## Contents

### PART 1  Introduction to SAS Infrastructure for Risk Management  1

**Chapter 1 • Welcome to SAS Infrastructure for Risk Management**  
- What Is SAS Infrastructure for Risk Management?  
- Using the SAS Infrastructure for Risk Management: Administrator’s Guide  
- What’s New in SAS Infrastructure for Risk Management 3.5  
- Related Documentation

**Chapter 2 • SAS Infrastructure for Risk Management Architecture**  
- SAS Infrastructure for Risk Management Architecture  
- SAS Infrastructure for Risk Management Data Flow  
- SAS Infrastructure for Risk Management Distributed Development

**Chapter 3 • SAS Infrastructure for Risk Management Federated Content**  
- SAS Infrastructure for Risk Management Federated Areas  
- The Folders in a Federated Area  
- SAS Infrastructure for Risk Management Federated Content

### PART 2  Deploying SAS Infrastructure for Risk Management  17

**Chapter 4 • Pre-installation Tasks**  
- Overview of the Pre-installation Tasks  
- Verify Your System Requirements  
- Obtain a Deployment Plan  
- Complete the Pre-installation Checklist That Accompanies Your Deployment Plan  
- Set Up SAS Infrastructure for Risk Management User Accounts  
- Create a SAS Software Depot  
- Grant Linux Directory Permissions  
- Check for SAS Installation Notes

**Chapter 5 • Installing SAS Infrastructure for Risk Management**  
- Overview of the Installation Tasks  
- Review the File System Structure  
- Install SAS Infrastructure for Risk Management  
- Install Hot Fixes  
- Configure an External Location to the Persistent Area  
- Install Federated Content

**Chapter 6 • Performing Post-installation Tasks**  
- Overview of the Post-installation Tasks  
- Use the Instructions File  
- Create Roles, Groups, and Users  
- Configure the Metadata Accounts for SAS Infrastructure for Risk Management  
- Apply SAS Security Updates
Chapter 12 • Troubleshooting

Gather Information ................................................................. 91
Enable Detailed Logging ....................................................... 93
Fix Your Web Application Log File Display ......................... 94
Log and Configuration File Locations .................................. 94
Part 1

Introduction to SAS Infrastructure for Risk Management

Chapter 1
Welcome to SAS Infrastructure for Risk Management ............ 3

Chapter 2
SAS Infrastructure for Risk Management Architecture ............ 5

Chapter 3
SAS Infrastructure for Risk Management Federated Content ....... 9
Chapter 1
Welcome to SAS Infrastructure for Risk Management

What Is SAS Infrastructure for Risk Management?
SAS Infrastructure for Risk Management is a high-performance job execution engine with a web-based user interface and a programming interface that is based on SAS.

SAS Infrastructure for Risk Management solutions are delivered as industry-specific content releases that are downloaded and installed after SAS Infrastructure for Risk Management is installed. The calculations that make up the solution content releases are performed using job flows in the SAS Infrastructure for Risk Management web application.

Alternatively, SAS Infrastructure for Risk Management can be ordered as part of the SAS Risk Analytics Builder package, which does not contain any content. With this package, SAS programmers can use SAS Infrastructure for Risk Management as a programming interface that enables them to easily create parallel programs that run on the SAS Infrastructure for Risk Management platform.

The SAS Infrastructure for Risk Management platform is designed to be customizable and flexible. The architecture of SAS Infrastructure for Risk Management provides a simplified way to develop and run the fastest analytics.

Using the SAS Infrastructure for Risk Management: Administrator’s Guide
This guide is for administrators who are responsible for installing and configuring SAS Infrastructure for Risk Management and the content that uses it as a platform.

This administrator must be able to perform the following tasks:
• Use SAS Download Manager to download a SAS Software Depot to each machine on which an installation is performed.

• Install and configure the SAS Intelligence Platform and the SAS Infrastructure for Risk Management platform and associated content modules.

• Use SAS Management Console to maintain the metadata for the servers, users, and other global resources that are required by the solution.

For information about how to use the SAS Infrastructure for Risk Management web application, see SAS Infrastructure for Risk Management: User’s Guide. For more information about SAS Infrastructure for Risk Management programming, see SAS Infrastructure for Risk Management: Programmer’s Guide.

What’s New in SAS Infrastructure for Risk Management 3.5

SAS Infrastructure for Risk Management 3.5 provides the following new features and enhancements:

• Ability to install stand-alone federated areas that do not require a server restart.
  See “Install a Stand-Alone Federated Area without a Server Restart” on page 81.

• Additional capabilities that enable additional user management actions, such as install federated areas and change ownership of job flow instances.
  See “Create Roles, Groups, and Users” on page 34.

• Enhanced library mapping definitions, including support of extended custom mapping definitions and the ability to separate data inputs (entities, base dates, configuration sets) into folders.
  See “Map SAS Infrastructure for Risk Management Libraries” on page 70.

• Full support for generic libraries, including the ability to import and export data as a Microsoft Excel spreadsheet or SAS data set.
  See “Generic Library Mapping” on page 73.

• Faster and more efficient support for uploading large data sets.

• SAS Infrastructure for Risk Management hot fix post-installation tool that verifies and automates post-installation steps that are required when you apply a SAS Infrastructure for Risk Management hot fix that includes the SAS Infrastructure for Risk Management server JAR.
  See “Run the SAS Infrastructure for Risk Management Hot Fix Post-installation Tool” on page 74.

Related Documentation

• SAS Infrastructure for Risk Management: User’s Guide
• SAS Infrastructure for Risk Management: Programmer’s Guide
Chapter 2
SAS Infrastructure for Risk Management Architecture

SAS Infrastructure for Risk Management operates in a three-tiered environment, as shown in the following figure:

- Server Tier
  - handles requests from the client tier and the middle tier
serves as an abstract layer between the data tier and the middle tier or between the data tier and the client tier

consists of SAS applications, such as the SAS Metadata Server and a SAS Application Server

**Middle Tier**

- receives and processes web requests from the client tier and passes these requests to the server tier and the data tier
- contains a web application server in addition to web applications such as the SAS Infrastructure for Risk Management web application

**Client Tier**

- initiates requests (via desktop client applications or web browsers) to perform the necessary work and to view formatted output
- contains the SAS Infrastructure for Risk Management graphical user interface (developed in HTML5)

---

### SAS Infrastructure for Risk Management Data Flow

The following figure shows the basic flow of data in SAS Infrastructure for Risk Management:

1. A user can supply data to a federated area in one of the following ways:
   - When the SAS Infrastructure for Risk Management server is down, the user submits data directly to the landing area of a federated area.
   - When the server is running, the user submits data directly to the input area of a federated area and SAS Infrastructure for Risk Management uses Live ETL to move the data into the landing area.
   - If the SAS Detail Data Store is in place, data can be drawn from the SAS Detail Data Store to the input area of a federated area.

2. Subsets of the input data are created in separate folders for each reporting period. These subsets of input data are created in the Read-Only staging or Read-Only landing area of the SAS Infrastructure for Risk Management federated area. Tables are versioned by date (8-character string – \textit{mmddyyyy}) or date and time (14-character string – \textit{mmddyyyyhhmmss}).

3. The output of the job flow is placed in the persistent area. The persistent area is a Read/Write area for input and output data (XLSX, XBRL, and SAS data sets).
Overview

SAS Infrastructure for Risk Management solutions are designed to support distributed development. Distributed development means that developers in different locations can independently develop code that runs on the SAS Infrastructure for Risk Management platform.

Distributed development has the following implications:

- Code that is developed in one location must not break code that is developed in another location.
- Subsequent releases of a SAS Infrastructure for Risk Management solution must support all changes or fixes that are deployed since the prior release, including additions to flows, code, and data.
- Developers are responsible for the integrity of their code.
- If you modify a subflow that is used by other flows, you can break those flows. For example, you might break the flows if you changed the number or nature of the outputs of a subflow. Therefore, coordination of development groups is also necessary to ensure the integrity of the code that is being developed.
- With the exception of loading data, all installed federated areas are read-only.
- The personal federated area can be modified within the parameters described in SAS Infrastructure for Risk Management: Programmer's Guide.
- Once installed, a federated area must never be removed.

Contributors

Contributors to the distributed development of SAS Infrastructure for Risk Management solutions include the following:

- SAS Research and Development
  SAS Research and Development provides the content that is included with your SAS Infrastructure for Risk Management solution.

- SAS Consultants
  SAS Consultants provide custom content that can be included in a future release of all SAS Infrastructure for Risk Management solutions.

- Consulting firms
  Consulting firms develop a custom product on top of SAS Infrastructure for Risk Management solutions.
Federated Content

SAS Infrastructure for Risk Management solutions are delivered as federated content. Federated content is computational and reporting logic that is designed, produced, and owned by people outside SAS Research & Development. This might be a SAS department that is not SAS Research and Development, a third-party consulting company, and so on.

For more information about federated content, see “SAS Infrastructure for Risk Management Federated Content” on page 9.
Chapter 3

SAS Infrastructure for Risk Management Federated Content

SAS Infrastructure for Risk Management Federated Areas

The Folders in a Federated Area

SAS Infrastructure for Risk Management Federated Content

What is Federated Content? ................................. 12
Federated Content Processing .......................... 12
Federated Job Flows ...................................... 12
Federated Tasks ............................................. 13
Federated Input Data ...................................... 13
How Federated Input Data Is Processed .............. 14
Personal Federated Area ................................. 15

SAS Infrastructure for Risk Management Federated Areas

The content that runs on the SAS Infrastructure for Risk Management platform shares the same architecture and layout, which is the federated area. A federated area uses a folder structure that conforms to specific SAS Infrastructure for Risk Management rules. The differences among content types are in the calculation content that is stored in the federated area.

Federated areas enable content to be developed and deployed independently of the SAS Infrastructure for Risk Management platform. Deploying new content or a new platform release should never break existing content.

The content of a federated area consists of the following elements:

- job flow definitions — files that describe the job flow
- code — task files (nodes), string message data, and macros
- input files — SAS data sets, CSV files, Microsoft Excel templates, and XBRL templates
- documentation and tooltip files — information that is presented to the end user through the graphical user interface

When you install SAS Infrastructure for Risk Management 3.5, the following federated areas are installed:
• **fa.0.3.5** — contains only elements that are required to make the platform run. There is no analytical content in the platform federated area. The platform federated area should not be modified.

• **fa.sample.3.5** — contains sample content that you can use to test the SAS Infrastructure for Risk Management installation and to use as a reference.

• **fa.user_name** — an optional personal federated area that is created on demand. You must have a personal federated area if you want to develop your own content. For information about developing SAS Infrastructure for Risk Management content, see *SAS Infrastructure for Risk Management: Programmer’s Guide*.

It is important to note the following rules about federated areas:

• They must be designed to work with other federated areas.

• They must not be altered, modified, or deleted once they are deployed.

  The one exception to this rule is that you can upload data to the input area or the landing area of a federated area other than the platform federated area.

• Tasks, job flows, and input data are *federated content*. This means that this content is shared across all federated areas. Therefore, do not change the definition of tasks, job flows, and data. Doing so can cause unpredictable results.

  All other content in a federated area is local to that federated area and cannot be shared with other federated areas.

---

**The Folders in a Federated Area**

All federated areas have the same basic folder structure. Custom federated areas might contain additional or fewer folders than the ones described in this section. SAS Infrastructure for Risk Management does not require all folders to be included in a federated area. However, a specific type of content must be located in the appropriate folder.

Here is an example of the basic folder structure of a federated area:
Here are descriptions of the contents of some of the folders that are located in a federated area:

- **client_scripts** — contains the job flow scripts that a content developer creates.
- **config** — contains files that a programmer uses to configure the behavior of job flows. Specifically, this folder contains the following files and folders:
  - **messages** — contains the labels that are visible in the SAS Infrastructure for Risk Management web application. The labels are for nodes, job flows (and subflows), and inputs and outputs.
  - **job_flow_definitions.csv** — lists the job flows that are available in the SAS Infrastructure for Risk Management web application.
  - **libnames.txt** — maps the SAS libraries for the input data that is used in job flows.
  - **macrovarload.txt** — lists the SAS data sets that define the global macro variables that must be loaded before a task executes.
- **input_area** — identifies the area to which you can load data directly into a federated area. You can load data into the input area when the SAS Infrastructure for Risk Management server is running.
- **jobflow** — contains job flow definitions or subdirectories that contain job flow definitions. Subfolders within the job flow folder are displayed as categories in the SAS Infrastructure for Risk Management web application. Only a single level of folder hierarchy is supported in the job flow folder.
- **landing_area** — identifies the read-only data mart of its federated area. It contains the data objects (for example, SAS data sets) that are required for the job flows that are defined in that federated area. You must shut the SAS Infrastructure for Risk Management server down before you load data into the landing area.
- **source** — contains the individual task files (programs) that are used in job flows. The source folder contains subfolders for each task type (for example, sas, Lua, and Java). Located in the task type folder is a **nodes** folder that holds the task file (for example, source / sas / nodes). Uncompiled SAS macros for a federated...
area must be stored in the `ucmacros` folder source / sas / ucmacros. Depending on the content, here are additional folders that might appear:

- **nodes** — contains the task files that are directly called by job flows. To make code more manageable, a single-level hierarchy of subfolders can be used in the `nodes` folder.
- **smd** — contains string messages (.smd files).
- **ucmacros** — contains the uncompiled macro files that are called by the task files in the `nodes` folder.

# SAS Infrastructure for Risk Management Federated Content

## What is Federated Content?

- *Federated content* is contained in federated areas.
- Federated content is the mechanism by which developers add custom content to SAS Infrastructure for Risk Management.
- Only job flows, SAS tasks, Java tasks, and input data are considered to be federated because the content is shared across all federated areas. All other content in a federated area (macros, Lua code, and so on) is not shared. This non-shared content is accessible only from within the federated area where the content is located.

## Federated Content Processing

- Job flows, tasks, and input data are shared across federated area. All other content is specific to the federated area in which it is located and is not shared. For example, a task in federated area 1 cannot call a macro in federated area 2.
- SAS Infrastructure for Risk Management searches for federated content in federated areas from the highest to lowest precedence (by the federated ID assigned in metadata and in alphabetical order), until it finds the content.

## Federated Job Flows

- Job flow files are shared across federated areas.
- When searching for a job flow definition, SAS Infrastructure for Risk Management searches the federated areas from the highest to lowest precedence. For example, if federated area 2 contains a file named flow1 and federated area 1 also contains a file named flow1, the file in federated area 2 is used for creating a new instance of a job flow.
- After a new instance is created, the instance does not change the definition. For example, if a flow1 file is added later to a federated area that is at a higher precedence, the existing instances of previously created flows that use this definition are not affected. However, new instances will use the new definition.
**Federated Tasks**

- Tasks that are identified within a job flow are searched for in federated areas from the highest to lowest precedence.
- Tasks with the same name are assumed to be the same content. Therefore, a task named task1.sas accepts the same input tables and produces the same output tables as other tasks with the same name, regardless of their federated location.
- Like job flow definition files, changing or adding a new version of a task does not affect existing job flow instances. However, new executions of an instance will use the newest definition of task1.sas.
- During execution of a task, the context of that execution environment is isolated to the federated area in which it resides. Any macro or Lua code that is called by the task must exist in the same federated area of the task.
- Tasks can have input and output files that are partitioned. Partitioned tasks enable large amounts of data to be partitioned into smaller units of data and calculated across multiple cores. A subsequent task recombines the results of the partitioned data.

For detailed information about partitioned tasks, see the documentation that is included in the generic sample federated area (fa.sample.3.5). The sample federated area contains sample flows that demonstrate the partitioning capabilities and functionality of SAS Infrastructure for Risk Management.

**Federated Input Data**

- Input data is shared across multiple federated areas.
- All input data that is used by SAS Infrastructure for Risk Management tasks must be mapped in the libnames.txt file that is located in the `config` folder of the federated area.

**CAUTION:**

Directly accessing SAS data sets that are not mapped via the libnames.txt file is not permissible. All tasks must define all of their inputs and outputs.

- All static input tables reside in the `landing_area` folder. Mappings are relative to the landing area. The file maps a logical name (using the LIBNAME statement) to a folder.

For example, `GLOBAL=%la/base/global` specifies the folder `base/global` within the federated area in the `landing_area` folder. The libref `GLOBAL` should refer to that path.
- Tasks can reference tables using one-, two-, or three-level names. Here are examples of table names:
  - `GLOBAL`
  - `GLOBAL.myglobal`
  - `GLOBAL.myglobal.sas7bdat`

*Note:* The latter two examples are processed identically. In the second example, the `sas7bdat` suffix is assumed by default. One-level names are processed somewhat differently than two- and three-level names.
SAS Infrastructure for Risk Management supports generic library mapping definitions in the libnames.txt file. Generic library mapping definitions enable access to data that is located outside of a SAS Infrastructure for Risk Management federated area. For example, this data might be located in a relational database management system, such as Hadoop, CAS, and so on.

SAS Infrastructure for Risk Management supports temporary library mapping definitions in the libnames.txt file. A temporary library is a data library that is promptly and automatically deleted as soon as it is no longer needed during the execution of a job flow. Temporary libraries minimize the disk space in the persistent area that is used by large data sets.

How Federated Input Data Is Processed

This section explains how federated input tables are processed by SAS Infrastructure for Risk Management.

Assume that the following three federated areas exist:

- com.sas.solutions.risk.irm.fa.0.3.5 — /sas-configuration-directory/Lev/AppData/SASIRM/fa.0.3.5
- com.sas.solutions.risk.irm.fa.2 — /sas-configuration-directory/Lev/AppData/SASIRM/fa2
- com.sas.solutions.risk.irm.fa.2.5 — /sas-configuration-directory/Lev/AppData/SASIRM/fa2.5

If a one-level name is specified, then SAS Infrastructure for Risk Management searches each libnames.txt file for the mapping in question in the federated area from the highest to lowest precedence.

For example, if the table references GLOBAL, then SAS Infrastructure for Risk Management searches the libnames.txt file in federated area 2.5. (Federated area 2.5 has the highest precedence because 2.5 is greater than 2.)

SAS Infrastructure for Risk Management is looking for a mapping for GLOBAL. If it finds a mapping, it adds the path to the concatenated LIBNAME statement that is used to define GLOBAL. This path is the first path in the LIBNAME statement. If the mapping is not found, the search continues through the federated areas for a libnames.txt file that contains a mapping for GLOBAL. If no mapping is found, the task fails with an error.

Processing two- or three-level names is similar to processing one-level names, except that SAS Infrastructure for Risk Management has the information that is required to verify that the actual table exists. As before, SAS Infrastructure for Risk Management searches for a mapping in the libnames.txt file. If it does not find a mapping, it searches the next federated area (by precedence). If SAS Infrastructure for Risk Management finds a mapping, it verifies that the file actually exists in the folder that is specified in the mapping.

Mapping enables content developers to overwrite a single table without having to override all tables using the same mapping (LIBNAME).

If SAS Infrastructure for Risk Management cannot locate the table, the task is not created and the SAS Infrastructure for Risk Management New Instance wizard reports an error that the instance cannot be created.

Consider the case of a pair of two-level names, GLOBAL.table1 and GLOBAL.table2, that use the same mapping that was previously described. Both tables reside in federated area 1, but only GLOBAL.table1 resides in federated area 2. The following LIBNAME statement is generated:
LIBNAME GLOBAL ('/sas-configuration-directory/Levn/AppData/SASIRM/fa2/landing_area/base/global' ')/sas-configuration-directory/Levn/AppData/SASIRM/fa1/landing_area/base/global');

According to the LIBNAME statement, the tables are located as follows:

- table1.sas7bdat is found in federated area 2 (sas-configuration-directory/Levn/AppData/SASIRM/fa2/landing_area/base/global)
- table2.sas7bdat is found in federated area 1 (sas-configuration-directory/Levn/AppData/SASIRM/fa1/landing_area/base/global)

The search for mappings uses the following case order:

1. as specified in the flow definition (for example, “GlobAl”, if so specified in the flow definition)
2. all uppercase (for example, “GLOBAL”)
3. all lowercase (for example, “global”)
4. initial capitalization (for example, “Global”)

Note: SAS recommends that you use three-level names in your job flow definitions and uppercase mapping in your libnames.txt files.

**Personal Federated Area**

SAS Infrastructure for Risk Management introduces support for a developer persona. When logging on to the SAS Infrastructure for Risk Management web application for the first time, the developer’s personal federated area is automatically created. A personal federated area is where a developer creates content using parallel programs called job flows.

For information about the SAS Infrastructure for Risk Management personal federated area, see *SAS Infrastructure for Risk Management: Programmer’s Guide.*
Part 2

Deploying SAS Infrastructure for Risk Management

Chapter 4
Pre-installation Tasks .................................................... 19

Chapter 5
Installing SAS Infrastructure for Risk Management ............... 23

Chapter 6
Performing Post-installation Tasks ................................. 33
Chapter 4
Pre-installation Tasks

Overview of the Pre-installation Tasks

Before you install SAS Infrastructure for Risk Management, complete the pre-installation tasks that are included in the following checklist.

Table 4.1 Pre-installation Checklist

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify your system requirements.</td>
</tr>
<tr>
<td></td>
<td>Obtain a deployment plan.</td>
</tr>
<tr>
<td></td>
<td>Complete the pre-installation checklist that accompanies your deployment plan.</td>
</tr>
<tr>
<td></td>
<td>Set up SAS Infrastructure for Risk Management User Accounts.</td>
</tr>
<tr>
<td></td>
<td>Grant Linux Directory Permissions.</td>
</tr>
<tr>
<td></td>
<td>Check for SAS Installation Notes.</td>
</tr>
</tbody>
</table>

Overview of the Pre-installation Tasks

1. Verify Your System Requirements
2. Obtain a Deployment Plan
3. Complete the Pre-installation Checklist That Accompanies Your Deployment Plan
4. Set Up SAS Infrastructure for Risk Management User Accounts
5. Create a SAS Software Depot
6. Grant Linux Directory Permissions
7. Check for SAS Installation Notes
Verify Your System Requirements

Ensure that your system meets the minimum system requirements for SAS Infrastructure for Risk Management.


Note: Depending on the federated content that is installed, the system requirements might differ.

Obtain a Deployment Plan

A deployment plan is a preselection of the software that is installed by the SAS Deployment Wizard. It contains a description of what the plan deploys, identifies the target machines, and lists the software to be installed and configured. The deployment file is an XML file that is named plan.xml.

SAS Infrastructure for Risk Management solution installation plan files are custom deployment plans that have been created by a SAS Installation Representative specifically for your site. The representative emails the XML file (or a ZIP file containing an XML file) to you.

Before installing, ensure that you copy the plan file to a location from which the SAS Deployment Wizard can obtain it during installation.

For more information about deployment plans, see SAS Intelligence Platform: Installation and Configuration Guide.

Complete the Pre-installation Checklist That Accompanies Your Deployment Plan

Your deployment plan download contains a checklist.pdf file and a checklist.rtf file. Both files contain the same pre-installation checklist, which you must complete before deploying a SAS Infrastructure for Risk Management solution.

The checklist includes tasks that are specific to your deployment. It also includes information about the third-party software, the operating system accounts and groups, and the ports that are required before starting the deployment.
Set Up SAS Infrastructure for Risk Management
User Accounts

Valid host operating system accounts are required for SAS Infrastructure for Risk Management administrative and product users. You can use existing operating system accounts.

SAS Infrastructure for Risk Management administrative and product users also require access to the workspace server.

If the workspace server is running on the Windows operating system, note that the operating system accounts must also have the Log on as a batch job privilege. In addition, the SAS General Servers account needs to have the Create Symbolic Link privilege.

These settings are located under Control Panel ⇒ Administrative Settings ⇒ Local Security Policy ⇒ Local Policies ⇒ User Rights Assignment.

Users can use internal metadata accounts instead of operating system accounts to access the software. The only account that must exist as an operating system account is the account that is used to launch the SAS Workspace Server (that is, the SAS General Server User).

Note: If you are installing SAS Infrastructure for Risk Management in a Windows x64 environment, ensure that you specify the account for SAS General Servers in the correct format if it is a domain account. If it is a domain account, you must specify the global login account as user@domain (not domain\user).

For more information about external user accounts, see SAS Intelligence Platform: Installation and Configuration Guide.

Create a SAS Software Depot

Download the software that is listed in your SAS Software Order with the SAS Download Manager. A SAS Software Depot is created, which includes the SAS installation data (SID) file. The SID file is used by the SAS system to install and license SAS software. After you have downloaded the SAS Software Depot, you can then use the SAS Deployment Wizard to install your software. Verify that Base SAS (SAS) is listed as a selected product. Then, select additional products that are specific to your environment.

For more information about creating a SAS Software Depot, see SAS Intelligence Platform: Installation and Configuration Guide.

Grant Linux Directory Permissions

To deploy SAS Infrastructure for Risk Management in Linux environments, you must create and grant Write permissions on the /etc/opt/vmware/vfabric directory. Refer to the SAS Pre-installation Checklist that is included with your deployment plan for instructions about how to set up this directory.
Check for SAS Installation Notes

Chapter 5
Installing SAS Infrastructure for Risk Management

Overview of the Installation Tasks

To install and configure SAS Infrastructure for Risk Management, complete the tasks that are included in the following checklist.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review the structure of the SAS Infrastructure for Risk Management file system.</td>
</tr>
<tr>
<td></td>
<td>Install and configure SAS Infrastructure for Risk Management.</td>
</tr>
<tr>
<td>(Optional)</td>
<td>Configure an external location for the SAS Infrastructure for Risk Management persistent area.</td>
</tr>
<tr>
<td></td>
<td>Install hot fixes.</td>
</tr>
<tr>
<td>(Optional)</td>
<td>Download and install the SAS Infrastructure for Risk Management solution’s federated content package.</td>
</tr>
</tbody>
</table>
## Review the File System Structure

By default, the following directories exist after you install and configure SAS Infrastructure for Risk Management:

<table>
<thead>
<tr>
<th>Directory</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAS-installation-directory</strong></td>
<td>• Linux: <code>/SAS-installation-directory/SASHome/</code></td>
</tr>
<tr>
<td></td>
<td>• Windows: <code>C:\Program Files\SASHome\</code></td>
</tr>
<tr>
<td><strong>!SASROOT</strong> (SAS Foundation Directory)</td>
<td>• Linux: <code>/SAS-installation-directory/SASHome/SASFoundation/9.4/</code></td>
</tr>
<tr>
<td></td>
<td>• Windows: <code>C:\Program Files\SASHome\SASFoundation\9.4\</code></td>
</tr>
<tr>
<td><strong>SAS-configuration-directory</strong></td>
<td>• Linux: <code>/SAS-installation-directory/SAS-configuration-directory/Levn/</code></td>
</tr>
<tr>
<td></td>
<td>• Windows: <code>C:\SAS\SAS-configuration-directory\Levn\</code></td>
</tr>
<tr>
<td><strong>SAS Infrastructure for Risk Management data directory</strong> (the product’s</td>
<td>• Linux: <code>/SAS-configuration-directory/Levn/AppData/SASIRM/</code></td>
</tr>
<tr>
<td>root data directory**</td>
<td>• Windows: <code>\SAS-configuration-directory\Levn\AppData\SASIRM\</code></td>
</tr>
<tr>
<td><strong>SAS Deployment Wizard installation summary</strong></td>
<td>• Linux: <code>/SAS-configuration-directory/Levn/Documents/DeploymentSummary.html</code></td>
</tr>
<tr>
<td></td>
<td>• Windows: <code>\SAS-configuration-directory\Levn\Documents\DeploymentSummary.html</code></td>
</tr>
<tr>
<td><strong>SAS Deployment Wizard configuration logs</strong></td>
<td>• Linux: <code>/SAS-configuration-directory/Levn/Logs/Configure</code></td>
</tr>
<tr>
<td></td>
<td>• Windows: <code>\SAS-configuration-directory\Levn\Logs\Configure</code></td>
</tr>
<tr>
<td><strong>Web application server logs</strong></td>
<td>• Linux: <code>/SAS-configuration-directory/Levn/Web/Logs</code></td>
</tr>
<tr>
<td><strong>Note:</strong> By default, some logging is enabled. You can configure</td>
<td>• Windows: <code>\SAS-configuration-directory\Levn\Web\Logs</code></td>
</tr>
<tr>
<td>additional logging in the SAS Management Console.</td>
<td></td>
</tr>
<tr>
<td><strong>SAS Infrastructure for Risk Management middle-tier staging directory</strong></td>
<td>• Linux: <code>/SAS-configuration-directory/Levn/Web/Staging</code></td>
</tr>
<tr>
<td></td>
<td>• Windows: <code>\SAS-configuration-directory\Levn\Web\Staging</code></td>
</tr>
</tbody>
</table>
Install SAS Infrastructure for Risk Management

You can install SAS Infrastructure for Risk Management on just one machine or on several machines as listed in your customized deployment plan (plan.xml file).

Although the SAS Deployment Wizard contains steps for all of the products that are a part of your deployment, this section describes only those steps that pertain to SAS Infrastructure for Risk Management. In addition, this installation example explains how to install on a single machine using the Typical prompting level.

The SAS Deployment Wizard pages that you see during installation depend on the following:

- the prompt level that you choose
- the SAS tier on which you are deploying SAS Infrastructure for Risk Management
- the contents of your custom order
- the plan.xml file

**CAUTION:**

Do not add spaces to the installation and configuration paths when installing SAS Infrastructure for Risk Management. If you add a space to the paths, it causes the SAS Infrastructure for Risk Management server to fail.

To install a SAS Infrastructure for Risk Management solution:

1. Using the SAS Installer account (or an account that is a member of the Windows Administrators group), log on to the machine on which to install the SAS Infrastructure for Risk Management solution.

2. Navigate to the highest-level directory in your SAS Software Depot.

3. Using the `setup` command that is appropriate for your operating system, start the SAS Deployment Wizard.

4. On the Select Deployment Type page, select Perform a Planned Deployment and ensure that both Install SAS Software and Configure SAS Software are selected.
5. On the Select Deployment Step and Products to Install page, select **Step 1: Server and Middle Tier** and click **Next**. (In this example, the server tier and the middle tier are installed on the same machine.)

6. On the Select Deployment Task page, select **Install SAS Software** and click **Next**.

7. On the SAS IRM Server Configuration page, enter a password for the SAS Infrastructure for Risk Management super user and click **Next**.

   ![SAS Deployment Wizard](image)

   **Note:** The IRM super user is a built-in internal account that has privilege levels significantly beyond those of most user accounts. A member of the super user accounts can perform system-level administrative tasks. The IRM super user is a member of the predefined **IRM:Access All Entities** role.

8. On the SAS IRM Database Configuration page, enter the credentials for accessing the SAS Infrastructure for Risk Management database and click **Next**.
9. (Optional) On the SAS IRM Mid-tier Configuration page, enter the name of the SAS Infrastructure for Risk Management solution that you are installing. The name that you enter is displayed on the banner of the web application. By default, SAS Infrastructure for Risk Management is displayed in the banner.

Note: When a web application is at 100% zoom and the screen resolution is 1280 x 1024, a limited number of letters, numbers, and spaces can be seen in the banner. In addition, do not use single or double quotation marks in the solution name.

10. When the Deployment Summary page is displayed, review the list of products to be installed and click Start.

The SAS Deployment Wizard launches the installation and configuration process and provides an ongoing status update.
11. When the installation and configuration process completes, the Deployment Complete page appears.

A status icon is displayed next to each software application. The status icon indicates whether the installation process completed successfully, completed with warnings, or completed with errors for that application.

If you ordered SAS Infrastructure for Risk Management as part of a solution (such as SAS Firmwide for Solvency II), after you install and configure SAS Infrastructure for Risk Management, you must download, unzip, and install the solution’s federated content. For information about downloading and installing federated content, see “Install Federated Content” on page 30.

Install Hot Fixes

Hot fixes that were released before the current maintenance release are automatically installed when you run the SAS Deployment Wizard. If additional hot fixes are available for your products, install them now.

To ensure that SAS Infrastructure for Risk Management functions correctly, install all the hot fixes for the following products:

- SAS Infrastructure for Risk Management 3.5
- SAS 9.4M5

Complete one or more of the following steps to find applicable hot fixes:

- Go to the Technical Support Hot Fixes page and download the hot fixes that are applicable to SAS Infrastructure for Risk Management and the fifth maintenance release of SAS 9.4.
- Use the SAS Hot Fix Analysis, Download and Deployment Tool to create a customized report that lists the hot fixes that are available for the installed SAS products. This tool also generates the scripts that automate the download of the hot fixes.
- Use SAS Deployment Manager to find and apply the hot fixes.

For more information about hot fixes, see SAS Deployment Wizard and SAS Deployment Manager 9.4: User’s Guide.

For information about applying SAS Security Updates to an existing deployment, see “Apply SAS Security Updates” on page 38.

For information about using the SAS Infrastructure for Risk Management hot fix post-installation tool to apply SAS Infrastructure for Risk Management server-tier hot fixes to an existing deployment, see “Run the SAS Infrastructure for Risk Management Hot Fix Post-installation Tool” on page 74.

Configure an External Location to the Persistent Area

When you install SAS Infrastructure for Risk Management, the default location of the persistent area is in the SAS Infrastructure for Risk Management root data directory:
The default location is recommended for most SAS Infrastructure for Risk Management deployments. However, there might be environments that require that you move the persistent area to a location outside of the SAS Infrastructure for Risk Management root directory. For example:

- The persistent area needs to be in a location with more storage.
- The persistent area needs to be in a location with faster storage.
- SAS Infrastructure for Risk Management is configured for grid computing, which requires the persistent area to be located on a shared area network.

**CAUTION:**

You can configure an external location for the persistent area in a fresh environment only. This is the environment that exists right after SAS Infrastructure for Risk Management is installed and before any job flows are executed. The persistent area cannot contain any data. If you need to move the location of the persistent area in an established SAS Infrastructure for Risk Management deployment, see “Change the Location of the Persistent Area” on page 69.

To configure a location for the persistent area that is outside of SAS Infrastructure for Risk Management:

1. Stop the SAS Infrastructure for Risk Management web application server.

   For a non-clustered environment, the web application server is SASServer8_1. For a clustered environment, the web application servers can include SASServer8_2, SASServer_3, and so on, and can be on the same machine or on different machines within the cluster.

   For more information about stopping SAS Web Application Servers, see *SAS Intelligence Platform: Middle-Tier Administration Guide*.

2. Copy or move the SAS Infrastructure for Risk Management persistent area (config/Lev1/AppData/SASIRM/pa) to the desired external location.

3. In SAS Management Console, add the new federated area property by completing the following steps:
   a. Connect to the appropriate metadata server as a SAS administrator (for example, sasadm@saspw).
   b. On the Plug-ins tab, verify that the correct repository is selected in the Repository field. The default repository is Foundation.
   c. Select Application Management ⇒ Configuration Manager ⇒ SAS Application Infrastructure.
   d. In the main pane, right-click SAS IRM Mid-Tier Server and select Properties. The IRM Mid-Tier Server Properties window is displayed.
   e. Click the Advanced tab, select the default entry for the persistent area and click Remove.
f. Click **Add**. The Define New Property dialog box is displayed.

![Define New Property dialog box](image)

In the **Property Name** field, specify the default property name of the persistent area (com.sas.solutions.risk.irm.server.pa) and in the **Property Value** field, enter the new location of the persistent area.

h. Click **OK**.

4. Click **OK**.

5. Restart the SAS Infrastructure for Risk Management web application server.

---

### Install Federated Content

SAS delivers the federated content for a solution as a downloadable content release that is located on the Downloads support page. If you are installing SAS Infrastructure for Risk Management as part of a solution, you must download and install the solution’s content release after you have installed SAS Infrastructure for Risk Management.

**Note:** Before installing federated content, ensure that you back up your system. For information about backing up your system, see “Back Up Content” on page 39.

To obtain the content release for your solution:

1. Access the Downloads page at support.sas.com/downloads/.
2. Locate the content release for your solution. You can search alphabetically, by product category, or by release date.
3. If prompted, enter your SAS Profile logon credentials and click **Sign in**.

4. To initiate the download, click the ZIP filename of the content release.

5. In the SAS License Validation window, enter your site number for verification and click **Submit**.

6. In the SAS License Agreement for Download window, click **Accept** to agree to the license agreement and proceed with the download.

7. After you have downloaded the content release for your SAS Infrastructure for Risk Management solution, use the installation instructions that are provided with the package to install and verify the content.
Overview of the Post-installation Tasks

After installing SAS Infrastructure for Risk Management, complete the post-installation tasks in the following checklist before using SAS Infrastructure for Risk Management.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Follow the instructions in the Instructions.html file.</td>
</tr>
<tr>
<td></td>
<td>Create roles, groups, and users.</td>
</tr>
<tr>
<td>Completed?</td>
<td>Task</td>
</tr>
<tr>
<td>------------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td>Configure metadata user accounts and assign the user to groups.</td>
</tr>
<tr>
<td></td>
<td>Access the SAS Infrastructure for Risk Management web application interface.</td>
</tr>
<tr>
<td></td>
<td>Apply SAS security updates.</td>
</tr>
<tr>
<td></td>
<td>Enable grid support.</td>
</tr>
</tbody>
</table>

**Use the Instructions File**

At the end of the installation process for SAS Infrastructure for Risk Management, the SAS Deployment Wizard produces a document named Instructions.html.

*Note:* If the server tier and the middle tier are hosted on separate machines, there is an Instructions.html file for each machine.

The Instructions.html file is located in the `SAS-configuration-directory/Lev/ Documents/` directory. Follow the instructions that are provided in the document.

**Create Roles, Groups, and Users**

*About Roles, Groups, and Users*

To use SAS Infrastructure for Risk Management, you must configure your roles, groups, and users.

- Roles
  Roles determine what a user can do within the application. Roles can be assigned to groups to allow a restricted set of users within that group to perform an activity.

- Groups
  A group consists of users who are classified by common traits or by common data access levels. Groups are typically used for granting users access to data. Groups can also be used within workflows to allow a restricted set of users to perform an activity.

- Users
  Every user who needs to log on to SAS Infrastructure for Risk Management must be defined in the SAS Metadata Repository. The user must be associated with one or more roles that permit one or more capabilities within SAS Infrastructure for Risk Management.

Use SAS Management Console to define roles, groups, and users. You can also use SAS Management Console to associate capabilities with roles. For more information, see *SAS Management Console: Guide to Users and Permissions*. 
Defining Roles

Roles in SAS Infrastructure for Risk Management are activity-based. You assign roles to groups, and those role assignments are cumulative.

For example, suppose a group is associated with Role 1 and Role 2. If Role 1 grants a group a specific capability but Role 2 does not, the group retains the capability that is granted by Role 1.

The following table lists the predefined roles for SAS Infrastructure for Risk Management. After you deploy the solution, ensure that these roles are defined in SAS Management Console.

Table 6.1 Predefined Roles and Capabilities

<table>
<thead>
<tr>
<th>Predefined Role</th>
<th>Description and Capabilities Assigned to the Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRM: Access All Entities</td>
<td>Description: The IRM Super User Entity Access Role</td>
</tr>
<tr>
<td></td>
<td>Capabilities:</td>
</tr>
<tr>
<td></td>
<td>• Allow Access to All Entities</td>
</tr>
<tr>
<td></td>
<td>• Allow Access to IRM</td>
</tr>
<tr>
<td></td>
<td>Note: By default, the SAS General Servers group, the SAS</td>
</tr>
<tr>
<td></td>
<td>IRM Super User, and if configured, the SAS Demo User are</td>
</tr>
<tr>
<td></td>
<td>assigned to the IRM: Access All Entities role.</td>
</tr>
<tr>
<td>IRM: Change Owner</td>
<td>Description: IRM Change Ownership of Job Flows Role</td>
</tr>
<tr>
<td></td>
<td>Capability: Can Change Owner</td>
</tr>
<tr>
<td>IRM: Install Federated Areas</td>
<td>Description: IRM Allow Install of Federated Areas Role</td>
</tr>
<tr>
<td></td>
<td>Capability: Allow Install of Federated Area</td>
</tr>
</tbody>
</table>

Defining Groups

A group in SAS Infrastructure for Risk Management is based on the area of work that is associated with the users in that particular group. You can add a user to multiple groups. Every group can be assigned one or more roles, and the capabilities of those roles are inherited by the group.

Defining Users

The SAS Infrastructure for Risk Management platform has a built-in internal super user (sasirmsu). This user is defined in SAS Management Console with the user ID sasirmsu@saspw. The sasirmsu super user is a member of IRM: Access All Entities role.

The SAS Deployment Wizard does not create application users by default. You must create users in SAS Management Console with the appropriate group and role permissions. For information about creating users, see “Configure the Metadata Accounts for SAS Infrastructure for Risk Management” on page 36.
Configure the Metadata Accounts for SAS Infrastructure for Risk Management

All users must have a metadata account on the SAS Metadata Server for the SAS Infrastructure for Risk Management web application. However, users are not required to have an operating system account. The steps for configuring a metadata account vary according to whether the user has an operating system account. For information about importing user accounts from another provider such as LDAP into the SAS metadata, see *SAS Intelligence Platform: System Administration Guide*.

**Configure a User Who Has an Operating System Account**

To configure a SAS Infrastructure for Risk Management metadata user account for a user who has an operating system account:

1. Log on to SAS Management Console as a SAS administrator (for example, sasadm@saspw).
2. Right-click the User Manager plug-in and select New ð User. The New User Properties window is displayed.
3. On the General tab:
   - a. In the Name field, enter a user ID for the user. This ID is used to log on to the application.
     - TIP  Avoid using spaces or special characters in the Name field. Not all components support spaces and special characters.
   - b. In the Display Name field, enter the name that you want to associate with the user ID.
4. On the Accounts tab:
   - a. Click New to create a new SAS Metadata account for the user. The New Login Properties window is displayed.
   - b. In the User ID field, enter the user ID. It corresponds to the user ID that is used to log on to SAS Infrastructure for Risk Management.
   - c. Select an Authentication Domain (for example, DefaultAuth), and click OK.
5. On the Group and Roles tab:
   - a. In the Available Groups and Roles section, select the group to which you want the user to belong. For example, select IRM: Access All Entities to permit the user access to all entities.
   - b. Move the group to the Member of section.
6. To create a custom role for granting access to selected entities and capabilities:
   - a. From the User Manager plug-in, select New Role.
   - b. In the Name field, enter the appropriate values:
     
     **IRM: action Entity entity_role entity_ID**. Here are descriptions of the values that you specify:

     * action — specifies the capabilities of the role. Possible values are Access (create, view, and modify job flow instances for a specified entity), Publish
(publish job flow instances of a specified entity), or **Delete** (delete job flow instances of a specified entity).

- **entity_role** — (Optional) Possible values are **Solo** or **Group** permissions. The default is **Group**.

- **entity_ID** — specifies the name of the entity.

Here is an example of a custom role that enables a user to publish instances for an entity named ENTITY_BE:

IRM: Publish Entity ENTITY_BE

Here is an example of a customer role that enables a user to create, view, and modify job flow instances for the same entity (ENTITY_BE):

IRM: Access Entity ENTITY_BE

7. To create the new user, click **OK**. The new user appears in the **User Manager** list.

**Configure a User Who Does Not Have an Operating System Account**

To configure a SAS Infrastructure for Risk Management metadata user account for a user who does not have an operating system account:

1. Log on to SAS Management Console as a SAS administrator (for example, sasadm@saspw).

2. Right-click the **User Manager** plug-in and select **New** ➔ **User**. The New User Properties window is displayed.

3. On the **General** tab:
   
a. In the **Name** field, enter a user ID for the user. This ID is used to log on to the application.  
   
   **Tip** Avoid using spaces or special characters in the **Name** field. Not all components support spaces and special characters.

   b. In the **Display Name** field, enter the name that you want to associate with the user ID.

4. On the **Accounts** tab:
   
a. Click **Create Internal Account**. The New Internal Account for New User window is displayed.

   b. Enter a password for the new user and click **OK**.

5. On the **Group and Roles** tab:
   
a. In the **Available Groups and Roles** section, select the group to which the user belongs. For example, select **IRM: Access All Entities** to enable the user to access all entities.

   b. Move the group to the **Member of** section.

6. To create a custom role for granting access to selected entities and capabilities:
   
a. From the **User Manager** plug-in, select **New Role**.

   b. In the **Name** field, enter:

   **IRM: action Entity entity_role entity_ID**. Here are descriptions of the values that you specify:
• **action** — specifies the capabilities of the role. Possible values are **Access** (create, view, and modify job flow instances for a specified entity), **Publish** (publish job flow instances of a specified entity), or **Delete** (delete job flow instances of a specified entity).

• **entity_role** — (Optional) Possible values are **Solo** or **Group** permissions. The default is **Group**.

• **entity_ID** — specifies the name of the entity.

Here is an example of a custom role that enables a user to publish instances for an entity named ENTITY_BE:

IRM: Publish Entity ENTITY_BE

Here is an example of a customer role that enables a user to create, view, and modify job flow instances for the same entity (ENTITY_BE):

IRM: Access Entity ENTITY_BE

7. To create the new user, click **OK**. The new user appears in the **User Manager** list.

---

**Apply SAS Security Updates**

As a part of the hot-fix process, SAS delivers security fixes.

After you apply a security fix, if any updated JAR files also exist in the SAS Infrastructure for Risk Management platform federated area (fa.0.3.5), you must manually copy those JAR files from where the files are installed to where they are located in the SAS Infrastructure for Risk Management platform federated area.

Here is a table that lists the JAR files by SAS security update that you have to manually copy to the SAS Infrastructure for Risk Management platform federated area after applying the security update.

*Table 6.2 SAS Security Updates and Updated JAR Files*

<table>
<thead>
<tr>
<th>SAS Security Update</th>
<th>Updated JAR Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAS Security Update 2018-12</td>
<td>commons_cl1_1.4.0.0_SAS_20180727143240/commons-cl1.jar</td>
</tr>
<tr>
<td>SAS Security Update 2018-09</td>
<td>commons_io_2.6.0.0_SAS_20180621100654/commons-io.jar</td>
</tr>
</tbody>
</table>

To obtain SAS Security Updates and to access detailed information about how to apply security updates to your SAS Infrastructure for Risk Management installation, see **SAS Security Updates and Hot Fixes**.

After you apply the security update:

1. Back up the SAS Infrastructure for Risk Management platform federated area.
2. Stop the SAS Infrastructure for Risk Management web application server.
3. Copy the updated JAR file or files from the SAS Versioned JAR Repository location:

/SASHome/SASVersionedJarRepository/eclipse/plugins/
to the SAS Infrastructure for Risk Management platform federated area location:

```
SAS-configuration-directory/LevN/AppData/SASIRM/fa.0.3.5/source/java/lib/
```

*Note:* Overwrite the existing JAR files in the SAS Infrastructure for Risk Management platform federated area.

4. Restart the SAS Infrastructure for Risk Management web application server.

---

**Configure SAS Infrastructure for Risk Management to Use HTTP over an SSL Connection**

To configure SAS Infrastructure for Risk Management to use HTTP over SSL:

1. Navigate to `/SASHome/SASVersionedJarRepository/eclipse/plugins/`

2. In the subdirectories, locate the following two SAS/SECURE JAR files: `sastpj.rutil_version-number.jar` and `sas.rutil_version-number.jar` where `version-number` is a variable that indicates the release of the file.

3. Copy the files to the Java file folder for the platform federated area `/sas_config_directory/LevN/AppData/SASIRM/fa.0.3.5/source/java/lib`.

4. Restart the SAS Infrastructure for Risk Management web application server.

For more information about configuring HTTP over an SSL connection, see *SAS Intelligence Platform: System Administration Guide*.

---

**Access the SAS Infrastructure for Risk Management Web Application**

You can access the SAS Infrastructure for Risk Management user interface through your web browser at `http://Your_Middle_Tier_Host:port/SASIRM`.

For more information about this URL and the port number, see the Instructions.html file that is generated for SAS Infrastructure for Risk Management.

By default, SAS Infrastructure for Risk Management is configured to run on port 7980 on Linux systems and on port 80 for Microsoft Windows. However, verify the port number by checking the Instructions.html file.

---

**Back Up Content**

It is recommended that you implement a system to back up and restore metadata, databases, and disk drive content that is generated by SAS Infrastructure for Risk
Ensure that the backup includes the SAS Infrastructure for Risk Management database and the persistent area. For more information about how to back up SAS content, see *SAS Intelligence Platform: System Administration Guide*.

### Configure the LOCKDOWN Feature

SAS 9.4 includes a LOCKDOWN statement. This statement limits the accessibility and activities of a SAS server by putting the server in a locked-down state. This function enables SAS administrators to limit the file access and directory access of the SAS servers to a user-defined list of approved locations. This list, referred to as a lockdown path list, is a whitelist. That is, it specifies which paths are accessible by SAS Infrastructure for Risk Management. You must configure your system so that SAS Infrastructure for Risk Management environments and any data that is used by these environments are included in this list.

For more information about the LOCKDOWN feature, see *SAS Intelligence Platform: System Administration Guide*.

When configuring the LOCKDOWN statement in your SAS Infrastructure for Risk Management environment, ensure that you specify the `ENABLE_AMS=JAVA` option as well as the `ENABLE_AMS` option for other components that you are using with SAS Infrastructure for Risk Management (for example, Hadoop).

*Note:* When you use LOCKDOWN, it is recommended that you put SAS Infrastructure for Risk Management in its own server context to prevent the `ENABLE_AMS=JAVA` option from affecting other SAS applications.

### Configure SAS Infrastructure for Risk Management Grid Computing

#### About SAS Infrastructure for Risk Management Grid Computing

A SAS Infrastructure for Risk Management grid computing implementation provides scalability by distributing computing tasks across multiple SAS workspace servers on a network.

SAS Infrastructure for Risk Management grid computing uses SAS Application Servers that are installed on each *grid node* (machine) in the grid computing implementation. Each application server context contains a SAS Logical Workspace Server with its own object spawner. The properties that are defined in the SAS Metadata Repository specify which servers to use in the SAS Infrastructure for Risk Management grid computing implementation.

*Note:* SAS Infrastructure for Risk Management grid computing environment is not implemented using SAS Grid Manager.

#### Prerequisites

You must meet the following prerequisites before performing a SAS Infrastructure for Risk Management grid installation:
• Verify that the deployment plan that you obtained from a SAS Installation Representative contains an additional SAS Application Server (with a logical workspace server and an object spawner).

This application server context must be installed on each of the grid nodes in your grid computing implementation. The only exception is that the initial application server context is created and used by SAS Infrastructure for Risk Management during a typical installation.

• Use the same SAS Installer account for all the servers, and use the same user to launch the workspace servers on all the grid nodes.

• To prevent permission and ownership issues with Linux implementations, all SAS solution users (for example, sas, sassrv, and so on) should have the same ID. In addition, the primary account of sas and sassrv should have the same ID.

Linux users can have local accounts. Here is an example:

- uid=200(sas) gid=2000(sas) groups=2000(sas)
- uid=201(sassrv) gid=2000(sas) groups=2000(sas)

• If you are installing SAS Infrastructure for Risk Management in a Windows x64 environment, ensure that you use domain accounts for the SAS Installer account and the SAS General Servers user group. In SAS Management Console, enter the accounts as user@domain (not domain\user).

• Ensure that the SASHome and SASConfig directories are installed on local disks that are not shared. In addition, the SAS Work folder should point to a local disk.

• Share all SAS Infrastructure for Risk Management federated areas and the persistent area. To share the federated areas and the persistent area, use a production file sharing system. An example is Global File System (GFS2) on Linux.

CAUTION:
Do not use Network File System (NFS) or Windows mapped drives. Do not use NFS, Windows mapped drives, or shared resources. Use of any of these strategies can cause intermittent and unreliable file issues.

As with a standard SAS Infrastructure for Risk Management installation, if the SAS Infrastructure for Risk Management middle tier is located on a separate machine from one or more workspace servers, no file sharing is required on the middle-tier machine.

Performing the SAS Infrastructure for Risk Management Grid Installation

1. Use the deployment plan and instructions.html file obtained from a SAS Installation Representative to perform your SAS Infrastructure for Risk Management installation. This installation should be on a local disk (not shared storage). (See Chapter 5, “Installing SAS Infrastructure for Risk Management,” on page 23.)

2. Use the sample job flows in the SAS Infrastructure for Risk Management located in the sample federated area (fa.sample.3.5) to verify that you can create and successfully execute SAS Infrastructure for Risk Management sample job flow instances.

After verifying that the SAS Infrastructure for Risk Management installation was successful, delete the job flow instances that you created.

3. Stop the SAS Infrastructure for Risk Management web application server (SASServer8_1), move the SAS Infrastructure for Risk Management federated areas
and the persistent area to the shared file system, and update the properties in SAS Management Console. (See “Configure an External Location to the Persistent Area” on page 28.)

Here is an example of the properties before you moved the federated areas and the persistent area to a shared file system:

Here is an example of the properties after you moved the federated areas and the persistent area to a shared file system:

4. Restart SASServer8_1 and verify that you can still successfully create and execute SAS Infrastructure for Risk Management sample job flow instances. (Then, you can delete these sample job flow instances.)

5. Use SAS Deployment Wizard to install a SAS Application Server context on each grid node in your installation and validate each new workspace server in SAS Management Console. (See SAS Intelligence Platform: Installation and Configuration Guide)

Note: You can continue to use SAS Infrastructure for Risk Management during this process.

6. After you have installed an application server context on all of the grid nodes, stop SASServer8_1.

7. In SAS Management Console, add the workspace server properties to the SAS IRM Mid-Tier component:

a. Connect to the appropriate metadata server as a SAS administrator (for example, sasadm@saspw).

b. On the Plug-ins tab, verify that the correct repository is selected. The default repository is Foundation.

c. Select Application Management ⇒ Configuration Manager ⇒ SAS Application Infrastructure
Configure SAS Infrastructure for Risk Management Grid Computing

43

d. In the main pane, right-click **SAS IRM Mid-Tier** and select **Properties**. The IRM Mid-Tier Properties window is displayed.

e. Click the **Advanced** tab and then click **Add** to define the properties for each grid node in the following format:

\[
\text{workspacesrv.logical.name}.n
\]

where \( n \) is a consecutive number from 2 to the number of grid nodes that you are adding (for example, the first additional server is \( \text{workspacesrv.logical.name}.2 \), the second additional server is \( \text{workspacesrv.logical.name}.3 \), and so on). Each has the property value of the application server context that you added.

*Note:* The property \( \text{workspacesrv.logical.name} \) will already exist. Do not modify the property.

Here is an example of how these properties might be defined if you are running a grid computing implementation that contains three grid nodes:

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Property Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>workspacesrv.logical.name</td>
<td>SASApp — Logical Workspace Server</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> This property exists. Do not modify this property.</td>
</tr>
<tr>
<td>workspacesrv.logical.name.2</td>
<td>SASApp2 — Logical Workspace Server</td>
</tr>
<tr>
<td>workspacesrv.logical.name.3</td>
<td>SASApp3 — Logical Workspace Server</td>
</tr>
</tbody>
</table>

f. Click **OK** to save the new properties. Click **OK** again to exit SAS Management Console.

g. Restart the SASServer8_1 and use the sample content to verify that you can successfully create and execute sample SAS Infrastructure for Risk Management job flow instances.

You can add or remove grid nodes at any time (except for the original SAS Infrastructure for Risk Management application server context (\( \text{workspacesrv.logical.name} \) **SASApp - Logical Workspace Server** shown in the preceding example).

Before adding or removing a grid node, stop SASServer8_1.
Part 3

Migrating and Upgrading SAS Infrastructure for Risk Management

Chapter 7
Upgrade and Migration Overview ............................ 47

Chapter 8
Migrating SAS Infrastructure for Risk Management ......... 49

Chapter 9
Upgrading SAS Infrastructure for Risk Management .......... 57
Chapter 7
Upgrade and Migration
Overview

About Migrating and Upgrading

You can move software from a previous release to the current release of SAS Infrastructure for Risk Management using either of the following two methods:

- migration
  The process of moving SAS metadata and other data and files from one instance of SAS Infrastructure for Risk Management to another instance of SAS, as part of an installation on a new machine.

  Migration typically involves new hardware. For example, you might migrate your machine from a development system to a production system, or you might migrate hardware from an older server to a newer server. Migration attempts to preserve as much of your current content and configuration as possible.

  For more information, see “Migrating SAS Infrastructure for Risk Management” on page 49.

- upgrade
  Involves updating SAS Infrastructure for Risk Management from a previous version to a new version on the same supporting platform.

  This option does not require new hardware and can be performed on the same operating system.

  For more information, see “Upgrading SAS Infrastructure for Risk Management” on page 57.

Releases That Support Migration or Upgrade

The following table lists the releases of SAS Infrastructure for Risk Management that can be migrated to the current release of SAS Infrastructure for Risk Management.
The following table lists the releases of SAS Infrastructure for Risk Management that can be upgraded to the current release of SAS Infrastructure for Risk Management.

<table>
<thead>
<tr>
<th>Migration from the Specified Release</th>
<th>Migration to SAS Infrastructure for Risk Management 3.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>No</td>
</tr>
<tr>
<td>3.2</td>
<td>Yes</td>
</tr>
<tr>
<td>3.3</td>
<td>Yes</td>
</tr>
<tr>
<td>3.4</td>
<td>Yes</td>
</tr>
<tr>
<td>3.5</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Upgrade from the Specified Release</th>
<th>Upgrade to SAS Infrastructure for Risk Management 3.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>No</td>
</tr>
<tr>
<td>3.2</td>
<td>Yes</td>
</tr>
<tr>
<td>3.3</td>
<td>Yes</td>
</tr>
<tr>
<td>3.4</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Chapter 8

Migrating SAS Infrastructure for Risk Management

About the Migration Process

When you migrate SAS Infrastructure for Risk Management, the same operating system must be running in the source environment and in the target environment.

To migrate SAS Infrastructure for Risk Management, complete the tasks that are included in the following checklist.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Review additional documentation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Design your migration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create a migration package in your source environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Back up your source system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Migrate SAS Infrastructure for Risk Management.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Migrate the solution’s federated content.</td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION:**
Ensure that you follow the steps included in this chapter when migrating a system. Performing any step that is not documented could result in an installation...
that SAS Infrastructure for Risk Management does not support. For questions about whether SAS Infrastructure for Risk Management supports a configuration step that is not clearly documented, contact SAS Technical Support (at http://support.sas.com/techsup) before you proceed.

Review Additional Documentation

Before you start your migration, review the following documents:

- **Quick Start Guide**
  This document is shipped with your SAS software and is also available online:
  - Linux: http://support.sas.com/documentation/installcenter/94/unx/index.html

- **Software Order Email (SOE)**
  This email is sent to your site to provide information about your order.

- **SAS order information (SOI)**
  The SOI file indicates when the order was placed and provides a list of the products that are in your order. The SOI is in your SAS Software Depot at /install_doc/order-number/soi.html.

- **SAS software summary**
  The summary provides information about the products that are in your order and specifies the software that supports your order. The SAS software summary is in your SAS Software Depot at install_doc/order-number/ordersummary.html.

  *Note:* The SAS Deployment Wizard installs only what is listed in the deployment plan. The SAS software summary might list more products than are included in the deployment plan.

- **SAS 9.4 system requirements**
  http://support.sas.com/resources/sysreq/index.html

- **System Requirements – SAS Infrastructure for Risk Management 3.5**

- **SAS Notes**

- **SAS Intelligence Platform: Migration Guide**
Design Your Migration

To design your migration, complete the following tasks:

  Compare these requirements to your current deployment and develop a plan for moving your SAS content (data and configuration) to a SAS Infrastructure for Risk Management 3.5 system.
- Run the SAS Migration Utility that is provided in your SAS Software Depot. The utility creates a migration analysis report that enables you to answer the following questions:
  - Which SAS products currently reside on each machine?
  - Which SAS products require maintenance before you can migrate them?
- Contact your SAS Installation Representative to obtain a valid SAS 9.4 deployment plan for your current SAS deployment.
- Schedule time for your migration so that users are aware of when the system is unavailable.

Create a Migration Package in Your Source Environment

Use the SAS Migration Utility to create a migration package that contains your current SAS data and configuration information from the source system. You use this migration package as input to the SAS Deployment Wizard when you migrate to the target system.

For information about how to use the SAS Migration Utility, see *SAS Intelligence Platform: Migration Guide*.

Migrate SAS Infrastructure for Risk Management

*Note:* The following migration process explains how to migrate a single machine installation.

When you perform a migration for SAS Infrastructure for Risk Management, the process is similar to a typical out-of-the-box deployment. The primary difference between the two methods is that during the SAS Deployment Wizard session, you select the **Perform Migration** option on the Migration Information page. The following points identify the differences between a typical out-of-the-box deployment and a migration.

**CAUTION:**

Before beginning the migration process, ensure that you back up your installation.

When migrating, note the following differences between a migration and a typical out-of-the-box deployment:
1. To configure all products in one execution of the SAS Deployment Wizard, click **Typical** on the Configuring Prompting Level page.

2. During a migration, SAS Deployment Wizard makes one configuration pass for the SAS Application tier. Therefore, you must select all products for configuration in a migration scenario.

3. To migrate SAS Infrastructure for Risk Management, select **Step 1: Server and Middle Tier** on the Select Deployment Step and Products to Install page.

4. On the Migration Information page, select **Perform migration** and click **Browse** to navigate to the migration package that was generated by the SAS Migration Utility.
5. Click Next.

For detailed information about each page of the SAS Deployment Wizard, see *SAS Intelligence Platform: Migration Guide*.

6. When complete, in the target environment, stop the SAS Infrastructure for Risk Management web application server.

7. Complete the migration by manually copying the federated areas and persistent area from the source system to the target system. For information about copying the federated content, see "Migrate Federated Content" on page 53.
a. From the Plug-ins tab, select Application Management ⇒ Configuration Manager ⇒ SAS Application Infrastructure.

b. Right-click IRM Mid-Tier Server and select Properties.

c. On the IRM Mid-Tier Server Properties window, select the Advanced tab.

d. Ensure that the Property Value of the `com.sas.solutions.risk.irm.server.pa` points to the location of the persistent area folder.

Note: The location of the persistent area must be exactly the same on the target system as it was on the source system.

4. Ensure that the contents of the persistent area are owned by the installer and that the SAS General Server user account owns data and messages.

5. To complete the migration, restart the SAS Infrastructure for Risk Management web application server.

Troubleshoot Migration Errors

If you receive any errors during migration, complete the following tasks on the target system:

1. Examine the SASIRMServer log to determine which instance or instances generated the error or errors. The SASIRMServer log is located in one of the following locations:
   - Linux: `SAS-configuration-directory/Levn/Web/Logs/SASServer8_1/`
   - Windows: `SAS-configuration-directory\Levn\Web\Logs\SASServer8_1\`

2. For each instance that did not successfully migrate, note the instance key, the instance name, and the error reason.

3. Uninstall the newer SAS Infrastructure for Risk Management installation and re-install the previous installation.

4. Restore the source system database backup.

5. Restore the source system persistent area backup.
6. Using your notes from Step 2, review each instance that did not successfully migrate, and address the issue or issues that caused the error. If necessary, re-create the instance.

7. Re-install the new version of SAS Infrastructure for Risk Management and migrate the federated content.

8. If necessary, repeat the steps 1 through 7 until all instances migrate successfully.
Chapter 9

Upgrading SAS Infrastructure for Risk Management

About the Upgrade Process

When you upgrade SAS Infrastructure for Risk Management, the same operating system must be running in the source environment and in the target environment.

When upgrading, ensure that you follow the instructions in the SAS Intelligence Platform documentation. For more information, see "SAS Intelligence Platform: Installation and Configuration Guide."

The steps to perform an upgrade are similar to those required for a migration. However, you do not have to copy the federated areas and the persistent areas since they are already located in the required location.

When performing an upgrade, ensure that you do not remove any federated areas. This includes the following:

- all of the platform federated areas from earlier releases (for example, com.sas.solutions.risk.irm.fa.0.3.2, com.sas.solutions.risk.irm.fa.0.3.3, and com.sas.solutions.risk.irm.fa.0.3.4)
- where applicable, earlier versions of QRT federated area
- earlier versions of the current federated areas

To upgrade SAS Infrastructure for Risk Management, complete the tasks that are included in the following checklist.

<table>
<thead>
<tr>
<th>Completed?</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Perform the pre-upgrade tasks.</td>
</tr>
<tr>
<td></td>
<td>Upgrade SAS Infrastructure for Risk Management.</td>
</tr>
</tbody>
</table>
Perform the Pre-upgrade Tasks

Before upgrading, ensure that you complete the following tasks:

2. Back up your existing system.
   
   **CAUTION:**
   
   The upgrade writes over the existing system. If any problems are encountered, it might be necessary to recover the existing system from backup. Keep in mind that your existing system can be corrupted to the point of being unusable and unrecoverable.

   **Note:** When you back up your system, ensure that you also back up the SAS Metadata Server. For more information, see SAS Intelligence Platform: System Administration Guide.

3. Understand how the SAS Deployment Wizard upgrades SAS software. For more information, see SAS Intelligence Platform: Installation and Configuration Guide.

4. Locate and familiarize yourself with your SAS software order. For more information, see SAS Intelligence Platform: Installation and Configuration Guide.

5. Download your order and create a SAS Software Depot. For instructions about how to download and create a SAS Software Depot, see “Create a SAS Software Depot” on page 21.

6. Stop all SAS services that are running in your environment.

Upgrade SAS Infrastructure for Risk Management

You upgrade SAS Infrastructure for Risk Management using the SAS Deployment Wizard.

When running the SAS Deployment Wizard from your SAS Infrastructure for Risk Management 3.5 depot, point to the location of your existing SAS-installation-directory. The SAS Deployment Wizard upgrades your installation to the new version.

For complete instructions about upgrading SAS Infrastructure for Risk Management from one version to another version on the same machine, see Differences in the SAS 9 and SAS Viya Platforms.
Troubleshoot Upgrade Errors

If you receive any errors when migrating federated content after upgrading your SAS Infrastructure for Risk Management, complete the following tasks:

1. Examine the SASIRMServer log to determine which instance or instances generated the error or errors. The SASIRMServer log is located in one of the following locations:
   - Linux: `SAS-configuration-directory/Levn/Web/Logs/SASServer8_1/`
   - Windows: `SAS-configuration-directory\Levn\Web\Logs\SASServer8_1\`

2. For each instance that did not successfully migrate, note the instance key, the instance name, and the error reason.

3. Uninstall the newer SAS Infrastructure for Risk Management installation and re-install the previous installation.

4. Restore the system database backup.

5. Restore the persistent area backup.

6. Using your notes from Step 2, review each instance that did not successfully migrate, and address the issue or issues that caused the error. If necessary, re-create the instance.

7. Re-install the new version of SAS Infrastructure for Risk Management and migrate the federated content.

8. If necessary, repeat the steps 1 through 7 until all instances migrate successfully.
Part 4

Administering SAS Infrastructure for Risk Management

Chapter 10
Performing Additional Administrative Tasks .................. 63

Chapter 11
Performing Programming Interface Administrative Tasks .... 79

Chapter 12
Troubleshooting ..................................................... 91
Chapter 10
Performing Additional Administrative Tasks

Configure Middle-Tier Server Clustering On SAS Infrastructure for Risk Management


Horizontal clustering is the practice of deploying SAS Web Application Server instances on multiple machines. This configuration can help improve performance (load...
balancing) and provide greater availability to guard against hardware failure. If one machine or web application server instance crashes (or an application on one server instance stops), the applications remain available on the other machines (failover).

For information about middle-tier server clustering, see *SAS Intelligence Platform: Middle-Tier Administration Guide*.

---

### Add Solution Federated Areas to an Existing Deployment

You can add any number of federated areas to run on a SAS Infrastructure for Risk Management deployment.

If you license more than one SAS Infrastructure for Risk Management solutions, you can install the second solution’s federated areas by completing the following tasks:

1. Download the federated content package for the additional solution. For more information, see “Install Federated Content” on page 30.

2. After you download the federated content for the additional solution, unzip the content package and use the installation instructions that are provided with the package to install the content.

3. Add the new content as a federated area to SAS Infrastructure for Risk Management. For information about how to add a content, see “Install Federated Content” on page 30.

Adding a new solution’s federated area requires an understanding of how these federated areas relate to each other.

**CAUTION:**

Adding a federated area is the only operation that you can perform on a federated area.

When working with federated areas, note that the following operations are not supported and could result in system and data corruption:

- removing an installed federated area
- modifying the content of an installed federated area, with the exception of loading data
- modifying the federated area ID of an installed federated area
- modifying the path of an installed federated area
- adding the same federated area twice using different federated area IDs

Before adding a federated area, note the following:

- SAS Infrastructure for Risk Management defines the property `com.sas.solutions.risk.irm.fa`

  This property is followed by a period-separated suffix that is the identifier for the federated area. For example, `com.sas.solutions.risk.irm.fa.1.0.3` defines a federated area with ID `1.0.3`.

Here is a full example of federated content that is supplied for a SAS Infrastructure for Risk Management federated area:
com.sas.solutions.risk.irm.fa.1.0.3=/sas-configuration-directory/Lev1/AppData/SASIRM/fa1

This statement defines a federated root of /sas-configuration-directory/Lev1/AppData/SASIRM/fa1.

- The ID for a federated area can contain numeric characters, alphabetic characters, and periods only.

Note: Identifiers that start with the number zero (0) are reserved for functionality content that is delivered by the SAS Infrastructure for Risk Management platform federated area. Do not use these identifiers when adding an additional federated area.

- The lexical ordering of identifiers determines the precedence of federated areas, as shown in the following example:
  
  com.sas.solutions.risk.irm.fa.0.3.5=/config/Lev1/AppData/fa.0.3.5
  com.sas.solutions.risk.irm.fa.2=/config/Lev1/AppData/fa_life
  com.sas.solutions.risk.irm.fa.cs=/config/Lev1/AppData/fa_cpmn
  com.sas.solutions.risk.irm.fa.sample.3.5=/config/Lev1/AppData/fa.sample.3.5

- When adding a federated area, you must define the property com.sas.solutions.risk.irm.fa and point to a location that is accessible to the workspace server.

To add an additional federated area:

1. Stop the SAS Infrastructure for Risk Management web application server by running the following command in the appropriate directory.
   
   tcruntime-ctl.sh stop

   For a non-clustered environment, the web application server is SASServer8_1. For a clustered environment, the web application servers can include SASServer8_2, SASServer_3, and so on, and can be on the same machine or on different machines within the cluster.

   For more information about stopping SAS Web Application Servers, see SAS Intelligence Platform: Middle-Tier Administration Guide.

2. Grant Read and Write permissions to the primary SAS group of the spawned server user.

3. In SAS Management Console, add the new federated area property by completing the following steps:
   
   a. Start SAS Management Console and connect to the appropriate metadata server as a SAS administrator (for example, sasadm@saspw).
   
   b. On the Plug-ins tab, verify that the repository is selected in the Repository field. The default repository is Foundation.
   
   c. Select Application Management ⇒ Configuration Manager ⇒ SAS Application Infrastructure.
   
   d. In the main pane, right-click SAS IRM Mid-Tier Server and select Properties. The IRM Mid-Tier Server Properties window is displayed.
   
   e. Click the Advanced tab and then click Add. The Define New Property dialog box is displayed.
In the Property Name field, enter `com.sas.solutions.risk.irm.fa.n`, where `n` is an ID that does not start with the number zero (0).

Note: Typically, you want the new property to have precedence. Therefore, the ID of the new federated area should be lexicographically greater than the ID of previous federated version IDs.

In the Property Value field, enter the federated area directory path.

Click OK.

f. Grant Read permissions to the spawned server on the federated area directory.

g. Restart the SAS Infrastructure for Risk Management web application server.

For more information about starting SAS Web Application Servers, see *SAS Intelligence Platform: Middle-Tier Administration Guide*.

---

**Load Data via Live ETL**

**Overview**

In SAS Infrastructure for Risk Management, you can use the *Live ETL* feature to upload new data sets without affecting server operations. In other words, Live ETL enables new data sets to be uploaded and associated job flows to be automatically recalculated while all server operations are available. These server operations include (but are not limited to) the following:

- logging in and logging out
- creating job flow instances
- deleting job flow instances
- modifying job flow instances
- executing job flow instances
Live ETL supports the creation of new input data. However, it does not support deleting input data.

Setting Permissions

Ensure that the following permissions are set up for the user-delivered federated areas:

- The landing areas and the contents under it have Write permission to the SAS General Server user.
- The input areas directories have Read and Write permission to the SAS General Server user.

Creating an Input Area

Because data sets in the landing area cannot be modified while job flow instances are running, you must create an input area into which you upload the new data. When creating the input area, note the following:

- The input area is located under the root of the federated area.
- There is one input area per federated area.
- To ensure compatibility with existing deployments, the path of the input area is \%FA/input_area, where \%FA is the path to the federated area.

Here is an example of the input area in the federated area:

```
/federated_area
  ...
  /landing_area
  /input_area
    /03312017
    entity.sas7bdat
    ...
    /03312016
    entity.sas7bdat
    ...
    funds.sas7bdat
    ...
    last_update.txt
    last_live_etl.success.txt
```

Invoking Live ETL

After you have uploaded the new data sets into the input area, invoke Live ETL by modifying the marker file named last_update.txt to update the file’s timestamp. The file is located in the input area. After the data has been uploaded to the input area and you update the marker file, Live ETL automatically performs the following tasks:

1. Stops the execution of all job flow instances that depend on the data that was uploaded.
2. Stops all new job flow execution requests that use the uploaded data.
3. Copies the content from the input area to the landing area.
4. Reloads the base dates and the configuration sets.
5. Updates the last_live.etl.success | failure.txt file to indicate whether the process completed successfully or with errors.

After the Live ETL process has been completed, all job flow instances that were affected by the upload have an OUT_OF_DATE status. If an affected instance is running, it is stopped and then marked OUT_OF_DATE. If a new instance is run during the Live ETL process, and is impacted by the Live ETL process, it is not executed and its status is set to OUT_OF_DATE.

Enable WebDAV Access to SAS Infrastructure for Risk Management Data

SAS Infrastructure for Risk Management uses WebDAV to provide users an easy way to access to the following types of SAS Infrastructure for Risk Management information:

- job flow definition files
- input and output SAS data sets and their corresponding Microsoft Excel files
- task log files
- the execution status of job flow instances and sub-flow instances
- the execution status of tasks
- the navigation hierarchy of the data

Before using WebDAV to access SAS Infrastructure for Risk Management data, note the following restrictions:

- The scope of data that a user can access is controlled by permissions that are associated with the user’s log on credentials.
- The content of a flow instance is accessible only to the owner of the flow. If the instance is shared, the content is accessible to users that have access to the business entities of the flow instance.
- The contents of the SAS Infrastructure for Risk Management WebDAV servlet are Read-Only and cannot be deleted.

SAS Infrastructure for Risk Management users can access the data store in a centralized location on a remote server using WebDAV by using either of the following methods:

- Access the data from a WebDAV drive that is mapped to your computer:
  1. Map the SAS Infrastructure for Risk Management WebDAV servlet drive to your computer. For information about mapping the WebDAV servlet drive to your computer, refer to the documentation for your operating system.
  2. Access the drive on your local system and click your user ID to navigate to the data that you want to access.

- Use the LIBNAME statement to directly map a libref to a WebDAV URL.

Associate a libref with a SAS library to enable access to WebDAV. The following example associates the libref that is named davdata with the WebDAV directory /users/mydir/datadir on the WebDAV server www.webserver.com:

```
libname davdata v9 "https://www.webserver.com/users/mydir/datadir"
webdav user="mydir" pw="12345";
```
For detailed information about using the LIBNAME statement for WebDAV server access, see SAS Global Statements: Reference.

View Task Inputs and Outputs in SAS Studio

To view SAS Infrastructure for Risk Management inputs and outputs files in SAS Studio:

1. In the SAS Infrastructure for Risk Management web application, open the job flow instance for which you want to view the inputs and outputs for a task.

2. Right-click the input or output icon for a task and select Open in SAS Studio from the pop-up menu. The data is displayed in SAS Studio.

When using this feature, note the following limitations:

- To download and view data sets in SAS Studio, your password must be saved in your user account properties metadata.

- SAS Infrastructure for Risk Management does not support Read-Only locks on resources. Therefore, when opening a SAS Infrastructure for Risk Management table in SAS Studio, SAS Infrastructure for Risk Management responds to the SAS Studio request to lock a Read-Only resource. When this occurs, a warning message is sent the SASIRMServer.log that indicates that the resource cannot be locked.

Change the Location of the Persistent Area

There are some conditions that might require that you change the location of the SAS Infrastructure for Risk Management persistent area in an established SAS Infrastructure for Risk Management deployment. One example of such a condition is that the location of the persistent area is running out of space.

**CAUTION:**

In an established SAS Infrastructure for Risk Management deployment, do not modify the path to the persistent area in SAS Management Console. Once job flows have been executed in a SAS Infrastructure for Risk Management deployment, you cannot modify the path to the persistent area in SAS Management Console. The only time that you can modify the path to the persistent area in SAS Management Console is in a fresh SAS Infrastructure for Risk Management installation, before any job flows are executed. (See “Configure an External Location to the Persistent Area” on page 28.)

To change the location of the persistent area in an established SAS Infrastructure for Risk Management deployment:

1. Copy the existing persistent area folder to a new location.

2. Create a symbolic link from the former location of the persistent area to its new location.

With a symbolic link, the output that SAS Infrastructure for Risk Management writes to the former location of the persistent area is rerouted to the new location.
Map SAS Infrastructure for Risk Management Libraries

About SAS Infrastructure for Risk Management Libraries Mapping

Each SAS Infrastructure for Risk Management federated area contains a libnames.txt file that is located in the config folder of that federated area. This file contains a mapping definition to each library that contains inputs for the tasks that are used in job flows. SAS Infrastructure for Risk Management resolves the library names using the mappings that are defined in the libnames.txt file. Therefore, you must define a mapping statement in the libnames.txt file for each library that contains inputs that are used by the job flows in the federated area.

SAS Infrastructure for Risk Management supports the following types of mapping definitions:

• SAS library mapping definitions
• dynamic custom mapping definitions
• generic library definitions (to simplify access to third-party data)
• temporary library definitions (for large data sets)

How the Inputs for SAS Infrastructure for Risk Management Are Defined

The inputs and outputs for SAS Infrastructure for Risk Management tasks and subflows can be defined using a three-part name.

Here is an example where the name of the input data set for a task is irm_cfg.byn_configuration.sas7bdat.

where:

Expanded enriched option instrument
Configuration table
Get Cardinality Options ByN
Cardinality table for options
• **irm_cfg** is the name of the library in which the input is located. (This location must be mapped in the libnames.txt file.)

• **byn_configuration** is the file name of the input data set.

• **sas7bdat** is the file extension of the input data set.

When a job flow instance is created, SAS Infrastructure for Risk Management resolves the library name **irm_cfg** using the mappings that are defined in the libnames.txt file.

### Static Mapping

Here is an example in which a user wants to create a job flow instance that is based on the following parameters:

- **Job flow location** = `/config/Lev1/AppData/SASIRM/fa.id`
- **Selected entity** = `ENTITY_BE`
- **Input data set** = `static.run_options.sas7bdat`
- **libnames.txt defined mapping** = `STATIC=%la/base/%et`

Here is an example of the mapping in the libnames.txt file:

```plaintext
# Static Mappings for non-version SAS libraries
# All keys should be upper case

STATIC=%la/base/%et
MAPPING=%la/base/%cs/mapping
IRM_CFG=%la/base/irm_cfg
STAGING=%la/%bd
```

where the configuration variable:

- `%la` references the landing area in the resolved federated area.
- `%bd` references the base date that the user selected when they created a job flow instance.
- `%cs` references the configuration set that the user selected when they created a job flow instance.
- `%et` references the entity that the user selected when they created a job flow instance.

When the user creates the job flow instance, SAS Infrastructure for Risk Management resolves the path to the `run_options.sas7bdat` input data set to the following:

```plaintext
config/Lev1/AppData/SASIRM/fa.id/landing_area/base/entity_be/
run_options.sas7bdat
```

### Extended Dynamic Custom Mapping

The macro variable (%mv) is a substitution configuration variable that you can use to configure more dynamic mapping definitions.

The %mv configuration variable enables you to use your own configuration variables to extend the mapping definitions for SAS data sets that contain name/value pairs. These data sets must be declared in the macrovarload.txt file that is in the config folder of a federated area.
Here is an example of how the %mv configuration variable is used in the mapping definition in the libnames.txt file:

%mv(libname.data_set_name.config_name)

where:

- **libname** is the name of the library in which the input is located. (You must map this location in the libnames.txt file.)

- **data_set_name** is the name of the file that contains the config_name and config_value set, without the file extension.

- **config_name** is the value of the macro variable.

To ensure data integrity after a job flow instance has been created, note that the following restrictions apply to the configurable data sets that are declared in the macrovarload.txt file:

- The data set cannot be modified from the Edit instance window in the SAS Infrastructure for Risk Management web application. All paths must resolve to characters (lowercase) on disk.

- All paths must resolve to characters (lowercase) on disk.

- The data set cannot be modified using the Download and Upload feature in the SAS Infrastructure for Risk Management web application.

Here is an example in which a user wants to create a job flow instance that is based on the following parameters:

- Job flow location = /config/Lev1/AppData/SASIRM/fa.id
- Input data set for a task = ACT.QUOTE_FX.SAS7BDAT
- Selected configuration set = SAMPLE_35_CONFIGURATION

Here is an example of the extended dynamic mapping in the libnames.txt file:

```plaintext
# Static Mappings for non-version SAS libraries
# All keys should be upper case

ACT=%la/%bd/%mv(STATIC.ANALYTICS_OPTION.ACT_SCHEME)
STATIC=%la/base/%et
MAPPING=%la/base/%cs/mapping
IRM_CFG=%la/base/irm_cfg
STAGING=%la/%bd
```

When the user creates the job flow instance, SAS Infrastructure for Risk Management resolves the path to the **STATIC.ANALYTICS_OPTION** input data set to the following:

/Config/Lev1/AppData/SASIRM/fa.id/landing_area/base/03312017/static/analytics_option.sas7bdat

The data set contains the following entries:

<table>
<thead>
<tr>
<th>CONFIG_NAME</th>
<th>CONFIG_VALUE</th>
<th>CONFIG_VALUE_DESC</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE</td>
<td>N</td>
<td>Indicate whether to write macro call</td>
</tr>
<tr>
<td>BINOMIAL_TREE_NSTEPS</td>
<td>12</td>
<td>Number of steps used in binomial tree</td>
</tr>
<tr>
<td>PTF_N_OBS</td>
<td>10000</td>
<td>Number of observations to expand f</td>
</tr>
<tr>
<td>ACT_SCHEME</td>
<td>IFRS</td>
<td>Account scheme</td>
</tr>
</tbody>
</table>
After SAS Infrastructure for Risk Management resolves the path to the STATIC.ANALYTICS_OPTION data set, it resolves the path to the ACT.QUOTE_FX.SAS7BDAT input data set to the following on disk:

/config/Lev1/AppData/SASIRM/fa.id/landing_area/03312017/ifrs/quotes_fx.sas7bdat

CAUTION:

If you use an existing configuration table for one of the dynamic library configurations, the table can no longer be edited for that job flow instance. Therefore, you might consider creating a custom table that contains a pointer to the dynamic library. You can create this table anywhere in the landing area.

Generic Library Mapping

Generic library mapping definitions enable access to third-party data that is located outside of a SAS Infrastructure for Risk Management federated area. For example, this data might be located in a relational database management system, Hadoop, CAS, and so on.

When working with generic libraries, note the following:

• In the libnames.txt file, all generic libraries must start with the keyword LIBREF (for example, LIBREF PGLIB=).

• The exact syntax for the LIBREF keyword follows the equal sign (=) in the libnames.txt file. Depending on the type of library that you are defining, the engine information, database, and schema might also be required.

• A generic library definition that contains $pa (persistent area) is ignored and flagged as an error.

• A generic library can be an input or output library, but not both. If the library is used as an output library, that output cannot be consumed as input by any other node. It is a terminal output. If the library is used as an input library, then it cannot be used an output in another node.

• If a generic library is used by multiple federated areas, it must be defined using the exact same definition in the libnames.txt file of the other federated areas.

• Generic libraries are supported for SAS tasks.

• The SAS General Servers group must own any required authentication domains or the user credentials must allow access to the external data. Therefore, you must specify the authentication domain of the generic library or specify the user credentials.

Here is a syntax that you use to define a generic library entry in the libnames.txt file:

LIBREF <LIB_NAME>=<engine_verbatim>; IRMAUTHDOMAIN=<Domain>,<user>

where:

• LIBREF is the keyword to begin the definition.

• LIB_NAME is the name of the generic library.

• engine_verbatim is the engine and location to use to access the files in the library.

• (Optional) IRMAUTHDOMAIN is the keyword to specify the authentication domain and user.

Here are two examples of generic libraries mapping definitions. The first example uses standard authentication and the second example uses user credentials.
**Temporary Library Mapping**

A temporary library is a data library that is promptly and automatically deleted as soon as it is no longer needed during the execution of a job flow. Using temporary libraries minimizes the disk space footprint of large data sets.

Before you define a temporary library, note the following restrictions:

- Because temporary data is nonpersistent data, it does not participate in the data object pooling process. Therefore, during the execution of a job flow, tasks with any temporary data as its input or output is always executed.
- You can define a temporary library only for libraries that are generated as SAS Task output.
- A NodeData object must provide a method (for example, Boolean isNonPersistentData()), which returns the value True, if the data is in a temporary data library.

Here is an example of the mapping definition that you enter in the libnames.txt file of the federated area in which you want to create the temporary library:

```
MK_CONF=%TMPLIB
```

---

**Run the SAS Infrastructure for Risk Management Hot Fix Post-installation Tool**

**About the Hot Fix Post-installation Tool**

Hot fixes that are released for SAS Infrastructure for Risk Management 3.5 and later include the SAS Infrastructure for Risk Management hot fix post-installation tool.

The SAS Infrastructure for Risk Management hot fix post-installation tool is a stand-alone Java executable. It verifies and automates post-installation steps that are required when you apply a SAS Infrastructure for Risk Management hot fix that includes the SAS Infrastructure for Risk Management server JAR.

You need to use this tool only when you apply SAS Infrastructure for Risk Management server tier hot fixes.

*Note:* The information and examples in this section use the default directories that are created during the SAS installation. The default path to the SASHome directory is `/local/install/SASHome`, and the default path to the SASConfig directory is `/local/install/SASConfig`. If you have not used the default paths, you must substitute your installation paths for the default paths that are used in the examples.

**Prerequisites**

Before you can run the hot fix post-installation tool:

- Install the applicable hot fix on the SAS Infrastructure for Risk Management server tier.
For information about installing the hot fix, see the instructions that are provided with the hot fix.

- Have the SAS Private Java Runtime Environment (JRE) in order to run the hot fix post-installation tool. The SAS Private JRE is provided as part of the standard SAS deployment process.
- Ensure that the SAS Web Infrastructure Platform Data Server is running.

**Actions Performed by the Hot Fix Post-Installation Tool**

When you run the SAS Infrastructure for Risk Management hot fix post-installation tool, it performs the following actions:

- Verifies that the SASHome directory exists and that it can be read.
- Verifies that the SASConfig folder exists and that it can be read and written to.
- Verifies that the SAS Infrastructure for Risk Management platform federated area exists and that it can be read and written to.
- Verifies that the SAS Versioned JAR Repository (VJR) exists and that it can be read.
- Locates and parses the VJR picklist.
- Locates all the versions of the SAS Infrastructure for Risk Management JAR files in the picklist.
- Verifies that the JAR file from which the hot fix post-installation tool was launched is the same file as the server JAR file in the picklist. If the JAR files do not match, the tool terminates the process.
- Copies all the SAS Infrastructure for Risk Management JAR files in the picklist to the SAS Infrastructure for Risk Management platform federated area.
- Copies and extracts all the SAS Infrastructure for Risk Management platform federated area classes to the appropriate locations in the platform federated area.
- Determines whether any SQL updates have not been applied to the SAS Infrastructure for Risk Management database and applies the updates as needed.
- Records the SAS Infrastructure for Risk Management database updates that are applied.

**Run the Hot Fix Post-installation Tool**

After you have installed the tool, you execute it by running the SAS Private JRE and pointing to the class that contains the hot fix.

To run the hot fix post-installation tool:

1. Using the SAS Installer account, log on to the SAS Infrastructure for Risk Management server.
2. To run the tool, execute the following command on the same command line:

```
/local/install/SASHome/SASPrivateJavaRuntimeEnvironment/9.4/jre/bin/
java -cp path_to_server_jar com.sas.solutions.risk.irm.server.utils.IRMHFHelper
    -home path_to_SASHome -config path_to_SASConfig
    -dbpassword password
```
If you are using Windows and a path that contains spaces, enclose the path in quotation marks. Here is an example:

- **home** "C:\Program Files\SASHome"

**Note:** The path to SASHome and SASConfig and the SAS Infrastructure for Risk Management database password are required arguments. Additional options might be required if the values that are specified in your installation differ from the default installation values in SAS Deployment Wizard. For more information about these options, see “Additional Supported Options” on page 76.

Here is an example of how to run the post-installation hot fix tool:

**Note:** The example contains default paths, and the SAS Infrastructure for Risk Management database password is "secret".

```
```

When you run the tool, it validates the values that are specified for the **-home** and **-config** options. If the values are not valid, the tool generates an error message and terminates. The tool verifies that the JAR file that is specified in the class path matches the server JAR file that is installed by the hot fix. If files do not match, the tool terminates, and the error message identifies the location of the server JAR file that should be used.

All error messages that are produced during the execution of the tool are sent to standard error, and all normal messages are sent to standard out. For more information about options and usage, use the **-help** option.

Here is an example of how to specify the **-help** option:

```
```

### Additional Supported Options

**Table 10.1** lists and describes the additional options for the command line for the SAS Infrastructure for Risk Management hot fix post-installation tool.

**Note:**
- For options that do not take a value, "None" is listed in the Value column.
- For options that do not have a default value, “None” is listed in the Default column.
- If a non-default value for an option was used during installation, that option is required. If the default value was used during installation, the option is not required.
- Following the class name (com.sas.solutions.risk.irm.server.utils.IRMHFHelper), options can be specified in any order.
<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
<th>Description</th>
<th>Default</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>-config</td>
<td>path_to_SASConfig</td>
<td>Specifies the absolute path to the SAS configuration folder.</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>-dbhost</td>
<td>host</td>
<td>Specifies the name of the SAS Infrastructure for Risk Management database host.</td>
<td>localhost</td>
<td>No</td>
</tr>
<tr>
<td>-dbname</td>
<td>name</td>
<td>Specifies the name of the SAS Infrastructure for Risk Management database to update.</td>
<td>irmdb</td>
<td>No</td>
</tr>
<tr>
<td>-dbpassword</td>
<td>password</td>
<td>Specifies the clear-text password to access the SAS Infrastructure for Risk Management Postgres database.</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>-dbport</td>
<td>port</td>
<td>Specifies the port of the SAS Infrastructure for Risk Management database.</td>
<td>9432</td>
<td>No</td>
</tr>
<tr>
<td>-dbuser</td>
<td>userid</td>
<td>Specifies the name of the SAS Infrastructure for Risk Management database user ID.</td>
<td>irmadmin</td>
<td>No</td>
</tr>
<tr>
<td>-encoding</td>
<td>name</td>
<td>Specifies the name of the encoding used to read the SAS Infrastructure for Risk Management picklist. This value is not typically required.</td>
<td>JVM default</td>
<td>No</td>
</tr>
<tr>
<td>-help</td>
<td>None</td>
<td>Displays information about tool usage and options.</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>-home</td>
<td>path_to_SASHome</td>
<td>Specifies the absolute path to the SAS home folder.</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>-jarfile</td>
<td>path_to_pgjar</td>
<td>Specifies the path to the Postgres JDBC JAR file (postgresql.jar). Typically, the tool locates this JAR file automatically. Use this option only if the tool’s attempt to locate the Postgres JDBC JAR file fails.</td>
<td>Path to the Postgres JDBC JAR file</td>
<td>No</td>
</tr>
<tr>
<td>-level</td>
<td>number</td>
<td>Specifies an integer that indicates the configuration level. For example, 1 indicates level 1, 2 indicates level 2, and so on.</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>-nosql</td>
<td>None</td>
<td>Disables SQL updates to the SAS Infrastructure for Risk Management database.</td>
<td>SQL updates are enabled</td>
<td>No</td>
</tr>
<tr>
<td>-preview</td>
<td>None</td>
<td>Provides a preview of the changes that would be applied. Although the SQL tracking table is created, it does not affect the operation of SAS Infrastructure for Risk Management. Note: If you specify this option, no changes to the system are applied. This option provides a preview of the changes only.</td>
<td>Off</td>
<td>No</td>
</tr>
<tr>
<td>Option</td>
<td>Value</td>
<td>Description</td>
<td>Default</td>
<td>Required?</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>-verbose</td>
<td>None</td>
<td>Generates additional messages during execution. This option is typically used for debugging purposes only.</td>
<td>Off</td>
<td>No</td>
</tr>
</tbody>
</table>
Chapter 11
Performing Programming Interface Administrative Tasks

About the SAS Infrastructure for Risk Management Programmer’s Interface That Is Based on SAS ........................................ 79
Configure the Development Environment ........................................ 79
Install a Stand-Alone Federated Area without a Server Restart ........... 81
   About Installing Stand-Alone Federated Areas ............................. 81
   Example Installation Scenarios ............................................. 83
Back Up and Restore Job Flow Instances ....................................... 86
   Backing Up Job Flow Instances ........................................... 86
   Restoring Job Flow Instances ............................................. 88

About the SAS Infrastructure for Risk Management Programmer’s Interface That Is Based on SAS

The SAS Infrastructure for Risk Management platform provides a SAS programming interface using SAS Studio. This interface provides the following capabilities:

- task and job flow development
- backup and restore job flow instances
- macros that simplify data partitioning
- data visualization

For information about using the programming interface, see SAS Infrastructure for Risk Management: Programmer’s Guide.

Configure the Development Environment

To configure the development environment, complete the following tasks on the SAS Infrastructure for Risk Management mid-tier server:

1. Enable development mode.
a. In SAS Management Console, select **Plug-ins ➔ Application Management ➔ Configuration Manager ➔ SAS Application Infrastructure**.

b. Right-click **IRM Mid-Tier Server** and select **Properties**.

c. In the IRM Mid-Tier Server Properties window, select the **Advanced** tab and add the property and value:

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Property Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.sas.solutions.risk.irm.server.devmode</td>
<td>true</td>
</tr>
</tbody>
</table>

d. Click **OK**.

2. Verify that Doxygen is installed and configured on the SAS Infrastructure for Risk Management server.

For information about installing Doxygen on your system, refer to the Doxygen documentation:

http://www.doxygen.nl/

3. Set the value for the Doxygen property in SAS Management Console.

a. Select **Plug-ins ➔ Application Management ➔ Configuration Manager ➔ SAS Application Infrastructure**.

b. Right-click **IRM Mid-Tier Server** and select **Properties**.

c. In the IRM Mid-Tier Server Properties window, select the **Advanced** tab and add the following property and value:

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Property Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.sas.solutions.risk.irm.sc.doxygen.path</td>
<td>path-to-the-Doxygen-binary-file</td>
</tr>
</tbody>
</table>

The value for the property varies depending on where Doxygen is installed. Here are two examples:

- **Windows**:
  
  C:\Program Files\doxygen\bin\doxygen.exe

- **UNIX**:

  /usr/bin/doxygen

d. Click **OK**.

4. Create a programmer’s account for each programmer who will be using the SAS Infrastructure for Risk Management scripting client to create parallel programs. This is the account that a programmer will use to log on to the SAS Infrastructure for Risk Management web application to automatically create their personal federated area.

The programmer’s account must have the same primary operating system group of the user account under which stored process servers and SAS workspace servers run.

Here is an example:

```bash
sudo useradd -g primary-OS-group user-ID
```

where:
primary-OS-group is the primary operating system group of the user account under which stored process servers and SAS workspace servers run.

user-ID is the user ID of the programmer’s account.

The configuration of the programmer’s account enables files and folders that are created to be discovered by stored process servers and SAS workspace servers.

Note: A programmer’s account can be a local account. However, it must be able to authenticate on the SAS metadata server and launch processes on the workspace server.

5. In SAS Management Console, select Environment Manager ⇒ User Manager. Right-click the programmer’s user name, and on the Account tab, store the user password to enable the user to perform the following tasks:

- In the SAS Infrastructure for Risk Management web application, open a job flow data set in SAS Studio.
- Execute scripting client macros or other statements that use the SAS WebDAV library engine in SAS Studio.

6. In SAS Management Console, configure the SAS Infrastructure for Risk Management metadata user account for each programmer account in the DefaultAuth authentication domain and as a member of IRM: Access All Entities.

7. Restart the SAS Infrastructure for Risk Management web application server.

For more information about starting SAS Web Application Servers, see SAS Intelligence Platform: Middle-Tier Administration Guide.

---

Install a Stand-Alone Federated Area without a Server Restart

This method of installing a federated area applies to stand-alone federated areas that are created in a SAS Infrastructure for Risk Management development environment. This method does not apply to federated areas that are delivered in a SAS Infrastructure for Risk Management solution content package. For information about installing federated areas in SAS Infrastructure for Risk Management solution content releases, see “Add Solution Federated Areas to an Existing Deployment” on page 64.

About Installing Stand-Alone Federated Areas

To install a stand-alone federated area, you use the %irm_fa_install() macro in SAS Studio.

```/* Un-authenticated */
%irm_install_fa(
   meta_host=somehost.na.sas.com
,   username=
,   passwd=
,   fa_src_path=
,   fa_tgt_path=
,   fa_id=
,   fa_tgt_path=
,   debug=
,   logOptions=
```
where:

meta_host=
(Required) name of the server that is running the SAS metadata server.

meta_port=
(Optional) port on which the SAS metadata server is listening. The default is 8561.

meta_repos=
(Optional) name of the metadata repository.

username=
(Optional in authenticated environments) user name credentials for logging on to SAS Infrastructure for Risk Management.

passwd=
(Optional in authenticated environments) password credentials, which can be plain text or encoded (masked during execution).

fa_src_path=
(Required) path, including the ZIP file name, of the source location of the federated area ZIP file.

fa_tgt_path=
(Required) path to the installation target location for the new federated area. The target location should not be the same location as the source federated area ZIP file location.

fa_id
(Optional) user-provided name for the federated ID. If provided, this ID becomes the new federated ID.

force_flg=
(Optional) flag that forces or cancels installation if the federated area is determined to be invalid. Specifying true forces the installation of the federated area even if it is invalid. It also forces the use of the fa_id if specified. Specifying false cancels the installation of the federated area if the federated area determined to be invalid. The default is false.

debug=
(Optional) determines the amount of execution information that is collected and logged. Valid values are true and false. The default is false.

logOptions=
(Optional) specifies the amount of macro execution information that is logged. It accepts a space-separated list of supported SAS options (for example, logOptions = source mprint mlogic symbolgen).

connection_type=
(Required for external connections) type of connection to the SAS Infrastructure for Risk Management server. Valid values are internal (for regular connections) and external (for redirected, reverse proxy type connections). The default is internal.

Before installing a federated area using the process documented in this section, note the following:

• To successfully install a new federated area, you must have the correct permissions on the IRM Mid-Tier Server in SAS Management Console. Specifically, you must be
a member of the IRM: Install Federated Areas role and with the Allow Install of Federated Area capability.

- From the top folder of the federated area, compress the federated area with any percentage of compression.

Note: We recommend that you use WinZip for compressing on Windows. If you select Send to > Compressed Compressed (zipped) folder, you might encounter issues during the installation process. On UNIX systems, you can use the zip command or other equivalents for creating a compressed file.

Here is an example of how the ZIP file should appear after you have compressed it correctly:

- The target location (to where you are copying the federated area) cannot be the same location as the location of the source federated area ZIP file. In addition, the target location must have Write permission.
- You have to copy the new federated area (with Read/Write permissions) to the server on which other federated areas reside.
- You must also provide the required macro parameters.

Example Installation Scenarios

Installing in an Authenticated or Unauthenticated Environment

If you are installing the federated area in an authenticated environment, you can leave the username and passwd parameters blank. When installing in an authenticated environment, the credentials of the logged-on user are used.

Example:

```c
/* Authenticated */
%irm_install_fa(
    meta_host=somehost.na.sas.com
    , username=
    , passwd=
    , fa_src_path=/local/install/New_FA/fa_new.zip
    , fa_tgt_path=/local/install/Config/Lev1/AppData/SASIRM/fa_new
    , fa_id=
    , force_flg=true
    , debug=true
    , logOptions=mprint mlogic symbolgen source
    , connection_type=/* Default: INTERNAL */
);
```

Install a Stand-Alone Federated Area without a Server Restart
In an unauthenticated environment, you must provide values for the `username` and `passwd` parameters that match those that are stored in metadata.

In addition, you must make sure that the macro location is included in the SASAUTOS path. Here are two examples:

In Linux:

```sas
OPTIONS SASAUTOS=('~/home/local/install/SASHOME/SASFoundation/9.4/ucmacros/rmifirmmva' SASAUTOS);
```

In Windows:

```sas
OPTIONS SASAUTOS=('C:\Program Files\SASHOME\SASFoundation\9.4\rmifirmmva\ucmacros" SASAUTOS);
```

Example:

```sas
/* Un-authenticated */
%irm_install_fa(
    meta_host=somehost.na.sas.com,
    username=sasdemo,
    passwd=XXXXXXXXXXXXXX,
    fa_src_path=/local/install/New_FA/fa_new.zip,
    fa_tgt_path=/local/install/Config/Lev1/AppData/SASIRM/fa_new,
    fa_id=*
    force_flg=true,
    debug=true,
    logOptions=mprint mlogic symbolgen source,
    connection_type=* Default: INTERNAL */
);
```

**Installing with a Value Specified for the fa_id Parameter**

When you install a federated area with a value that is specified for the `fa_id` parameter, the value is registered as the new federated ID only if it is unique in the system and the `force_flg` parameter is set to `true`. If these conditions are not met, you receive a response from the server that indicates that there is a duplication issue and the new federated area is not installed.

The value that you specify for the `fa_id` parameter must comply with the standard SAS Infrastructure for Risk Management federated ID naming rules:

- The identifier for a federated area can contain numeric characters, alphabetic characters, and periods only.
- Identifiers that start with the number zero (0) are reserved for functionality content that is delivered by the SAS Infrastructure for Risk Management platform federated area. Also, an identifier cannot start with the letter, z. Therefore, do not use identifiers that start with 0 or the letter z.

Example:

```sas
/* Specify fa_id */
%irm_install_fa(
    meta_host=somehost.na.sas.com,
    username=*
    password=*
    fa_src_path=/local/install/New_FA/fa_new.zip,
    fa_tgt_path=/local/install/Config/Lev1/AppData/SASIRM/fa_new,
    fa_id=machine.learning /* must be unique */
    fa_id=force_flg=true,
    debug=true,
    logOptions=mprint mlogic symbolgen source,
    connection_type=* Default: INTERNAL */
);
```
When successfully executed, the content of the federated area ZIP file (fa_new.zip) is copied to the target location and the value that you specified for the `fa_id` parameter is added to metadata.

Note: The newly installed federated area might not be the highest among the other federated areas that are already installed on the server.

**Figure 11.1** New Federated Area in IRM Mid-Tier Server Properties

**Figure 11.2** New Federated Area Folder

---

**Installing without a Value Specified for the fa_id Parameter**

When you install without specifying a value for the `fa_id` parameter, the federated area ID is automatically generated as the highest in the system and added to metadata.

Example:

```/* No value for fa_id */
$irm_install_fa{
    meta_host=somehost.na.sas.com
    , username=
    , passwd=
    , fa_src_path=/local/install/New_FA/fa_new.zip
    , fa_tgt_path=/local/install/Config/Lev1/AppData/SASIRM/fa_new
    , fa_id=
    , force_flg=true
    , debug=true
    , logOptions=mprint mlogic symbolgen source
    , connection_type=/* Default: INTERNAL */
};```
For example, when the server has only the platform federated area (fa.0.3.5) and the sample federated area (fa.sample.3.5) installed, the sample federated ID is the highest. When a new federated area is installed, a higher federated ID (fa.sb in the following example) is generated. This ID is now the highest in the system.

Figure 11.3 New Federated Area in IRM Mid-Tier Server Properties

---

**Installing with the force_flg Parameter Set**

The values for the `force_flg` parameter are `true` and `false`. If you do not specify a value for the parameter when you execute the `%irm_fa_install()` macro, `false` is the default.

If you set `force_flg=true`, the following actions occur:

- The new federated area is installed even if the federated area is determined to be invalid (the checksums differ).
- If you specified a value for the `fa_id` parameter, it is used as the federated area ID for the newly installed federated area.

If you set `force_flg=false`, the following actions occur:

- The new federated area is not installed if it is determined to be invalid.
- If you specified a value for the `fa_id` parameter, it is not used. The next higher federated area ID is generated and used for the newly installed federated area.

---

**Back Up and Restore Job Flow Instances**

SAS Infrastructure for Risk Management provides two scripts that a user can use to back up all information specific to job flow instances in a Microsoft Excel file. After backing up a user’s instances, the file is used to restore the instances on a different machine or a different version of SAS Infrastructure for Risk Management. These scripts are executed in SAS Studio (connected to a SAS Infrastructure for Risk Management server). The information in this section assumes that users have logged on to SAS Infrastructure for Risk Management and created job flow instances.

**Backing Up Job Flow Instances**

Before you back up job flow instances, ensure that the users who created the instances that you are backing up have passwords that have been configured for their user accounts.
To verify that SAS Infrastructure for Risk Management users have passwords that have been configured for their accounts:

1. In SAS Management Console, select User Manager from the Plug-ins tab.
2. Right-click the user name and select Properties ⇒ Accounts.
3. In the logins defined for the user list, select the user row and click Edit. The Edit Login Properties dialog box is displayed.
4. If necessary, enter a password in the Password field and the same password in the Confirm Password field, and click OK.
5. Exit SAS Management Console.

To back up instances created by a specific user:

1. Log on to SAS Studio as the user who created or modified the job flow instances that you are backing up.
2. Press F4 to open a new SAS program in the work area.
3. In the work area, click the Code tab, enter the following:

   ```
   %irm_bkup_instances(debug={TRUE | FALSE}, logOptions= ,
   bkup_file_path=path-to-where-to-create-the-backup-file
   ```

   where:
   - debug — Enables or disables debug logging. The default is False.
   - logOptions — Specifies standard SAS logging options such as mprint, mlogic, symbolgen, and so on. The default is blank.
   - bkup_file_path — Specifies the path to a writable location where the backup file will be created.
4. Click ✨

After executing the script, the following should occur:

- A tabular display of instances created by or shared with the logged in user should appear in the Results tab
- A ZIP file named bkup_inst_YYYYMMDD_HH-MI-SS.zip is located in the Navigation pane under Files (Home). To view the contents of the file, double-click the name of the file. Inside the ZIP file is an .xlsx file named existing_instances_username.xlsx, where username is the name of the user whose job flow instances you backed up. This file contains the tabular listings that are displayed under the Results tab.

  **Note:** The ZIP file is saved at the location that you specified for the bkup_file_path parameter. You will use this ZIP file to restore the job flow instances.

- If a job flow instance had uploaded input data, the uploaded data sets are located in instance-specific folders. The name of the folder is the instance key. The name of the folder that contains the data sets corresponds to the libref of the data sets in the job flow instance.

  **Note:** To view any errors or warnings that occurred during the execution of the backup script, click the Log tab.
Restoring Job Flow Instances

After you have backed up job flow instances, you can restore the instances on a different machine or different version of SAS Infrastructure for Risk Management.

1. Copy the ZIP file of the backed up instances to the target machine.

2. If desired, you can unzip the file and edit the existing_instances_username.xlsx file. You can change the names of instances or delete the row of an instance if you do not want to re-create it on the target machine. If you make edits, ensure that you save the file. It is not necessary to re-zip the file after making edits.

3. Log on to the SAS Infrastructure for Risk Management web application as the same user that executed the backup instances process.

4. Ensure the following:
   - That there are no instances with the same name as an instance in the .xlsx file of backed up instances.
   - That the user on the target machine has the same roles (such as access entities, publishing entities, and so on) as they had on the source machine.
   - That the user has Write permissions to where the ZIP file or unzipped directory is copied over.

5. Log on to SAS Studio as the same user who executed the backup instances process.

6. Press F4 to open a new SAS program in the work area.

7. In the work area, click the Code tab, enter the following:

   ```sas
   %irm_restore_instances(bkup_dir=absolute-path, debug={TRUE | FALSE},
   logOptions= , pollInterval=number-of-seconds, maxWait=max-seconds
   
   where:
   • backup_dir — Specifies the absolute path to the backed up instances, including the ZIP file or directory name if the file is unzipped.
   • debug — (Optional) Enables or disables debug logging. The default is FALSE.
   • logOptions — (Optional) Specifies standard SAS logging options such as mprint, mlogic, symbolgen, and so on. The default is blank.
   • pollInterval — (Optional) Number of seconds between checks of instance creation. The default is 10.
   • maxWait — (Optional) Maximum number of seconds to wait for an instance creation to complete. The default is 3600.
   
   8. Click ✨.

   After executing the script, the following should occur:
   • A tabular display of instances created in the restore session should be displayed in the Results tab
   • A ZIP file named restore_inst_YYYYMMDD_HH_MI_SS is located in the Navigation pane under Files (Home). You can view the contents of this file in SAS Studio or by navigating to the physical location of the file on the target machine. Inside the ZIP file should be an .xlsx file named latest_instances_username.xlsx, where username is the name of the user whose job flow instances you restored. This file contains the tabular listings that are displayed under the Results tab.
• Instances with status of 4 (success) or of 6 (published) are created. Other instances, if any, in the existing_instances_username.xlsx are ignored.

• Instances with the same name that exist on the target machine are not created again. If the debug parameter in macro invocation is set to TRUE, a list of these duplicated instances is printed to the log. To view this list, click the Log tab. To enable the restore instances procedure to create duplicate instances, you must delete the instances on the target machine or edit the names of the instances in the source .xlsx file.
Chapter 12

Troubleshooting

Gather Information

Overview

When troubleshooting, try to isolate and describe the problem and the context in which it occurs.

Specific error messages and warnings from SAS logs can help resolve a problem. Start at the top of SAS logs and search for the first error message. An initial error can cause many subsequent errors. Resolving the first error might eliminate subsequent errors.

Awareness of the following general classes of information can help expedite troubleshooting:

- operating system and configuration information
- a detailed description of the problem that includes the error messages and the action that was performed when the problem was encountered
- log files
- other files or screen shots
- sample test data

Before contacting SAS Technical Support, it is recommended that you review the SAS Knowledge Base for installation, problem, and usage notes. For more information, see the support website at http://support.sas.com/resources.
Also, it is recommended that you check for any hot fixes that might be available. For a list of hot fixes, see the SAS Hot Fix Downloads website.

You can use the SAS Hot Fix Analysis, Download and Deployment Tool to help automate deployment of hot fixes. This tool analyzes the SAS deployment registry and creates a customized report that lists hot fixes available for the installed SAS products. In addition, it generates scripts that automate the deployment of the hot fixes.

You can contact SAS Technical Support at http://support.sas.com/techsup.

**Information about Your Environment and Configuration**

If you request help from SAS Technical Support, be prepared with the following information:

- The site number for your organization.
- The name of your company.
- The SAS SAS Infrastructure for Risk Management release number.
- The SAS release number (including the maintenance level or the patch level number).
- The list of installed SAS software releases and the hot fixes that are based on your SAS Deployment Registry. For information about how to obtain this list, see http://support.sas.com/kb/35/968.html.
- The number of tiers that are used in your SAS installation and the version of the operating system that is used for each tier.
- The hardware platform, the operating environment, the amount of physical memory, and the number of processors.
- The server language and locale settings.
- A list of any nonstandard customizations that you have incorporated in the installation.
- The version of the SAS Infrastructure for Risk Management solution’s content. For information about where to find the content version number, see the content help.

**Problem Description**

Provide a complete description of the problem. Include a description of the general task being performed, your role and permissions, and what occurred during the SAS session. Provide details such as the following:

- Are you working with new data or updating existing data?
- How is the problem reproduced?
- What browser and release are you using?
- Is the problem locale-specific? If so, which locales are having problems?
- When did the problem first occur?
- Were any changes made that might have caused the problem? In particular, were any permissions changed on directories? Such changes can have unforeseen consequences.
Sample Test Data

If possible, capture the information entered that caused the problem. In certain situations, SAS Technical Support might request your data load files so that they can replicate your operating environment.

Enable Detailed Logging

SAS Infrastructure for Risk Management uses log4j to perform logging. When SAS Infrastructure for Risk Management begins running, the log4j configuration files for SAS Infrastructure for Risk Management are read from one of the following locations:

- Linux: `SAS-configuration-directory/Lev\n/Web/Common/LogConfig/
- Windows: `SAS-configuration-directory\Lev\n/Web\Common\LogConfig\`

The configuration file names are SASIRM-log4j.xml and SASIRMServer-log4j.xml.

SAS Infrastructure for Risk Management writes information to the following log files, which are located in `SAS-configuration-directory/Lev\n/Web/Logs/SASServer8_1/` by default:

- SASIRM.log — contains messages from the SAS Infrastructure for Risk Management client.
- SASIRMServer.log — contains messages from the SAS Infrastructure for Risk Management server.

To debug a problem, you can change the log level to DEBUG.

SAS Infrastructure for Risk Management should run under this logging level only for capturing additional log information. Do not use this logging level for daily operations of SAS Infrastructure for Risk Management.

CAUTION:

Excessive logging can degrade performance. Therefore, use the DEBUG level only when directed by SAS Technical Support.

For detailed information about logging, see `SAS Intelligence Platform: Middle-Tier Administration Guide`.


To enable DEBUG logging for SAS Infrastructure for Risk Management:

1. Navigate to the `SASIRMServer-log4j.xml` configuration file that is located in one of the following directories:
   - Linux: `SAS-configuration-directory/Web/Common/LogConfig/
   - Windows: `SAS-configuration-directory\Web\Common\LogConfig\`

   Note: For most troubleshooting purposes, enable DEBUG logging in the `SASIRMServer-log4j.xml` configuration file.

2. Locate the following code:

```xml
<logger name="com.sas.solutions.risk.irm" additivity="false">
  <level value="INFO"/>
<appender-ref ref="SAS_FILE"/>
```
3. Replace “INFO” with “DEBUG” and save the file.

   <logger name="com.sas.solutions.risk.irm" additivity="false">
     <level value="DEBUG"/>
     <appender-ref ref="SAS_FILE"/>
     <appender-ref ref="SAS_CONSOLE"/>
   </logger>

4. Restart the SAS Infrastructure for Risk Management web application server.

---

**Fix Your Web Application Log File Display**

In some environments (for example, Simplified Chinese), SAS Infrastructure for Risk Management web application log files that are viewed in a web browser contain unreadable content. Log files are unreadable because SAS Infrastructure for Risk Management web application log files are not created with UTF-8 character encoding, but they are displayed on the web browser in UTF-8 character encoding.

To fix the display of an unreadable log file in a Windows environment:

1. Stop the SAS Infrastructure for Risk Management web application server.
2. Navigate to the \SAS-configuration-directory\config\Lev\Web\WebAppServer\SASServer8_1\conf directory.
3. In the wrapper.conf file, add the following statement:

```
wrapper.java.additional.n=-Dfile.encoding=UTF-8
```

   where \(n\) is the next available digit in the series of additional Java parameters.
4. Restart the SAS Infrastructure for Risk Management web application server.

To fix an unreadable log file display in a Linux environment:

1. Stop the SAS Infrastructure for Risk Management web application server.
2. Navigate to the /SAS-configuration-directory/config/Levn/Web/WebAppServer\SASServer8_1/bin\ directory.
3. Use the setenv.sh to set the Java environment to the UTF-8 encoding as follows:

```
JVM_OPTS="-Dfile.encoding=UTF-8"
```
4. Restart the SAS Infrastructure for Risk Management web application server.

---

**Log and Configuration File Locations**

The following table lists the log files that might contain relevant logging information.
### Table 12.1 Log Files

<table>
<thead>
<tr>
<th>File</th>
<th>Default Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration logs</td>
<td><code>/SAS-configuration-directory/Logs/Configure</code></td>
</tr>
<tr>
<td>SAS Infrastructure for Risk Management web logs</td>
<td><code>/SAS-configuration-directory/Web/Logs</code></td>
</tr>
<tr>
<td>Note: By default, the log files for the SAS Infrastructure for Risk Management application do not appear at this location unless they are configured in SAS Management Console.</td>
<td></td>
</tr>
</tbody>
</table>
| SAS Infrastructure for Risk Management Log4J       | SAS Infrastructure for Risk Management uses the open-source Java library Log4j for application logging. The logging behavior is configured in the `SASIRM-log4j.xml` file and in the `SASIRMServer-log4j.xml` file (located in `/SAS-configuration-directory/Web/Common/LogConfig/`) for the SAS Infrastructure for Risk Management middle tier. Most of the details in these files, especially the various logging levels, should not be modified. However, you can customize some information by modifying these files. Here are examples of information that you can modify:  
  - the location of the log file  
  - file storage properties  
  - use of rolling logs  
  - the number of log files  
  - the maximum size of log files |
| Object spawner log                                 | `/SAS-configuration-directory/ObjectSpawner/Logs`                                |
| SAS Workspace Server logs                          | `/SAS-configuration-directory/SASApp/WorkspaceServer/Logs`                      |
| SAS Metadata Server log                            | `/SAS-configuration-directory/SASMeta/MetadataServer/Logs`                      |

**Note:** Note that the paths in the preceding table are different if you choose to set up common directories.
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.