SAP security and deployment best practices in InfoSphere Information Server Pack for SAP Applications 7.1

Sergej Schuetz (sersch@de.ibm.com)
Software Architect
IBM

This tutorial shows how to deploy the SAP side components of the InfoSphere® Information Server Pack for SAP Applications 7.1. It covers the stage types and gives an overview of the relevant installation and security administration concepts.

Introduction

This tutorial accompanies "Security and deployment best practices for InfoSphere Information Server Packs for SAP applications, Part 1: A security primer," covering the changed security aspects, most notably the transition from SAP authorization profiles to roles.

SAP security in SAP Pack 7.1

During a project in which InfoSphere Information Server is used for data exchange with SAP, one or more technical SAP user accounts is needed for the DataStage® jobs to connect to the SAP system. Therefore, the ETL development team needs to work with the SAP basis administrator to obtain user IDs for the SAP system with the appropriate permissions.

All user accounts and authorizations in SAP are maintained separately for each SAP client. An SAP client is an isolated partition of the system identified by a three-digit number. All DataStage SAP connections operate on a given client, so all authorization rules need to be applied to the correct SAP client as well. Used accounts in SAP are managed using the transaction su01.

In addition to assigning basic properties like user name and password, you can also assign the authorizations that the user needs using this transaction.
Figure 1. Roles assigned to an SAP user

Using the InfoSphere Pack for SAP requires different authorizations depending on the stages you intend to use. These need to be configured appropriately by an SAP basis administrator.

Authorization profiles and roles

SAP systems have two concepts for user authorization:

- **Profile**—A profile is a collection of authorization objects, usually technically related. For example, the profiles B_ALE_ALL and S_IDOC_ALL give a user the permissions to perform ALE operations and process IDocs, respectively.
- **Role**—A role is a functional entity associated with a collection of authorization objects realized using a profile. Roles are usually targeted at specific tasks that certain users perform. Assigning a role to a user automatically generates a profile.

SAP Pack authorization requirements

Several authorization role templates are provided with the SAP Pack. The roles are made available as transport request files that can be directly imported into an SAP system.

The authorization roles provided for the SAP Pack are composed of standard SAP authorizations where possible, but also contain authorizations specifically configured for the use with the SAP Pack.

To provide basic level access, you have to additionally assign standard authorization profiles to the user as follows:
• S_IDOC_ALL and B_ALE_ALL to use the IDoc stage functionality
• Specific BAPI / RFM authorization requirements depending on the individual functions used in DataStage jobs that use the BAPI stage
• S_TMW_CREATE to use the Change and Transport System (CTS) functionality in the ABAP Extract stage. The user is also required to have a developer key when using CTS to upload ABAP programs.

The authorization roles provided with the SAP Pack are as follows:

Z-DS-ADM-ALL-V7-1
Z-DS-DESIGN-V7-1
Z-DS-DESIGN-ABAP-V7-1
Z-DS-DESIGN-BAPI-V7-1
Z-DS-DESIGN-IDOC-V7-1
Z-DS-DESIGN-RM-V7-1
Z-DS-RUNTIME-V7-1
Z-DS-RUNTIME-ABAP-V7-1
Z-DS-RUNTIME-BAPI-V7-1
Z-DS-RUNTIME-IDOC-V7-1

Z-DS-RUNTIME-IDOC-SERVER-V7-1

• Z-DS-ADM-ALL-V7-1 is the composite role that includes all sub-roles for the design-time and the runtime authorizations.
• Z-DS-DESIGN-V7-1 is the composite design-time role that contains all sub-roles needed to create and run SAP Pack jobs. It can be used in a development environment where tasks like job design and unit testing are performed.
• Z-DS-RUNTIME-V7-1 is the composite runtime role that contains only the sub-roles needed to run SAP Pack jobs. It is more restrictive and can be used in a production environment where only activities needed during the actual job run should be allowed.

Installing the provided SAP transport files

For instructions on how to install the SAP transport request files containing the authorization roles, refer to Installing the SAP server components for IBM InfoSphere Pack for SAP Applications 7.1.
Mapping the SAP authorizations to development, test, and production environments

On the development SAP system, DataStage jobs are designed and unit-tested. To perform these tasks, the technical SAP user needs design-time as well as runtime privileges for the stages to be used in the jobs to be developed.

The testing environment should simulate the production environment. On this system, the technical SAP user should be assigned only the runtime authorizations needed for the stages used in jobs that are to run in the production environment.

In the production environment, the most restrictive security policies are usually in place. As a result, only the absolutely necessary privileges should be granted to the technical SAP user, which means only the runtime authorizations needed for the stages used in the jobs running in production.

Detailed information on the different authorizations needed for each stage type at design and runtime can be found in the stage-specific sections below.

Stage-specific authorization details

This section contains specific information on authorizations needed for each stage, depending on the respective phase in the life cycle of the DataStage job. Use it as a reference for the predefined roles provided with the SAP Pack or as a guide for customizing authorization roles according to your needs.

Use SAP transaction PFCG to create or modify an authorization role or to adjust the imported authorization roles.

The Release column in the tables below denotes which SAP releases support the specific authorization object.

ABAP extract stage

Role Z-DS-DESIGN-ABAP-V7-1— ABAP stage authorizations (job design) are shown in Table 1. The role also contains the authorizations for running jobs.

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16 RFC_NAME: QOWK, RFC1, SALF, SAPLCRFC, SDIFRUNTIME, SDTB, SDTX, SIMG, SXBP, SXMI, SYST, TREX_ADMIN_TOOL, ZETL, ZETL_V7_1RFC_TYPE: FUGR</td>
<td>R/3 ECC 6</td>
</tr>
<tr>
<td>S_DEVELOP</td>
<td>BC_C</td>
<td>ABAP Workbench</td>
<td>ACTVT: 01, 02, 03, 06, 16</td>
<td>R/3</td>
</tr>
</tbody>
</table>
Table 2. ABAP stage authorizations for running jobs

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RFC_NAME: QOWK, RFC1, SALF, SDIFRUNTIME, SXBP, SXMI, SYST, ZETL, ZETL_V7_1RFC_TYPE: FUGR</td>
<td>ECC 6</td>
</tr>
<tr>
<td>S-devel</td>
<td>BC_C</td>
<td>ABAP Workbench</td>
<td>ACTVT: 03</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>OBJTYPE: *</td>
<td>ECC 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PROGOBJNAME: *</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>P_GROUP: *</td>
<td></td>
</tr>
<tr>
<td>S_TABU_DIS</td>
<td>BC_A</td>
<td>Table Maintenance</td>
<td>ACTVT: 03</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DISBERCLS: *</td>
<td>ECC 6</td>
</tr>
<tr>
<td>S_AMD_S_FCD</td>
<td>BC_A</td>
<td>System Authorizations</td>
<td>NADM</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ECI: 2</td>
<td>ECC 6</td>
</tr>
<tr>
<td>S_BTCH_JOB</td>
<td>BC_A</td>
<td>Background Processing: Operations On Background Jobs</td>
<td>JOBACTION: RELE</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JOBGROUP: *</td>
<td>ECC 6</td>
</tr>
<tr>
<td>S_DATASET</td>
<td>BC_A</td>
<td>Authorization for file access</td>
<td>ACTVT: 34</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FILENAME: *</td>
<td>ECC 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PROGRAM: Y*, Z*</td>
<td></td>
</tr>
<tr>
<td>S_XMI_PROD</td>
<td>BC_A</td>
<td>Authorization for External Management Interface</td>
<td>EXTCOMPANY: IBM Corp.</td>
<td>R/3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>EXTPRODUCT: DATASTAGE</td>
<td>ECC 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>INTERFACE: XBP</td>
<td></td>
</tr>
<tr>
<td>S_RFC_ADM</td>
<td>AAAB</td>
<td>Administration for RFC Destination</td>
<td>ACTVT: 01, 03, 36</td>
<td>ECC 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ICF_VALUE: * RFCDEST:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RFC_TYPE: *</td>
<td></td>
</tr>
</tbody>
</table>

**Note:**

- **S_DEVELOP**— You can adjust OBJNAME according to the naming convention you want to use for ABAP programs generated by the ABAP stage (for example, specify Z_DS* instead of *).
- **S_RFC_ADM**— You can adjust RFCDEST according to the naming conventions that you want to use for the RFC destinations used for communication with the ABAP stage.
- **S_TABU_DIS**— Assign this SAP-defined authorization profile to the user that configures the ABAP jobs. This profile grants the required authorizations to add the ABAP program by means of a transport request (CTS) to your SAP System. The user must have a developer key assigned to create transport requests.

**Role Z-DS-RUNTIME-ABAP-V7-1**

ABAP stage authorizations for running jobs are shown in Table 2.
S_ADMI_FCD | BC_A | System Authorizations | NADM | R/3 ECC 6
--- | --- | --- | --- | ---
S_BTCJOB | BC_A | Background Processing: Operations On Background Jobs | JOBACTN: RELE JOBGROUP: * | R/3 ECC 6
S_DATASET | BC_A | Authorization for file access | ACTVT: 34 FILENAME: * PROGRAM: Y*, Z* | R/3 ECC 6
S_XMI_PROD | BC_A | Authorization for External Management Interface | EXTCOMPANY: IBM Corp. EXTPRODUCT: DATASTAGE INTERFACE: XBP | R/3 ECC 6
S_RFC_ADM | AAAB | Administration for RFC Destination | ACTVT: 01, 03, 06 ICF_VALUE: *RFCDEST: *RFCTYPE: * | ECC 6

Note:

- **S_DEVELOP** — You can adjust OBJNAME according to the naming convention you want to use for ABAP programs generated by the ABAP stage (for example, specify z_ds* instead of *)
- **S_RFC_ADM** (ECC6 only) — This authorization is only needed if you enable automatic creation and deletion of the RFC destination in the ABAP stage. You can adjust RFCDEST according to the naming conventions you want to use for the RFC destinations used for communication with the ABAP stage.

**BAPI stage**

**Role Z-DS-DESIGN-BAPI-V7-1** — BAPI stage authorizations for job design are shown in Table 3. The role also contains the authorizations for running jobs.

**Table 3. BAPI stage authorizations for job design**

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16 RFC_NAME: BAPT, RFC1, SDIFRUNTIME, SEMS, SWOR, SYSTRFC_TYPE: FUGR</td>
<td>R/3 ECC 6</td>
</tr>
</tbody>
</table>

Note: Each BAPI call has specific authorization requirements. For more information about the required authorizations, see the BAPI documentation.

**Role Z-DS-RUNTIME-BAPI-V7-1**

— BAPI stage authorizations for running jobs are shown in Table 4.

**Table 4. BAPI stage authorizations for running jobs**

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
</table>
Note: Each BAPI call has specific authorization requirements. For more information about the required authorizations, see the BAPI documentation.

IDoc stages

Role Z-DS-DESIGN-IDOC-V7-1— This role is intended for the design of IDoc Extract and Load jobs. It should also to be used for configuring IDoc types in DataStage Administrator for SAP. This role also contains the authorizations for running jobs.

Table 5. IDoc stage authorizations for job design

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16 RFC_NAME: EDIMEXT, RFC1, SDIFRUNTIME, SDTX, SYSTRFC_TYPE: FUGR</td>
<td>R/3</td>
</tr>
<tr>
<td>S_TABU_DIS</td>
<td>BC_A</td>
<td>Table Maintenance</td>
<td>ACTVT: 03 DISBERCLS: *</td>
<td>R/3</td>
</tr>
</tbody>
</table>

Note: Assign the following SAP-defined authorization profile to the user performing the IDoc job configuration: S_IDOC_ALL.

Role Z-DS-RUNTIME-IDOC-V7-1— Intended for running IDoc Extract and Load jobs. For extracting IDocs from SAP, you also need to assign the Z-DS-RUNTIME-IDOC-SERVER-V7-1 role (see below).

Table 6. IDoc stage authorizations for running jobs

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16 RFC_NAME: EDIN, RFC1, SDIFRUNTIME, SYSTRFC_TYPE: FUGR</td>
<td>R/3</td>
</tr>
</tbody>
</table>

Note: Assign the SAP-defined authorization profile to the user running the jobs: B_ALE_ALL.

IDoc server (listener)

Role Z-DS-RUNTIME-IDOC-SERVER-V7-1— Intended for extracting IDocs from SAP. It should be assigned to the SAP user specified in the default SAP log-on details of the DataStage SAP connection since this is the log-on the IDoc server uses. The following screenshot shows the location of the default SAP log-on details in DataStage Administrator for SAP.
Table 7. Authorizations for the IDoc server

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16 RFC_NAME: RFC1, SDIFRUNTIME, SYSTRFC_TYPE: FUGR</td>
<td>R/3 ECC 6</td>
</tr>
</tbody>
</table>

**Note:** Assign the SAP-defined authorization profile to the user performing the IDoc Server: S_IDOC_ALL.

Rapid Modeler for SAP
Role Z-DS-DESIGN-RM-V7-1

The authorizations for extracting table and IDoc metadata are shown in Table 8.

Table 8. Authorizations for extracting table and IDoc metadata

<table>
<thead>
<tr>
<th>Authorization Object</th>
<th>Authorization Class</th>
<th>Description</th>
<th>Authorization Definition</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>S_RFC</td>
<td>AAAB</td>
<td>Authorization Check for RFC Access</td>
<td>ACTVT: 16 RFC_NAME: RFC1, SDIFRUNTIME, SDTB, STDX, SYSTRFC_TYPE: FUGR</td>
<td>R/3 ECC 6</td>
</tr>
</tbody>
</table>

| S_TABU_DIS           | BC_A                | Table Maintenance | ACTVT: 03 DISBERCLS: * | R/3 ECC 6 |
**Note:** Assign the following predefined authorization profile to the SAP user configured in the Rapid Modeler preferences: **S_IDOC_ALL**. For running the generated ABAP and IDoc jobs, use the ABAP and IDoc runtime authorizations listed above.

**Known issues**

**Overlapping authorizations**

Some authorization roles may cover more permissions than necessary, enabling additional actions. For example: A user with the role Z-DS-DESIGN-ABAP-V_1 or Z-DS-DESIGN-BAPI-V7-1 is able to run IDoc Extract jobs, even though this capability should be limited to users with the roles Z-DS-DESIGN-IDOC-V7-1 or Z-DS-RUNTIME-IDOC-V7-1.

**Reason:** Some SAP authorizations don't have the necessary granularity or overlap, resulting in excess permissions given to users. This is an internal characteristic of SAP software and is outside of the influence of IBM products.

**Conclusion**

We have now learned how to deploy the SAP components of InfoSphere Information Server Pack for SAP Applications 7.1 by mapping authorizations through various stages on development, test, and production environments.
Resources

- The Information Management area on developerWorks provides resources for architects, developers, and engineers.
- Stay current with developer technical events and webcasts focused on a variety of IBM products and IT industry topics.
- Follow developerWorks on Twitter.
- Watch developerWorks demos ranging from product installation and setup demos for beginners, to advanced functionality for experienced developers.
- Get involved in the developerWorks Community. Connect with other developerWorks users while you explore developer-driven blogs, forums, groups, and wikis.
About the author

Sergej Schuetz

Sergej Schuetz is a software engineer. He has worked on SAP integration tools for more than six years. He has worked on the Information Server SAP integration team both as a software developer and as an architect.

© Copyright IBM Corporation 2015
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)