make sure that the LASR authorization service is enabled by verifying that the **Use LASR authorization service** check box is selected. This setting is on the **Options** tab in the Properties window for the SAS LASR Analytic Server’s connection object.

- Make sure that each LASR library for the target server has a unique server tag. The LASR authorization service identifies each library by its server tag. If the LASR authorization service cannot uniquely identify each library, it cannot acquire definitive authorization decisions, so it denies access. See “Server Tags” on page 54.

  **Note:** If duplicate server tags are the cause, the LASR authorization service log contains the message: **Access Error - Multiple libraries found in metadata with matching libref.** The log (SASLASRAuthorizationVersion.log) is located in the SAS configuration directory under /Web/Logs/server.

- In the metadata definitions for the SAS LASR Analytic Servers in the deployment, make sure that each server uses a unique port. If multiple servers on a host are assigned to the same port, data cannot be accessed. See “Add a SAS LASR Analytic Server” on page 41.

**Issue:** Users cannot access a particular LASR table.

Resolution:

- On the table’s **Authorization** page, make sure that users have the ReadMetadata and Read permissions for the LASR table. Also, make sure that the SAS Trusted User’s ReadMetadata access is not blocked. See “Setting Permissions” on page 29.

- On the table’s **Authorization** page, look for any conditional grants ☑️. To restore access, remove any permission conditions that are no longer valid. If appropriate, set new conditions.

  **Note:** A table that has a conditional grant becomes inaccessible if its metadata is updated with information that renders the permission condition invalid. For example, a permission condition might reference a column that is no longer part of the table.

- Make sure that each LASR table for the target LASR library has a unique name. For example, a copy-and-paste action in the data builder can result in multiple tables that have the same name within a particular library. To restore access, delete one of the tables. See “Unload, Reload, or Delete Tables” on page 18.

  **Note:** The LASR authorization service identifies each table by its LASR name, which is a combination of the library’s server tag and the table’s name. If the LASR authorization service cannot uniquely identify each table, it cannot acquire definitive authorization decisions, so it denies access.

- Make sure that concurrent user logons are allowed. See “Policy.ConcurrentUserLogins” on page 61.

**Issue:** Certain application features are not visible to certain users.

Resolution:
Make sure that the user has the appropriate capabilities. See Appendix 1, “Reference: Roles and Capabilities,” on page 121.

Make sure that the user is not connected to a guest access URL. See “Supporting Guest Access” on page 66.

**Issue:** You cannot take a capability away from a user.

**Resolution:**

- Make sure that the user is not in any role that provides that capability. Consider indirect and implicit memberships, as well as direct memberships. Remember that all registered users are automatically members of the PUBLIC and SASUSERS groups. See “Predefined Roles” on page 121.

- Make sure that the user is not in the **Metadata Server: Unrestricted** role.

**Issue:** You cannot access a third-party DBMS table from SAS Visual Analytics Administrator.

**Resolution:**

- From the main menu bar, select **File ▶ Clear Credentials Cache**. Then, attempt access again. If you are prompted for a user ID and password, enter DBMS credentials.

- If the third-party DBMS uses proprietary authentication, you might need to store a DBMS user ID and password. See How to Store Passwords for a Third-Party Server in the SAS Intelligence Platform: Security Administration Guide.

**Issue:** You cannot register tables.

**Resolution:**

- Make sure that you have the necessary metadata-layer permissions. See “Permissions by Task” on page 31.

- Make sure that you have Read access to the physical source tables (host-layer permissions).

- On Windows, make sure that your host account has the **Log on as a batch job** Windows privilege. See “Host Account Privileges” on page 7.

- If you are prompted for a user ID and password, enter host credentials for the workspace server.

**Issue:** When you attempt to run exported code, you cannot connect to the metadata server.

**Resolution:**

- Metadata server connection information is not included in exported code. Either supply connection information or use a SAS session that already includes connection information (for example, the SAS DATA Step Batch Server). For information about metadata server connection options, see SAS Language Interfaces to Metadata.

---

**Server Operation and Monitoring**

**Issue:** You cannot start a SAS LASR Analytic Server.
Resolution:
- Make sure that any host-layer requirements are met. See “Host Account Privileges” on page 7.
- Make sure that each server on a particular host uses a unique port number.
- If the error is Procedure LASR not found, make sure that the SAS Application Server that is selected in your SAS Visual Analytics Administrator preferences (File ▶ Preferences) has a valid license for SAS Visual Analytics software.
- If a message or log indicates that a path is not in the list of accessible paths, see “Locked-Down Servers” on page 58.

Issue: You cannot stop a SAS LASR Analytic Server.
Resolution:
- Make sure that you have the Administer permission for the server.
- Make sure that any host-layer requirements are met. See “Host Account Privileges” on page 7.
- If the error is Procedure LASR not found, make sure that the SAS Application Server that is selected in your application preferences (File ▶ Preferences) has a valid license for SAS Visual Analytics software.
- Make sure that concurrent user logons are allowed. See "Policy.ConcurrentUserLogins" on page 61.

Issue: The SAS LASR Analytic Server Monitor graphs are blank.
Resolution:
- Make sure that the SAS LASR Analytic Server is running.
- Make sure that the SAS LASR Analytic Server is distributed. Monitoring is not supported for non-distributed servers.
- Make sure that the TKGrid location in the service.properties file is correct. The file is located in the SAS configuration directory under /Applications/SASVisualAnalyticsVersion/HighPerformanceConfiguration.
  
Note: Any changes that you make to the High-Performance Analytics environment install location field in a server definition in SAS Management Console must also be manually made in the monitoring server’s properties file.
- Restart the monitoring server. See “Managing the Monitoring Server” on page 78.

Issue: On the Process Monitor tab, table details are not provided.
Resolution:
- Make sure that the middle-tier machine has the necessary network name resolution. See “Network Name Resolution” on page 78.

Issue: On the LASR Servers tab, per-instance memory gauges are not available.
Resolution:
- For a non-distributed server, the memory gauges are not supported.
For a distributed server, make sure that the middle-tier machine has the necessary network name resolution. See “Network Name Resolution” on page 78.

Data Load and Import

**Issue:** Users cannot import data.

**Resolution:**
- Make sure that users can access the SAS LASR Analytic Server host using an account that has the necessary privileges. See “Host Account Privileges” on page 7.
- Make sure that users have the necessary metadata-layer permissions for the output folder and LASR library. See “Setting Permissions” on page 29.
- Make sure that the designated server supports the job execution service. See “Designating a SAS Application Server” on page 86.
- Make sure that concurrent user logons are allowed. See “Policy.ConcurrentUserLogins” on page 61.
- For imports to the public area, make sure that the library, server, and folder that are referenced by the va.publicLASRLibrary, va.publicLASRServer, and va.defaultPublicFolder configuration properties exist. See “Configuration Properties: SAS Visual Analytics” on page 90.
- For imports of local files to a LASR library that supports reload-on-start, make sure that users have host access to the associated data provider library. See “Reload-on-Start” on page 15.

**Issue:** Users cannot browse to locate a source data set (when importing a SAS data set from a server).

**Resolution:**
- In SAS Management Console, make sure the pooled workspace server validates.
- Make sure the account under which the pooled workspace server runs (for example, **sassrv**) has host access to the data set.

**Note:** The pooled workspace server is used only to browse to the source data set. The import action is performed by a standard workspace server.

**Issue:** You cannot load a table from co-located Hadoop.

**Resolution:**
- Make sure that the source library is paired with a LASR library through a match between the HDFS path and the server tag. For example, tables in an HDFS library with the path `/users/sasdemo` must be loaded to a LASR library that has `users.sasdemo` as its server tag. See “Add a SAS LASR Analytic Library” on page 43.

**Note:** The message for this issue includes the following statement: You have selected to load a table from co-located storage into a library that has a server tag that does not match the path in co-located storage.
Make sure that the Hadoop server and the SAS LASR Analytic Server have identical, fully qualified host names in the **Associated Machine** field in their metadata definitions.

- For the Hadoop server, select the **Options** tab.
- For the SAS LASR Analytic Server, select the **Options** tab, click the **Advanced Options** button, and select the **Additional Options** tab.

**Note:** The message for this issue describes the HDFS library as unidirectional.

**Issue:** On the LASR Tables tab, tables are not listed.

**Resolution:**

- Make sure that the middle-tier machine has the necessary network name resolution. See "**Network Name Resolution**" on page 78.
- Make sure that the filter (in the tab’s toolbar) is not hiding tables that you expect to see.

**Issue:** In the **Load a Table** window, the **OK** button is disabled.

**Resolution:**

- In the **LASR Table** section, enter a name. Click in one of the other fields in the window, and then click **OK**. In general, values in the **Load a Table** window are pre-populated. An exception is when you directly load a table to a library that already contains a table that has the same name as the source table.

**Issue:** You cannot change the name of the output table when loading data from a co-located data provider.

**Resolution:**

- Add the table to the co-located data provider again. In that transaction, assign a different name to the output table. When you load data from a co-located data provider, you cannot choose a different name for the output table. See "**Interactive Load**" on page 17.

### Search, Themes

**Issue:** The search index is stale.

**Resolution:**

- Verify that the indexing server is running. If necessary, restart the indexing server. See "**How the Search Index Is Created**" on page 74.

**Issue:** Custom themes are not applied to reports.

**Resolution:**

- Make sure that the custom themes exist in the current environment. Custom themes are not promoted with the reports that use them. See "**Promotion of Custom Themes**" on page 70.
Troubleshooting: SAS Mobile BI

Issue: A user cannot open reports in an offline device.
Resolution:
- Make sure that the user is not unrestricted and is not in any role that provides the capability that prevents this action. See “Purge Mobile Report Data” on page 125.

Issue: A user is prompted for an application passcode.
Resolution:
- Make sure that the user is not unrestricted and is not in any role that provides the capability that introduces this requirement. See “Require Passcode on Mobile Devices” on page 125.

Issue: On the Mobile Devices tab, a message indicates that a list is not currently in use.
Resolution:
- By design, only one list (either the blacklist or the whitelist) is in use. See “About Managing Mobile Devices” on page 45.

Permission Origins

Introduction

Permission origins identify the source of each effective permission in the metadata authorization layer. This information can be useful in troubleshooting. It answers the question: Why is this identity granted (or denied) this permission?

In the origins answer, only the controlling (winning, highest precedence) access control is shown. If there are multiple tied winning controls, they are all shown. Other, lower precedence controls are not shown in the answer.

Origins information is available on an object’s Authorization page. See “About the Authorization Page” on page 34.

Simple Permission Origins

The following table provides simple examples of permission origins answers. In each example, we are interested in why UserA has an effective grant on FolderA. In each example, UserA is a direct member of both GroupA and GroupB. Each row in the table is for a different (independent) permissions scenario. In the table, the first column depicts the contents of the Origins window. The second column interprets the information.
### Table 8.1 Origins: Simple Examples

<table>
<thead>
<tr>
<th>Origins Information</th>
<th>Source of UserA's Effective Grant on FolderA</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ UserA [Explicit]</td>
<td>On FolderA, an explicit grant for UserA</td>
</tr>
<tr>
<td>✓ GroupA [Explicit]</td>
<td>On FolderA, an explicit grant for GroupA</td>
</tr>
<tr>
<td>✓ GroupB [Explicit]</td>
<td>Note: Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).</td>
</tr>
<tr>
<td>✓ GroupA [ACT: GroupARead]</td>
<td>On FolderA, an ACT pattern grant for GroupA (from a directly applied ACT)</td>
</tr>
<tr>
<td>✓ SASUSERS [ACT: GenRead]</td>
<td>On FolderA, an ACT pattern grant for SASUSERS (from a directly applied ACT)</td>
</tr>
<tr>
<td>✓ GroupA [ACT: GroupARead]</td>
<td>On FolderA, ACT pattern grants for GroupA and GroupB (from two different directly applied ACTs)</td>
</tr>
<tr>
<td>✓ GroupB [ACT: GroupBRead]</td>
<td>Note: Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).</td>
</tr>
<tr>
<td>✓ GroupA [ACT: GroupABRead]</td>
<td>On FolderA, ACT pattern grants for GroupA and GroupB (from the same directly applied ACT)</td>
</tr>
<tr>
<td>✓ GroupB [ACT: GroupABRead]</td>
<td>Note: Two settings are shown because they are tied and they both win (UserA is a direct member of GroupA and GroupB).</td>
</tr>
<tr>
<td>✓ UserA is unrestricted.</td>
<td>UserA's status as an unrestricted user (someone who is unrestricted is always granted all permissions)</td>
</tr>
</tbody>
</table>

### Inherited Permission Origins

In many cases, the controlling setting is not on the current object. Instead, the controlling setting is defined on a parent object and inherited by the current object.

The following table provides examples in which the controlling setting comes from a parent object. Because the source of the effective permission is a parent object, the answer must identify which parent object has the controlling setting. For this reason, the answers in the following examples identify both a parent object (the object that has the controlling setting) and the controlling setting, itself.

In each example, we are interested in why UserA has an effective grant on FolderA. In each example, UserA is a direct member of both GroupA and GroupB. Each row in the table is for a different (independent) permissions scenario. In the table, the first column depicts the contents of the Origins window. The second column interprets the information.
### Table 8.2 Origins: Inheritance Examples

<table>
<thead>
<tr>
<th>Origins Information</th>
<th>Source of UserA's Effective Grant on FolderA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="ParentFolderA" /> <img src="image" alt="UserA" /> [Explicit]</td>
<td>On ParentFolderA, an explicit grant for UserA</td>
</tr>
<tr>
<td><img src="image" alt="ParentFolderA" /> <img src="image" alt="GroupA" /> [Explicit]</td>
<td>On ParentFolderA, an explicit grant for GroupA</td>
</tr>
<tr>
<td><img src="image" alt="ParentFolderA" /> <img src="image" alt="GroupA" /> [Explicit] <img src="image" alt="GroupB" /> [Explicit]</td>
<td>On ParentFolderA, explicit grants for GroupA and GroupB</td>
</tr>
<tr>
<td><img src="image" alt="ParentFolderA" /> <img src="image" alt="GroupA" /> [ACT: GroupARead]</td>
<td>On ParentFolderA, an ACT pattern grant for GroupA (from a directly applied ACT)</td>
</tr>
<tr>
<td><img src="image" alt="GreatGrandParentFolderA" /> <img src="image" alt="SAS USERS" /> [ACT: GenRead]</td>
<td>On GreatGrandParentFolderA, an ACT pattern grant for SAS USERS (from a directly applied ACT)</td>
</tr>
<tr>
<td><img src="image" alt="ParentFolderA" /> <img src="image" alt="GroupA" /> [ACT: GroupARead] <img src="image" alt="GroupB" /> [ACT: GroupBRead]</td>
<td>On ParentFolderA, ACT pattern grants for GroupA and GroupB (from two different directly applied ACTs)</td>
</tr>
<tr>
<td><img src="image" alt="GrandParentFolderA" /> <img src="image" alt="GroupA" /> [ACT: GroupABRead] <img src="image" alt="GroupB" /> [ACT: GroupABRead]</td>
<td>On GrandParentFolderA, ACT pattern grants for GroupA and GroupB (from the same directly applied ACT)</td>
</tr>
</tbody>
</table>
About SAS LASR Analytic Server

Introduction

SAS LASR Analytic Server is an analytic platform that provides secure, multi-user concurrent access to in-memory data. With high-performance, multi-threaded, analytic code that processes client requests at extraordinarily high speeds, the server enables business analysts to easily explore data and discover relationships. The server handles both big data and smaller sets of data. The server can be distributed or non-distributed.
To add server instances, operate the server, or monitor the server, see Chapter 4, “Managing Servers,” on page 37.

For comprehensive information, see the **SAS LASR Analytic Server: Reference Guide**.

**Distributed Server**

A distributed SAS LASR Analytic Server runs on multiple blades in a chassis.

A distributed server can use parallel I/O for the following actions:

- interactive loads from a co-located data provider. See “Co-Located Data Providers” on page 127.
- self-service imports from a (configured) remote data provider. See “Optimization: Parallel Loading” on page 12.

**Non-Distributed Server**

A non-distributed SAS LASR Analytic Server runs on a single machine. All of the in-memory analytic features that are available for a distributed server are also available for a non-distributed server. A non-distributed server does not use a co-located data provider, does not read data in parallel, and does not use the administrator’s memory gauges, Resource Monitor tab, or Process Monitor tab.

**TIP** If you have the required software license, you can convert a non-distributed server to run in distributed mode. See the **SAS Visual Analytics: Installation and Configuration Guide**.

**Depictions of Data Loading**

**Introduction**

This topic provides illustrated examples of selected data loading paths.

Here is some general information about the figures in this topic:

- The figures are simplified abstractions, intended as aids for conceptual understanding. For detailed requirements and technical diagrams, see the **SAS High-Performance Analytics Infrastructure: Installation and Configuration Guide**.
- The left side of each figure depicts physical data (on-disk and in-memory). Movement of data is indicated by arrows.
- The right side of each figure depicts corresponding metadata. For actions that generate a metadata object, the output table object is outlined in red.
Non-Distributed Server: Serial I/O

For a non-distributed server, data transfer is always serial. The following example depicts interactive loading of a registered table to a non-distributed server.

Figure 9.1 Serial Load to a Non-Distributed Server

Distributed Server: Serial I/O

The following example depicts serial loading of a registered table to a distributed server. The data is transferred to the root node of the server, distributed evenly among the machines in the cluster, and then loaded to memory.

Figure 9.2 Serial Load to a Distributed Server
Distributed Server: Parallel I/O: Co-Located Hadoop

This example depicts parallel loading from co-located Hadoop. First, a source table that is already registered in metadata is added to HDFS.

**Figure 9.3 Add to HDFS**

Next, the table is loaded in parallel from HDFS.

**Figure 9.4 Parallel Load from a Co-Located Data Provider**

Distributed Server: Parallel I/O: Remote Data Provider

This example depicts parallel loading from a remote data provider. Here are some key points:
In this example, parallel loading occurs because the remote data provider supports massively parallel processing (MPP), the action is a self-service import action, and all of the configuration requirements have been met. See “Optimization: Parallel Loading” on page 12.

To coordinate the load, the remote embedded process software on the analytics cluster cooperates with the SAS Embedded Process on each node in the data storage cluster.

It is not necessary for each node in the analytics cluster to map to a specific node in the data storage cluster. For this reason, parallel loading from a remote data provider is sometimes referred to as an asymmetric action.

With a remote data provider, the source table does not have to be registered in metadata or staged to an intermediate location.

In the following figure, the source data is already distributed on a data storage cluster. The data storage cluster is on different hardware than the cluster where the SAS LASR Analytic Server runs. The example depicts the data transfer that is initiated by a self-service import action.

**Figure 9.5  Parallel Load from a Remote Data Provider**

**TIP** The output library (in this example, Visual Analytics LASR) must have the appropriate VA.EP.Capable.engine-name attribute set to Yes. See “Optimization: Parallel Loading” on page 12.

**TIP** A high-performance analytics environment that supports this type of data transfer has an install path such as:

```
/opt/TKGrid_RSP
```
Memory Usage: A Closer Look

For a distributed server, SAS Visual Analytics Administrator provides two distinct expressions of memory usage:

- In the main menu bar, the overall memory gauge provides a practical estimate of effective capacity.

  The value for the overall memory gauge is calculated as follows:

  \[
  \frac{(\text{total allocations} - \text{SASHDAT allocations})}{\text{total memory for the cluster}}
  \]

  total allocations

  all memory allocations for all processes on the cluster.

  SASHDAT allocations

  memory that is allocated for tables that have been loaded from HDFS. These tables are stored in a highly efficient manner that keeps them instantly available on demand but consumes memory only when the data is accessed. For this reason, the overall gauge does not count SASHDAT allocations as used memory.

- In the Virtual Memory column on the LASR Servers tab, each individual gauge indicates how much memory is currently being used by a particular server instance (process).

  The individual gauges express memory usage from the traditional systems perspective, disregarding the memory-sparing efficiencies of SASHDAT allocations. The individual gauges can help you analyze capacity for the hypothetical scenario in which all tables are accessed simultaneously.

  The value for each individual gauge is calculated as follows:

  \[
  \frac{(\text{total allocations for this instance})}{\text{total memory for the cluster}}
  \]

  Note: The per-instance information on the Process Monitor tab also uses the preceding calculation to express memory usage.

  **TIP** On the LASR Servers tab, the sum of the individual gauges matches the overall memory gauge only if there are no SASHDAT allocations.

LASR-Related Metadata Objects

Metadata objects that are related to the SAS LASR Analytic Server include the following:

LASR Analytic Server
- a metadata definition for a LASR Analytic Server process

LASR Analytic Server connection
- a metadata representation of one instance of a LASR Analytic Server
LASR library
   a metadata representation of a data library that is associated with a LASR Analytic Server connection

LASR table
   a metadata representation of a table that has been loaded to memory in a LASR Analytic Server

The following figure depicts the relationships among these metadata objects.

Figure 9.6 Server, Connection, Libraries, and Tables

The preceding figure illustrates these points:
- Each server has one (multi-user) connection.
- Each connection can have multiple libraries.
- Each library can have multiple tables.
- Each deployment can have multiple servers.
How In-Memory Tables Are Identified

The following figure depicts an example of the mapping of metadata objects to corresponding in-memory data.

Figure 9.7 Uniqueness Requirements

The preceding figure illustrates these uniqueness requirements:

- Each host-port combination must be unique.
- Within a server instance (a host-port combination), each server tag must be unique. See “Server Tags” on page 54.
- Within a server tag, each table name must be unique.
- The fully qualified in-memory name for a table (in the format host-name:port/server-tag.table-name) must be unique.

Note: The metadata does not always reflect the current state of the SAS LASR Analytic Server. For example, when you unload a table from memory, the corresponding table object is not deleted from metadata.
Advanced Options: SAS LASR Analytic Server

Introduction

This topic documents advanced options in the metadata definition for a SAS LASR Analytic Server. For information about the basic options, see “Add a SAS LASR Analytic Server” on page 41.

Note: For a non-distributed server, the only applicable advanced options are Server lifetime, Signature files location on server, and Enable logging.

Version Information

The options are for descriptive, record-keeping purposes only. Here are suggested values:

- Major version number: 9
- Minor version number: 4
- Software version: 9.4

Memory Limits

The following options affect the circumstances in which a distributed SAS LASR Analytic Server rejects certain tasks:

Data loading (%)

specifies a percentage of used physical memory above which tables cannot be loaded to memory. If the server (in combination with any other processes on a machine) exceeds the specified value, operations that add tables or append rows fail. For example, if the value for this field is 80, and more than 80% of memory is already in use, tables cannot be loaded. If this field is blank, the value that is set on the server instance is used.

Note: Tables that are loaded from co-located Hadoop do not count toward this limit.

External processes (%)

specifies a percentage of used physical memory above which external processes (such as SAS High-Performance Analytics procedures) cannot retrieve data. If the server (in combination with any other processes on a machine) exceeds the specified value, affected processes cannot retrieve data. For example, if the value is 80, and more than 80% of memory is already in use, affected processes cannot retrieve data. If this field is blank, the value that is set on the server instance is used.

Logging Options

The logging options are as follows:
Enable logging
   Enables logging in a SAS LASR Analytic Server.

Path to log files
   The path where the log file for a distributed server is placed.
   
   Note: For a non-distributed server, log files are always written to the
   signature files directory.

Maximum file size (MB)
   Specifies the size of the log file (in megabytes) before the log file is rolled
   over. The default is 100 MB.

Maximum rollover files
   Specifies how many rotating log files can be used before older log files are
   overwritten. The default is 10.

Keep log files when the server terminates
   Select Yes to leave log files in the file system when the server terminates.
   The default value is No, and the files are removed.

Additional logging parameters
   This field is reserved for use in the future.

Additional Options

   The Additional Options tab includes the following items:

   Vendor
      SAS

   Associated Machine
      Select the server’s host. If the host is not listed, click New to add it.

   Force overwrite of server description file
      This field is not used.

   Signature files location on server
      The host directory where signature files are written. The specified location
      must exist on the machine that is identified as the High-Performance
      Analytics environment host. (See the Options tab of the Properties
      window for the server’s connection object.)

      CAUTION! It is important to protect the specified directory. See “Signature
      Files” on page 53.

      Unless you specify a custom value, signature files are written to the following
      location:

      Windows Specifics: \AppData\SASVisualAnalytics
      \VisualAnalyticsAdministrator\sigfiles (in the SAS configuration
      directory)

      UNIX Specifics: /tmp

   Server lifetime
      By default, the server runs forever. This is appropriate in most environments.

      To set a maximum run time, specify a value in seconds. For example, if you
      specify 3600, the server stops after it runs for 60 minutes.

      For a distributed server, you can also set a time-out period so that the server
      stops after an interval of inactivity. The time-out is specified in parentheses
after the first value. For example, if you specify the value as 3600 (600), then after the server runs for 60 minutes, it starts tracking any inactivity. If no action requests are received within 10 minutes, the server stops.

**Display detailed diagnostics**
By default, detailed diagnostics are not displayed.

The connection object’s Advanced Options window includes this option:

**Server description file**
Leave this field blank. SAS Visual Analytics does not use this setting.

---

**Extended Attributes: SAS LASR Analytic Server**

**Introduction**

This topic documents extended attributes in the metadata definition for a SAS LASR Analytic Server.

Extended attributes are on the server’s **Extended Attributes** tab in SAS Management Console.

**TIP**  Extended attributes for autostart, autoload, and reload-on-start are at the library level, not the server level. See “Convenience Features” on page 10.

**Reference**

VA.TextAnalyticsBinaryLocation
location of SAS linguistic files that support text analytics. The files are in the SAS installation directory as follows (unless a custom location is specified):

**UNIX Specifics:** /SASFoundation/Version/misc/tktg (for a non-distributed server), /opt/TKTGDat (for a distributed server)

**Windows Specifics:** \SASFoundation\Version\tktg\sasmisc

**Reference: Predefined LASR Libraries**

This topic documents the standard configuration of the predefined LASR libraries.

**Note:** Paths that begin with /AppData or /Applications are host locations within a SAS configuration directory.

**Note:** Paths that begin with /Products or /Shared Data are metadata folders.
Table 9.1  The General-Purpose LASR Library

<table>
<thead>
<tr>
<th>Name</th>
<th>Visual Analytics Public LASR (libref: LASRLIB, server tag: VAPUBLIC)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The library name must match the value of a configuration property. See “va.publicLASRLibrary” on page 92.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>/Shared Data/SAS Visual Analytics/Public</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The location must match the value of a configuration property. See “va.defaultPublicFolder” on page 92.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data server</th>
<th>Public LASR Analytic Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The server name must match the value of a configuration property. See “va.publicLASRServer” on page 92.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Intended use</th>
<th>The default output library for import and load actions for all registered users (SASUSERS). This library is sometimes referred to as the public LASR library.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Autostart</th>
<th>Enabled</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Autoload</th>
<th>Enabled (To use autoload, start the scheduled task. See “Autoload” on page 20.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data:</td>
<td>/AppData/SASVisualAnalytics/VisualAnalyticsAdministrator/AutoLoad</td>
</tr>
<tr>
<td>Scripts:</td>
<td>/Applications/SASVisualAnalyticsVersion/VisualAnalyticsAdministrator</td>
</tr>
<tr>
<td>LASR table objects:</td>
<td>/Shared Data/SAS Visual Analytics/Public/LASR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reload-on-start</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Library:</td>
<td>Visual Analytics Public Data Provider (libref: DPPUBLIC)</td>
</tr>
<tr>
<td>Directory:</td>
<td>/AppData/SASVisualAnalytics/VisualAnalyticsAdministrator/PublicDataProvider</td>
</tr>
<tr>
<td>LASR table objects:</td>
<td>/Shared Data/SAS Visual Analytics/Public/LASR</td>
</tr>
<tr>
<td><strong>Table 9.2  The Restricted LASR Library</strong></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Visual Analytics LASR (libref: VALIBLA, server tag: HPS)</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>/Products/SAS Visual Analytics Administrator</td>
</tr>
<tr>
<td><strong>Data server</strong></td>
<td>LASR Analytic Server</td>
</tr>
<tr>
<td><strong>Intended use</strong></td>
<td>An output library to which only administrators can import and load data. This library is sometimes referred to as the non-public, private, or limited availability LASR library. All registered users have Read access to this library.</td>
</tr>
<tr>
<td><strong>Autostart</strong></td>
<td>Not enabled</td>
</tr>
<tr>
<td><strong>Autoload</strong></td>
<td>Not enabled (To use autoload, set extended attributes, and start the scheduled task. See “Autoload” on page 20.)</td>
</tr>
<tr>
<td></td>
<td>Data: /AppData/SASVisualAnalytics/VisualAnalyticsAdministrator/AutoLoad/VALIBLA</td>
</tr>
<tr>
<td></td>
<td>Scripts: /Applications/SASVisualAnalyticsVersion/VisualAnalyticsAdministrator/VALIBLA</td>
</tr>
<tr>
<td></td>
<td>LASR table objects: /Shared Data/SAS Visual Analytics/AutoLoad/VALIBLA</td>
</tr>
<tr>
<td><strong>Reload-on-start</strong></td>
<td>Not enabled</td>
</tr>
</tbody>
</table>
Part 3

Appendixes

Appendix 1
Reference: Roles and Capabilities .................. 121

Appendix 2
Reference: Co-Located Data Providers .................. 127
Predefined Roles

Here are the predefined roles for SAS Visual Analytics:

**Visual Analytics: Basic**
- provides functionality for guest access (if applicable) and entry-level users.
- This role serves two distinct purposes:
  - This role enables all registered users to access the home page and to view reports in the web viewer. This role does not provide commenting or personalization features.
  - In a deployment that supports guest access, this role provides functionality at the guest access URLs. See “Supporting Guest Access” on page 66.

**Visual Analytics: Report Viewing**
- provides commenting and personalization features, in addition to baseline functionality.

**Visual Analytics: Analysis**
- provides the ability to create reports and explore data, in addition to report viewing functionality.

**Visual Analytics: Data Building**
- provides the ability to prepare data in the data builder, in addition to analysis functionality.

**Visual Analytics: Administration**
- provides the ability to perform administrative tasks in the administrator, in addition to most other capabilities.

For role membership information, see “Membership Structure” on page 6.

To manage roles, see the SAS Management Console: Guide to Users and Permissions.

The following table documents the initial capabilities for each role:
### Table A1.1 Capabilities by Role

<table>
<thead>
<tr>
<th>Capability</th>
<th>Basic</th>
<th>Report Viewing</th>
<th>Analysis</th>
<th>Data Building</th>
<th>Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Visual Analytics Version</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Report and Stored Process</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Create Report</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explore Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Build Custom Graph</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Add and View Comments</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Export Data</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Export or Print as PDF</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Email</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Personalization</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Visual Analytics Version: Self-Service Import</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Import and Load Data</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Import Local Files</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Import SAS Data Sets from a Server</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Import from data-source</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Visual Analytics Version: Advanced</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Build Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capability</td>
<td>Basic</td>
<td>Data Building</td>
<td>Administration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>---------------</td>
<td>----------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Environment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Mobile Devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Collections</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purge Mobile Report Data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Require Passcode on Mobile Devices</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual Analytics Hub Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage LASR Analytic Server</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Authorization</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browse HDFS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual Analytics Explorer Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual Analytics Admin Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual Analytics Transport Service Version</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administer Hub</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Refresh Data</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export as Image</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export as Report</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Capability Descriptions

Here are descriptions of the SAS Visual Analytics capabilities:

Visual Analytics Version
   View Report and Stored Process
      Access the web and mobile viewers. View reports and stored process
      output. (Access to the mobile viewers is also affected by device-level
      constraints. See “Managing Devices” on page 45.)

   Create Report
      Access the designer. Create and modify reports.

   Explore Data
      Access the explorer. Create and modify explorations. (In some contexts,
      the explorer is a separately licensed add-on product.)

   Build Custom Graph
      Access the graph builder. Create and modify graph template objects for
      use in the designer.

   Add and View Comments
      Add comments, view comments, and edit your own comments.

      Note: In order to delete comments and edit other users’ comments, you
      need the capabilities that are listed under SAS Application
      Infrastructure ▶ Comments. Consider adding those capabilities to the
      Visual Analytics: Administration role or making any users that need
      these capabilities members of the Comments: Administrator role.

   Export Data
      Export data to other applications.

   Export or Print as PDF
      Export or print reports and explorations as PDF files.

   Email
      Send a link to a report or exploration via e-mail.

   Personalization
      Use individualized features such as setting preferences, accessing
      recently viewed objects, and managing favorites.

Visual Analytics Version: Self-Service Import
   Import and Load Data
      A prerequisite for access to self-service import functionality in the
      designer and the explorer. See “Self-Service Import” on page 11.

   Import Local Files
      Import spreadsheets, delimited files, and SAS data sets from your
      computer.

   Import SAS Data Sets from a Server
      Import remote data sets.

   Import from data-source
      Import data from a third-party data source (for example, Import from
      Oracle).
Visual Analytics Version: Advanced

Build Data
Access the data builder. Set advanced load options in the explorer and the designer.

Manage Environment
Access the administrator. Additional capabilities are required to perform particular tasks.

Manage Mobile Devices
Blacklist or whitelist mobile devices. (The Manage Environment capability is also required.)

Create Collections
Create groups of bookmarks to objects.

Visual Analytics Transport Service Version

Purge Mobile Report Data
Causes cached data on mobile devices to be purged when reports are closed. For users who do not have this capability, cached data is retained locally on the mobile device for use in offline mode.

Note: Because unrestricted users always have all capabilities, their mobile data is always purged when they close reports. In general, you should not use an unrestricted identity (for example, sasadm@saspw) to view reports.

Require Passcode on Mobile Devices
Requires users to enter an application passcode on their devices each time they use SAS Mobile BI. For users who do not have this capability, an application passcode is not required.

Note: Because unrestricted users always have all capabilities, they are always subject to the application passcode requirement. In general, you should not use an unrestricted identity (for example, sasadm@saspw) to view reports.

See “viewerservices.passcode.attempts” on page 89 and “viewerservices.passcode.timeout” on page 89.

Visual Analytics Hub Version

Administer Hub
Create and manage custom lists. Access the Manage Shared View of Right Pane action. See “Customizing the Home Page” on page 70.

Visual Analytics Explorer Version

Refresh Data
Refresh data for explorations.

Export as Image
Export images of explorations to a local machine.

Export as Report
Export explorations as reports to SAS folders.

Visual Analytics Admin Version

The Manage Environment capability is a prerequisite for all tasks in SAS Visual Analytics Administrator.

Manage LASR Analytic Server
Access the LASR tabs and the folders tree. For a distributed server, this capability makes a link to the SAS High-Performance Computing Management Console available from the Tools menu.
Monitor LASR Analytic Server
   Access the **Monitor** tabs. This capability is applicable to deployments that use a distributed server.

Manage Authorization
   Set metadata-layer permissions.

Browse HDFS
   Access the **HDFS** tab. This capability is applicable to deployments that use co-located Hadoop.

**TIP** Capabilities for add-ons and other solutions are not included in this document. For information about capabilities for another product, see the documentation for that product.
Appendix 2

Reference: Co-Located Data Providers

Co-Located Data Providers ........................................................................... 127
Co-Located Hadoop .................................................................................... 127
  Introduction ............................................................................................. 127
  About the HDFS Tab ............................................................................... 128
  Add an HDFS Library .............................................................................. 132
  Delete an HDFS Table ............................................................................ 133
Alternate Providers of Co-Located Data ......................................................... 133

Co-Located Data Providers

A co-located data provider contains source data that is stored on the hardware where a distributed SAS LASR Analytic Server runs. Tables in a co-located data provider can be loaded to the distributed server in parallel.

For an illustrated example, see "Distributed Server: Parallel I/O: Co-Located Hadoop" on page 108.

TIP For the most current list of supported co-located data providers, see the Install Center at support.sas.com.

Co-Located Hadoop

Introduction

Co-located Hadoop is a deployment of Hadoop that meets the following criteria:

- The deployment runs on the same hardware as a distributed SAS LASR Analytic Server.
- The deployment incorporates services that SAS High-Performance Deployment of Hadoop provides.

SAS High-Performance Deployment of Hadoop adds services to Apache Hadoop (and other supported Hadoop distributions) to provide the following integrated functionality:
SAS uses a special file format (with the filename suffix SASHDAT) to store tables in HDFS. Like any file that is stored in HDFS, a SASHDAT file is distributed as a series of blocks. Copies of blocks are stored to provide data redundancy.

SAS enhances the block distribution algorithm to make sure that blocks are distributed evenly. Because SAS LASR Analytic Server reads blocks of data directly, the even block distribution contributes to an even workload on the machines in the cluster.

This integration enables a distributed SAS LASR Analytic Server to use HDFS to read SASHDAT tables in parallel at very impressive rates.

Note: Basic HDFS commands are documented in the SAS LASR Analytic Server: Reference Guide.

About the HDFS Tab

Introduction

To open the HDFS tab, select Tools ▶ Explore HDFS from the main menu bar in SAS Visual Analytics Administrator.

Note: The HDFS tab is available in deployments that use co-located Hadoop. Only users that have the Browse HDFS capability can access the HDFS tab.

The HDFS tab provides a host-layer view of HDFS folders and tables. The view is not mediated by metadata or by your permissions. Instead, a privileged Hadoop account retrieves the information that this tab displays.

You can use the HDFS tab to perform the following tasks:

- Browse HDFS folders and tables.
- View row count, columns, column information, and block information for tables that have been added to HDFS. Information about block distribution, block redundancy, and measures of block utilization is provided.
- Delete HDFS tables that are stored in SASHDAT format. (Files that are not SASHDAT files are listed, but they cannot be deleted.)

System Properties

To view HDFS system properties, click 📋. The following table describes the fields:

<table>
<thead>
<tr>
<th>Table A2.1</th>
<th>HDFS System Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>Command for setting permissions</td>
<td>This setting is not used.</td>
</tr>
<tr>
<td>Set permissions as root?</td>
<td>This setting is not used.</td>
</tr>
<tr>
<td>Command for getting file information</td>
<td>This setting is not used.</td>
</tr>
<tr>
<td>Data directories</td>
<td>Specifies the directory that is used to store blocks.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Name Node</td>
<td>Specifies the host name of the machine that is used as the Hadoop NameNode.</td>
</tr>
<tr>
<td>Live Data Nodes</td>
<td>Specifies the number of Hadoop DataNodes that are reachable.</td>
</tr>
<tr>
<td>Dead Data Nodes</td>
<td>Specifies the number of Hadoop DataNodes that are not available.</td>
</tr>
</tbody>
</table>

**Basic File Information**

To view basic file information, select a file. The following information is provided:

*Table A2.2  Basic File Information*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies the name of the file.</td>
</tr>
<tr>
<td>Size</td>
<td>Specifies the file size. This value includes the disk space required to store the data in blocks and metadata about the file.</td>
</tr>
<tr>
<td>Date Modified</td>
<td>Specifies the date on which the file was created or replaced.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the HDFS directory.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies the description that is stored with the data. The description is displayed beside the table name in the explorer interface.</td>
</tr>
<tr>
<td>Copies</td>
<td>Specifies the number of redundant copies of the data.</td>
</tr>
<tr>
<td>Block Size</td>
<td>Specifies the number of bytes that are used to store each block of data.</td>
</tr>
<tr>
<td>Number of Variables</td>
<td>Specifies the number of columns in the HDFS table.</td>
</tr>
<tr>
<td>Owner</td>
<td>Specifies the user account that added the data to HDFS.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the primary UNIX group for the user account.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Specifies the Read, Write, and Execute access permissions for owner, group, and other.</td>
</tr>
<tr>
<td>SASHDAT file?</td>
<td>Specifies whether the file is in the SASHDAT format. <strong>Yes</strong> indicates that the file is in the SASHDAT format.</td>
</tr>
</tbody>
</table>

**Note:** The HDFS tab might display multiple files for a table as the table is being added to HDFS. After the table is added, the multiple files disappear.
Table Information

To view column information, select a table, and click [icon]. The following information is provided:

Table A2.3  Column Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column Name</td>
<td>Specifies the column name from the source table.</td>
</tr>
<tr>
<td>Label</td>
<td>Specifies the label for the data set column when the table was added to HDFS.</td>
</tr>
<tr>
<td>Type</td>
<td>Numeric or Character. Numeric variables are encoded as 1.</td>
</tr>
<tr>
<td>Offset</td>
<td>Specifies the starting position for the variable in the SASHDAT file.</td>
</tr>
<tr>
<td>Length</td>
<td>Specifies the storage used by the variable.</td>
</tr>
<tr>
<td>Format</td>
<td>Specifies the format associated with the variable.</td>
</tr>
<tr>
<td>Format Length</td>
<td>Specifies the format length of the format that existed on the variable when it was added to HDFS. This value is zero if the variable did not have a format when it was added to HDFS.</td>
</tr>
<tr>
<td>Precision</td>
<td>Specifies the precision portion of the format for number formats.</td>
</tr>
<tr>
<td>Length (Formatted)</td>
<td>Specifies the length of the variable when formatting is applied.</td>
</tr>
</tbody>
</table>

To view the row count, select a table, and click [icon]. The following information is provided:

Table A2.4  Row Count Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rows</td>
<td>Specifies the number of rows in the data.</td>
</tr>
<tr>
<td>Blocks</td>
<td>Specifies the number of HDFS blocks that are used to store the data.</td>
</tr>
<tr>
<td>Allocated</td>
<td>Specifies the number of bytes allocated to store the data. The value is a multiple of the block size and the number of blocks. This value is smaller than the file size because it does not include the space needed for the SASHDAT file header.</td>
</tr>
<tr>
<td>Used</td>
<td>Specifies the number of bytes within the allocated blocks that are used for storing rows of data.</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
Utilization | Specifies the percentage of allocated space that is used for storing rows of data.

**Block Detail Information**

To view block details, select a file, and click . The following information is provided:

**Table A2.5 Block Detail Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>Specifies the machine in the cluster that stores the block of data.</td>
</tr>
<tr>
<td>Block Name</td>
<td>Specifies the filename for the block.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the directory to the block.</td>
</tr>
<tr>
<td>Record Length</td>
<td>Specifies the sum of the column lengths for the variables in the data.</td>
</tr>
<tr>
<td>Records</td>
<td>Specifies the number of rows stored in the block. Because redundant blocks are listed in the table, the sum of the records listed does not equal the number of rows in the data.</td>
</tr>
<tr>
<td>Owner</td>
<td>Specifies the user account that added the data to HDFS.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies the primary UNIX group for the user account that stored the data.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Specifies the Read, Write, and Execute access permissions for owner, group, and other.</td>
</tr>
</tbody>
</table>

You can sort by the column headings to identify anomalies. It is normal for several blocks to be stored on the same machine. However, it is not normal for the values of **Record Length**, **Owner**, **Group**, or **Permissions** to be different from row to row.

The files added to HDFS are stored as blocks. One block is the preferred block, and additional copies of the blocks are used to provide data redundancy. The Block Distribution dialog box offers two ways to view this information. The **Block Detail View** tab enables you to select a block number and view the host names that store the original or redundant blocks. The **Node Detail View** enables you to select a host name and view the block numbers that are stored on the machine.
Block Distribution Information

To view the block distribution, select a table, and click 🏛️. The following information is provided:

Table A2.6  Block Distribution Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Size</td>
<td>Specifies the size of the file in bytes.</td>
</tr>
<tr>
<td>Block Size</td>
<td>Specifies the block size for the file.</td>
</tr>
<tr>
<td>Blocks</td>
<td>Specifies the number of blocks used to store the original copy of the data.</td>
</tr>
<tr>
<td>Machines Used</td>
<td>Specifies the number of machines in the cluster that have original or redundant blocks for the file.</td>
</tr>
<tr>
<td>Copies</td>
<td>Specifies the number of redundant block copies of the data.</td>
</tr>
</tbody>
</table>

On the Block Detail View tab, you can select a block number. This enables you to view how many copies of the block exist and the host names for the machines that store the blocks. The value in the Total Copies column equals the number of redundant copies of the block plus the original block. You can select the column heading to sort the rows. In an ideal distribution, the number of total copies is equal for all blocks.

On the Host Detail View tab, you can expand a host name node, and then view the block numbers that are stored on that machine. When you select the block number, the host name and any additional machines with copies of the block are identified in the host name list.

Add an HDFS Library

Introduction

The main reason for creating a new library of the type SAS Data in HDFS is to support an additional HDFS directory. For each HDFS directory, you need a designated HDFS library (and a corresponding LASR library).

Instructions


2. In the New Library wizard, select High-Performance Analytics ➤ SAS Data in HDFS Library. Click Next.

3. Enter a name. If necessary, adjust the location. Click Next.

4. Move a SAS Application Server (for example, SASApp) to the Selected servers list. Click Next.

5. Set library properties as follows. Click Next.
Assign the library to a Hadoop server by entering settings as follows:

- **Database Server**: Select a server from the drop-down list.
- **Connection**: Use the pre-selected value (which prepends the selected server name with the string `Connection:`).
- **Default Login**: Use the default value (None).

Click Next.

Review settings. Click Finish.

Next, create a corresponding LASR library. See “Add a SAS LASR Analytic Library” on page 43.

### Delete an HDFS Table

1. Right-click on the table in the Folders pane, and select Delete.

2. In the confirmation window, if you want to delete the physical table with the metadata object that represents it, select the Remove from HDFS storage check box.

   **TIP** You can also delete an HDFS table from the HDFS tab. Select the table, and click in the tab’s toolbar.

### Alternate Providers of Co-Located Data

**Note**: This topic is applicable to only highly specialized configurations that use a co-located data provider other than co-located Hadoop.

Here are some details:

- Only tables that conform to applicable third-party database limitations can be added to an alternate provider.
- To add a table to an alternate provider, right-click the table in SAS Visual Analytics Administrator, and select Add to a Data Server.
- For data that is loaded from an alternate provider, SAS variable names are used as data item names (in applications such as the explorer).

- Each alternate provider library must have a corresponding LASR library. The LASR library’s server tag must match the alternate provider library’s libref.

- With an alternate provider, the middle-tier machine is configured as a client of the database. The middle-tier client machine must have network name resolution for host names.
access control template
a reusable named authorization pattern that you can apply to multiple resources. An access control template consists of a list of users and groups and indicates, for each user or group, whether permissions are granted or denied. Short form: ACT.

authorization
the process of determining the permissions that particular users have for particular resources. Authorization either permits or denies a specific action on a specific resource, based on the user's identity and on group memberships.

capability
an application feature that is under role-based management. Typically, a capability corresponds to a menu item or button. For example, a Report Creation capability might correspond to a New Report menu item in a reporting application. Capabilities are assigned to roles.

credentials
the user ID and password for an account that exists in a particular authentication provider.

data set
See SAS data set

grid host
the machine to which the SAS client makes an initial connection in a SAS High-Performance Analytics application.

group
a collection of users who are registered in a SAS metadata environment. A group can contain other groups as well as individual users.

Hadoop Distributed File System
a framework for managing files as blocks of equal size, which are replicated across the machines in a Hadoop cluster to provide fault tolerance. Short form: HDFS

libref
a SAS name that is associated with the location of a SAS library. For example, in the name MYLIB.MYFILE, MYLIB is the libref, and MYFILE is a file in the SAS library.

metadata identity
a metadata object that represents an individual user or a group of users in a SAS metadata environment. Each individual and group that accesses
secured resources on a SAS Metadata Server should have a unique metadata identity within that server.

role
a set of capabilities within an application that are targeted to a particular group of users.

SAS authentication
a form of authentication in which the target SAS server is responsible for requesting or performing the authentication check. SAS servers usually meet this responsibility by asking another component (such as the server's host operating system, an LDAP provider, or the SAS Metadata Server) to perform the check. In a few cases (such as SAS internal authentication to the metadata server), the SAS server performs the check for itself. A configuration in which a SAS server trusts that another component has pre-authenticated users (for example, web authentication) is not part of SAS authentication.

SAS data set
a file whose contents are in one of the native SAS file formats. There are two types of SAS data sets: SAS data files and SAS data views.

SAS Stored Process
a SAS program that is stored on a server and defined in metadata, and which can be executed by client applications. Short form: stored process.

SAS table
another term for SAS data set.

SASHDAT file
the data format used for tables that are added to HDFS by SAS. SASHDAT files are read in parallel by the server.

theme
da collection of specifications (for example, colors, fonts, and font styles) and graphics that control the appearance of an application.

unrestricted identity
a user or group that has all capabilities and permissions in the metadata environment due to membership in the META: Unrestricted Users Role (or listing in the adminUsers.txt file with a preceding asterisk).

web authentication
a configuration in which users of web applications are verified at the web perimeter, and the metadata server trusts that verification
## Index

### A
- adding users 6
- alerts 72
- autoload 20
  - library-level attributes 26
  - autostart 38

### C
- capabilities 35
  - descriptions 124
    - for the predefined roles 121
    - in custom roles 35
  - co-located data providers 127
  - co-located Hadoop 127

### D
- data loading 10
  - autoload 20
  - interactive 18
  - reload-on-start 15

### E
- esri 76

### G
- geo maps 75
  - data sets 76
- getting started 5
  - adding users 6
  - load a table 18
  - open the administrator 5
  - start a server 37
- guest access 66

### H
- HDFS tab 128
- high-cardinality data 81
  - client-side thresholds 82
  - middle-tier thresholds 82

### K
- kiosk
  - See guest access

### L
- LASR authorization service 51
  - caching 53
  - security key 52
  - libraries
    - adding LASR libraries 43
    - HDFS 132
  - locked-down servers 58
  - logging 79
    - for autoload 26
    - for reload-on-start 16
  - permissions 80
  - SAS Information Retrieval Studio 74
  - SAS LASR Analytic Server 113
  - SAS LASR Analytic Server Monitor 79
  - schema validation errors 81
  - search index load script 75

### M
- mobile devices
  - See SAS Mobile BI

### O
- OpenStreetMap 75
permissions 29
  by task 31
  conditional 33
  definitions 30
  inherited 102
  origins 101
  setting 32

reload-on-start 15
  library-level attributes 16
roles 35
  custom 35
  predefined 121
row-level security 55
  identity-driven 57
  precedence 55
  set interactively 33
  syntax (basic, batch) 56
  syntax (Text tab) 56

SAS Information Retrieval Studio 74
  managing the server 74
SAS LASR Analytic Server 4
  adding 42
  adding libraries 43
  distributed 106
  lifetime 114
  logging 113
  managing 37
  memory limits 113
  metadata objects 110
  monitoring 39
  non-distributed 106
SAS LASR Analytic Server Monitor 77
  logging 79
  managing 78
  troubleshooting 79
SAS Mobile BI 45
  advanced properties 87
  blacklisting 45
  capabilities 125
  customizing 87
  enabling the whitelist 47
  image resizing 88
  logging 81
  security 61
  troubleshooting 101
  whitelisting 46
SAS Visual Analytics Administrator 5
  Authorization page 34
  HDFS tab 128
  LASR Servers tab 110
  Mobile Devices tab 47
  Process Monitor tab 40
  Resource Monitor tab 39
  troubleshooting 95
  user preferences 85
Search Interface to SAS Content 74
  security
    data 51
    locked-down servers 58
    mobile 61
    passwordless SSH 62
    row-level 55
    SAS token authentication 59
    web authentication 59
server tags 54
  signature files 53
  start a server
    autostart 38

tables
  deleting from HDFS 133
  registering 17
  reloading to memory 18
  staging 18
  unloading from memory 18
  valid names 11
themes 69
transport services
  See SAS Mobile BI

web authentication 59