SAS® Federation Server 4.2: Migration Guide

SAS® Documentation
March 7, 2019

The correct bibliographic citation for this manual is as follows: SAS Institute Inc. 2016. *SAS® Federation Server 4.2: Migration Guide*. Cary, NC: SAS Institute Inc.

SAS® Federation Server 4.2: Migration Guide

SAS Institute Inc., SAS Campus Drive, Cary, NC 27513-2414

September 2016

4.2-P2:fedsrvmig

Contents

Chapter 1

Migration and Upgrade for SAS Federation Server 4.2

Introduction

SAS Federation Server upgrade and migration is a multi-step process. In addition to migrating the system catalog, user data is migrated from the DataFlux Authentication Server to SAS Metadata Server. To upgrade to SAS Federation Server 4.2 from earlier versions, you must perform certain tasks to update your databases and configuration files.

- SAS Federation Server 4.1 to 4.2 Migration: Use the SAS Migration Utility with the SAS Deployment Wizard to perform a migration. During migration, users are ported from DataFlux Authentication Server to SAS Metadata Server. Post-migration tasks are required.
- SAS Federation Server 3.x to 4.2: Manual migration: Use the procedure outlined in "Migrating SAS Federation Server Versions 3.x". Run PROC ASEXPORT to export users from DataFlux Authentication Server. Post-migration tasks are required.
- SAS Federation Server 4.1 to 4.2 Upgrade: Uses the SAS Deployment Wizard to upgrade an existing environment, replacing the previous version of software. This upgrade requires more than one pass to install additional components. During the upgrade, users are ported from DataFlux Authentication Server to SAS Metadata Server. Post-migration tasks are required.
- SAS Federation Server 3.x to 4.2 Upgrade: Uses the SAS Deployment Wizard to upgrade an existing environment but requires more than one pass to install additional components, such as servers required for SAS Federation Server Manager. During

the upgrade, users are ported from DataFlux Authentication Server to SAS Metadata Server. Post-migration tasks are required.

In addition to the SAS migration package, the SAS Deployment Wizard also relies on a SAS Software Depot that contains installation files. The depot contains a deployment plan that tells the wizard which components to install and configure. However, DataFlux Authentication Server is not included in the plan because previous versions were installed independent of the SAS platform. If you want to migrate users and groups to SAS Metadata Server, you must add DataFlux Authentication Server to the plan.

See the *SAS Intelligence Platform: Migration Guide* for details about migration.

Plan File

You need a plan file to install SAS Federation Server and associated software. Obtain a plan file from your SAS consultant. The requirement for a plan file also applies to upgrades because there are additional products to install and configure after the upgrade completes.

DataFlux Authentication Server

SAS Federation Server content, such as users and groups, is migrated from DataFlux Authentication Server using the ASEXPORT procedure. This procedure runs automatically during the SAS Deployment Wizard configuration process. The ASEXPORT procedure migrates domains, users, and groups from DataFlux Authentication Server to a SAS Metadata Server in your SAS Federation Server environment. Here is additional information and requirements for DataFlux Authentication Server:

- DataFlux Authentication Server does not automatically appear in a plan. If you plan to migrate content to SAS Metadata Server, your deployment must include both of the following components:
  - SAS Authentication Server 4.1
  - DataFlux Authentication Server Configuration
- If you are migrating from SAS Federation Server 3.2, the SAS Deployment Wizard needs to be run twice, because at first, the system does not recognize Authentication Server to update its configuration. For SAS Federation Server 4.1 to the first maintenance release for SAS Federation Server 4.1, the system will behave such that no extra run of the SAS Deployment Wizard is needed.
- SAS Foundation, also referred to as Base SAS, is required software for DataFlux Authentication Server. This software is needed to run PROC ASEXPORT.
- The administrator account configured in SystemUsers in the as_serv_aspsql.xml configuration file, must also be specified under TrustedUsers in that same file.
- PROC ASEXPORT does not export shared logins. Shared logins must be re-created in SAS Metadata Server.

See the *DataFlux Authentication Server: Administrator's Guide* for additional details about the system user and PROC ASEXPORT.

SAS Federation Server Configuration Considerations

Configuration Files

If any custom configuration changes were made to existing configuration files, such as server configurations or SQL Logging, copy these files before migrating content. You can later update the new configuration files with your custom configurations. However, with the addition of SAS Metadata Server, some of these configurations might not be needed in SAS Federation Server 4.2. See the "Configuration Reference" in the *SAS Federation Server: Administrator's Guide* for additional information.

SQL Logging

The SQL Logging database file does not require upgrade or migration. However, configuration for SQL Logging does need to be refreshed after upgrading SAS Federation Server. No matter the type of upgrade or migration, you must always refresh SQL Logging because the path for the SQL_LOG database is no longer valid after an upgrade. You should perform this task even if the migration was automated, or if a SAS Federation Server 4.2 to 4.2 migration was performed.

SAS Federation Server Manager

SAS Data Management Data Server Dependency

Starting with SAS Federation Server 4.2, the SAS Federation Server Manager has a new dependency on the SAS Data Management Data Server. As a result of this dependency, the SAS Data Management Data Server must be installed and configured before the SAS Federation Server Manager can be successfully installed and configured. In a new installation, the SAS Deployment Manager installs the components in the required order.

SAS Web Application Functionality

Starting with SAS Federation Server 4.2, SAS Federation Server Manager functions as a SAS web application on the mid-tier. With this new functionality, there is no longer a need to start a separate server process. Start-up is managed through the SAS Web Application Server scripts and accessed with a unique URL that is noted in Instructions.html.

Scheduled Cache Refresh Jobs

Prior to installation of SAS Federation Server Manager 4.2, assess the scheduled cache refresh jobs, including CRON, that you want to carry over to the new version. After SAS Federation Server Manager 4.2 has been installed and configured, you must re-create these jobs, because they are not carried over from previous versions of SAS Federation Server Manager. See Post Migration and Upgrade Tasks on page 24 for additional information.

Chapter 2

Migrating SAS Federation Server

Migrating SAS Federation Server 4.1 to Version 4.2

Overview

Migration of SAS Federation Server from version 4.1 to 4.2 is prepared using the SAS Migration Utility and run using the SAS Deployment Wizard. The SAS Deployment Wizard also provides the opportunity to port users from DataFlux Authentication Server to SAS Metadata Server.

Performing the Migration

Prerequisites

Address the following items for DataFlux Authentication Server before running a migration:

- DataFlux Authentication Server does not automatically appear in a plan. If you plan to migrate content to SAS Metadata Server, your deployment must include both of the following components:
  - SAS Authentication Server 4.1
  - DataFlux Authentication Server Configuration

- SAS Foundation, also referred to as Base SAS, is required on the target DataFlux Authentication Server to run PROC ASEXPORT. Install the third maintenance release for SAS Foundation 9.4 with all applicable hotfixes.
- The administrator account configured in **SystemUsers** must also be configured as a **TrustedUser** in the **`as_serv_aspsql.xml`** configuration file. See the *DataFlux Authentication Server: Administrator's Guide* for details about configuring this account.

Using a Migration Properties File

The *SAS 9.4 Intelligence Platform: Migration Guide* contains instructions about creating a SAS Migration Package. The SAS Migration Utility must be run before installing and configuring the new version of the software. Create a SAS Migration properties file for each server tier, starting with SAS Metadata Server.

In migration utility properties files, when specifying Windows paths or domains as a part of a user ID, you must escape any backslashes (\) with another backslash character. For example:

```
SMU.config.dir=C:\\SAS\\config\\913BIPlatform\\Levn
SMU.user=mydomain\\sasadm
```

The migration utility does not recognize blank spaces in the directory path.

Note: SAS supplies a migration utility template file (smu.properties.template) that provides examples that show how to use various properties. You can find this file in your SAS Software Depot in the **`/smu`** subdirectory underneath utilities.

When you are finished, review the migration analysis reports and fix any discrepancies. Move the migration package to the target server in preparation to run the SAS Deployment Wizard.

Run the SAS Deployment Wizard

After moving your migration packages, launch the SAS Deployment Wizard from the SAS Install Depot. Follow the onscreen instructions and proceed through the steps until you get to the migration dialog box that prompts for the location for the SAS Migration Utility package. Select the check box and fill in the location where the SAS Migration Utility package can be found. Here are a few important items to note:

- Use the plan file that is associated with the migration that you are performing. The SAS Deployment Wizard does not detect an incorrect plan until late in the process.
- When running the SAS Deployment Wizard, you are prompted for an external account for data management that is used to export users from DataFlux Authentication Server. Replace the default account (sasdmadm) with the system user account that you configured as a trusted user. See the preceding prerequisites. This account must be a valid external account located on the target machine.
- Run the SAS Deployment Wizard for each tier that you are migrating.

At the end of the migration process, the SAS Deployment Wizard produces an HTML document named Instructions.html. If your server tier and middle tier are hosted on separate machines, each machine has an Instructions.html file. Follow the instructions that are provided in the HTML documents.

Review Instructions.html

When you port users from DataFlux Authentication Server, a validation job is run at the end of the deployment. The validation job returns warnings for the objects that could not be exported and logs warnings in the instructions file generated at the end of the SAS

Deployment Wizard process. However, a warning is not generated if all of the users, groups, and domains were successfully exported from DataFlux Authentication Server and imported to SAS Metadata Server. A warning might look like this:

```
The process to automatically port the users did not complete successfully.
 Please review the log file:
 /install/userID/config/Lev1/Logs/Configure/dfauthsvrc_asproc.result.log
 for more information on why theDataFlux Authentication Server users,
 groups and domains were not successfully ported to the SAS Metadata Server.
```

See the *DataFlux Authentication Server: Administrator's Guide* for details about reconciling unsuccessful exports.

SAS Federation Server Manager

SAS Federation Server Manager is included as an upgrade for the mid-tier platform. However, when SAS Federation Server Manager is the only SAS mid-tier product and SAS application servers have not been previously configured, you should use the instructions for upgrading SAS Federation Server Manager.

After installing SAS Federation Server Manager 4.2, you must re-create any cache refresh scheduled jobs that were running in the previous version. Scheduled jobs include cache refresh and custom CRON schedules. See 'Post-Installation Tasks'.

Post-Migration Tasks

Following migration, it is necessary to perform additional steps to make your existing configuration work with the new version. See "Post-Migration and Upgrade Tasks for SAS Federation Server" for a list of items to configure for SAS Federation Server.

Migrating SAS Federation Server Versions 3.x

Overview

Migration of earlier versions of SAS Federation Server (for example, version 3.1) is a manual process. You need to back up and restore the SAS Federation Server and DataFlux Authentication Server databases and move the data to the new platform. Once the data is in place, you migrate content to the SAS Federation Server 4.2 server. In addition, you port users and groups from DataFlux Authentication Server to SAS Metadata Server using PROC ASxport. These instructions are explained in the following topics.

Prerequisites

Here are the prerequisites for migration of SAS Federation Server 3.x:

- SAS Federation Server 3.x and DataFlux Authentication Server 3.x are installed and configured.
  - The installation location for SAS Federation Server 3.x is **SASHome\fedserver*server_instance***.

  - The default installation location for DataFlux Authentication Server 3.x is ***drive*:\ProgramFiles\DataFlux\Authserver*server_instance***, referred to as **<*authserver*>** in the following instructions.
- SAS Federation Server 4.2 and DataFlux Authentication Server 4.1 have been installed as out-of-the-box configurations.
- You need login information for DataFlux Authentication Server and SAS Metadata Server to run PROC ASEXPORT.
- SAS Foundation (Base SAS) is required on DataFlux Authentication Server to run PROC ASEXPORT.
- Your shared login key should be accessible. The Shared Login key can be found in SAS Federation Server Manager in Federation Server Properties, on the **Security** tab.
- Copy any configuration files that have been customized for your environment to a directory accessible by SAS Federation Server.
- You need access to the *DataFlux Authentication Server 4.2: Administrator's Guide, Second Edition* for instructions to run PROC ASEXPORT.

Migrating 3.x Versions to 4.2

Backing Up the Source Databases

Use the following task to prepare the source DataFlux Authentication Server 3.x and SAS Federation Server 3.x for migration. This task uses a UNIX operating system. However, this task also applies to Windows operating systems. Use Windows services when you need to start or stop the servers. If you need additional information, see "Stopping and Restarting the Servers".

1. Stop the SAS Federation Server by issuing the following command:

   ```
   ./dfsadmin.sh stop
   ```

   DataFlux Authentication Server should continue to run at this point.

   Note: **dfsadmin.sh** is located in the **/bin** directory of the federation server installation path.

   If you are migrating to an operating system that is different from the source 3.x system, proceed to step 3.

2. Make a copy of the federation server database, syscat.tdb, from **<*fedserver*>/var** and place it in a network directory that is accessible from the target 4.2 system:

   ```
   cp syscat.tdb <networklocation>/syscat.tdb
   ```

3. Back up the federation server system catalog, syscat.tdb, using the following command:

   ```
   <fedserver>/bin/dfsutil backup -db syscat <networklocation>/syscat.tdb
   ```

4. Stop the DataFlux Authentication Server by issuing the following command:

   ```
   ./dasadmin.sh stop
   ```

   Note: The **dasadmin.sh** command is located in the **/bin** directory of the DataFlux Authentication server installation path.

If migrating to an operating system that is different from the source 3.x system, proceed to step 6.

5. Copy the authentication server database, asdb.tdb, from the **`<authserver>/var`** directory to a network location that is accessible from the 4.2 target system.

   ```
   cp asdb.tdb <networklocation>/asdb.tdb
   ```

6. If you are migrating to a different operating system, back up asdb.tdb by running the dasutil command on the 3.x system:

   ```
   <authserver>/bin/dasutil backup -db asdb <networklocation>/asdb.tdb
   ```

Migrating Content to the Target 4.2 Server

Once you have all of your backups and copies in place, migrate content to SAS Federation Server 4.2 on the target server. This task uses a UNIX operating system but also applies to Windows operating systems. Use Windows services when you need to perform a start or stop for the servers.

Note: Perform these tasks on the target system.

1. Stop SAS Federation Server using dfsadmin, located in **`/bin`** of the configuration path:

   a. Change the directory to point to **`/bin`** of the configuration path:

   ```
   cd <SASconfigDir>/Lev1/FederationServer/bin
   ```

   b. Issue a stop command:

   ```
   ./dfsadmin.sh stop
   ```

2. Stop DataFlux Authentication Server:

   a. Change the directory of the DataFlux Authentication Server to point to **`/bin`** of the installation path:

   ```
   cd <SASHome>/DataFluxAuthenticationServer/4.1/authserver/bin
   ```

   b. Issue a stop command:

   ```
   ./dasadmin stop
   ```

3. Open the dfs_entities.dtd file, located at **`<SASconfig>/Lev1/FederationServer/etc/dfs_entities.dtd`**, and make note of the location for **cfg.TRANPATH** .

4. Navigate to the **cfg.TRANPATH** location that you noted in the preceding step, and move the system catalog, syscat.tdb to syscat.tdb.origbackup:

   ```
   cd <SASConfig>/Lev1/FederationServer/var
    mv syscat.tdb syscat.tdb.origbackup
   ```

Proceed to step 6 if your 4.2 system is a different operating system than the source 3.x system.

5. Navigate to the cfg.TRANPATH location:

   ```
   cd <SASConfig>/Lev1/FederationServer/var
   ```

   and copy the 3.x syscat.tdb to the new cfg.TRANPATH location for version 4.2:

```
cp <networklocation>syscat.tdb syscat.tdb
```

6. Perform this step only if the 4.2 system is a different operating system than the source system:

   a. On the 4.2 system, navigate to the **cfg.TRANPATH** location:

   ```
   cd <SASConfig>/Lev1/FederationServer/var
   ```

   b. Use the dfsutil restore command to copy the 3.x syscat.tdb:

   ```
   <SASConfig>/Lev1/FederationServer/bin/dfsutil
    restore -db syscat <networklocation>/syscat.tdb
   ```

7. Navigate to the **/var** directory on the DataFlux Authentication Server and back up the asdb.tdb database file:

```
cd <SASHome>/DataFluxAuthenticationServer/4.1/authserver/var
 mv asdb.tdb asdb.tdb.origbackup
```

Proceed to step 9 if your 4.2 system is a different operating system than the source 3.x system.

---

8. Copy the asdb.tdb file from your 3.x network location to the **/var** directory of the 4.1 DataFlux Authentication Server:

```
cd <SASHome>/DataFluxAuthenticationServer/4.1/authserver/var>
 cp /<networklocation>/asdb.tdb asdb.tdb
```

9. Perform this step only if the 4.2 system is a different operating system than the source system. Use the dasutil restore command to copy 3.x asdb.tdb (created in the previous section) to the DataFlux Authentication Server **/var** directory.

```
cd <SASHome>/DataFluxAuthenticationServer/4.1/authserver/var

 <SASHome>/DataFluxAuthenticationServer/4.1/authserver/bin/dasutil
 restore -db asdb <networklocation>/asdb.tdb
```

10. Perform the following steps to verify that the administrator account (system user) configured in as_server_aspsql.xml is also configured as a trusted user.

    a. Navigate to the **/etc** directory of the DataFlux Authentication Server (for example, **<SASHome>/DataFluxAuthenticationServer/4.1/authserver/etc**).

    b. Open as_server_aspsql.xml for editing, and locate the SystemUsers and TrustedUsers option sets. Make sure that the SystemUsers Account is also reflected as a TrustedUsers Account. If not, add the SystemUsers account to the TrustedUsers Account:

```
<OptionSet name="SystemUsers">
        <Option name="Account">bcisas</Option>
    </OptionSet>

<OptionSet name="TrustedUsers">
        <Option name="Account">carynt\user</Option>
        <Option name="Account">bcisas</Option>
    </OptionSet>
```

11. Start the DataFlux Authentication Server from the **/bin** directory. Here is an example:

```
<SASHome>/DataFluxAuthenticationServer/4.1/authserver/bin/dasadmin start
```

12. Shared login accounts are not migrated. Therefore, you must create the new account as a shared login group using SAS Management Console. See “Shared Logins” for details.

    Note: There is no particular order in which shared logins should be created. You can create shared logins during or after migration.

13. You are ready to begin exporting users and groups from the DataFlux Authentication Server.

Export Users and Groups

Use PROC ASEXPORT to export users and groups from DataFlux Authentication Server and move them to SAS Metadata Server. Run PROC ASEXPORT using the upgraded version, the first maintenance release of DataFlux Authentication Server 4.1. In general, you want to export all content in a single export command. Users and groups should be added in the same export step so that group memberships are properly affiliated. If you run separate export steps, then you must manually assign group memberships for any users and groups that were previously added. Note that PROC ASEXPORT does not change membership relationships (member-of and contained members) for existing users and groups. Doing so might change authorization results in SAS Metadata Server.

When you are finished exporting users, you can run a validation, which determines whether problems were encountered. See the *DataFlux Authentication Server: Administrator’s Guide* for details about PROC ASEXPORT.

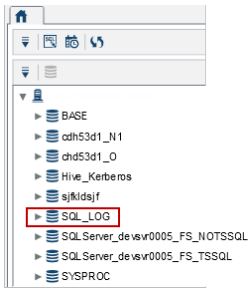
Refresh SQL Logging

This task applies if you are using SQL Logging on the 3.x SAS Federation Server. To refresh SQL Logging, drop the SQL_LOG data service and restart SAS Federation Server as outlined in the following task:

1. Delete the SQL_LOG data service using one of the following methods:

   a. Use SAS Federation Server Manager to delete the SQL_LOG data service. Locate the federation server object in the tree and delete the associated SQL_LOG data service.

   Figure 2.1 *Deleting SQL_LOG*

   b. Use administration DDL on SAS Federation Server to Issue a DROP DATA SERVICE command:

   ```
   DROP DATA SERVICE SQL_LOG CASCADE
   ```

2. Stop and restart SAS Federation Server. Upon server restart, a new SQL_LOG data service is created with a correct path to the SQL Logging database.

Note: No matter the type of migration, you must always refresh SQL Logging because the path to the SQL_LOG database is no longer valid after an upgrade.

SAS Federation Server Manager

After SAS Federation Server Manager 4.2 has been installed, you must re-create any cache refresh scheduled jobs that were running in the previous version. Scheduled jobs include custom CRON schedules. See 'Post-Installation Tasks'.

Back Up and Restore a System Database (Manual Only)

Overview

The SAS Deployment Wizard ensures backup and restore of the system catalog (SYSCAT). However, if you need to perform a backup and restore manually, use the following procedure.

Note: You can also use these tasks if you want to preserve your current SQL Logging database or move it to the new server.

Use **dfsutil** to back up and restore the system catalog. This utility is provided with SAS Federation Server installation and is located in **`/bin`** of the configuration directory (for example, **`/SAS/config/Levn/FederationServer/bin`**).

CAUTION:

When running backup or restore for versions prior SAS Federation Server 4.2, use dfsutil located in the installation path of SAS Federation Server. For example, [installation root:]/..SASHome/FedServer/*server_name*/bin>

The following tasks describe how to use dfsutil to perform a backup and restore for a SAS Federation Server database.

Back up a Database

To back up a database, use the **`-db`** parameter with the dfsutil command and include the name of the database in your backup statement. Note that you can run this command while the server is running but it is not suggested if you are performing a migration. Here is an example of a backup command for SYSCAT:

```
configuration-path\bin\dfsutil backup -db syscat \path_to_backup
```

Restore a Database

To restore a database, use the **`-db`** parameter with the dfsutil command. Here is an example of a restore command for SYSCAT:

```
local_disk/install/config/Levn/FederationServer/bin/dfsutil restore
 -db syscat \path\to\backup
```

Stopping and Restarting the Servers

Windows

Several of the tasks presented in this guide require stopping and restarting the DataFlux Authentication Server and SAS Federation Server. On the Windows platform, SAS Federation Server runs as a Windows service, which is accessible through Administrative Tools.

1. Select **Start** ⇨ **Settings** ⇨ **Control Panel**.
2. Open **Administrative Tools** ⇨ **Computer Management**.
3. Expand the **Services and Applications** folder.
4. Click **Services** and select **SAS Federation Server**.
5. Select **Stop** or **Restart** the service.

UNIX

To start or stop SAS Federation Server on a UNIX platform, use dfsadmin.sh utility, located in **`SAS/Config/Lev[n]/FederationServer/bin`**. Run dfsadmin.sh using this command syntax:

```
dfsadmin.sh start|stop
```

- To start SAS Federation Server, issue the following command: **`dfsadmin.sh -start`**.
- To stop SAS Federation Server, issue the following command: **`dfsadmin.sh -stop`**.

Chapter 3

Upgrading SAS Federation Server

Upgrade SAS Federation Server 4.1 to 4.2

About the Upgrade

Upgrade is a method that enables you to upgrade to an existing environment, replacing the previous version of software. During the upgrade, users are ported from DataFlux Authentication Server to SAS Metadata Server. Use the SAS Deployment Wizard to run the upgrade for SAS Federation Server and associated software.

Prerequisites

DataFlux Authentication Server requires the following software or configurations for a successful upgrade:

- SAS Foundation (Base SAS 9.4m3) is needed to run PROC ASEXPORT, which ports users and groups to SAS Metadata Server.
- The administrator account configured in **SystemUsers** must also be configured as a **TrustedUser** in the `as_serv_aspsql.xml` configuration file. This account is used in place of the default data management account during the upgrade. See the *DataFlux Authentication Server: Administrator's Guide* for details about configuring this account.

- A plan file is required to complete the updates for SAS Federation Server Manager.

Perform an Upgrade

Run the SAS Deployment Wizard to perform an upgrade. Stop all services, or daemons before running the SAS Deployment Wizard:

1. Launch the SAS Deployment Wizard from the SAS Install Depot. Follow the onscreen instructions and proceed through the steps.
2. At the **External Account** dialog box, use the authentication server's system user account to override the default, sasdmadm.
3. At the end of the upgrade process, the SAS Deployment Wizard produces an HTML document named UpdateInstructions.html. If your server tier and middle tier are hosted on separate machines, each machine has an UpdateInstructions.html file. Follow the instructions that are provided in the HTML documents.
4. Complete the post-migration (upgrade) tasks for SAS Federation Server.

Review UpdateInstructions.html

When you port users from DataFlux Authentication Server, a validation job is run at the end of the deployment. The validation job returns warnings for the objects that could not be exported and logs warnings in the instructions file generated at the end of the SAS Deployment Wizard process. A warning is not generated if all of the users, groups, and domains were successfully exported from DataFlux Authentication Server and imported to SAS Metadata Server. A warning might look like this:

```
The process to automatically port the users did not complete successfully.
 Please review the log file:
 /install/userID/config/Lev1/Logs/Configure/dfauthsvrc_asproc.result.log
 for more information on why theDataFlux Authentication Server users,
 groups and domains were not successfully ported to the SAS Metadata Server.
```

See the *DataFlux Authentication Server: Administrator's Guide* for details about reconciling unsuccessful exports.

You will also see additional instructions to install and configure the SAS Data Management Data Server to accommodate SAS Federation Server Manager. After SAS Data Management Data Server is installed, rerun the SAS Deployment Wizard in configure mode, and select configure the SAS Federation Server Manager mid-tier, along with SAS Web Application Server. A plan file is required to complete this task.

Upgrade SAS Federation Server 3.2 to 4.2

About the Upgrade

This task is an upgrade to an existing environment, replacing the previous version of SAS Federation Server and associated software. The following scenario is based on a single-machine deployment.

Prerequisites

DataFlux Authentication Server requires the following software and configuration for a successful upgrade:

- SAS Foundation (Base SAS) is required on the source DataFlux Authentication Server to run PROC ASEXPORT.
- The administrator account configured in **SystemUsers** must also be configured as a **TrustedUser** in the `as_serv_aspsql.xml` configuration file. This account is used in place of the default data management account during the upgrade. See the *DataFlux Authentication Server: Administrator's Guide* for details about configuring this account.

Perform an Upgrade

Launch the SAS Deployment Wizard from the SAS Install Depot. Follow the screen prompts and instructions to proceed through these steps:

- Step 1 – Perform an Upgrade Installation: Run the SAS Deployment Wizard, which recognizes the existing installation and switches to upgrade mode. At the end of installation, when presented with the option to update the configuration, you will end the installation. Step 2 addresses configuration.
- Step 2 – Perform an Upgrade Configuration: In this step, you complete the upgrade process with updated components. However, DataFlux Authentication Server has not yet been upgraded to the first maintenance release.
- Step 3 – Run the SAS Deployment Wizard Installation: In step 3, you run the SAS Deployment Wizard installation using a plan file for the current order. You install missing components such as SAS Data Management Data Server, which is a requirement for SAS Federation Server Manager.
- Step 4: Run the SAS Deployment Wizard Configuration: In this step, you run the SAS Deployment Wizard Configuration to complete the configuration of SAS Federation Server and DataFlux Authentication Server. After completing configuration, PROC ASEXPORT begins to migrate users from DataFlux Authentication Server to SAS Metadata Server, logging issues if any arise.

Note: Stop all services or daemons before running the SAS Deployment Wizard.

1. Step 1: **Perform an Upgrade Installation**
   a. Select Deployment Task: **Install SAS Software**.
   b. Review the list of products to be installed or upgraded.
   c. Review the Deployment Summary and click **Start**.
   d. Cancel the deployment at Specify Configuration Directory. Clear the **Configuration Directory** check box, and exit the installation.
2. Step 2: **Perform an Upgrade-in-Place Configuration**
   a. Start SAS Metadata Server.
   b. Launch SAS Deployment Manager. The **Update Existing Configuration** option is selected to update the configuration of recently updated products.

c. At **Specify Connection Information**, enter the SAS Metadata Server administrator user ID and password. Proceed to enter connection information through the next dialog boxes until you reach **Deployment Complete**.

Review Warnings and Notices in UpdateInstructions.html. SAS Federation Server Manager Mid-Tier Configuration should report a warning that a configured instance of SAS Data Management Data Server was not found. The warning might look similar to the following:

"The following error occurred during upgrade in place configuration for SAS Federation Server Manager Mid-Tier: A configured instance of SAS Data Management Data Server was not found. SAS Data Management Data Server must be previously configured in order to complete the upgrade process for SAS Federation Server Manager Mid-Tier."

Note: You might also see the same error for SASServer13, which is added with SAS Data Management Data Server in the following step.

To reconcile this error, SAS Data Management Server is added in the following step.

3. Step 3: **SAS Deployment Wizard Installation**

   In this step, you can add new products based on current requirements. A plan file is required to add additional products, such as SAS Data Management Data Server.

   a. Select Deployment Task: **Install SAS software**

   b. Specify the deployment type: Planned deployment, install SAS software

   c. Specify the path to your deployment plan.

   d. Specify configuration information and user accounts on the next several dialog boxes. When you get to **DataFlux Authentication Server: Trusted User**, override the default account with the system/trusted user account specified earlier in Prerequisites.

   Review the Deployment Summary after the SAS Deployment Wizard is finished running.

4. Step 4 – **SAS Deployment Wizard Configuration**

   At this step, SAS Deployment Wizard is run again to update configuration of products added in Step 3 and products updated in step 1, but not yet configured.

   a. Select Deployment Task: **Install SAS software**.

   b. Specify the deployment type: **Planned deployment**, **configure SAS software**.

   c. Specify the path to your deployment plan.

   d. Select the products to configure, which should include DataFlux Authentication Server and SAS Data Management Data Server.

   e. Proceed through the dialog boxes entering configuration and user account information. Click **Start** at the Deployment Summary.

After the deployment completes, review the Warnings and Notices in Instructions.html.

Review Instructions.html

If there were problems porting users from DataFlux Authentication Server to SAS Metadata Server, you will see a warning similar to the following:

"The process to automatically port the users did not complete successfully. Please review the log file: **`C:\SAS\Config\Lev1\Logs\Configure \dfauthsvrc_asproc.result.log`** for more information about why the DataFlux Authentication Server users, groups and domains were not successfully ported to the SAS Metadata Server."

See the *DataFlux Authentication Server: Administrator's Guide* for details about reconciling errors and manually exporting users.

Post-Migration Tasks

Following upgrade, it is necessary to perform additional steps to make your existing configuration work with the new version. See "SAS Federation Server" for a list of items to configure for SAS Federation Server.

Upgrade SAS Federation Server Manager 4.1

About this Upgrade

There might be instances when SAS Federation Server Manager 4.1 is the only product installed on the mid-tier platform. If no other SAS mid-tier products are installed, SAS Federation Server Manager does not have the required mid-tier components to upgrade to version 4.2. In this case, use the following task to install and upgrade SAS Federation Server Manager 4.2. Federation Server Manager 4.2 has a dependency on the SAS Data Management Data Server and the web application server, SASServer13. You must add SAS Data Management Data Server 2.1 if it is not already installed. A plan file is required to install SAS Data Management Data Server as an add-on.

Note: You should use this procedure when SAS Federation Server Manager 4.1 is the only SAS mid-tier product and SASApp and WIP have not been previously configured.

After upgrading SAS Federation Server Manager, the application functions as a SAS Web Application and no longer requires a separate server start-up. Start-up is managed with the SAS Web Application Server scripts and accessed through a new URL, which is noted in Instructions.html.

Performing the Upgrade

Use the following task to install SAS Federation Server Manager 4.2 alongside the upgraded servers. SAS Federation Server Manager 4.2 requires a new product deployment after upgrading other server tiers in your environment. This task uses the SAS Deployment Wizard with the required plans:

1. Run the SAS Deployment Wizard to perform an upgrade–in–place on the metadata tier and the server tier.
2. After performing the upgrade on the metadata tier and the server tier, run the SAS Deployment Wizard again on the server tier to deploy SAS Data Management Data Server as an add-on.
3. Run the SAS Deployment Wizard on the mid-tier machine in Update mode. The SAS Deployment Wizard should automatically detect that it needs to run updates. After installing the updates, the SAS Deployment Wizard launches the SAS Deployment Manager, which gives you the option to run a UIP configuration. To proceed, you

must first cancel the SAS Deployment Manager and stop the SAS Deployment Wizard.

CAUTION:

You want to cancel the SAS Deployment Manager because you cannot perform a 4.1 -> 4.2 UIP configuration for Federation Server Manager due to limitations in the stand-alone environment.

4. After closing the SAS Deployment Manager and SAS Deployment Wizard from the initial run, launch the SAS Deployment Wizard again to deploy SAS Federation Server Manager 4.2. This requires a plan file.

Review UpdateInstructions.html after the SAS Deployment Wizard has finished.

Note: Other upgrade scenarios for SAS Federation Server Manager are addressed during the normal upgrade process. Review UpdateInstructions.html to take actions such as installation of SAS Data Management Data Server and configuration of SAS Federation Server Manager on the mid-tier.

Chapter 4

Post-Migration and Upgrade Tasks

SAS Federation Server

Refresh SQL Logging

No matter the type of migration, you must always refresh SQL Logging because the path to the SQL_LOG database is no longer valid after migration. You should perform this task even if the migration was automated, or if a 4.2 to 4.2 migration was performed. Use the following task to refresh SQL Logging in SAS Federation Server 4.2:

1. Delete the SQL_LOG data service using one of the following methods:
   a. Delete the SQL_LOG data service in SAS Federation Server Manager: Locate the federation server object in the tree, and delete the associated SQL_LOG data service.
   b. Issue a DROP DATA SERVICE command using administrative DDL: **`DROP DATA SERVICE SQL_LOG CASCADE`**.
2. Stop and restart SAS Federation Server. Upon server restart, a new SQL_LOG data service is created with a correct path to the SQL Logging database.

Create a Shared Login Account

PROC ASEXPORT does not recognize shared login accounts and as a result, shared logins are not exported. Therefore, you must create the new account as a shared login group using SAS Management Console. The shared login group serves as the actual shared login account, so the name of the group object should reflect the phrase ‘shared login’. The shared

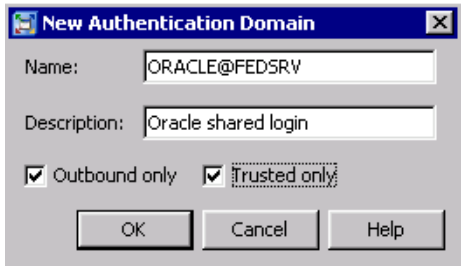
1. On the **Plug-ins** tab, select **User Manager**.

2. Right-click and select **New** ⇨ **Group**.
3. In the Properties dialog box:
   a. On the **General** tab, enter a name for the shared login (for example, *Oracle Shared Login for FedServer*).
   b. On the **Members** tab, add users and groups who will use the shared login.
   c. On the **Accounts** tab, add the account and login information.
      - **Authentication Domain**: The authentication domain must be created using this format: **`<data_service_domain>@<shared_login_key>`**. For example, if the domain for the data service is ORACLE and the shared login key is FEDSRV, then the shared login domain must be **`ORACLE@FEDSRV`**.

        Note: If you do not know your shared login key, check Federation Server properties, **Security** tab in SAS Federation Server Manager, or use the CONFIG_DATA_SERVICES information view for SAS Federation Server. The shared login key is reflected in the DATA column for the '__SERVER__' data service.

        Select **Outbound only** and **Trusted only** for the domain.

      Figure 4.1 *New Shared Login Authentication Domain*



   d. On the **Authorizations** tab, ensure that the SAS Administrators group has these permissions:
      - **ManageMemberMetadata**
      - **ManageCredentialsMetadata**
      - **ReadMetadata**
      - **WriteMetadata**

System User Accounts

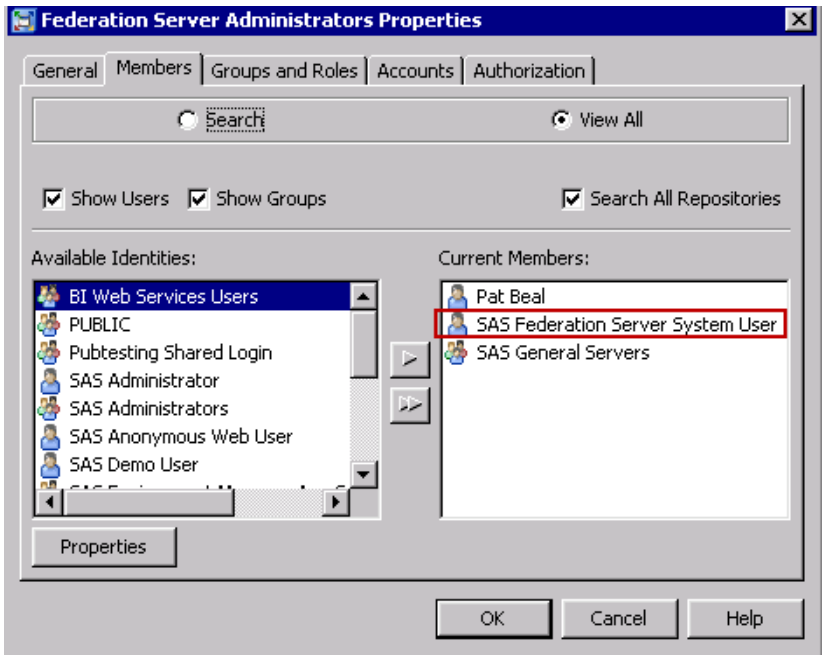
A SystemUsers option set is not configured in SAS Federation Server 4.2 as it has been in previous releases. For SAS Federation Server 4.2, add your system user to the Federation Server Administrators group in SAS Metadata Server.

1. Identify your system users from the 3.2 configuration in **`C:\SAS\Config\Lev1\FederationServer\etc\dfs_serv_common.xml`**. Here is an example:

```
<SystemUsers>
    <Option name="Account">CARYNT\###adm</Option>
    <Option name="Account">CARYNT\###test</Option>
</SystemUsers>
```

2. Add the system user, or users, to the Federation Server Administrators group in SAS Metadata Server. Using SAS Management Console, navigate to the Federation Server Administrators group by selecting **Environment Management** ⇨ **User Manager**, and select the **Federation Server Administrators** group in the right pane.
3. Open **Federation Server Administrators Properties** and select the **Members** tab.
4. Select your system user from **Available Identities** and click the arrow to move the user to the **Current Members** of the Federation Server Administrators group.

Figure 4.2 *Federation Server Administration Properties*



5. Click **OK** when you are finished adding users.

Validation Log

After exporting data from DataFlux Authentication Server to SAS Metadata Server, the SAS Deployment process runs a validation program that verifies the content that was moved successfully and logs any errors, if they occur. The validation log provides a list of objects that were not migrated, including users, user logins and groups. The results are logged in a file called **sqlfpkg_serv_%d_%S{hostname}_%S{pid}.log**, located with SAS Federation Server logs. Here is the naming convention for the log name:

Where:

- %d is the date
- %S{hostname} is the name of the host
- %S{pid} is the process ID of the script starting the federation server

The validation program is located in the **`/etc/migrate`** directory of SAS Federation Server. To perform a manual validation, run asexport_default_validate.sas in a SAS session and specify connection options to the DataFlux Authentication Server and SAS Metadata Server.

Validation is also run at SAS Federation Server start-up to ensure that there are no issues with the newly migrated objects in the federation server environment. An empty log file indicates success. There are no issues to report. Once it has been determined that migration was successful, you can turn off this logger by removing the following section from dfs_log.xml:

```
<!-- Application message logger (migration information) -->
  <logger name="App.SQLFPkg.UTL">
     <level value="Debug"/>
     <appender-ref ref="SQLFPkgLog"/>
  </logger>
```

See *SAS Federation Server: Administrator's Guide*, "Server Logging Configuration" for additional details.

Residual Server Services

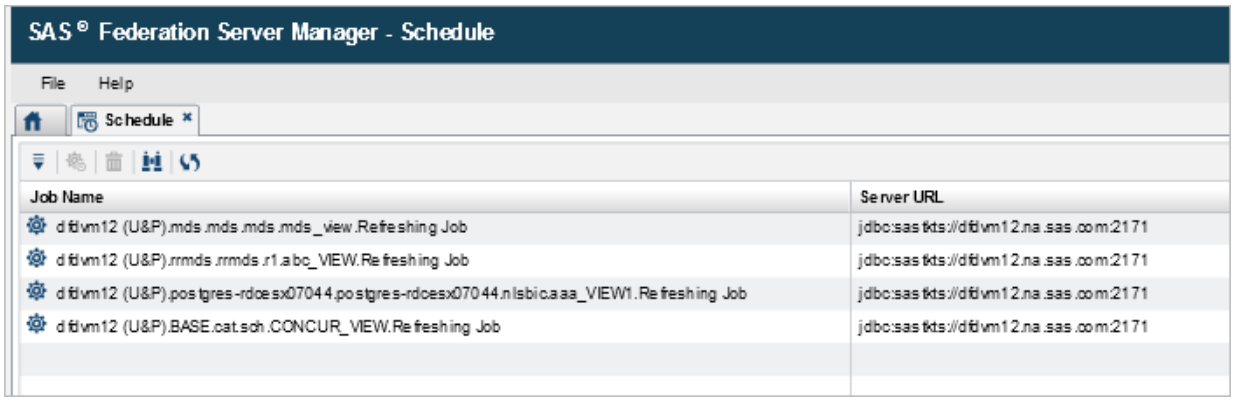
Because of the nature of migration, previous versions of DataFlux Authentication Server and SAS Federation Server, including SAS Federation Server Manager, are not removed during the upgrades. Therefore, you might see residual services or daemons in your environment. To remove these, you must uninstall the older versions of DataFlux Authentication Server, SAS Federation Server, and SAS Federation Server Manager. If any custom configurations were made to your environment, you might want to copy your configuration files before removing the software.

SAS Federation Server Manager

SAS Federation Server Manager Scheduled Jobs

After SAS Federation Server Manager 4.2 has been installed, you must re-create any cache refresh scheduled jobs that were running in the previous version. Scheduled jobs include custom CRON schedules. To view scheduled jobs, click the **Schedule** icon on the **Home** tab toolbar. The **Schedule** tab opens from where you can select a job to determine its schedule.

Figure 4.3 *SAS Federation Server Manager Scheduled Jobs*



Chapter 5

Wire Protocol Drivers

Updating ODBC Drivers

Wire Protocol ODBC Drivers

SAS Federation Server 4.2 is installed with release 7.1.5 of the Wire Protocol ODBC drivers. All of the existing ODBC DSNs should use the new Wire Protocol ODBC drivers and modifications are not necessary. However, if you are running ODBC on UNIX, you must make some minor modifications.

Note: If performing an upgrade from 3.2 to 4.2, the existing odbc.ini is copied to the **`SASHome/SASFederationServer/4.2/fedserver/etc`** directory for the 4.2 installation.

Modifying ODBC for UNIX

To use the new DataFux branded drivers, take one of the following actions:

- Configure the existing odbc.ini file to point to the new drivers in the SAS Home directory. For example, change the **`Driver=`** value as shown in this example:

  ```
  Driver=<4.2_SASHome>/SASFederationServer/4.2/fedserver/lib/FXora27.so
  ```

- Use the **dfdbconf** tool to configure existing data sources to use the new drivers. You should already have ODBCINI and ODBCINST set from a previous installation. If using dfdbconf, you must export the ODBCINI environment variable. The environment variable for ODBCINST is set when you execute **dfsadmin** for SAS Federation Server 4.2. Here are examples of the syntax:

  ```
  export ODBCINI=<4.2_SASHome>/SASFederationServer/4.x/fedserver/etc/odbc.ini
  export ODBCINI=<4.2_SASHome>/SASFederationServer/3.x/fedserver/etc/odbc.ini
  ```

Appendix 1

ASEXPORT Procedure

Overview: ASEXPORT Procedure

The ASEXPORT procedure is a SAS procedure used to migrate metadata from DataFlux Authentication Server to SAS Metadata Server. The procedure supports direct object migration through the SAS Open Metadata Interface. It also supports the creation of an export package that is compatible with PROC METADATA.

The following steps illustrate the workings of the ASEXPORT procedure:

1. The META= connection and filter parameters are used to connect to SAS Metadata Server..
2. The AS= connection and filter parameters are used to connect to DataFlux Authentication Server.
3. The MATCH, MATCH SINGLETON, ADD, and DELETE statements use these working sets to build up the mappings between DataFlux Authentication Server and SAS Metadata Server objects.
4. The LIST statement lists them.

5. The EXPORT statement exports them to a file, forwards them to the SAS Metadata Server, or both.
6. The file created by the EXPORT statement can be used directly by the METADATA procedure as its IN= procedure option.

Concepts: ASEXPORT Procedure

Overview

The matches between DataFlux Authentication Server and SAS Metadata Server objects are managed internally by the relationships in the tabular data represented in the following three schemas:

- AS Schema
- META Schema
- X Schema

Note that the maximal set of working objects available for export is controlled by the various filters specified on the procedure statement.

AS Schema

The AS schema includes the working set of DataFlux Authentication Server objects that are extracted using the initial filters specified in the AS(FILTER) procedure suboptions. The AS schema is a one-to-one tabular snapshot of Authentication Server objects read in using the META/FILTER options.

This schema consists of the following tables:

DOMAINS
: extracted using the AS(FILTER(DOMAINS)) suboption.

USERS
: extracted using the AS(FILTER(USERS)) suboption.

GROUPS
: extracted using the AS(FILTER(GROUPS)) suboption.

LOGINS
: extracted using the AS(FILTER(LOGINS)) suboption.

The AS schema contains a representation of the DataFlux Authentication Server objects currently in the working set of source objects. These objects are available for selection into the working set of export mappings in the X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP tables. The schema is displayed in the following sample:

```
create table AS.DOMAINS
(
   NAME              NVARCHAR(256)  NOT NULL,
   NAME_N            NVARCHAR(256)  NOT NULL,
   "DESC"            NVARCHAR(256)  NOT NULL,
   IS_CS_USERID      NCHAR(1)       NOT NULL,
   IS_DQ_USERID      NCHAR(1)       NOT NULL,
```

```
   IS_UPN_USERID     NCHAR(1)       NOT NULL
);
create table AS.USERS
(
   ID                NCHAR(32)      NOT NULL,
   NAME              NVARCHAR(256)  NOT NULL,
   NAME_N            NVARCHAR(256)  NOT NULL,
   "DESC"            NVARCHAR(256)  NOT NULL,
   ENABLED           NCHAR(1)       NOT NULL
);
create table AS.LOGINS
(
   FQLN              NVARCHAR(256)  NOT NULL,
   DOMAIN_N          NVARCHAR(256)  NOT NULL,
   NAME              NVARCHAR(256)  NOT NULL,
   USER_ID           NCHAR(32)      NOT NULL
);
create table AS.GROUPS
(
   ID                NCHAR(32)      NOT NULL,
   NAME              NVARCHAR(256)  NOT NULL,
   NAME_N            NVARCHAR(256)  NOT NULL,
   "DESC"            NVARCHAR(256)  NOT NULL,
   OWNER_ID          NCHAR(32)
);
```

META Schema

The META schema includes the working set of SAS Metadata Server objects extracted using the initial filters specified in the META(FILTER) procedure suboptions.

This schema consists of the following tables:

DOMAINS
: extracted using the META(FILTER(DOMAINS)) suboption.

USERS
: extracted using the META(FILTER(GROUPS)) suboption.

GROUPS
: extracted using the META(FILTER(GROUPS)) suboption.

LOGINS
: extracted using the META(FILTER(LOGINS)) suboption.

The META schema contains a representation of the SAS Metadata Server objects currently in the working set of destination objects. These objects are available for selection into the working set of export mappings in the X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP tables. The schema is displayed in the following sample:

```
create table META.DOMAINS
(
   ID                NCHAR(17)      NOT NULL,
   AS_ID             NVARCHAR(128),
   NAME              NVARCHAR(60)   NOT NULL,
   NAME_N            NVARCHAR(60)   NOT NULL,
   "DESC"            NVARCHAR(200)  NOT NULL,
```

```
   OUTBOUND_ONLY     NCHAR(1)       NOT NULL,
   TRUSTED_ONLY      NCHAR(1)       NOT NULL
);
create table META.USERS
(
   ID                NCHAR(17)      NOT NULL,
   AS_ID             NCHAR(32),
   NAME              NVARCHAR(60)   NOT NULL,
   NAME_N            NVARCHAR(60)   NOT NULL,
   "DESC"            NVARCHAR(200)  NOT NULL
);
create table META.LOGINS
(
   ID                NCHAR(17)      NOT NULL,
   AS_ID             NVARCHAR(128),
   FQLN              NVARCHAR(128)  NOT NULL,
   NAME              NVARCHAR(60)   NOT NULL,
   "DESC"            NVARCHAR(200)  NOT NULL,
   DOMAIN_ID         NCHAR(17)      NOT NULL,
   OWNER_ID          NCHAR(17)      NOT NULL,
   TRUSTED_ONLY      NCHAR(1)       NOT NULL
);
create table META.GROUPS
(
   ID                NCHAR(17)      NOT NULL,
   AS_ID             NVARCHAR(32),
   NAME              NVARCHAR(60)   NOT NULL,
   NAME_N            NVARCHAR(60)   NOT NULL,
   "DESC"            NVARCHAR(200)  NOT NULL
);
```

X Schema

The X schema includes normalized content, views, and joined result sets produced from matches between objects represented in the AS and META schemas.

This schema consists of the following tables or views:

DOMAIN_MAP
: contains the working set of (AS:Domain, OMSOBJ:AuthenticationDomain) domain mappings currently queued for export.

USER_MAP
: contains the working set of (AS:Group, OMSOBJ:IdentityGroup) group mappings currently queued for export.

GROUP_MAP
: contains the working set of (AS:Group, OMSOBJ:IdentityGroup) group mappings currently queued for export.

AS_LOGINS_N
: contains views of AS.LOGINS with additional FQLN_N column where the column contains a normalized fully qualified login name that can be matched with logins in MS.LOGINS. Login name qualification and normalization is governed by the naming rules inferred from the AS.DOMAINS(IS_CS_USERID, IS_DQ_USERID, IS_UPN_USERID) columns.

MS_LOGINS_N
: contains views of MS.LOGINS with additional FQLN_N column where the column contains a normalized fully qualified login name that can be matched with logins in AS.LOGINS. Login name qualification and normalization is governed by the naming rules inferred from the AS.DOMAINS(IS_CS_USERID, IS_DQ_USERID, IS_UPN_USERID) columns.

The X schema contains the working set of DataFlux Authentication Server:SAS Metadata Server export mappings. These mappings are used along with utility tables to assist in matching and selection criteria when using the MATCH, MATCH SINGLETON, ADD, and REMOVE statements.

The contents are listed in following table:

Table A1.1 *X Schema Contents*

Table or View	Description
X.DOMAIN_MAP	Current working set of domain object mappings.
X.USER_MAP	Current working set of user object mappings.
X.GROUP_MAP	Current working set of group object mappings.
X.AS_LOGINS_N	View of AS.LOGINS with normalized fully qualified login name column, FQLN_N.
X.MS_LOGINS_N	View of META.LOGINS with normalized fully qualified login name, FQLN_N.

The schema is displayed in the following sample:

```
create table X.DOMAIN_MAP
(
   AS_NAME              NVARCHAR(256)  NOT NULL,
   AS_NAME_N            NVARCHAR(256)  NOT NULL,
   AS_DESC              NVARCHAR(256)  NOT NULL,
   AS_IS_CS_USERID      NCHAR(1)       NOT NULL,
   AS_IS_DQ_USERID      NCHAR(1)       NOT NULL,
   AS_IS_UPN_USERID     NCHAR(1)       NOT NULL,
   META_ID              NCHAR(17),
   META_AS_ID           NVARCHAR(128),
   META_NAME            NVARCHAR(60)   NOT NULL,
   META_NAME_N          NVARCHAR(60)   NOT NULL,
   META_DESC            NVARCHAR(200)  NOT NULL,
   META_OUTBOUND_ONLY   NCHAR(1)       NOT NULL,
   META_TRUSTED_ONLY    NCHAR(1)       NOT NULL
);
create table X.USER_MAP
(
   AS_ID                NCHAR(32)      NOT NULL,
   AS_NAME              NVARCHAR(256)  NOT NULL,
   AS_NAME_N            NVARCHAR(256)  NOT NULL,
   AS_DESC              NVARCHAR(256)  NOT NULL,
   AS_ENABLED           NCHAR(1)       NOT NULL,
   META_ID              NCHAR(17),
```

```
   META_AS_ID           NCHAR(32),
   META_NAME            NVARCHAR(60)   NOT NULL,
   META_NAME_N          NVARCHAR(60)   NOT NULL,
   META_DESC            NVARCHAR(200)  NOT NULL
);
create table X.GROUP_MAP
(
   AS_ID                NCHAR(32)      NOT NULL,
   AS_NAME              NVARCHAR(256)  NOT NULL,
   AS_NAME_N            NVARCHAR(256)  NOT NULL,
   AS_DESC              NVARCHAR(256)  NOT NULL,
   AS_OWNER_ID          NCHAR(32),
   META_ID              NCHAR(17),
   META_AS_ID           NCHAR(32),
   META_NAME            NVARCHAR(60)   NOT NULL,
   META_NAME_N          NVARCHAR(60)   NOT NULL,
   META_DESC            NVARCHAR(200)  NOT NULL
);
create view X.AS_LOGINS_N as
   select AL.*,
          case
             when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FF' then
                upper(AL.NAME)
             when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FT' then
                AL.NAME
             when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'TF' then
                upper(AL.NAME) || '@' || AL.DOMAIN_N
             else
                AL.NAME || '@' || AL.DOMAIN_N
          end as "FQLN_N"
   from AS.LOGINS        AL,
        X.DOMAIN_MAP_ALL DX
   where AL.DOMAIN_N = DX.AS_NAME_N
;
create view X.MS_LOGINS_N as
   select ML.*,
          case
             when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FF' then
                upper(ML.NAME)
             when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'FT' then
                ML.NAME
             when (DX.AS_IS_DQ_USERID || DX.AS_IS_CS_USERID) = 'TF' then
                upper(ML.NAME) || '@' || DX.AS_NAME_N
             else
                ML.NAME || '@' || DX.AS_NAME_N
          end as "FQLN_N"
   from META.LOGINS      ML,
        X.DOMAIN_MAP_ALL DX
   where ML.DOMAIN_ID = DX.META_ID
;
```

Syntax: ASEXPORT Procedure

Requirement: The target SAS Metadata Server and the source DataFlux Authentication Server must be running. Connection information for these servers must be available. A trusted user must also be available.

Tip: PROC ASEXPORT supports RUN-group processing.

See: Open Metadata Interface in *SAS Language Interfaces to Metadata*

PROC ASEXPORT<*proc-options*>;
MATCH DOMAIN | USER | GROUP / <*match-options*>;
MATCH SINGLETON DOMAIN | USER | GROUP / <*match-options*>;
ADD DOMAIN | USER | GROUP / <*add-options*>;
REMOVE DOMAIN | USER | GROUP / <*remove-options*>;
LIST <*type-list*> / <*list-options*>;
EXPORT / <*export-options*>;
UNDO;

Statement	Task	Example
PROC ASEXPORT	Export or migrate DataFlux Authentication Server content.	Ex. 1
MATCH	Match DataFlux Authentication Server objects with an equivalent SAS Metadata Server objects and place the matches into the working set of export mappings.	Ex. 1
MATCH SINGLETON	Match a single DataFlux Authentication Server object with an equivalent SAS Metadata Server object and place the match into the working set of export mappings.	Ex. 1
ADD	Add DataFlux Authentication Server objects that are unmatched in the working set of SAS Metadata Server objects to the working set of export mappings.	Ex. 1
REMOVE	Remove objects matching the specified criteria from the working set of export mappings.	Ex. 1
LIST	List the current working set of export mappings in the SAS log.	Ex. 1
EXPORT	Export the working set of export mappings and clear the mapping tables, X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP.	Ex. 1
UNDO	Undo changes to the working set of export mappings. These mappings result from the most recent MATCH, MATCH SINGLETON, ADD, or	Ex. 1

Statement	Task	Example
	REMOVE statement that was not followed by a RUN or EXPORT statement.	

PROC ASEXPORT Statement

Exports or migrates DataFlux Authentication Server content.

Syntax

PROC ASEXPORT

<METACON=(*SAS-Metadata-Server-connection-arguments*)>

<ASCON=(*DataFlux-Authentication-Server-connection-arguments*)>

<OUT=*fileref*>

<HEADER=NONE | SIMPLE | FULL>

<VERBOSE>

;

Optional Arguments

METACON=(*metadata-server-connection-arguments*)

Server connection arguments establish communication with SAS Metadata Server. The metadata system options are used in place of omitted attributes.

FILTER=*(filter-strings)*

is the set of filter strings used to retrieve the working set of SAS Metadata Server objects using a templated GetMetadataObjects query with a XMLSelect search criteria. There is one filter per object type. If a filter is "*" or is omitted, then no subsetting is done when retrieving the objects and all objects of the associated metadata type are retrieved.

METACON uses the following filter strings:

DOMAINS="*XMLSelect-search-filter*"

specifies a valid XMLSelect search= string used to match objects of type AuthenticationDomain.

USERS="*XMLSelect-search-filter*"

specifies a valid XMLSelect search= string used to match objects of type Person.

GROUPS="*XMLSelect-search-filter*"

specifies a valid XMLSelect search= string used to match objects of type IdentityGroup.

Restriction The GROUPS option is not supported for SAS Business Data Network.

LOGINS="Select-filter"

specifies the search criteria used to match objects of type Login. The filter is the value of the Search= attribute of the Logins association specified in the query template.

PASSWORD="*password*"
is the password for the authenticated user ID on SAS Metadata Server.

Alias PW= or METAPASS=

PORT=*number*
is the TCP port that SAS Metadata Server listens to for requests. This port number was used to start the SAS Metadata Server.

Alias METAPORT=

Requirement Do not enclose the port number in quotation marks.

REPOSITORY=*repository-name*
is the name of the repository to use for all SAS Metadata Server requests. The repository name must be *foundation*.

Alias METAREPOSITORY=

SERVER="*host-name*"
is the host name or network IP address of the computer that hosts SAS Metadata Server. The value LOCALHOST can be used if the SAS session is connecting to SAS Metadata Server on the same computer.

Alias METASERVER= or HOST= or IPADDR=

USER="*authenticated-user-ID*"
is an authenticated user ID on SAS Metadata Server. SAS Metadata Server supports several authentication providers.

Alias METAUSER= or ID= or USERID=

Alias META=

ASCON=(*authentication-server-connection-arguments*)
server connection arguments establish communication with DataFlux Authentication Server.

FILTER=(*filter-strings*)
is the set of filter strings used to retrieve the working set of DataFlux Authentication Server objects. Filter strings are simple name and value pairs or value lists where values are ODBC pattern strings or constants. There is one filter per object type. If a filter is "*" or is omitted, then no subsetting is done when retrieving the objects and all objects of the associated type are retrieved.

ASCON uses the following filter strings:

DOMAINS="*domains-filter*"
specifies a valid domain search filter. The following filter columns are supported :

caseSensitivity=*TRUE|T|YES|1|FALSE|F|NO|0*	specifies to select domains with principal identities matching the specified case sensitivity Boolean. The specified value is compared as case insensitive.
description=*domain-description*	specifies to select domains that pass the specified description pattern. The

	specified value is compared as case insensitive and should be quoted.
domain=*domain-name* | *(domain-name1, domain-name2 ...)*	specifies to select domains that meet the specified pattern. Values are compared as case insensitive and can be quoted.
partOfLogin=*TRUE|T|YES|1| FALSE|F|NO|0*	specifies to select domains that match the specified part of login Boolean. The specified value is compared as case insensitive.
isUPN=*TRUE|T|YES|1|FALSE| F|NO|0*	specifies to select domains that match the specified is UPN Boolean. The specified value is compared as case insensitive.

USERS="*XMLSelect-search-filter*"
specifies a valid user search filter. The following filter columns are supported:

subject=*user-name* | *(user-name1, user-name2 ...)*	specifies to select users that match the specified names. Values are compared case insensitive and can be quoted.
identifier=*user-identifier* | *(user-identifier1, user-identifier2 ...)*	specifies to select users that match the unique user identifiers. Values are compared as case insensitive.
description=*user-description*	specifies to select users that pass the specified user description pattern. Values are compared as case insensitive and should be quoted.
enabled=*TRUE|T|YES|1| FALSE|F|NO|0*	specifies to TRUE if the user is enabled.

GROUPS="*XMLSelect-search-filter*"
specifies a valid group search filter. The following filter columns are supported:

group=*group-name* | *(group-name1, group-name2 ...)*	specifies the name of group. Values are compared as case insensitive and can be quoted.
identifier=*group-identifier* | *(group-identifier1, group-identifier2 ...)*	specifies to select groups that match the unique group identifiers. Values are compared as case insensitive.
description=*group-description*	specifies to select groups that pass the specified group description pattern. Values are compared as case insensitive and should be quoted.
ownerName=*group-owner-name*	specifies the name of group's user owner. The value is compared as case insensitive and can be quoted.

Restriction The GROUPS option is not supported for SAS Business Data Network.

LOGINS=”*Select-filter*”
specifies a valid user login search filter. The filter is the value of the Search= attribute of the Logins association specified in the query template. The select filter is a domain name or list of domain names, specified as follows:

```
domain-name | (domain-name1, domain-name2 …)
```

PASSWORD=“*password*”
is the password for the authenticated user ID on DataFlux Authentication Server.

Alias PW=

PORT=*number*
is the TCP port that DataFlux Authentication Server listens to for requests. This port number was used to start the DataFlux Authentication Server.

Requirement Do not enclose the port number in quotation marks.

SERVER="*host-name*"
is the host name or network IP address of the computer that hosts DataFlux Authentication Server. The value LOCALHOST can be used if the SAS session is connecting to DataFlux Authentication Server on the same computer.

Alias HOST= or IPADDR=

URI="*IOM-uri*"
is the complete IOM uri specification of DataFlux Authentication Server. A URI can be specified instead of the server and port.

USER="*authenticated-user-ID*”
is an authenticated user ID on DataFlux Authentication Server. DataFlux Authentication Server supports several authentication providers.

Alias ID= or USERID=

OUT=*fileref*
specifies an XML file used by the EXPORT statement to store either the output result returned by SAS Metadata Server or the input that would have been submitted to SAS Metadata Server when exported using the NOFORWARD option. The value must be a fileref, not a pathname. Therefore, you must first submit a FILENAME statement to assign a fileref to a pathname. In most cases, the output XML string is identical to the input XML string, with the addition of the requested values within the XML elements.

If the OUT= argument is omitted and the VERBOSE option is specified, PROC ASEXPORT output is written to the SAS log.

Note: PROC ASEXPORT can generate large XML output. You might need to specify a large LRECL value or RECFM=N (streaming output) to avoid truncation of long output lines.

Note: Under z/OS, fixed-length records in the XML method call are not supported by PROC METADATA. Specify RECFM=V (or RECFM=N as suggested above) when you create the XML method call.

Alias OUTFILE=

Restriction SAS Business Data Network does not support z/OS connections.

HEADER= NONE | SIMPLE | FULL
specifies whether to include an XML header in the output FILE= and OUT= XML files. The declaration specifies the character-set encoding for web browsers and XML parsers to use when processing national language characters in the output XML file.

NONE
omits an encoding declaration. Web browsers and parsers might not handle national language characters appropriately.

SIMPLE
inserts an XML header that specifies the XML version number: This is the default value when the HEADER= argument is not specified.

FULL
inserts an XML declaration that represents the encoding that was specified when creating the output XML file. The source for the encoding varies, depending on the operating environment. In general, the encoding value is taken from the ENCODING= option specified in the FILENAME statement, or from the ENCODING= system option.

SAS attempts to use that encoding for the output XML file (and in the XML header). The encoding can vary. A single encoding can have multiple names or aliases that can appear in the XML header. These names might not be valid or recognized in all XML parsers. When generating the encoding attribute in the XML header, SAS attempts to use an alias that will be recognized by Internet Explorer. If the alias is not found, SAS attempts to use a name that will be recognized by Java XML parsers. If the name is not found, SAS uses an alias by which SAS will recognize the encoding. For information about encoding and transcoding, see *SAS National Language Support (NLS): Reference Guide*.

VERBOSE
specifies to print input or output XML strings to the SAS log.

MATCH Statement

Matches DataFlux Authentication Server objects with an equivalent SAS Metadata Server objects and places the matches into the working set of export mappings. The MATCH statement name is followed by the type of object being matched for export. This object type can be DOMAIN, USER, or GROUP. The MATCH statement has two options, CRITERIA= and LOG.

Syntax

MATCH <*type*> / <*match-options*>;
<CRITERIA="*match-criteria*">
<LOG>

Optional Arguments

CRITERIA="*match-criteria*"
specifies match criteria used to associate DataFlux Authentication Server objects and SAS Metadata Server objects for insertion into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched.

The following table lists those entities per object type:

Table A1.2 *Match Entities*

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in AS.DOMAINS and META.DOMAINS
USERS	All columns in AS.USERS, META.USERS, X.AS_LOGINS_N, and X.MS_LOGINS_N
GROUPS	All columns in AS.GROUPS and META.GROUPS

The MATCH statement *always* joins objects using the default matching criteria per object type and then subsets based on the CRITERIA= WHERE clause specified. If omitted, a CRITERIA= value of "1=1" is implied so that no further subsetting occurs.

The following table documents the default match criteria per object type:

Table A1.3 *MATCH Criteria*

Type	Default CRITERIA= value
DOMAINS	(AS.DOMAINS.NAME_N=META.DOMAINS.NAME_N) and (META.DOMAINS.AS_ID is NULL)
USERS	(X.AS_LOGINS_N.USER_ID=AS.USERS.ID) and (X.MS_LOGINS_N.FQLN_N=X.AS_LOGINS_N.FQLN_N) and (META.USERS.ID=X.MS_LOGINS_N.OWNER_ID) and (META.USERS.AS_ID is NULL)
GROUPS	(AS.GROUPS.NAME_N=META.GROUPS.NAME_N) and (META.GROUPS.AS_ID is NULL)

LOG
specifies to print match results in the SAS log.

MATCH SINGLETON Statement

Matches a single DataFlux Authentication Server object with an equivalent SAS Metadata Server object and places the match into the working set of export mappings. The MATCH SINGLETON statement name is followed by the type of object being matched for eventual export. The object type can be DOMAIN, USER, or GROUP. The MATCH SINGLETON statement has two options, CRITERIA and LOG.

Syntax

MATCH SINGLETON <*type*> | <*match-singleton-options*>;
<CRITERIA="*match-criteria*">

<LOG>

Optional Arguments

CRITERIA="*match-criteria*"

specifies match criteria used to associate a single DataFlux Authentication Server object with a single SAS Metadata Server object for insertion into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched.

The following table lists those entities per object type:

Table A1.4 *MATCH SINGLETON Entities*

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in AS.DOMAINS and META.DOMAINS
USERS	All columns in AS.USERS, META.USERS, X.AS_LOGINS_N, and X.MS_LOGINS_N
GROUPS	All columns in AS.GROUPS and META.GROUPS

The MATCH SINGLETON statement *always* joins objects using the default matching criteria per object type and then subsets based on the user's CRITERIA= WHERE clause. If omitted, a CRITERIA= value of "1=1" is implied such that no further subsetting occurs. Specifying criteria that produces more than one match results in an error, and no additional mapping is queued for export. The following table documents the default match singleton criteria per object type:

The following table documents the default match singleton criteria per object type:

Table A1.5 *MATCH SINGLETON Criteria*

Type	Default CRITERIA= value
DOMAINS	*The domain is neither already exported nor queued for export in the current working set of export mappings.*
USERS	(X.AS_LOGINS_N.USER_ID=AS.USERS.ID) and (X.MS_LOGINS_N.OWNER_ID= META.USERS.ID) and *The user is neither already exported nor queued for export in the current working set of export mappings.*
GROUPS	*The group is neither already exported nor queued for export in the current working set of export mappings.*

LOG

specifies to print match results in the SAS log.

ADD Statement

Adds DataFlux Authentication Server objects that are unmatched in the working set of SAS Metadata Server objects to the working set of export mappings. The ADD statement name is followed by the type of object being added for export. The object type can be DOMAIN, USER, or GROUP. The ADD statement has two options, CRITERIA and LOG.

Syntax

ADD <*type*> | <*add-options*>;

<CRITERIA="*match-criteria*”>

<LOG>

Optional Arguments

CRITERIA="*match-criteria*"

specifies criteria used to select DataFlux Authentication Server objects into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched.

The following table lists those entities per object type:

Table A1.6 *ADD Entities*

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in AS.DOMAINS
USERS	All columns in AS.USERS, X.AS_LOGINS_N
GROUPS	All columns in AS.GROUPS

The ADD statement *always* selects AS objects using the default criteria per object type and then subsets based on the CRITERIA= WHERE clause specified. If omitted, a CRITERIA= value of “1=1” is implied such that no further subsetting occurs.

The following table documents the default add criteria per object type:

Table A1.7 *ADD Criteria*

Type	Default CRITERIA= value
DOMAINS	The domain is neither already exported nor queued for export in the current working set of export mappings.

Type	Default CRITERIA= value
USERS	(X.AS_LOGINS_N.USER_ID=AS.USERS.ID) and *The user is neither already exported nor queued for export in the current working set of export mappings.*
GROUPS	*The group is neither already exported nor queued for export in the current working set of export mappings.*

LOG
specifies to print ADD statement results in the SAS log.

REMOVE Statement

Removes objects matching the specified criteria from the working set of export mappings. The REMOVE statement name is followed by the type of objects being removed from the working set of export mappings. The object type can be DOMAIN, USER, or GROUP. The REMOVE statement has two options, CRITERIA and LOG.

Syntax

REMOVE <*type*> / <*remove-options*>;
<CRITERIA="*match-criteria*">
<LOG>

Optional Arguments

CRITERIA="*match-criteria*"
specifies criteria used to select DataFlux Authentication Server objects into the working set of export mappings. The criteria must be valid SQL WHERE syntax that does not use the WHERE keyword. It must reference only the SQL entities available for the type of objects being matched:

```
remove domains / criteria="x.domain_map.as_name_n='EURNET'" log;
```

The following table lists those entities per object type:

Table A1.8 *REMOVE Criteria*

Type	SQL Entities Available in Match Criteria WHERE Clause
DOMAINS	All columns in X.DOMAIN_MAP
USERS	All columns in X.USER_MAP
GROUPS	All columns in X.GROUP_MAP

The MATCH statement always selects objects mapped for export (those accumulated via the prior MATCH, MATCH SINGLETON, and ADD statements) using the specified criteria. The default CRITERIA= value is always “1=1” such that all export mappings are cleared.

LOG
specifies to print REMOVE statement results in the SAS log.

LIST Statement

Lists the current working set of export mappings in the SAS log. The LIST statement name is optionally followed by the type of objects being listed. The object type can be DOMAIN, USER, or GROUP. The LIST statement has one option, VERBOSE.

Syntax

LIST <*type*> / <*list-options*>;
<VERBOSE>

Optional Argument

VERBOSE
verbose output.

EXPORT Statement

Exports the working set of export mappings and clears the mapping tables, which are X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP. EXPORT. EXPORT has four options, NOFORWARD, VERBOSE, NOVERBOSE, and NEWGROUPSUFFIX.

Syntax

EXPORT <*export-options*>;
<NOFORWARD>
<VERBOSE>
<NOVERBOSE>
<NEWGROUPSUFFIX=’*suffix-value*’>

Optional Arguments

NOFORWARD
prevents forwarding of generated XML to the metadata server. When NOFORWARD is specified, the OUT= file will contain SAS Metadata Server input XML. Otherwise, it will contain output response XML.

VERBOSE
specifies to print generated input or output response XML to the SAS log. The VERBOSE option is ignored if the NOVERBOSE is also specified. The VERBOSE option is implied if the procedure’s OUT= option is omitted because the log becomes the destination for generated or response XML.

NOVERBOSE
specifies to not print generated input or output response XML to the SAS log. The NOVERBOSE option overrides the VERBOSE option of the procedure and EXPORT statements. The NOVERBOSE option is ignored if the procedure's OUT= option is omitted.

NEWGROUPSUFFIX='*suffix-value*'
allows export of all groups into SAS Metadata Server without matching. Exports objects that have been added and matched, adding the specified string to the name of each new group exported. Care should be taken to avoid producing target group names exceeding 60 characters in length, which is the limit of the Name attribute of IdentityGroup objects.

Details

The EXPORT statement exports all export mappings and clears the mapping tables, which are X.DOMAIN_MAP, X.USER_MAP and X.GROUP_MAP.

Each new exported object and existing matched object is mapped in metadata using the ExternalIdentities association to an ExternalIdentity object with the following attributes:

- For new objects, ImportType='AuthenticationServer.Import'
- For matched or "tagged" objects, ImportType='AuthenticationServer.Match'
- Context='AuthenticationServer.ID'
- Name='AS:Server/*server-name*', where the server name consists of the fixed 'AS:Server/' prefix followed by the PUBLIC group identifier of the source DataFlux Authentication Server.

The export process creates mappings between source DataFlux Authentication Server objects and target SAS Metadata Server objects. Multiple DataFlux Authentication Server domains can map to the same SAS Metadata Server AuthenticationDomain object. Other object types map 1:1 in the two stores. However, exports from multiple DataFlux Authentication Server instances can also produce n:1 mappings. The Name attribute of the ExternalIdentity objects used in the mappings uniquely identifies the source DataFlux Authentication Server.

The EXPORT statement writes SAS Metadata Server output into the file specified by the OUT option or the SAS log if the VERBOSE procedure statement option is specified and the OUT= option is omitted. If the NOFORWARD option is specified, then the statement unconditionally writes input XML into the file specified by the OUT= option or the SAS log if OUT= is omitted. If the OUT= option is specified, then the XML is also written to the SAS log if the EXPORT statement's NOVERBOSE option is omitted and either the procedure's VERBOSE option or the EXPORT statement's VERBOSE option is specified.

UNDO Statement

Undoes changes to the working set of export mappings. These changes result from the most recent MATCH, MATCH SINGLETON, ADD, or REMOVE statement that was not followed by a RUN or EXPORT statement.

Syntax

UNDO;

Example: Exporting from a DataFlux Authentication Server to a SAS Metadata Server

Features: PROC ASEXPORT statement
MATCH SINGLETON statement
MATCH statement
ADD statement
LIST statement
EXPORT statement

Details

This example demonstrates the following actions:

- specify metadata values
- create explicit singleton matches between these two domains
- auto-match domains by name
- add remaining unmatched domains
- perform explicit user matching
- auto-match users by FQLN
- add remaining unmatched users
- list everything for review
- create an input file (per noforward) for PROC METADATA that we can review

Assign a file reference. The FILENAME statement assigns a libref to an external SAS library that contains a permanent SAS catalog.

```
filename asx 'C:\TableServer\asexport.xml';
```

Specify metadata values.

```
proc ASEXPORT meta=
              (
                 user='username' password='password'
                 server='localhost'
                 port=port_number
                 repos='repositoryID'
                 filter=(DOMAINS "*"
                         USERS   "*"
                         GROUPS  "*"
                         LOGINS  "Login[Domain/AuthenticationDomain
[@OutboundOnly='0']]")
              )
              as=
              (
                 server='localhost'
                 user='username'
```

```
                  pass='password'
                  port=port_number
                  filter=(DOMAINS "domain=(domain_names)"
                          USERS   "enabled=TRUE subject=(ADMUSER,
Shared_Login_Manager, tsadm, 'USER%')"
                          LOGINS  "(login IDs for included domains)")
              )
              verbose
              tracefile='C:\TableServer\asexport.trace' traceloc=SQL
traceflags='319'
              retain
              out=asx
              ;
```

Create explicit singleton matches between these two domains.

```
   match singleton DOMAIN / criteria="as.domains.name_n='LOCAL' and
meta.domains.name_n='domain_name'" log;
   match singleton DOMAIN / criteria="as.domains.name_n='UNIX' and
meta.domains.name_n='domain_name'" log;
```

Auto-match domains by name.

```
   match DOMAINS / log;
```

Add remaining unmatched domains.

```
   add DOMAINS / log;
```

Perform explicit user matching. Attempt at least one user that has a matching Login. Nothing should match.

```
   match singleton USER / criteria="as.users.name_n='SHARED_LOGIN_MANAGER'
and meta.users.name_n='FEDERATION SERVER SHARED LOGIN MANAGER'" log;
   match singleton USER / criteria="as.users.name_n='USER1' and
meta.users.name_n='TSADM'" log;
   match singleton USER / criteria="as.users.name_n='TSADM' and
meta.users.name_n='TSADM'" log;
```

Auto-match users by FQLN.

```
   match USERS / log;
```

Add remaining unmatched users.

```
   add USERS / log;
```

List everything for review.

```
   list DOMAINS USERS;
```

Create an input file (per noforward) for proc METADATA that we can review.

```
   export / noforward noverbose;
```

End processing of PROC ASEXPORT.

```
quit;
```