## Content

1. **Getting Started.** ................................................................. 7
   1.1 Overview of SAP Data Services. ......................................... 7
   SAP Data Services and the SAP solution portfolio. ................. 7
   Software benefits. ............................................................. 7
   Associated software. .......................................................... 9
   Interfaces. ........................................................................ 9
   1.2 Naming Conventions. ...................................................... 9

2. **Data Services Architecture.** ............................................. 12
   2.1 Architecture overview. .................................................. 12
   2.2 Standard components. .................................................. 12
   Designer. ......................................................................... 13
   Repository. ...................................................................... 14
   Job Server. ...................................................................... 14
   Access Server. .................................................................. 15
   Management Console. ..................................................... 15
   Adapter SDK. ................................................................... 17
   2.3 Management tools. ....................................................... 18
   License Manager. ............................................................. 18
   Repository Manager. ....................................................... 18
   Server Manager. ............................................................. 18
   2.4 Operating system platforms. ......................................... 19
   2.5 Distributed architecture. .............................................. 19
   Host names and port numbers. .......................................... 20
   DSN-less and TNS-less connections. .................................. 20
   2.6 SAP integration. ........................................................... 21

3. **Security.** ......................................................................... 23
   3.1 Securing administrative functions. ................................. 23
   3.2 Message client library. .................................................. 23
   3.3 Temporary cache files. .................................................. 23
   Encrypting certain temporary cache files. ............................ 24
   3.4 Configuring SSL for Data Services components. ............. 25
   Protected communication paths. ........................................ 25
   Default certificates. ......................................................... 27
   Copying certificates in a distributed installation. .................. 27
   Enabling or disabling SSL on communication paths. ............ 28
Using custom certificates ...................................................... 30
Generating keys and signing certificates ........................................ 31
3.5 Configuring SSL for the CMS connection ........................................ 32
3.6 SSL for Metadata Browsing and View Data Services .......................... 32
 Configuring SSL for Metadata Browsing and View Data Services ............ 32
 Creating a keystore file and certificates using the Data Services tool .......... 34
3.7 Password encryption ............................................................ 34
 Encryption key storage locations ............................................ 35
 Encrypting passwords manually ............................................. 35
3.8 Password protection for a Data Services repository .......................... 36
 Setting Data Services repository permissions in the CMC .................... 36
4 User and rights management .................................................... 38
4.1 User management .............................................................. 38
4.2 Group management ............................................................ 38
 Detailed application rights .................................................... 39
 Viewing application rights assigned to a group ................................ 41
 Managing application rights for a group ...................................... 41
5 Repository management ......................................................... 43
5.1 Registering a repository in the CMC ........................................ 43
5.2 Managing security settings for repositories in the CMC .................... 44
 Viewing rights for a user or group on a repository .......................... 45
 Assigning users and groups to an access control list for a repository ........ 45
 Detailed repository rights ..................................................... 46
6 Server management ............................................................. 47
6.1 Setting UNIX environment variables ....................................... 47
 Configuring additional database connectivity ................................ 48
6.2 Starting services automatically .............................................. 49
6.3 History retention and Job Server log retention ............................... 50
 USPS-required log files and reports ......................................... 50
 Setting the History Retention Period ....................................... 51
 Setting the Job Server Log Retention Period ................................ 52
6.4 Configure ODBC data sources on UNIX ................................... 53
 Using the Connection Manager for UNIX systems .......................... 53
 Configuring ODBC data sources on UNIX using DSN connections ........ 57
 Configuring other ODBC data sources .................................... 65
6.5 Configure SSL for Microsoft SQL Server .................................. 70
 Configuring SSL for Microsoft SQL Server database on Windows ........ 71
 Configuring SSL for Microsoft SQL Server database on Unix .............. 72
6.6 Configure DSN SSL for SAP HANA ......................................... 72
Cryptographic libraries and global.ini settings ........................................ 73
Configuring SSL for SAP HANA datastore on Windows ............................. 74
Configuring SSL for SAP HANA datastore on Unix ................................ 75
6.7 Enable MIT Kerberos for HP Vertica SSL protocol ............................. 77
6.8 Creating a DSN for HP Vertica ........................................................... 79
6.9 Using the ODBC Driver Selector on Windows for server name connections ........................................................... 81
6.10 Using the Repository Manager ............................................................ 81
6.11 Using the License Manager ................................................................. 83
6.12 Using the Server Manager on Windows ................................................ 83
Configuring Job Servers ................................................................. 83
Configuring run-time resources ............................................................ 86
Configuring Access Servers ............................................................... 87
Configuring SSL paths ................................................................. 88
Verifying that Job and Access servers are running ..................................... 89
6.13 Using the Server Manager on UNIX systems ........................................... 89
Configuring Job Servers on UNIX ....................................................... 91
Configuring run-time resources ............................................................ 93
Configuring Access Servers ............................................................... 94
Configuring SSL paths ................................................................. 95
Starting or stopping the service ........................................................... 96
Configuring SMTP email ................................................................. 97
6.14 Configuring Metadata Browsing Service and View Data Service ............. 97
Metadata Browsing Service configuration parameters .................................. 98
View Data Services configuration parameters ........................................... 99
6.15 Data Services CMC application settings ................................................... 101
7 Monitoring .................................................................................. 103
7.1 Monitoring jobs ........................................................................ 103
Viewing overall status of executed jobs ................................................ 103
Statistics ................................................................................. 104
Ignoring error status ................................................................. 106
Deleting batch job history data .......................................................... 106
Stopping a running job .................................................................. 106
Deleting trace, monitor, and error logs for a batch job ............................... 106
8 Lifecycle management ............................................................................. 108
8.1 Migration basics .......................................................................... 108
Development phases ........................................................................ 108
Migration mechanisms and tools ........................................................... 110
8.2 Preparing for migration ................................................................ 112
Naming conventions for migration ...................................................... 113
Datastore and system configurations ...................................................... 116
8.3 Export/Import. ................................................................. 119
   Exporting/importing objects. ........................................... 119
   Backing up repositories. ............................................... 125
   Maintaining Job Server performance. ............................. 125
8.4 The Enhanced Change and Transport System (CTS+). ............ 126
8.5 Data Services Object Promotion Management. .................... 127
   About object promotion. ............................................... 127
   Overview of Data Services Object Promotion Management. .... 127
   Requirements for object promotion. ............................... 127
   Object promotion user interface. .................................. 130
   Configuring object promotion. ..................................... 132
   Promoting objects. .................................................... 135
9   Integration with SAP and SAP Solution Manager. .................... 140
9.1 Integration overview. ................................................... 140
   SAP System Landscape Directory (SLD). ......................... 140
   Solution Manager Diagnostics (SMD). ............................ 140
9.2 SLD and SAP Solution Manager integration checklist. ............ 140
9.3 Managing System Landscape Directory registration. ............. 141
   Data Services registration in the SLD. ........................... 141
   Configuring SLD in Server Manager (Windows). ................ 142
   Creating a sldest.cfg.key file for the SLDReg. .................. 142
   Configuring SLD in Server Manager (Unix). ..................... 143
   When is SLD registration triggered? ............................. 144
9.4 Performance and availability monitoring. ......................... 144
   Solution Manager Diagnostics (SMD) overview. ................ 144
   SMD agent guidelines. .............................................. 145
   Configure your system for SMD. ................................... 146
   Enabling performance instrumentation on Windows. ............ 146
   Enabling performance instrumentation on UNIX and Linux. .... 147
   Heartbeat monitoring. .............................................. 148
   Alert monitoring. .................................................... 148
10  Command line administration. ....................................... 149
10.1 Command lines overview. .......................................... 149
10.2 License Manager. ..................................................... 149
   Configuring License Manager on Unix. .......................... 150
   Starting License Manager. ......................................... 150
10.3 Connection Manager (Unix). ...................................... 151
10.4 Repository Manager (Windows). .................................. 151
10.5 Repository Manager (Unix). ...................................... 154
10.6 Server Manager (Windows). ...................................... 156
1 Getting Started

1.1 Overview of SAP Data Services

About this section

This section introduces SAP Data Services and explains its place in the SAP solution portfolio.

1.1.1 SAP Data Services and the SAP solution portfolio

The SAP solution portfolio delivers extreme insight through specialized end-user tools on a single, trusted business intelligence platform. This entire platform is supported by SAP Data Services. On top of SAP Data Services, the SAP solution portfolio layers the most reliable, scalable, flexible, and manageable business intelligence (BI) platform which supports the industry’s best integrated end-user interfaces: reporting, query and analysis, and performance management dashboards, scorecards, and applications.

True data integration blends batch extraction, transformation, and loading (ETL) technology with real-time bi-directional data flow across multiple applications for the extended enterprise.

By building a relational datastore and intelligently blending direct real-time and batch data-access methods to access data from enterprise resource planning (ERP) systems and other sources, SAP has created a powerful, high-performance data integration product that allows you to fully leverage your ERP and enterprise application infrastructure for multiple uses.

SAP provides a batch and real-time data integration system to drive today's new generation of analytic and supply-chain management applications. Using the highly scalable data integration solution provided by SAP, your enterprise can maintain a real-time, on-line dialogue with customers, suppliers, employees, and partners, providing them with the critical information they need for transactions and business analysis.

1.1.2 Software benefits

Use SAP Data Services to develop enterprise data integration for batch and real-time uses. With the software:

- You can create a single infrastructure for batch and real-time data movement to enable faster and lower cost implementation.
- Your enterprise can manage data as a corporate asset independent of any single system. Integrate data across many systems and reuse that data for many purposes.
- You have the option of using pre-packaged data solutions for fast deployment and quick ROI. These solutions extract historical and daily data from operational systems and cache this data in open relational databases.
The software customizes and manages data access and uniquely combines industry-leading, patent-pending technologies for delivering data to analytic, supply-chain management, customer relationship management, and Web applications.

1.1.2.1 Unification with the platform

SAP Data Services provides several points of platform unification:

- Get end-to-end data lineage and impact analysis.
- Create the semantic layer (universe) and manage change within the ETL design environment.

Data Services deeply integrates the entire ETL process with the business intelligence platform so you benefit from:

- Easy metadata management
- Simplified and unified administration
- Life cycle management
- Trusted information

1.1.2.2 Ease of use and high productivity

SAP Data Services combines both batch and real-time data movement and management to provide a single data integration platform for information management from any information source, for any information use.

Using the software, you can:

- Stage data in an operational datastore, data warehouse, or data mart.
- Update staged data in batch or real-time modes.
- Create a single graphical development environment for developing, testing, and deploying the entire data integration platform.
- Manage a single metadata repository to capture the relationships between different extraction and access methods and provide integrated lineage and impact analysis.

1.1.2.3 High availability and performance

The high-performance engine and proven data movement and management capabilities of SAP Data Services include:

- Scalable, multi-instance data-movement for fast execution
- Load balancing
- Changed-data capture
- Parallel processing
1.1.3 Associated software

Choose from other SAP solution portfolio software options to further support and enhance the power of your SAP Data Services software.

1.1.3.1 SAP Metadata Management

SAP BusinessObjects Metadata Management provides an integrated view of metadata and its multiple relationships for a complete Business Intelligence project spanning some or all of the SAP solution portfolio. Use the software to:

- View metadata about reports, documents, and data sources from a single repository.
- Analyze lineage to determine data sources of documents and reports.
- Analyze the impact of changing a source table, column, element, or field on existing documents and reports.
- Track different versions (changes) to each object over time.
- View operational metadata (such as the number of rows processed and CPU utilization) as historical data with a datetime.
- View metadata in different languages.

For more information on SAP Metadata Management, contact your SAP sales representative.

1.1.4 Interfaces

SAP Data Services provides many types of interface components. Your version of the software may provide some or all of them.

You can use the Adapter SDK to develop adapters that read from and/or write to other applications.

In addition to the interfaces listed above, the Nested Relational Data Model (NRDM) allows you to apply the full power of SQL transforms to manipulate, process, and enrich hierarchical business documents.

For a detailed list of supported environments and hardware requirements, see the Product Availability Matrix (PAM) available at: [https://apps.support.sap.com/sap/support/pam](https://apps.support.sap.com/sap/support/pam). This document includes specific version and patch-level requirements for databases, applications, web application servers, web browsers, and operating systems.

1.2 Naming Conventions

In this documentation, the following naming conventions apply:
Terminology

- “Data Services system” refers to “SAP Data Services”.
- “BI platform” refers to “SAP BusinessObjects BI platform”.

**Note**
The BI platform components required by Data Services may also be provided by SAP BusinessObjects Information platform services (IPS).

- “CMC” refers to the Central Management Console provided by the BI or IPS platform.
- “CMS” refers to the Central Management Server provided by the BI or IPS platform.

Variables

Table 1:

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;INSTALL_DIR&gt;</code></td>
<td>The installation directory for the SAP software.</td>
</tr>
<tr>
<td></td>
<td>Default location:</td>
</tr>
<tr>
<td></td>
<td>- For Windows: C:\Program Files (x86)\SAP BusinessObjects</td>
</tr>
<tr>
<td></td>
<td>- For UNIX: $HOME/sap businessobjects</td>
</tr>
<tr>
<td><code>&lt;BIP_INSTALL_DIR&gt;</code></td>
<td>The root directory of the BI or IPS platform.</td>
</tr>
<tr>
<td></td>
<td>Default location:</td>
</tr>
<tr>
<td></td>
<td>- For Windows: <code>&lt;INSTALL_DIR&gt;\SAP BusinessObjects Enterprise XI 4.0</code></td>
</tr>
<tr>
<td></td>
<td>- For UNIX: <code>&lt;INSTALL_DIR&gt;/enterprise_xi40</code></td>
</tr>
<tr>
<td><code>&lt;LINK_DIR&gt;</code></td>
<td>The root directory of the Data Services system.</td>
</tr>
<tr>
<td></td>
<td>Default location:</td>
</tr>
<tr>
<td></td>
<td>- All platforms</td>
</tr>
<tr>
<td></td>
<td>- <code>&lt;INSTALL_DIR&gt;/Data Services</code></td>
</tr>
<tr>
<td></td>
<td>This system environment variable is created automatically during installation.</td>
</tr>
</tbody>
</table>

Note
These paths are the same for both the SAP BusinessObjects BI platform and SAP BusinessObjects Information platform services.
<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DS_COMMON_DIR&gt;</td>
<td>The common configuration directory for the Data Services system.</td>
</tr>
<tr>
<td></td>
<td>Default location:</td>
</tr>
<tr>
<td></td>
<td>• Windows (Vista and newer)</td>
</tr>
<tr>
<td></td>
<td>ALLUSERSPROFILE\SAP BusinessObjects\Data Services</td>
</tr>
<tr>
<td></td>
<td>• Windows (Older versions)</td>
</tr>
<tr>
<td></td>
<td>ALLUSERSPROFILE\Application Data\SAP BusinessObjects\Data Services</td>
</tr>
<tr>
<td></td>
<td>• UNIX systems (for compatibility)</td>
</tr>
<tr>
<td></td>
<td>&lt;LINK_DIR&gt;</td>
</tr>
<tr>
<td></td>
<td>This system environment variable is created automatically during installation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Starting with Data Services 4.2 SP6, users can designate a different default location for DS_COM-</td>
</tr>
<tr>
<td></td>
<td>COMMON_DIR. If you cannot find the DS_COMMON_DIR in the listed default location above, ask your</td>
</tr>
<tr>
<td></td>
<td>System Administrator to find out where the default location is for DS_COMMON_DIR.</td>
</tr>
<tr>
<td>&lt;DS_USER_DIR&gt;</td>
<td>The user-specific configuration directory for the Data Services system.</td>
</tr>
<tr>
<td></td>
<td>Default location:</td>
</tr>
<tr>
<td></td>
<td>• Windows (Vista and newer)</td>
</tr>
<tr>
<td></td>
<td>USERPROFILE\AppData\Local\SAP BusinessObjects\Data Services</td>
</tr>
<tr>
<td></td>
<td>• Windows (Older versions)</td>
</tr>
<tr>
<td></td>
<td>USERPROFILE\Local Settings\Application Data\SAP BusinessObjects \Data Services</td>
</tr>
<tr>
<td></td>
<td>This user environment variable is created automatically during installation.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This variable is used only for Data Services client applications on Windows, such as the Designer.</td>
</tr>
<tr>
<td></td>
<td>&lt;DS_USER_DIR&gt; is not used on UNIX platforms.</td>
</tr>
</tbody>
</table>
2 Data Services Architecture

2.1 Architecture overview

This section outlines the overall platform architecture, system, and service components that make up the SAP Data Services platform. The information helps administrators understand the system essentials and help to form a plan for the system deployment, management, and maintenance.

Data Services is designed for high performance across a broad spectrum of user and deployment scenarios. For example:

- Developers can integrate Data Services into your organization’s other technology systems by using web services, Java, or .NET application programming interfaces (APIs).
- End users can access, create, edit, and interact with Data Services projects and reports using specialized tools and applications that include:
  - Designer
  - Management Console
    - Administrator
    - Impact and Lineage Analysis
    - Operational Dashboard
    - Auto Documentation
    - Data Validation
    - Data Quality Reports
- IT departments can use data and system management tools that include:
  - Central Management Console (CMC)
  - Management Console
  - Server Manager
  - Repository Manager

To provide flexibility, reliability, and scalability, Data Services components can be installed on one or across many machines.

Server processes can be “vertically scaled” (where one computer runs several, or all, server-side processes) to reduce cost, or “horizontally scaled” (where server processes are distributed between two or more networked machines) to improve performance. It is also possible to run multiple, redundant versions of the same server process on more than one machine, so that processing can continue if the primary process encounters a problem.

2.2 Standard components

The following diagram illustrates how SAP Data Services components fit in with other software in the SAP portfolio.
Note

If you do not have a full SAP BusinessObjects BI platform installation, the basic components required by Data Services can also be provided by SAP BusinessObjects Information platform services.

For a detailed list of supported environments and hardware requirements, see the Product Availability Matrix (PAM) available at: https://apps.support.sap.com.sap/support/pam/. This information includes specific version and patch-level requirements for databases, applications, web application servers, web browsers, and operating systems.

2.2.1 Designer

The Designer is a development tool with an easy-to-use graphical user interface. It enables developers to define data management applications that consist of data mappings, transformations, and control logic.

Use the Designer to create applications containing work flows (job execution definitions) and data flows (data transformation definitions).

To use the Designer, create objects, then drag, drop, and configure them by selecting icons in flow diagrams, table layouts, and nested workspace pages. The objects in the Designer represent metadata. The Designer interface
allows you to manage metadata stored in a repository. From the Designer, you can also trigger the Job Server to run your jobs for initial application testing.

Related Information

Repository [page 14]
Job Server [page 14]

2.2.2 Repository

The SAP Data Services repository is a set of tables that hold user-created and predefined system objects, source and target metadata, and transformation rules. Set up repositories on an open client/server platform to facilitate sharing metadata with other enterprise tools. Each repository must be stored on an existing RDBMS and registered in the Central Management Console (CMC).

Each repository is associated with one or more Job Servers which run the jobs you create. There are two types of repositories:

- Local repository
  A local repository is used by an application designer to store definitions of objects (like projects, jobs, work flows, and data flows) and source/target metadata.

- Central repository
  A central repository is an optional component that can be used to support multi-user development. The central repository provides a shared object library allowing developers to check objects in and out of their local repositories.

While each user works on applications in a unique local repository, the team uses a central repository to store the master copy of the entire project. The central repository preserves all versions of an application's objects, so you can revert to a previous version if needed.

Multi-user development includes other advanced features such as labeling and filtering to provide you with more flexibility and control in managing application objects.

For more details, see the Management Console Guide and the Designer Guide.

2.2.3 Job Server

The SAP Data Services Job Server starts the data movement engine that integrates data from multiple heterogeneous sources, performs complex data transformations, and manages extractions and transactions from ERP systems and other sources. The Job Server can move data in either batch or real-time mode and uses distributed query optimization, multi-threading, in-memory caching, in-memory data transformations, and parallel processing to deliver high data throughput and scalability.

While designing a job, you can run it from the Designer which tells the Job Server to run the job. The Job Server retrieves the job from its associated repository, then starts an engine to process the job. In your production environment, the Job Server runs jobs triggered by a scheduler or by a real-time service managed by the Access Server. In production environments, you can balance job loads by creating a Job Server group (multiple Job Servers) which executes jobs according to overall system load.
Engine

When Data Services jobs are executed, the Job Server starts engine processes to perform data extraction, transformation, and movement. The engine processes use parallel processing and in-memory data transformations to deliver high data throughput and scalability.

Service

The Data Services service is installed when Job and Access Servers are installed. The service starts Job Servers and Access Servers when you restart your system. The Windows service name is SAP Data Services. The UNIX equivalent is a daemon named AL_JobService.

Related Information

Access Server [page 15]

2.2.4 Access Server

The SAP Data Services Access Server is a real-time, request-reply message broker that collects message requests, routes them to a real-time service, and delivers a message reply within a user-specified time frame. The Access Server queues messages and sends them to the next available real-time service across any number of computing resources. This approach provides automatic scalability because the Access Server can initiate additional real-time services on additional computing resources if traffic for a given real-time service is high. You can configure multiple Access Servers.

Service

The Data Services service is installed when Job and Access Servers are installed. The service starts Job Servers and Access Servers when you restart your system. The Windows service name is SAP Data Services. The UNIX equivalent is a daemon named AL_JobService.

2.2.5 Management Console

Administrator

The Administrator provides browser-based administration of SAP Data Services resources including:
- Scheduling, monitoring, and executing batch jobs.
- Configuring, starting, and stopping real-time services.
- Configuring Job Server, Access Server, and repository usage.
- Configuring and managing adapters.
- Managing users.
- Publishing batch jobs and real-time services via Web services.

**Metadata Reports applications**

The Metadata Reports applications provide browser-based analysis and reporting capabilities on metadata that is:

- Associated with your SAP Data Services jobs
- Associated with other SAP solution portfolio applications associated with Data Services

Metadata Reports provide several applications for exploring your metadata:

- Impact and lineage analysis
- Operational dashboards
- Auto documentation
- Data validation
- Data quality

### 2.2.5.1 Impact and Lineage Analysis reports

Impact and Lineage Analysis reports include:

- **Datastore Analysis**
  For each datastore connection, view overview, table, function, and hierarchy reports. SAP Data Services users can determine:
  ○ What data sources populate their tables
  ○ What target tables their tables populate
  ○ Whether one or more of the following SAP BusinessObjects solution portfolio reports uses data from their tables:
    ○ Business Views
    ○ Crystal Reports
    ○ SAP BusinessObjects Web Intelligence documents
    ○ SAP BusinessObjects Desktop Intelligence documents

- **Business View analysis**
  View the data sources for Business Views in the Central Management Server (CMS). You can view business element and business field lineage reports for each Business View. Crystal Business View users can determine what data sources populate their Business Views and what reports use their views.

- **Report analysis**
  View data sources for reports in the Central Management Server (CMS). You can view table and column lineage reports for each Crystal Report and Web Intelligence Document managed by CMS. Report writers can determine what data sources populate their reports.
• Dependency analysis
  Search for specific objects in your repository and understand how those objects impact or are impacted by other SAP Data Services objects and reports. Metadata search results provide links back into associated reports.

2.2.5.2 Operational Dashboard reports

Operational dashboard reports provide graphical depictions of SAP Data Services job execution statistics. This feedback allows you to view at a glance the status and performance of your job executions for one or more repositories over a given time period. You can then use this information to streamline and monitor your job scheduling and management for maximizing overall efficiency and performance.

2.2.5.3 Auto Documentation reports

Auto documentation reports provide a convenient and comprehensive way to create printed documentation for all of the objects you create in SAP Data Services. Auto documentation reports capture critical information for understanding your jobs so you can see at a glance the entire ETL process.

After creating a project, you can use Auto documentation reports to quickly create a PDF or Microsoft Word file that captures a selection of job, work flow, and/or data flow information including graphical representations and key mapping details.

2.2.5.4 Data Validation dashboard

Data Validation dashboard reports provide graphical depictions that let you evaluate the reliability of your target data based on the validation rules you created in your SAP Data Services batch jobs. This feedback allows business users to quickly review, assess, and identify potential inconsistencies or errors in source data.

2.2.5.5 Data Quality reports

Data Quality reports allow you to view and export Crystal Reports for batch and real-time jobs that include statistics-generating transforms. Report types include job summaries, transform-specific reports, and transform group reports.

2.2.6 Adapter SDK

The SAP Data Services Adapter SDK provides a Java platform for rapid development of adapters to other applications and middleware products such as EAI systems. Adapters use industry-standard XML and Java technology to ease the learning curve. Adapters provide all necessary styles of interaction including:
• Reading, writing, and request-reply from SAP Data Services to other systems.
• Request-reply from other systems to SAP Data Services.

2.3 Management tools

SAP Data Services has several management tools to help you manage your components.

2.3.1 License Manager

License Manager can be used in command-line mode only. Use it to manage your product activation keycodes—the alphanumeric codes that are referred to each time that you run certain software.

Related Information

License Manager [page 149]

2.3.2 Repository Manager

The Repository Manager allows you to create, upgrade, and check the versions of local and central repositories.

2.3.3 Server Manager

The Server Manager allows you to add, delete, or edit the properties of Job Servers and Access Servers. It is automatically installed on each computer on which you install a Job Server or Access Server.

Use the Server Manager to define links between Job Servers and repositories. You can link multiple Job Servers on different machines to a single repository (for load balancing) or each Job Server to multiple repositories (with one default) to support individual repositories (separating test from production, for example).

The Server Manager is also where you specify SMTP server settings for the smtp_to email function. Also add or edit System Landscape Directory (SLD) registration information for Data Services registration in the SLD tab of the Server Manager.
Related Information

Using the Server Manager on Windows [page 83]
Using the Server Manager on UNIX systems [page 89]

2.4 Operating system platforms

For a complete list of supported operating systems and hardware requirements, see the Product Availability Matrix (PAM) available at: https://apps.support.sap.com/sap/support/pam.

This document includes specific version and patch-level requirements for databases, applications, web application servers, web browsers, and operating systems.

2.5 Distributed architecture

SAP Data Services has a distributed architecture. An Access Server can serve multiple Job Servers and repositories. The multi-user licensed extension allows multiple Designers to work from a central repository. The following diagram illustrates both of these features.
You can distribute software components across multiple computers, subject to the following rules:

- Engine processes run on the same computer as the Job Server that spawns them.
- Adapters require a local Job Server.

Distribute components across a number of computers to best support the traffic and connectivity requirements of your network. You can create a minimally distributed system designed for developing and testing or a highly distributed system that can scale with the demands of a production environment.

### 2.5.1 Host names and port numbers

Communication between a Web application, the Access Server, the Job Server, and real-time services occurs through TCP/IP connections specified by IP addresses (or host names) and port numbers.

If your network does not use static addresses, use the name of the computer as the host name. If connecting to a computer that uses a static IP address, use that number as the host name for Access Server and Job Server configurations.

To allow for a highly scalable system, each component maintains its own list of connections. You define these connections through the Server Manager, the Administrator, the Repository Manager, and the Message Client library calls (from Web client).

For more information about the default port numbers used by Data Services, see the “Port assignments” section of the Installation Guide.

### 2.5.2 DSN-less and TNS-less connections

Data Services provides server name connections to databases that you use as a source or target Data Services repository.

Server name connections are also known as “DSN-less” and “TNS-less” connections. Server name connections eliminate the need to configure the same DSN (ODBC Data Source Name) or TNS (Transparent Network Substrate) entries on every machine in a distributed environment.

For the Data Services repository, the following database types are supported:

- For Oracle databases, you specify the server name, database name, and port instead of the TNS name.
- For DB2, MySQL, and SAP HANA databases, you specify the server name, database name, and port instead of the DSN name.

**Note**

When you install Data Services, the repository defaults to a DSN-less or TNS-less connection. If you choose not to use a server name connection:

- Defer repository creation to after installation.
- Invoke the Repository Manager to subsequently create the repository.
  - On Windows, select the option *Use TNS name or Use data source name (DSN).*
On UNIX, specify the `-s` option to not use a server name connection.

- Log in to the Central Management Console (CMC) to register the repository and select the repository connection type on the Data Services Repository Properties screen:
  - For an Oracle database, select `Yes` in the drop-down list for *Use TNS name*.
  - For a DB2, MySQL, or SAP HANA database, select `Yes` in the drop-down list for *Use data source name (DSN)*.

*Note*

This Data Services repository connection type setting on the CMC determines the connection type for logging into the Designer, running jobs, scheduling jobs, and so on.

For Data Services sources and targets, the following database types are supported for DSN-less and TNS-less connections:

- DB2 UDB
- Informix
- MySQL
- Netezza
- Oracle
- SAP HANA
- SAP Sybase IQ
- Teradata

*Note*

For the most current list of supported databases for server name connections, see the Release Notes.

**Related Information**

Administrator Guide: Using the Repository Manager [page 81]
Administrator Guide: Registering a repository in the CMC [page 43]
Administrator Guide: Configuring Job Servers [page 83]
Administrator Guide: Configuring Job Servers on UNIX [page 91]
Administrator Guide: Using the Windows ODBC Driver Selector for DSN-less connections [page 81]
Administrator Guide: Configuring ODBC data sources on UNIX using DSN-less connections [page 54]

**2.6 SAP integration**

SAP Data Services integrates with your existing SAP infrastructure with the following SAP tools:

- SAP System Landscape Directory (SLD)
- SAP Solution Manager
- CTS Transport (CTS+)
- Monitoring with CA Wily Introscope

Table 2:

<table>
<thead>
<tr>
<th>SAP tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP System Landscape Directory (SLD)</td>
<td>The system landscape directory of SAP NetWeaver is the central source of system landscape information relevant for the management of your software life-cycle. By providing a directory comprising information about all installable software available from SAP and automatically updated data about systems already installed in a landscape, you get the foundation for tool support to plan software life-cycle tasks in your system landscape. The SAP Data Services installation program registers the vendor and product names and versions with the SLD, as well as server and front-end component names, versions, and location.</td>
</tr>
<tr>
<td>SAP Solution Manager</td>
<td>The SAP Solution Manager is a platform that provides the integrated content, tools, and methodologies to implement, support, operate and monitor an organization's SAP and non-SAP solutions. Non-SAP software with an SAP-certified integration is entered into a central repository and transferred automatically to your SAP System Landscape Directories (SLD). SAP customers can then easily identify which version of third-party product integration has been certified by SAP within their SAP system environment. This service provides additional awareness for third-party products besides our online catalogs for third-party products. SAP Solution Manager is available to SAP customers at no extra charge, and includes direct access to SAP support and SAP product upgrade path information.</td>
</tr>
<tr>
<td>CTS Transport (CTS+)</td>
<td>The Change and Transport System (CTS) helps you to organize development projects in ABAP Workbench and in Customizing, and then transport the changes between the SAP systems in your system landscape. As well as ABAP objects, you can also transport Java objects (J2EE, JEE) and SAP-specific non-ABAP technologies (such as Web Dynpro Java or SAP NetWeaver Portal) in your landscape.</td>
</tr>
<tr>
<td>Monitoring with CA Wily Introscope</td>
<td>CA Wily Introscope is a web application management product that delivers the ability to monitor and diagnose performance problems that may occur within Java-based SAP modules in production, including visibility into custom Java applications and connections to back-end systems. It allows you to isolate performance bottlenecks in NetWeaver modules including individual Servlets, JSPs, EJBs, JCO's, Classes, Methods and more. It offers real-time, low-overhead monitoring, end-to-end transaction visibility, historical data for analysis or capacity planning, customizable dashboards, automated threshold alarms, and an open architecture to extend monitoring beyond NetWeaver environments.</td>
</tr>
</tbody>
</table>
3 Security

This section details the ways in which SAP Data Services addresses enterprise security concerns, thereby providing administrators and system architects with answers to typical questions regarding security.

Data Services relies on the Central Management Server (CMS) for authentication and security features. This section highlights differences and additional information specific to your Data Services system.

For complete information about the security features provided by the CMS, see the SAP BusinessObjects BI Platform Administrator Guide or the SAP BusinessObjects Information Platform Services Administrator Guide.

3.1 Securing administrative functions

To ensure security for your Data Services environment, use a firewall to prevent unintended remote access to administrative functions.

In a distributed installation, you need to configure your firewall so that the Data Services components are able to communicate with each other as needed.

For information about configuring ports on your firewall, see your firewall documentation. Also see the “Port assignments” topic in the Installation Guide

3.2 Message client library

The Message Client libraries (Java and C++) used in real-time services, does not require authorization to connect. Therefore, it is important to use caution when using these libraries.

For more information about using the Message Client library, see the SAP Data Services Integrator Guide.

3.3 Temporary cache files

In Data Services, temporary cache files are generated for a variety of functions and operations. Profiling, joins, table comparison, sorting, lookup, and group_by are some examples. Because these files are not encrypted, by
default, care should be taken when working with confidential or other sensitive data. Both pageable and persistent caches create data files that are not encrypted, by default.

**Temporary file location**

The temporary files that Data Services creates are stored in %COMMON_DIR%/log/pCache/<repository_string>/. These files can be secured using the appropriate permissions at the OS level.

**Pageable cache and key data**

The pageable cache option in a data flow stores data in temporary files that are removed automatically after a data flow finishes executing.

**Persistent cache**

Data Services provides a datastore called Persistent cache. The data in persistent cache is not encrypted, and it is your responsibility to secure it using OS file/directory permissions.

**long data**

When long data (BLOB or CLOB) data is large, the data is stored in temporary cache files.

If long data is cached (for a join, sort, or table comparison, for example), the cache file is deleted when the data flow finishes executing.

A long data cache file is also deleted when the data is out of scope. For example:

- The data is loaded into a target.
- The data is filtered out by a Query transform.
- A long datatype is converted to a varchar.

**3.3.1 Encrypting certain temporary cache files**

There are types of temporary cache files that can be encrypted, if necessary. These include:

- Persistent cache datastore files
- Pageable cache data flow files
- Functions such as lookup, search_replace, distinct, group_by, and so on.
Transforms such as Data Quality transforms and Table Comparison

To encrypt these files:

1. Open the `DSConfig.txt` file, located in `%DS_COMMON_DIR%\conf`.
2. Set the `pageable_cache_encrypt_data` parameter, in the `String` section, to `yes`.
3. Save and close the file.

**Note**

Encrypting these files can have a significant negative impact on performance. Remember that these files are deleted immediately after the data flow finishes executing.

### 3.4 Configuring SSL for Data Services components

Secure Sockets Layer (SSL) is a cryptographic protocol that provides security and data integrity for communications over networks. Transport Layer Security (TLS) is the standard specification published by the IETF that is based on earlier SSL specifications.

The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications confidentially over the network using cryptography.

#### 3.4.1 Protected communication paths

Within the SAP Data Services platform, SSL is supported for all communication paths between components that communicate over a network.

The following diagram illustrates the communication channels within the Data Services architecture that support SSL.
All TCP/IP communication paths support SSL/TLS. Depending on your web application server communication, clients using HTTP may switch to the HTTPS protocol.

Additionally, when you use a server group and set the distribution level to “Sub data flow”, the TCP/IP communication path between sub data flows on different job servers within the server group is also protected by SSL.
3.4.2 Default certificates

By default, a set of SSL certificates is created during installation for secure communication between Data Services components.

You can choose to use your own certificates by configuring them after installation has finished. The default certificates use 1024-bit RSA keys and are valid for 30 years.

Related Information

Using custom certificates [page 30]
Copying certificates in a distributed installation [page 27]

3.4.3 Copying certificates in a distributed installation

When different Data Services components are installed on different machines and each installation has its own root and intermediate certificate authority (CA) configuration, you must manually copy the trusted certificates from one machine to all other machines.

i Note

Trusted certificate files refers to root and intermediate CA certificate files. These files have a .crt extension, and can be located in the <LINK_DIR>/ssl/trusted_certs folder.

👉 Remember

When you copy trusted certificates from one host machine to another, you must always copy the files to and from the <LINK_DIR>/ssl/trusted_certs folder on each respective machine.

1. If the Job Server and Access Server are installed on different machines, configure the hosts with the new certificates.
   a. Copy the trusted certificates from the Access Server to the Job Server host.
   b. On the Job Server host machine, run the following script to refresh the <LINK_DIR>/ssl/trusted_certs/jssecacerts keystore file:
      ○ On Windows: <LINK_DIR>/bin/SetupJavaKeystore.bat
      ○ On UNIX: <LINK_DIR>/bin/SetupJavaKeystore.sh
      This allows adapters that communicate with the Access Server to use the new certificates.
   c. Copy the trusted certificates from the Job Server to the Access Server host.
   d. Restart the job service on both the Job Server and Access Server host machines.

2. If the Access Server and Management Console are installed on different machines, configure the Management Console host with the new certificates.
   a. Copy the trusted certificates from the Access Server to the Management Console host.
b. On the Management Console host machine, run the following script to refresh the `<LINK_DIR>/ssl/trusted_certs/jssecacerts` keystore file:
   - On Windows: `<LINK_DIR>/bin/SetupJavaKeystore.bat`
   - On UNIX: `<LINK_DIR>/bin/SetupJavaKeystore.sh`

c. Restart the web application server that is hosting the Management Console.

3. If the Access Server and message client are installed on different machines, configure the message client host with the new certificates.
   a. Copy the trusted certificates from the Access Server to the message client host.
   b. If the message client uses Java, import the trusted certificates into the keystore used by the message client application.
      For information about creating keystores, see the JDK help for the `keytool` command.

4. If the Job Server and job launcher or external scheduler are installed on different machines, configure the job launcher or external scheduler host with the new certificates.

   Copy the trusted certificates from the Job Server to the job launcher or external scheduler host.

   **Note**

   If the scheduled job connects to multiple Job Servers through a server group, copy the trusted certificates from all Job Servers within the group.

3.4.4 Enabling or disabling SSL on communication paths

Because Data Services uses multiple communication paths, there are different ways to enable or disable SSL for any given path.

You may choose to enable or disable SSL for certain paths, depending on your security and performance requirements.

<table>
<thead>
<tr>
<th>Communication path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For adapter management</td>
<td>You can configure SSL for adapter management by enabling SSL support on your Job Servers. Enabling SSL for adapter management protects the communication path used between your Job Servers and adapters, and message broker clients. To configure SSL on a Job Server, use the Server Manager.</td>
</tr>
<tr>
<td>Communication path</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>For real-time messaging</td>
<td>You can configure SSL for real-time messaging by enabling SSL support on your Access Servers. Enabling SSL for real-time messaging protects the communication path used between your Access Servers and their real-time clients.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>By default, SSL is enabled for real-time messaging. If you disable it on an Access Server, be sure to disable it on any message clients or adapters that communicate with that Access Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>SSL can be enabled or disabled on a per-server basis. You are not required to configure it the same way for all Access Servers.</td>
</tr>
<tr>
<td></td>
<td>To configure SSL on an Access Server, use the Server Manager.</td>
</tr>
<tr>
<td>For peer-to-peer communication</td>
<td>You can configure SSL for peer-to-peer communication by configuring SSL for run-time resources. Enabling SSL for run-time resources protects the communication path used between different sub data flows running on different Job Servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>If you run multiple Job Servers within a server group, configure SSL the same way on each Job Server.</td>
</tr>
<tr>
<td></td>
<td>To configure SSL for run-time resources, use the Server Manager.</td>
</tr>
</tbody>
</table>
### Communication path

<table>
<thead>
<tr>
<th>Communication path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>For other communication paths</td>
<td>SSL is mandatory for some communication paths within the Data Services architecture. For example, SSL is always enabled on the communication paths between a Job Server and the following clients: The Administrator application in the Management Console, Designers, The job launcher, Access Servers, The job execution engine, Other Job Servers within a server group, The job service used for monitoring. You must ensure that each client has the correct certificates in these situations, but there is no additional configuration to perform.</td>
</tr>
</tbody>
</table>

**Note**

You need to copy the certificates from the Job Server to the Access Server, Management Console, and external job launcher hosts. In all other cases, the certificates are exchanged automatically.

---

### 3.4.5 Using custom certificates

While SAP Data Services includes a set of SSL certificates by default, you can also choose to use your own certificates. Depending on the nature of your Data Services deployment, not all steps below may be required.

1. Generate certificates as needed, and have them signed by a trusted certificate authority (CA).
   - For more information, see the “Generating keys and sign certificates” section.

2. Copy all required certificates to the Data Services client machines.

**Note**

Each Data Services client requires the certificates for all CAs in the certificate chain when validating the certificate of the Data Services server. The certificates within a certificate chain are called trusted CAs.
certificates and must be present on the local machine. In most cases, the certificate chain is the same for all clients, and therefore the same certificates must be present on all client machines.

3. If you are using Java-based clients, use the JDK `keytool` utility to generate a keystore containing the trusted certificates.

4. Configure server certificate and keyfile paths with the Server Manager.

5. Configure certificates for the Designer.
   a. Choose `Tools > Options` within the Designer.
   b. Navigate to the SSL category under Designer.
   c. Specify the locations of the certificate file, the private key file, and the trusted certificates folder.

If you change any SSL options other than *Use SSL protocol for profiler*, you must restart both the Designer and any Data Services servers.

**Related Information**

- Configuring SSL paths [page 88]
- Generating keys and signing certificates [page 31]

### 3.4.6 Generating keys and signing certificates

To use your own custom certificates for SSL security in Data Services, you must generate the certificates and have them signed by a trusted certificate authority (CA), such as VeriSign.

1. Generate the RSA key and certificate using the `openssl` tool.

   ```
   openssl req -config <LINK_DIR>/ssl/conf/openssl.conf -new -newkey rsa:1024 -nodes -keyout <mykey.pem> -out <myreq.pem>
   ```

   where `<mykey.pem>` is the name of the key file to generate, and `<myreq.pem>` is the name of the certificate file to generate.

   **Note**

   By default, `openssl` is installed to `<LINK_DIR>/bin`. For more information about available options and commands, see the `openssl` documentation.

2. Send the RSA private key and certificate files to your external CA.

3. After you receive the signed certificate from your CA, use the Server Manager to specify the path to the new certificate and private key file.

   **Note**

   Trusted certificates from an external CA must be in PEM format. The signed certificates should be copied to the `<LINK_DIR>/ssl/trusted_certs` directory.
Related Information

Configuring SSL paths [page 88]
Configuring SSL paths [page 95]

3.5 Configuring SSL for the CMS connection

You can use the Secure Sockets Layer (SSL) protocol for all network communications between SAP Data Services clients and the Central Management Server (CMS).

To set up SSL for all CMS communication, you need to perform the following steps:

- Deploy the SAP BusinessObjects BI platform or Information platform services with SSL enabled.
- Create key and certificate files for each machine in your deployment.
- Configure the location of these files in the Central Configuration Manager (CCM) and your web application server.

For Data Services, you also need to use the `sslconfig` utility to configure all components that log into the CMS for SSL, including:

- Designer
- Job Servers
- External schedulers and the job launcher
- Management Console (if deployed to a different web application server than the SAP BusinessObjects BI platform or Information platform services web tier)

**Note**

For J2EE web application servers, configure SSL by modifying the startup script.

By default, the utility is installed in the following location:

- For Windows:
  `<INSTALL_DIR>`\SAP BusinessObjects Enterprise XI 4.0\win32_x86\sslconfig.exe
- For UNIX:
  `<INSTALL_DIR>/sap_bobj/enterprise_xi40/<platform>/boe_sslconfig`

Where `<platform>` matches your UNIX platform.

For more information about using `sslconfig` and configuring the CMS and its clients for SSL, see “Configuring the SSL protocol” in the SAP BusinessObjects BI Platform Administrator Guide or the SAP BusinessObjects Information Platform Services Administrator Guide.

3.6 SSL for Metadata Browsing and View Data Services

You can use the Secure Sockets Layer (SSL) protocol for all network communications between the SAP Data Services backend engine and the following EIM Adaptive Processing Server services:
- Metadata Browsing Service
- View Data Service

Data Services provides these services, but they are used by other SAP software products, such as the Data Insight module of SAP Information Steward.

Data Services provides the following files by default:

- Keystore file
  The server side (Metadata Browsing Service or View Data Service) requires a Java Server keystore file which contains a single key and all the certificates that are part of the certificate chain involved in signing the key. Passwords for the keystore file and the key are also required.
  Data Services places the default keystore file and password files under the `<LINK_DIR>\ssl\mds` folder.

- Trusted Certificates
  These certificates are used for signing the key that is stored in the Java keystore used on the server side. The client side (the Data Services backend engine) uses these trusted certificates to communicate with the server.
  Data Services places the trusted certificates under `<LINK_DIR>\ssl\mds\trusted_certs` folder.

### 3.6.1 Configuring SSL for Metadata Browsing and View Data Services

To enable and configure SSL communications for Metadata Browsing and View Data Services:

1. Log into the Central Management Console (CMC) as a user with administrative rights to the Data Services application.
2. Go to the “Applications” management area of the CMC.
   The “Applications” dialog box appears.
3. Right-click the Data Services application and select Settings.
   The “Settings” dialog box appears.
4. In the drop-down list for Enable SSL communication for Metadata Browsing and View Data Services, select “Yes”.
5. If you want to use the default keystore and certificates (that Data Services provides or that you generate using the Data Services tool), take the following steps:
   a. In the drop-down list for Use Default SSL Settings, select “Yes”.
   b. Click Save.
6. If you do not want to use the default keystore and certificates and generated your own outside of Data Services, take the following steps:
   a. Ensure that your keystore is a Java keystore file that contains a single key with all the certificates that are part of the certificate chain involved in signing the key. You must provide a password for the key and a password for the keystore file.
   b. Ensure that your keystore file exists in the `<LINK_DIR>\ssl\mds` folder and the corresponding certificate files are placed under `<LINK_DIR>\ssl\mds\trusted_certs` folder.
   c. If you have multiple Metadata Browsing Service or View Data Service instances associated with the same CMS server, you must copy the keystore and certificate files to all the machines where these instances are installed.
   d. In the drop-down list for Use Default SSL Settings, select “No”.
e. In the **KeyStore File** box, enter the name of the KeyStore file that you want to use.
f. Enter the KeyStore password.
g. Enter the Key password.
h. Click **Save**.

7. **Restart the** EIM.AdaptiveProcessingServer **as follows:**
   a. Go to the “Servers” management area of the CMC
   b. Expand the “Service Categories” node and select “Enterprise Information Management Services”.
   c. Select “EIMAdaptiveProcessingServer” in the right pane.
   d. Click 

### 3.6.2 Creating a keystore file and certificates using the Data Services tool

While SAP Data Services provides a keystore file and set of SSL certificates for the Metadata Browsing Service and View Data Service, you can also create a new key and certificates using the Data Services tool.

To create a new keystore file and SSL certificates to be used as the default SSL settings for the Metadata Browsing Service and View Data Service:

1. **Run the MDSSetupJavaKeyStore tool.**
   a. In a command-line window, change directory to `\bin`

```
   cd \bin
```
   b. Run "MDSSetupJavaKeyStore.bat"

   MDSSetupJavaKeyStore

   The MDSSetupJavaKeyStore tool creates the following files:
   - **Keystore file** DSJavaKeyStore.keystore in `\ssl\mds` containing a single key and all the certificates that are part of the certificate chain involved in signing the key
   - **File sslks.key** in `\ssl\mds` containing the key password
   - **File ssistore.key** in `\ssl\mds` containing the keystore password

2. If you already configured and enabled SSL for Metadata Browsing Service and View Data Service, restart the EIM.AdaptiveProcessingServer.
   The restart picks up the new keystore and certificate files as the default ones if you selected “Yes” for the option **Use Default SSL Settings**.

3. If you have not yet configured SSL for these services, see Configuring SSL for Metadata Browsing and View Data Services [page 33].

### 3.7 Password encryption

Within the SAP Data Services system, all passwords are encrypted using the AES algorithm with 128-bit keys.
3.7.1 Encryption key storage locations

Because passwords can be stored in multiple places within the Data Services system, an individual key is associated with each storage location.

Table 4:

<table>
<thead>
<tr>
<th>Password location</th>
<th>Associated key location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local repository</td>
<td>REPOKEY column in the AL_VERSION table</td>
</tr>
<tr>
<td>Central repository</td>
<td>REPOKEY column in the AL_VERSION table</td>
</tr>
<tr>
<td>Management Console</td>
<td>admin.key located in the same directory as admin.xml</td>
</tr>
<tr>
<td>Access Server</td>
<td>AS.key located in the same directory as AS.xml</td>
</tr>
<tr>
<td>Adapter SDK</td>
<td>&lt;DS_COMMON_DIR&gt;/adapters/adapter.key</td>
</tr>
<tr>
<td>DSConfig.txt</td>
<td>&lt;DS_COMMON_DIR&gt;/conf/DSConfig.key</td>
</tr>
<tr>
<td>Data Services-managed schedules</td>
<td>If the schedule uses a password file, the password is stored in the password file.</td>
</tr>
<tr>
<td></td>
<td>If the schedule does not use a password file, the password is located in the job command line.</td>
</tr>
<tr>
<td>External scheduler command lines</td>
<td>If the schedule uses a password file, the password is stored in the password file.</td>
</tr>
<tr>
<td></td>
<td>If the schedule does not use a password file, the password is located in the job command line.</td>
</tr>
</tbody>
</table>

⚠️ Caution

For encryption keys that are stored in files, Data Services protects the security of the key file with strong OS permissions. For example, the software sets owner-only read & write access to the file (chmod 600 on UNIX systems). You should also protect the key file by restricting user access to the server host machine when possible.

3.7.2 Encrypting passwords manually

In most instances, password encryption is handled automatically by the various Data Services applications and utilities. However, for some tasks, you may need to manually encrypt a password. For example, you may want to generate a data flow on the fly for use with the object creation XML toolkit. If your data flow contains a datastore that requires a password, it needs to be encrypted before you can import and run it successfully.

When you need to manually encrypt a password, you can use the al_encrypt command-line utility installed with the software.

Related Information

Password encryption [page 164]
3.8 Password protection for a Data Services repository

When you log in to the Data Services Designer or open a Data Quality report in the Management Console, by default, you are prompted to enter the user name and password for the Data Services repository you are accessing. You can turn off this default behavior by granting permissions in the BI Platform or Information platform services Central Management Console.

In the CMC, when you grant the *Allow user to retrieve repository password* right, the Data Services' repository password will be sent from the CMS to the client (Designer or Management Console: DQ reports). Although this password is encrypted, and the communication channel can be secured through SSL, sending passwords could pose a risk, and malicious users could obtain access to the password. You can selectively grant this right for repositories. For example, you may want to grant the right for development repositories but not for production repositories.

**Related Information**

Repository management [page 43]

3.8.1 Setting Data Services repository permissions in the CMC

Use the following steps to add permissions for users to automatically retrieve the Data Services repository password when logging on to the Designer and for accessing Data Quality reports.

1. On the Home page of the CMC, click *Data Services*.
2. On the left side of the CMC, select *Repositories*.
4. Select the *Data Services Designer Users* group (for Designer access) or the *Data Services Monitor Users* group (for Data Quality reports access), and then click the *Assign Security* button.
5. In the *Assign Security* window, click the *Advanced* tab.
6. Click *Add/Remove Rights*.
7. On the left of the *Add/Remove Rights* window, click *Application*, and select *Data Services Repository*.
8. Under *Specific Rights for Data Services Repository*, select *Granted* for either or both of the following options:
   - *Allow user to retrieve repository password*
   - *Allow user to retrieve repository password that user owns*
9. Click *OK*.

By following the preceding steps, you have given all users in the Data Services Designer Users group (or the Data Services Monitor Users group) permissions for all Data Services repositories.
Note

If you have a Data Services development or test repository, for example, to which you would like to restrict access, you can do this on a case-by-case basis. To do this, access the Add/Remove Rights window using the following steps:

1. On the Home page of the CMC, click Data Services.
2. On the left side of the CMC, select Repositories, and then select the repository that you want edit rights for.
3. Continue with step 3 above to complete your task.
4 User and rights management

SAP Data Services uses the Central Management Server (CMS) for user accounts and rights management.

This section covers information and procedures specific to administrating Data Services. For detailed information about user accounts and rights management, see the SAP BusinessObjects BI Platform Administrator Guide or the SAP BusinessObjects Information Platform Services Administrator Guide.

4.1 User management

In the Users and Groups management area of the Central Management Console (CMC), you can specify the details required for a user to access Data Services. In addition to creating a user account, you must also grant the user access to any repositories they need to work with.

By default, the Data Services installation program does not create any user accounts. You can use the CMC to create new user accounts, or assign existing user accounts to the Data Services group accounts.

For detailed information about creating user accounts, see “Managing Enterprise and general accounts” in the SAP BusinessObjects BI Platform Administrator Guide or the SAP BusinessObjects Information Platform Services Administrator Guide.

Related Information

Managing security settings for repositories in the CMC [page 44]

4.2 Group management

Groups are collections of users who share the same account privileges. Therefore, you may create groups that are based on department, role, or location. Groups enable you to change the rights for users in one place (a group) instead of modifying the rights for each user account individually. Also, you can assign object rights to a group or groups.

In the Users and Groups area of the Central Management Console (CMC), you can create groups that give a number of people access to the report or folder. This enables you to make changes in one place instead of modifying each user account individually.

In addition to the basic SAP BusinessObjects BI platform or Information platform services group accounts, Data Services includes several default group accounts:
Table 5:

<table>
<thead>
<tr>
<th>Account name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Services Administrator</td>
<td>Members of this group have access to all Data Services administrative functionality.</td>
</tr>
</tbody>
</table>
| Data Services Multi-user Administrator| Members of this group are limited to managing secure central repositories. This role is a subset of the Data Services Administrator role. Multi-user administrators can:  
  - Add and remove secure central repositories.  
  - Manage users and groups.  
  - View secure central repository reports. |
| Data Services Monitor User            | Members of this group have access limited to options available from the Status tabs. For example, a monitor user can abort batch jobs but cannot execute or schedule them. A monitor user can restart, abort, or shut down an Access Server, service, adapter instance, or client interface but cannot add or remove them. |
| Data Services Profiler Administrator  | Members of this group are limited to managing profiler repositories. This role is a subset of the Administrator role. Profiler administrators can:  
  - Manage profiler tasks in any profiler repository.  
  - Manage the Profiler configuration. |
| Data Services Profiler User           | Members of this group are limited to managing profiler tasks in the profiler repository that is configured for the user. |
| Data Services Operator                | Members of this group have all Administrator privileges except they cannot modify repository, access, or CMS servers nor update datastore settings. |
| Data Services Designer                | Members of this group have access to the Designer. Note that application rights and repository security rights are two separate sets of rights. For more information about repository rights, see [Detailed repository rights](#). |

4.2.1 Detailed application rights

Application rights are assigned to each user group. The default application rights granted to each group are described in the following table.

**Note**

The Data Services Administrator group account is granted access to all of the available Data Services application rights.

Table 6:

<table>
<thead>
<tr>
<th>Right name</th>
<th>Designer Users</th>
<th>Monitor Users</th>
<th>Multi-user Administrator</th>
<th>Operator Users</th>
<th>Profiler Admin. Users</th>
<th>Profiler Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Administrator</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to Auto Documentation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to Data Quality Reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to Designer</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to Impact and Lineage</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Right name</td>
<td>Designer Users</td>
<td>Monitor Users</td>
<td>Multi-user Administrator</td>
<td>Operator Users</td>
<td>Profiler Admin. Users</td>
<td>Profiler Users</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Access to Operational Dashboard</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access to Validation Dashboard</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Administrator overview</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Execute batch job</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage access server configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage adapter configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage batch job history</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage central repository groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage certification log configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage datastore and substitution param config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Object Promotion Configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Object Promotion Import</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage profiler configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage real-time client interface status</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage real-time logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage real-time service status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage real-time status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage RFC client and server configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage server group configurations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Manage status interval configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage webservices configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View adapter status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>View batch job history</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Data Quality sample data</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View profiler status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View internal information in log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View real-time client interface status</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View real-time logs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View real-time service status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>View real-time status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
## Right name

<table>
<thead>
<tr>
<th>Right name</th>
<th>Designer Users</th>
<th>Monitor Users</th>
<th>Multi-user Administrator</th>
<th>Operator Users</th>
<th>Profiler Admin. Users</th>
<th>Profiler Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>View RFC client status</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View server group information</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Validation sample data</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View webservices status</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

### Note

Application rights and repository security rights are two separate sets of rights. When a repository is registered, the owner is granted full access to the repository. By default, other Designer users have no access to the repository.

## Related Information

- Viewing application rights assigned to a group [page 41]
- Managing application rights for a group [page 41]
- Detailed repository rights [page 46]

### 4.2.2 Viewing application rights assigned to a group

Your account must be a member of the Administrators user group or a member of the Data Services Administrator Users group to be able access the CMC function for managing user security.

To view a group’s currently assigned application rights:

1. On the Home page of the CMC, select Manage > Applications.
2. In the Application Name list, double-click Data Services Application.
3. Select User Security to display the user groups.
4. Highlight the user group you want to view and click View Security.

The Permissions Explorer opens and displays all of the current application rights that are assigned to your selected user group.

### 4.2.3 Managing application rights for a group

Your account must be a member of the Administrators user group or a member of the Data Services Administrator Users group to be able access the CMC function for managing user security.

To manage a group’s assigned application rights:
1. On the Home page of the CMC, select Manage > Applications.
2. In the Application Name list, double-click Data Services Application.
3. Select User Security to display the configured Data Services application user groups.
4. Highlight the user group or add a user to manage their application rights.
5. Click Assign Security.
6. In the Assign Security window, select the Advanced tab.
7. On the Advanced tab, select Add/Remove rights.
8. In the Add/Remove Rights window, select to add or remove each of the specific right you want to change for this group.
9. Click Apply to save your changes.

Members of the modified group will be granted or denied the application rights you modified for the group the next time they log in.
5 Repository management

Before you can access Data Services repositories in other components such as the Designer and Management Console, you must configure them appropriately.

In general, you follow this workflow to configure a Data Services repository.

1. Create the repository in a database using the Repository Manager.
2. Register the repository in the Central Management Console (CMC).
3. Manage security settings for the repository in the CMC.

5.1 Registering a repository in the CMC

1. Log into the Central Management Console (CMC) as a user with administrative rights to the Data Services application.
2. Go to the Data Services application:
   - Click Data Services from the CMC home screen OR
   - Click the Data Services icon
3. Configure a repository:
   - Choose Manage Configure Repository OR
   - Right-click Repositories in the navigation tree and click Configure Repository
   The Add Data Services Repository screen is displayed.
4. Specify a name and optionally a description for the repository.
   The name and description will be displayed to users when they log into applications such as the Designer and Management Console.
5. Enter the connection information for the repository database.
   The details required depend on the type of database containing the repository and the connection type you choose.
   
   ➤ Tip
   For Microsoft SQL Server and SAP Sybase databases, it is recommended that you do not use localhost as the server name when registering the Data Services repository in the CMC. If you use localhost, other machines will be unable to connect to the repository.

   a. For an Oracle database, the default connection type is TNS-less. If you want to use a TNS connection, select Yes in the drop-down menu for Use TNS Name and enter the TNS Name if no value appears. If the Data Services repository was created using a TNS connection, the software fills in TNS Name. Otherwise, you must enter the TNS Name.
Note

If you created a repository on Oracle RAC, prior to registering in the CMC, you need to configure TNS Name on the local CMS machine. Then the TNS name will be filled in automatically based on the connection string provided when you register in the CMC.

b. For a DB2, MySQL or SAP HANA database, the default connection type is DSN-less. If you want to use a DSN connection, select Yes in the drop-down menu for Use Data Source Name (DSN) and enter the Data Source Name (DSN) if no value appears. If the Data Services repository was created using a DSN connection, the software fills in Data Source Name (DSN). Otherwise, you must enter the Data Source Name (DSN).

Note

If you subsequently edit the properties of the Data Services repository on the CMC to change the connection type to a TNS or DSN connection, you must fill in TNS Name or Data Source Name (DSN).

Note

If you are using DNS or TNS connections in a distributed installation, the database connection to the repository must be configured the same on each machine as in the CMC. For example, if an Oracle repository is configured with the TNS name Ora_DS in the CMC, Designer and Job Server machines must also have the Ora_DS TNS name configured.

6. If you are registering a profiler repository, choose Yes for Is Profiler Repository.
   a. Enter the host name of the web application server hosting the profiler.
   b. Enter the port number used by the web application server hosting the profiler.

7. Click Test Connection. The application attempts to verify the connection details without adding the repository to the CMC. If the connection is not successful, review the error message and correct the repository connection information.

8. Click Save to add the repository to the CMC.

The Data Services application screen is displayed, and the new repository appears in the list of registered repositories.

Related Information

DSN-less and TNS-less connections [page 20]
Using the Repository Manager [page 81]

5.2 Managing security settings for repositories in the CMC

You can manage security settings for repositories registered in the CMC with the security options on the Manage menu. These options let you assign users and groups to the access control list for the repository, view the rights that a user or group has, and modify the rights that the user or group has to the repository.
1. Log into the Central Management Console (CMC) as a user with administrative rights to the Data Services application.

2. Navigate to the Data Services application:
   - Click Data Services on the CMC home screen OR
   - Click the Data Services icon

3. Click Repositories in the navigation tree to display the list of registered repositories.

5.2.1 Viewing rights for a user or group on a repository

In general, you follow this work flow to view rights for a user or group on a repository.

1. Select the repository for which you want to view security settings.

   - The User Security dialog box appears and displays the access control list for the repository.

3. Select a user or group from the access control list, and click View Security.
   - The Permissions Explorer launches and displays a list of effective rights for the user or group on the repository.

5.2.2 Assigning users and groups to an access control list for a repository

An access control list specifies the users that are granted or denied rights to a repository. In general, you follow this work flow to assign a user or group to an access control list, and to specify the rights that the user or group has to the repository.

1. Select the repository to which you want to add a user or group.

   - The User Security dialog box appears and displays the access control list for the repository.

3. Click Add Principals.
   - The Add Principals dialog box appears.

4. Move the users and groups you want to add from the Available users/groups list to the Selected users/groups list.

5. Click Add and Assign Security.

6. Select the access levels you want to grant the user or group:
   - To grant read-only access to the repository, select View.
   - To grant full read and write access to the repository, select Full Control.
   - To deny all access to the repository, select No Access.
5.2.3 Detailed repository rights

Repository rights are assigned to each access control list. Users and groups in the access control list can be granted full control, view access, or no access rights to a repository.

The following table describes the repository rights available to full control and view access.

Table 7:

<table>
<thead>
<tr>
<th>Right name</th>
<th>Full control</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add objects to the folder</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Copy objects to another folder</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Delete objects</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Edit objects</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Modify the rights users have to objects</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Replicate content</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Securely modify right inheritance settings</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Securely modify right users have to objects</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Translate objects</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use access level for security assignment</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View objects</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Note**

Application rights and repository security rights are two separate sets of rights. When a repository is registered, the owner is granted full access to the repository. By default, other Designer users have no access to the repository.

Related Information

Detailed application rights [page 39]
6 Server management

6.1 Setting UNIX environment variables

When you install SAP Data Services on UNIX platforms, the Job Server requires that certain environment variables be set up. To set up these variables, users who run or administer Job Servers must run a script (al_env.sh).

Run this script with the syntax required by your environment. For example:

```
$ cd $LINK_DIR/bin/
$ . ./al_env.sh
```

You can also add this command to your login script so that it is always configured. For example, add the following line to the .profile:

```
. $LINK_DIR/bin/al_env.sh
```

If the script fails to run, no error messages appear. To make sure that the variables’ values are properly set, check one or more of the following:

Table 8:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>$LINK_DIR</td>
<td>Data Services installation directory (set by the installation program).</td>
</tr>
<tr>
<td>$DS_COMMON_DIR</td>
<td>References $LINK_DIR for compatibility (set by the installation program).</td>
</tr>
<tr>
<td>$SHLIB_PATH</td>
<td>If you want to use a 64-bit Oracle client, $LINK_DIR/bin must be listed before any 64-bit Oracle shared library path.</td>
</tr>
<tr>
<td>$LD_LIBRARY_PATH</td>
<td>For Solaris or Linux. Must include $LINK_DIR/bin and the location of the database libraries. If you want to use a 64-bit Oracle client, $LINK_DIR/bin must be listed before any 64-bit Oracle shared library path.</td>
</tr>
<tr>
<td>$LIBPATH</td>
<td>For AIX. Must include $LINK_DIR/bin and the location of the database libraries. If you want to use a 64-bit Oracle client, $LINK_DIR/bin must be listed before any 64-bit Oracle shared library path.</td>
</tr>
<tr>
<td>$ORACLE_SID</td>
<td>Required for an Oracle source, target, or repository.</td>
</tr>
<tr>
<td>$ORACLE_HOME</td>
<td>Required for an Oracle source, target, or repository. If you want to use a 64-bit Oracle client, this must point to the 64-bit Oracle installation.</td>
</tr>
<tr>
<td>$DB2INSTANCE</td>
<td>Required for a DB2 source, target, or repository.</td>
</tr>
</tbody>
</table>
### Variable Details

<table>
<thead>
<tr>
<th>Variable</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>$DB2DIR</td>
<td>Required for a DB2 source, target, or repository.</td>
</tr>
<tr>
<td>$SYBASE</td>
<td>Required for a SAP ASE source, target, or repository.</td>
</tr>
<tr>
<td>$SYBASE_OCS</td>
<td>Required for a SAP ASE source, target, or repository.</td>
</tr>
<tr>
<td>$ODBCINI</td>
<td>Required for ODBC sources or targets, including MySQL and SAP HANA.</td>
</tr>
<tr>
<td>$PATH</td>
<td>Must include $LINK_DIR/bin and <code>&lt;databasehome&gt;</code>/bin.</td>
</tr>
</tbody>
</table>

**Tip**

Use the `echo` command to verify environment variable settings.

If the variable settings are not properly configured and you start any Data Services utility, error messages indicate that database server files are missing.

If you see such an error, verify that `al_env.sh` contains commands to set the appropriate database home locations. Run `al_env.sh` for the account used by the Job Server, or start the Job Server using an account that has all necessary environment variables defined in its `.profile`.

**Tip**

If you want to use the RFC Server Interface in the Management Console on a 64-bit UNIX platform, see the `Management Console Guide` for additional environment configuration information.

### 6.1.1 Configuring additional database connectivity

When you install SAP Data Services on UNIX platforms, the installation setup program configures the following by default:

- **DSN or TNS connections for the repository database**
  
  To use a DSN-less or TNS-less connection, defer repository creation to after installation and when you subsequently invoke the Repository Manager, specify the `-s` option to use a server name connection.

- **Database connectivity for the repository only**
  
  To access other database systems as sources and targets in your jobs, you need to add the appropriate configuration information to the `al_env.sh` file. Use the Connection Manager that is installed with Data Services to set the environment variables required for the following database types:
  
  - Attunity
  - DB2 on iSeries or zSeries
  - Informix
  - MySQL
  - Netezza
  - Oracle
  - SAP HANA
  - SAP ASE
  - SAP Sybase IQ
- SAP Sybase SQL Anywhere
- SQL Server
- Teradata

**Note**
For the most current list of databases types supported by the Connection Manager, see the *Product Availability Matrix (PAM)* at [https://apps.support.sap.com/sap/support/pam](https://apps.support.sap.com/sap/support/pam).

**Related Information**
- Using the Connection Manager for UNIX systems [page 53]
- Configuring ODBC data sources on UNIX using DSN connections [page 57]
- Configuring ODBC drivers on UNIX for data sources using DSN-less connections [page 54]

## 6.2 Starting services automatically

### On Windows

The SAP Data Services service and packaged Tomcat service start automatically when the computer restarts. The Data Services service then starts Job Servers and Access Servers on the restarted computer.

You can change service startup to *Manual* in the Windows services window.

**Note**
To manually log in Web applications, refer to “Configuring tracing for web applications” section in the *Information platform services Administration Guide*.

### On UNIX

To start Job and Access Servers automatically when the server restarts, you must install the `actaservices` script with root privileges.

**Run the $LINK_DIR/bin/autostrt.sh script:**

```bash
# cd $LINK_DIR/bin/
# autostrt.sh $LINK_DIR
```
6.3 History retention and Job Server log retention

The job execution history files and the Job Server logs contain data that you may need to produce internal statistics, regulatory reports, or other nonregulatory reports.

You set the time period for the software to retain the data. The time period also determines when the software automatically and permanently deletes this data. Therefore, know what these logs contain before you make the retention period settings.

**Tip**

If you intend to create reports based on specific jobs, transforms, time periods, and job statistics, make local backup copies of the job execution files and the Job Server log files before the retention period expires.

Why delete any files at all? The software appends information to existing log files for each job that you run. As a result, the files can get large, which can slow processes and effect software performance. Therefore, establish some sort of maintenance management procedure.

**Caution**

You can select to delete job server and history files for a specific batch job in the Data Services Management Console. The software deletes the selected job, history, and log files, and ignores the settings for retention periods in the CMC.

For more information about deleting jobs, history, and log files for the selected job in the Data Services Management Console, see the Management Console Guide.

**Related Information**

- USPS-required log files and reports [page 50]
- Deleting batch job history data [page 106]
- Monitoring jobs [page 103]

6.3.1 USPS-required log files and reports

The default setting for the History Retention Period is 30 days, which does not provide enough time to generate some USPS reports.

If you have postal certification requirements such as CASS certification, you are required to submit log files to the postal authorities on a periodic basis. For example, if you have included the USA Regulatory Address Cleanse transform in your data flow, and you use the DSF2 or NCOALink functionality and have CASS enabled, you must submit certification log files to the USPS each month. With that in mind, set the log retention period so that you will not lose data prior to the creation and submission of the logs (thus submitting incomplete log files to the USPS).
The default setting of 30 days does not provide enough time for you to export and send the log files to the USPS by the monthly due date. And 30 days does not account for months that include 31 days. Therefore we recommend setting the history retention to longer (50 days for example) to ensure that you submit complete monthly logs to the USPS. Set the number of days in **History Retention Period** in the CMC.

In addition to sending monthly data to the USPS, you are required to have report data available for the USPS to examine for several years after the job is processed. (Make sure you are aware of current USPS rules for data retention by viewing your USPS licensing agreement.) To ensure that you retain all required reports and logs before the data is deleted from the repository, we recommend that you export the required reports and logs from the repository to a local folder on a monthly basis. This also prevents the repository contents from becoming so large that the export process “times out” due to the volume of statistics retained.

### Related Information

[Setting the History Retention Period](#) [page 51]

### 6.3.2 Setting the History Retention Period

The **History Retention Period** provides an automatic way to save or delete the job execution history.

You can view currently stored job execution history files with the Administrator application in the Data Services Management Console.

**⚠️ Caution**

Many history files contain job statistics for statistical reports and other information required for regulatory reports. Make sure that you understand what your job history files are used for before you set a number of days to delete them.

1. In the Central Management Console (CMC), select **Applications**.
2. Right-click **Data Services Application** from the **Application Name** column and select **Settings**.
   
   The **Data Services Application Settings** window opens.
3. Type a number in the **History Retention Period** text box. The number sets the number of days the software retains the job execution history files.

<table>
<thead>
<tr>
<th>Value</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Default setting. Software retains job history files for 30 days.</td>
</tr>
<tr>
<td>0</td>
<td>Software does not retain job history files.</td>
</tr>
</tbody>
</table>
4. Click **Save**.

After you click **Save**, the software may take up to an hour to apply the settings because of background processing.

For information about regulatory statistics and log files, see the Designer Guide. For information about data quality reports and troubleshooting the Administrator in the Data Services Management Console, see the Management Console Guide. Also see information about trace and error logs in the Management Console Guide.

**Related Information**

- History retention and Job Server log retention [page 50]
- Setting the Job Server Log Retention Period [page 52]
- USPS-required log files and reports [page 50]

### 6.3.3 Setting the Job Server Log Retention Period

The Job Server Log Retention Period provides an automatic way to delete the Job Server log files such as the server_event*.logs.

You can view currently stored Job Server log files in the Data Services Management Console using the Administrator application.

**Caution**

Many log files contain job statistics and other information for statistical and regulatory reports. Make sure that you understand what your Job Server log files are used for before you set the number of days to delete them.

1. In the Central Management Console (CMC), select **Applications**.
2. Right-click **Data Services Application** from the Application Name column and select **Settings**.

   The Data Services Application Settings window opens.

3. Type a number in the Job Server Log Retention Period text box. The number sets the number of days in which the software retains the Job Server log files.

<table>
<thead>
<tr>
<th>Value</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Default setting. Software retains Job Server logs for 30 days.</td>
</tr>
<tr>
<td>0</td>
<td>Software does not retain Job Server logs</td>
</tr>
</tbody>
</table>
4. Click **Save**.

After you click **Save**, the software may take up to an hour to apply the settings because of background processing.

For information about regulatory statistics and log files, see the Designer Guide. For information about data quality reports and troubleshooting the Administrator in the Data Services Management Console, see the Management Console Guide.

---

### Related Information

- History retention and Job Server log retention [page 50]
- Setting the History Retention Period [page 51]
- USPS-required log files and reports [page 50]

### 6.4 Configure ODBC data sources on UNIX

Information and instructions to configure various ODBC drivers and data sources on UNIX operating systems.

#### 6.4.1 Using the Connection Manager for UNIX systems

Use the Data Services Connection Manager on UNIX to create, edit, or delete ODBC data sources and ODBC drivers after installation.

To use the graphical user interface for Connection Manager, you must install the GTK+2 library. The GTK+2 is a free multi-platform toolkit that creates user interfaces. For more information about obtaining and installing GTK +2, see [http://www.gtk.org](http://www.gtk.org).

1. For DSN connections, set `$ODBCINI` to the location of the database client vendor’s ODBC .ini file. Do not point to the Data Service ODBC .ini file. Make sure that the file is readable and writeable. For example, for DataDirect drivers that are installed in the default location, you would point here:

   ```
   $LINK_DIR/DataDirect/odbc/odbc.ini
   ```

2. Invoke the Connection Manager by entering the following commands:

   ```
   $ cd $LINK_DIR/bin/
   $ ./DSConnectionManager
   ```

   The **SAP Data Services Connection Manager** window opens.
Note

If the GTK+2 library is not installed, the command-line user interface starts. The remaining steps assume you have the user interface.

3. For DSN connections, open the Data Sources tab and configure data sources as needed. See the following sections for specific data sources.
4. For server name connections, open the Drivers tab to configure ODBC drivers.
5. Click Restart Services to restart the EIM Adaptive Process Service and Data Services Job Service.

Related Information

Using the ODBC Driver Selector on Windows for server name connections [page 81]

6.4.1.1 Configuring ODBC drivers on UNIX for data sources using DSN-less connections

On UNIX and Linux platforms, SAP Data Services requires an ODBC driver library for ODBC data sources using DSN-less connections. The UNIX ODBC driver configuration file:

- Contains driver names that reference ODBC driver libraries.
- Is an ODBC instance file referenced by the $ODBCINST environment variable.

Tip

For natively supported ODBC databases, you do not need to manually configure the ODBC instance file. Instead, set $ODBCINST to the name of the ODBC instance file and use the Data Services Connection Manager to properly configure the ODBC driver library.

6.4.1.1.1 Configuring native ODBC drivers on UNIX

Run the Connection Manager to configure the ODBC driver library and associated environment variables required to run a Data Services job that contains one of the following source or target database types using DSN-less connections:

- DB2 UDB
- Informix
- MySQL
**Note**
For MySQL driver, set $ODBCSYSINI (instead of $ODBCINST) and make sure $ODBCSYSINI/odbcinst.ini exists. If you do not set $ODBCSYSINI, Data Services will, by default, use /etc/odbcinst.ini for the instance file.

- Netezzta
- Oracle
- SAP HANA
- SAP Sybase IQ
- Teradata

**Note**
For the most current list of database types supported for DSN-less connections, see the Release Notes.

1. For a DSN-less connection, set $ODBCINST to a file in which the Connection Manager will define the ODBC driver according to your input on the **Drivers** tab. Ensure that the file is readable and writable. For example:

   ```bash
   export ODBCINST=<dir-path>/odbc.inst
touch $ODBCINST
   ```

2. Invoke the Connection Manager by entering the following command:

   ```bash
   $LINK_DIR/bin/DSConnectionManager.sh
   ```

3. Click the **Drivers** tab, and click **Add**.
   a. On the **Select Database Type** window, select the database type and click **OK**. The **Configuration for...** window appears with the value filled in for ODBC Inst File.
   b. Provide values for the driver properties. For the relevant driver properties for each database type, see Properties for ODBC data sources using DSN-less connections [page 56].

4. Provide values for the following properties (they will not be saved for further use).
   - Server name
   - Port (if relevant)
   - Database (if relevant)
   - User name
   - Password

5. If you want to test the connection, click **Test Connection**.

6. Click **Restart Services** to restart the following services:
   - Both the EIM Adaptive Process Service and Data Services Job Service if Data Services is installed at the same location (machine and folder) as Information Platform Services (IPS) or BI platform. A prompt will appear for the CMS password.
   - Only the Data Services Job Service if Data Services is installed without IPS or BI platform.

7. If you will run another command such as the Repository Manager, source the al_env.sh script to set the environment variables.
   By default, the script is located at `<LINK_DIR>/bin/al_env.sh`. 
6.4.1.2 Properties for ODBC data sources using DSN-less connections

The Connection Manager configures the $ODBCINST file based on the property values that you enter on the Drivers tab. The following table lists the properties that are relevant for each database type.

Table 11:

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Properties on Drivers tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>• ODBC Inst File</td>
</tr>
<tr>
<td></td>
<td>• Driver Version</td>
</tr>
<tr>
<td></td>
<td>• Unix ODBC Lib Path</td>
</tr>
<tr>
<td></td>
<td>• Driver Name</td>
</tr>
<tr>
<td></td>
<td>• Driver</td>
</tr>
<tr>
<td></td>
<td>• Server Name</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Database</td>
</tr>
<tr>
<td></td>
<td>• User Name</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td>SAP HANA</td>
<td>• ODBC Inst File</td>
</tr>
<tr>
<td></td>
<td>• Driver Version</td>
</tr>
<tr>
<td></td>
<td>• Driver Name</td>
</tr>
<tr>
<td></td>
<td>• Driver</td>
</tr>
<tr>
<td></td>
<td>• Server Name</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• User Name</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td>Teradata</td>
<td>• ODBC Inst File</td>
</tr>
<tr>
<td></td>
<td>• Driver Version</td>
</tr>
<tr>
<td></td>
<td>• Driver Name</td>
</tr>
<tr>
<td></td>
<td>• Driver</td>
</tr>
<tr>
<td></td>
<td>• Server Name</td>
</tr>
<tr>
<td></td>
<td>• User Name</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td>Netezza</td>
<td>• ODBC Inst File</td>
</tr>
<tr>
<td></td>
<td>• Driver Version</td>
</tr>
<tr>
<td></td>
<td>• Driver Name</td>
</tr>
<tr>
<td></td>
<td>• Driver</td>
</tr>
<tr>
<td></td>
<td>• Server Name</td>
</tr>
<tr>
<td></td>
<td>• Port</td>
</tr>
<tr>
<td></td>
<td>• Database</td>
</tr>
<tr>
<td></td>
<td>• User Name</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
</tbody>
</table>
### Database Type

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Properties on Drivers tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Sybase IQ</td>
<td>• ODBC Inst File&lt;br&gt;• Driver Version&lt;br&gt;• Driver Name&lt;br&gt;• Driver&lt;br&gt;• Server Name (This is also known as the host name. For example, a host name may be vanpgc13b9.)&lt;br&gt;• Port&lt;br&gt;• Engine Name (This is also known as the server name. For example, a server name may be vanpgc13b9_iqdemo.)&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Informix</td>
<td>• ODBC Inst File&lt;br&gt;• Driver Version&lt;br&gt;• Driver Name&lt;br&gt;• Informix Home Path&lt;br&gt;• Server Name&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>DB2 UDB</td>
<td>• DB2 Client Path&lt;br&gt;• Driver Version&lt;br&gt;• Server Name&lt;br&gt;• Port&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Oracle</td>
<td>• Oracle Home Path&lt;br&gt;• Driver Version&lt;br&gt;• Server Name&lt;br&gt;• Port&lt;br&gt;• SID&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
</tbody>
</table>

### 6.4.2 Configuring ODBC data sources on UNIX using DSN connections

On UNIX and Linux platforms, SAP Data Services requires an ODBC driver manager library and ODBC driver library to configure ODBC data sources using data source name (DSN) connections.

Some ODBC driver vendors include ODBC driver manager and ODBC driver capabilities in one single library, while others separate them into two individual libraries.
To accommodate all ODBC vendors, Data Services requires configurations in two different files for DSN connections:

1. The UNIX ODBC driver manager configuration file (<LINK_DIR>/bin/ds_odbc.ini). This file contains DSN instances that reference ODBC driver manager libraries.

   **Tip**

   For natively supported ODBC databases, you do not need to manually configure `ds_odbc.ini`. Instead, use the Data Services Connection Manager to properly configure the ODBC driver manager library.

2. The ODBC vendor’s configuration files (referenced by the `$ODBCINI` environment variable). This file contains DSN instances that reference the ODBC driver libraries, as well as the database server connection information.

   **Note**

   One ODBC configuration file can contain multiple DSN instances. For example, a file referenced by `$ODBCINI` may contain DSNs for MySQL, Netezza, and Teradata.

### 6.4.2.1 Configuring native ODBC data sources

Data Services supports several ODBC data sources natively with DSN connections, including:

- Attunity
- DB2 on iSeries or zSeries
- Informix
- MySQL
- Netezza
- SAP HANA
- SAP ASE
- SAP Sybase IQ
- SQL Server
- Teradata

**Note**

For the most current list of natively supported ODBC data sources, see the *Release Notes*.

You can use the Connection Manager to set the Data Services ODBC configuration and associated environment variables required to run a Data Services job that contains a source or target that is one of the above database types. Other generic ODBC data sources require additional manual configuration.

To run the Connection Manager to configure an ODBC source with a DSN connection:

1. Set `$ODBCINI` to a file in which the Connection Manager will define the DSN according to your input on the *Data Sources* tab. Ensure that the file is readable and writable.

   For example:

   ```bash
   export ODBCINI=<dir-path>/odbc.ini
   ```
1. Invoke the Connection Manager by entering the following command:
   $LINK_DIR/bin/DSConnectionManager.sh
2. Click the Data Sources tab, and click Add to display the list of database types.
3. On the Select Database Type window, select the database type and click OK.
   The Configuration for... window appears with some of the connection information filled in with information that the Connection Manager detected:
   ○ The absolute location of the odbc.ini file in which the DSN will be defined
   ○ Driver (if relevant for database type)
   ○ Driver Version (if relevant for database type)
4. Provide values for additional connection properties (such as Server Name, Instance, or Port) for the specific database type.
   For a list of relevant properties for each database type, see Properties for ODBC data sources using DSN connections [page 60].
5. Provide the following properties (they will not be saved for further use).
   ○ User name
   ○ Password
6. If you want to test the connection, click Test Connection.
7. Click Restart Services to restart the following services:
   Restart Services
   ○ Both the EIM Adaptive Process Service and Data Services Job Service if Data Services is installed at the same location (machine and folder) as Information Platform Services (IPS) or BI platform. A prompt will appear for the CMS password.
   ○ Only the Data Services Job Service if Data Services is installed without IPS or BI platform.
8. If you will run another command such as the Repository Manager, source the al_env.sh script to set the environment variables.
   By default, the script is located at $LINK_DIR/bin/al_env.sh.

Related Information

Configuring other ODBC data sources [page 65]
Properties for ODBC data sources using DSN connections [page 60]
6.4.2.2 Properties for ODBC data sources using DSN connections

The Connection Manager configures the $ODBCINI file based on the property values that you enter on the Data Sources tab. The following table lists the properties that are relevant for each database type.

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Properties on Data Sources tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Unix ODBC Lib Path&lt;br&gt;• Driver&lt;br&gt;• Driver Version&lt;br&gt;• Server Name&lt;br&gt;• Port&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>SQL Server</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Server Name&lt;br&gt;• Port&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>SAP HANA</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Driver&lt;br&gt;• Server Name&lt;br&gt;• Instance&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>DB2 on iSeries or zSeries</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Server Name&lt;br&gt;• Port&lt;br&gt;• Location&lt;br&gt;• Collection&lt;br&gt;• Package Collection&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Database Type</td>
<td>Properties on Data Sources tab</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Teradata</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Teradata Install Path&lt;br&gt;• Teradata Version&lt;br&gt;• Server Name&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Netezza</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Driver&lt;br&gt;• Driver Version&lt;br&gt;• Server Name&lt;br&gt;• Port&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Sybase IQ</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Driver&lt;br&gt;• Server Name (This is also known as the host name. For example, a host name may be vanpgc13b9.)&lt;br&gt;• Port&lt;br&gt;• Engine Name (This is also known as the server name. For example, a server name may be vanpgc13b9_iqdemo.)&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>SAP ASE</td>
<td>• Sybase Home Path&lt;br&gt;• OCS&lt;br&gt;• Server Name&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Informix</td>
<td>• ODBC Ini File&lt;br&gt;• DSN Name&lt;br&gt;• Driver&lt;br&gt;• Server Name&lt;br&gt;• Database&lt;br&gt;• User Name&lt;br&gt;• Password</td>
</tr>
<tr>
<td>Attunity</td>
<td>• Attunity Driver Path</td>
</tr>
</tbody>
</table>
6.4.2.3 Configuring MySQL ODBC for DSN connections

Run the Connection Manager to set the Data Services ODBC configuration and associated environment variables required to run a Data Services job that contains a MySQL source or target.

1. Follow the same steps as in Configuring native ODBC data sources [page 58].
2. The MySQL ODBC connector driver (libmyodbc<version>.so) has a dependency on the unixODBC driver manager (libodbc.so) provided by www.unixodbc.org.
   a. If you do not already have the unixODBC driver manager on your system, you must acquire and build the driver manager to resolve this dependency.
   b. Make sure you have the directory location of libodbc.so from the unixODBC installation as the first directory in the beginning of LD_LIBRARY_PATH/LIBPATH/SHLIB_PATH.

   **Caution**
   If the first directory in LD_LIBRARY_PATH/LIBPATH/SHLIB_PATH has libodbc.so from a location other than the unixODBC installation, a job using MySQL as source/target/repository may not work as expected.

6.4.2.3.1 Installing the unixODBC driver for Linux

To install the unixODBC driver, you must be using a version of Linux supported by SAP Data Services.

There are two ways to install the unixODBC libraries on Linux:

1. Install the bundled rpm unixODBC package on the Linux installation CD. For example, the the rpm package name on Redhat 5 64-bit is unixODBC-2.2.11-7.1.
2. Download and install the 64-bit unixODBC (x86_64) package from the following location: [http://sourceforge.net/projects/unixodbc/files/unixODBC/2.2.14/unixODBC-2.2.14-linux-x86-64.tar.gz/download](http://sourceforge.net/projects/unixodbc/files/unixODBC/2.2.14/unixODBC-2.2.14-linux-x86-64.tar.gz/download)

6.4.2.3.2 Building and installing the unixODBC driver for AIX

To install the unixODBC driver, you must be using a version of AIX supported by SAP Data Services, have the VisualAge C++ compiler (version 6.0 or greater), and download the unixODBC source.

1. Download and extract the unixODBC package.

   **Note**
   The downloaded file will be named unixODBC-2.2.12.tar.tar.

   b. Rename the unixODBC package.

```
mv unixODBC-2.2.12.tar.tar unixODBC-2.2.12.tar.gz
```
c. Extract the package with `gunzip` and `tar`.

```
gunzip unixODBC-2.2.12.tar.gz
tar -xvf unixODBC-2.2.12.tar
```

d. Change to the newly created `unixODBC-2.2.12` directory.

```
cd $TEMP/unixODBC-2.2.12
```

2. Make the libraries and programs.

a. Ensure that `xlC` (the C++ compiler) is in the `PATH` environment variable, and add it if necessary.

   ○ Using ksh:

   ```
   export PATH=/usr/vacpp/bin:$PATH
   ```

   ○ Using csh:

   ```
   setenv PATH /usr/vacpp/bin:$PATH
   ```

b. Configure the C compiler to be thread-enabled:

```
export CC=xlc_r
export CCC=xlc_r
```

c. To compile a 64-bit version of the driver manager using the `xlc_r` compilers, set the `OBJECT_MODE` and `CFLAGS` environment variables:

```
export OBJECT_MODE=64
export CFLAGS=-q64
```

d. Build the package.

```
./configure --enable-gui=no --enable-drivers=no
make
make install
```

**Note**

By default, the files are installed to `/usr/local`. You can specify a different location by altering the `prefix` option:

```
./configure --prefix=<new_location> --enable-gui=no --enable-drivers=no
```

where `<new_location>` is the location where you want to install the unixODBC libraries.

e. If you will be dynamically loading the driver manager from `/prefix/lib`, extract `libodbc.a`, `libodbcinst.a`, and `libodbccr.a`.

```
ar -x -X 64 libodbc.a
ar -x -X 64 libodbcinst.a
ar -x -X 64 libodbccr.a
```

f. Create the dynamically linked library.

```
ln -s libodbcinst.so.1 libodbcinst.so
```

3. Add the unixODBC library to the `$LIBPATH` environment variable.
For example:

```bash
export LIBPATH=<install_path>:\$LIBPATH
```

where `<install_path>` is the location where all the unixODBC libraries are installed.

### 6.4.2.3.3 Building and installing the unixODBC driver for Solaris

To install the unixODBC driver, you must be using a version of Solaris supported by SAP Data Services, have the Sun C++ compiler (version 5.5 or greater), and download the unixODBC source.

1. Download and extract the unixODBC package.
   
   **Note**
   
   The downloaded file will be named `unixODBC-2.2.12.tar.tar`.
   
   b. Rename the unixODBC package.

   ```bash
   mv unixODBC-2.2.12.tar.tar unixODBC-2.2.12.tar.gz
   ```

   c. Extract the package with `gunzip` and `tar`.

   ```bash
   gunzip unixODBC-2.2.12.tar.gz
tar -xvf unixODBC-2.2.12.tar
   ```

   d. Change to the newly created `unixODBC-2.2.12` directory.

   ```bash
   cd $TEMP/unixODBC-2.2.12
   ```

2. Make the libraries and programs.
   a. Ensure that CC (the C++ compiler) is in the `PATH` environment variable, and add it if necessary.

   - Using ksh:
     ```bash
     export PATH=/home4/thirdparty/software/sunonecc/8.0-sj/SUNWspro/bin/CC:
     $PATH
     ```

   - Using csh:
     ```bash
     setenv PATH /home4/thirdparty/software/sunonecc/8.0-sj/SUNWspro/bin/CC:
     $PATH
     ```

   b. Build the package using the standard GNU autoconf process.

   ```bash
   ./configure CFLAGS="-xarch=v9" LDFLAGS="-xarch=v9" CXXFLAGS="-xarch=v9" --enable-gui=no
   make
   make install
   ```
By default, the files are installed to `/usr/local`. You can specify a different location by altering the prefix option:

```
./configure --prefix=<new_location>/unixODBC CFLAGS="-xarch=v9" LDFLAGS="-xarch=v9" CXXFLAGS="-xarch=v9" --enable-gui=no
```

where `<new_location>` is the location where you want to install the unixODBC libraries.

3. Add the unixODBC library to the `$LD_LIBRARY_PATH` environment variable. For example:

```
export LD_LIBRARY_PATH=<install_path>/unixODBC/lib:$LD_LIBRARY_PATH
```

where `<install_path>` is the location where all the unixODBC libraries are installed.

### Troubleshooting

You might need to troubleshoot the following situations:

- To determine whether all dependent libraries are set properly in the environment variables, you can use the `ldd` command on the ODBC driver manager library and the ODBC driver library. For example:

```
ldd tdata.so
```

If you see that any dependent libraries are missing, ensure that you have added the environment settings to the session running the job service, or consult your ODBC driver vendor’s documentation.

- If an error occurs when using the Connection Manager, invoke it from the command line by using the `-c` option, and use the `-d` option to show details in the log. For example:

```
$LINK_DIR/bin/DSConnectionManager.sh -c -d
```

The log file path is `$LINK_DIR/log/DSConnectionManager.log`. Possible errors include the following:

- The Connection Manager cannot connect to database
- The Data Services Job Server cannot connect to database

### Configuring other ODBC data sources

In addition to the natively-supported ODBC data sources, Data Services can access other ODBC data sources when you use the bundled DataDirect ODBC driver or another ODBC driver.
Tip

It is recommended that you use the Data Services Connection Manager to configure ODBC data sources such as Microsoft SQL server and DB2 on zSeries or iSeries. The Connection Manager is an interactive user interface that simplifies the manual configuration steps of the DataDirect ODBC driver. For details about using the Connection Manager, see Configuring native ODBC data sources [page 58].

If you want to use the DataDirect ODBC driver to connect to ODBC data sources such as Microsoft SQL server and DB2 on zSeries or iSeries from Data Services on a Linux or Unix platform, follow these steps:

1. Add the data source to the Data Services ODBC driver manager configuration file (<LINK_DIR>/bin/ds_odbc.ini).
   For Microsoft SQL Server:
   ```
   [test_Microsoft_SQL_SERVER]
   Driver = <install_location>/lib/[DA][DD]sqls<xx>.so
   RebrandedLib = TRUE
   ```
   where `<install_location>` is the location of the DataDirect ODBC driver.
   For DB2 on zSeries or iSeries:
   ```
   [test_DB2]
   Driver = <install_location>/lib/[DA][DD]db2<xx>.so
   RebrandedLib = TRUE
   ```
   where `<install_location>` is the location of the DataDirect ODBC driver.

   **Note**
   
   RebrandedLib = TRUE is required when using the SAP rebranded Data Direct driver.

2. Add the data source to the ODBC vendor's configuration file (referenced by $ODBCINI).

   **Note**
   
   The version number and driver filenames are subject to change with each release. Access $LINK_DIR/DataDirect/odbc/odbc.ini to view the current version information.

   **Note**
   
   EnableQuotedIdentifiers = 1 is required for Microsoft SQL server
For Microsoft SQL Server:

```
[test_Microsoft_SQL_SERVER]
Driver=<install_location>/lib/[DA][DD]msss<xx>.so
Description=DataDirect <current version number> SQL Server Wire Protocol
AlternateServers=
AnsINPW=Yes
ConnectionRetryCount=0
ConnectionRetryDelay=3
Database=<database_name>
EnableQuotedIdentifiers=1
HostName=<SQL_Server_host>
LoadBalancing=0
LogonID=
Password=
PortNumber=<SQL_Server_server_port>
QuotedId=No
ReportCodePageConversionErrors=0
DriverExpirationBehavior=1
```

where `<install_location>` is the location of the DataDirect ODBC driver.

For DB2 on zSeries or iSeries:

```
[test_DB2]
Driver=<install_location>/lib/[DD][DA]db2<xx>.so
Description=DataDirect <current version number> DB2 Wire Protocol
AddStringToCreateTable=
AlternateID=
AlternateServers=
ApplicationUsingThreads=1
AuthenticationMethod=0
CatalogSchema=
CharsetFor65535=0
#Collection applies to z/OS and iSeries only
Collection=<collection_name>
ConnectionRetryCount=0
ConnectionRetryDelay=3
#Database applies to DB2 UDB only
Database=<database_name>
DefaultIsolationLevel=1
DynamicSections=200
EncryptionMethod=0
GrantAuthid=PUBLIC
GrantExecute=1
GSSClient=native
HostNameInCertificate=
IpAddress=<DB2_server_host>
LoadBalancing=0
#Location applies to z/OS and iSeries only
Location=<location_name>
LogonID=
Password=
PackageCollection=<package_collection>
PackageOwner=
ReportCodePageConversionErrors=0
TcpPort=<port number>
TrustStore=
TrustStorePassword=
UseCurrentSchema=1
ValidateServerCertificate=1
WithHold=1
XMLDescribeType=-10
```

where `<install_location>` is the location of the DataDirect ODBC driver.
3. Run the $LINK_DIR/DataDirect/odbc/odbc.sh script to add the environment settings to the session running the job service.

6.4.3.2 Driver manager configuration file for DSN connections

Enclose data source names in square brackets. Properties follow on subsequent lines and use PropertyName = PropertyValue. For example:

```
[test_source]
Driver   = /path/to/driver
OdbcConformanceLevel  =
LazyLoading =
ODBC64SqlHandleSize =
ODBC64SqlLenSize =
DriverUnicodeType =
```

In this example, test_source is the name of data source that can be loaded using the specified driver library file. Default values apply when optional properties are left blank.

Follow these guidelines when editing the $LINK_DIR/bin/ds_odbc.ini file:

- Each data source name must at least have a driver property defined, which allows the driver manager to load the driver when connecting to the database.
- The pound sign (#) as the first character in any line denotes a comment.
- All leading blanks and trailing blanks in data source names and properties are ignored.

The following table lists the data source configuration parameters for ds_odbc.ini (and ds_odbc.ini.sample):

Table 13:

<table>
<thead>
<tr>
<th>Key</th>
<th>Required</th>
<th>Valid value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver</td>
<td>Yes</td>
<td>A full path including the ODBC driver library name. The directory containing the dependent libraries must be in the shared library path (for AIX, LIBPATH; for Solaris or Linux, LD_LIBRARY_PATH). Check vendor documentation for what you need to add to the shared library path.</td>
<td>Driver=/home/mysql/myodbc/lib/libmyodbc3_r.so</td>
</tr>
<tr>
<td>Key</td>
<td>Required</td>
<td>Valid value</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
</tbody>
</table>
| OdbcConformanceLevel   | No       | A decimal value specifying the ODBC conformance level of driver. Default value is 0, in which case the driver detects by loading 2.x followed by 3.x functions from the driver. When any value greater than or equal to 4.0 is specified, the driver manager prints a run time error.  
**Note**  
An ODBC driver can be compliant to either 2.x or 3.x or both. The UNIX ODBC driver manager detects if the driver is 2.x or 3.x compliant and loads the respective compatible ODBC API functions. If the driver is both 2.x and 3.x compliant, then the driver manager only loads the 2.x ODBC API. You can override this behavior by specifying, for example,  
OdbcConformanceLevel = 3.0. As a result, the ODBC driver manager only loads 3.x ODBC API functions.                                                                 | OdbcConformanceLevel = 0  
OdbcConformanceLevel = 3.0                                                                                                                   |
| LazyLoading            | No       | You can specify a Boolean TRUE/YES or FALSE/NO. Default value is FALSE. The UNIX ODBC Driver Manager loads the ODBC driver and instructs the operating system to load all of its dependent libraries. This flag is useful when certain dependent libraries of the ODBC driver are not required and the ODBC vendor recommends to load the library in lazy mode. | LazyLoading=TRUE                                                                                      |
| ODBC64SqlHandleSize    | Yes      | 32 or 64  
If blank or other, the software uses the default value of 64. The standard definition of the SQLHANDLE data type in 64-bit ODBC is 64-bit integer. However, some ODBC drivers do not conform to this standard; therefore, use this parameter to specify the actual size of SQLHANDLE. DataDirect 64-bit ODBC drivers conform to the standard, so ignore or set to 64 for DataDirect. For other 64-bit ODBC drivers, contact your vendor to determine the actual size of SQLHANDLE.  
**Note**  
This option is required only for 64-bit platforms.                                                                                          | ODBC64SqlHandleSize=  
64                                                                                                                                           |
### Key

<table>
<thead>
<tr>
<th>Key</th>
<th>Required</th>
<th>Valid value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODBC64SqlLenSize</td>
<td>Yes</td>
<td>32 or 64</td>
<td>ODBC64SqlLenSize=64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If blank or other, the software uses the default value of 64. The standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>definition of the SQLLEN data type in 64-bit ODBC is 64-bit integer. However,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>some ODBC drivers do not conform to this standard; therefore, use this</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>parameter to specify the actual size of SQLLEN. DataDirect 64-bit ODBC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>drivers conform to the standard, so ignore or set to 64 for DataDirect. For</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>other 64-bit ODBC drivers, contact your vendor to determine the actual size</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>of SQLLEN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This option is required only for 64-bit platforms.</td>
<td></td>
</tr>
<tr>
<td>DriverUnicodeType</td>
<td>Yes</td>
<td>1 (for UTF16)</td>
<td>DriverUnicodeType=2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 (for UTF8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If blank, other, or not detectable, the software uses the default value of 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This integer value specifies the ODBC driver Unicode type. DataDirect SQL</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Server ODBC driver only supports W functions; for this driver, specify 2.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This option is required only for ODBC drivers that only support W functions.</td>
<td></td>
</tr>
</tbody>
</table>

### 6.5 Configure SSL for Microsoft SQL Server

Configure Microsoft SQL Server database to use SSL protocol for all network transmissions between the database server and SAP Data Services.

**Caution**

Only an administrator or someone with sufficient experience should configure SSL encryption for Microsoft SQL Server database.

**Note**

This feature is available in SAP Data Services version 4.2 SP 7 (14.2.7.0) or later.
To set up SSL for Microsoft SQL Server database datastores, perform the following tasks:

- Import the Microsoft SQL Server certificate into the trusted root certificate store for the client server. For Windows, use the Microsoft Management Console (MMC). For Unix, use the Data Services Certificate Manager (DSCertManager.sh). The import process configures your client to trust the root authority of the database certificate.
- Enable SSL encryption in the Microsoft SQL Server database datastore.

**Note**

Enabling SSL encryption slows down job performance.

**Related Information**

- Configuring SSL for Microsoft SQL Server database on Unix [page 72]
- Configuring SSL for Microsoft SQL Server database on Windows [page 71]

### 6.5.1 Configuring SSL for Microsoft SQL Server database on Windows

Configure SSL for Microsoft SQL Server database on Windows so that you can create a SSL-enabled Microsoft SQL Server database datastore.

Obtain a private key file and server certificate for Microsoft SQL Server from a trusted authority. You can also create your own private key file and server certificate. This feature is available in SAP Data Services version 4.2 SP 7 (14.2.7.0) or later.

1. Open Microsoft Management Console (MMC).
2. Select to import the Microsoft SQL Server database certificate file to the trusted root certificates folder of the current computer or the current user. Close MMC.
3. Test the SSL connection from SQL Server client:
   - a. Open SQL Server client and enter the connection information.
   - b. Select **Use Encryption**.
   - c. Test connection.

   If you cannot connect to the database server, check your SSL configurations.
4. In Data Services Designer, create the Microsoft SQL Server database datastore. Make sure to select the required SSL options:
   - Select On Premise for the **Database Sub-Type**.
   - Select Yes for **Use SSL encryption**.

   For instructions to create a Microsoft SQL Server database datastore, see the [Designer Guide](#).
6.5.2 Configuring SSL for Microsoft SQL Server database on Unix

Configure SSL for Microsoft SQL Server database on Unix so that you can create a SSL-enabled Microsoft SQL Server database datastore.

Obtain a private key file and server certificate for Microsoft SQL Server from a trusted authority. You can also create your own private key file and server certificate. This feature is available in SAP Data Services version 4.2 SP 7 (14.2.7.0) or later.

1. Run the Data Services Certificate Manager script located at `<LINK_DIR>/bin/DBCertManager.sh`.
2. Enter 1 for Specify database index.
3. Enter the certificate directory location.
4. For Input certificate files, enter the certificate file name, or use "*" for a wildcard search. Use a space between file names or pattern names.
   
   For example, use the wildcard `*.crt` to have the script locate all matched certificate files and merge them into `<LINK_DIR>/ssl/dbdatastore_certs/DS_MSSQL_cert.pem`.
   
   If the `.pem` file already exists, the software asks you to choose to overwrite, append, or cancel.
5. In Data Services Designer, create the Microsoft SQL Server database datastore. Make sure to select the required SSL options:
   
   ○ Select On Premise for the Database Sub-Type.
   ○ Select Yes for Use SSL encryption.

   For instructions to create a Microsoft SQL Server database datastore, see the Designer Guide.

Data Services uses the hard-coded certificate file for SSL server authentication.

Optional. Modify the hard-coded certificate file to a specified certificate file.

6.6 Configure DSN SSL for SAP HANA

Configure SAP HANA database datastores to use SSL encryption for all network transmissions between the database server and SAP Data Services.

⚠️ Caution

Only an administrator or someone with sufficient experience should configure SSL encryption for SAP HANA.

This feature is available in SAP Data Services version 4.2 SP 7 (14.2.7.0) or later.

Configure SSL on both the SAP HANA server side and the Data Services (client) side.

SSL encryption is applicable when you use an SAP HANA database datastore. SSL encryption for SAP HANA database datastore requires a DSN connection. You cannot use a DSN-less connection.

ℹ️ Note

Enabling SSL encryption slows down job performance.
The tasks involved with enabling SSL encryption require you to have either the SAPCrypto library or the OpenSSL library. These libraries may have been included with the database or with the platform you use. You can download the latest versions from the SAP Support Portal. To configure the server side, you make settings in the communication section of the global.ini file.

For more information about cryptographic libraries and settings for secure external connections in the global.ini file for SAP HANA database, see the SAP HANA Network and Communication Security section of the SAP HANA Security Guide.

Related Information

Configuring SSL for SAP HANA datastore on Unix [page 75]
Configuring SSL for SAP HANA datastore on Windows [page 74]

6.6.1 Cryptographic libraries and global.ini settings

When you create an SAP HANA database datastore with SSL encryption, configure the database server and SAP Data Services for certificate authentication.

On the database server side, you make settings in the communications section of the global.ini file based on the cryptographic library you use.

For more information about cryptographic libraries and settings for secure external connections in the global.ini file for SAP HANA database, see the SAP HANA Network and Communication Security section of the SAP HANA Security Guide.

Table 14: SSL providers for SAP HANA

<table>
<thead>
<tr>
<th>SSL provider</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAPCrypto</td>
<td>1. Install SAPCrypto if necessary.</td>
</tr>
<tr>
<td></td>
<td>2. Set the environment variable “SECUDIR” in your system to the location of the SAPCrypto library.</td>
</tr>
<tr>
<td></td>
<td>3. Ensure that you set the global.ini based on the information in the SAP HANA database documentation.</td>
</tr>
<tr>
<td></td>
<td>4. Import the SAP HANA server certificate into your SAP Data Services trusted certificate folder using Microsoft Management Console.</td>
</tr>
</tbody>
</table>
SSL provider | Requirements
--- | ---
OpenSSL | Installed by default with your operating system.

1. Make suggested `global.ini` connection settings and then restart the server. (For suggested `global.ini` settings, see SAP HANA database documentation.)
2. Configure an SAP HANA data source with SSL information using ODBC Administrator (Windows) or the `DSConnectionManager.sh` script (Unix).
3. Create the SAP HANA database datastore using the SSL DSN you created in a previous step.
4. Import the server certificate using Microsoft Management Console (Windows).

Related Information

- Configuring SSL for SAP HANA datastore on Unix [page 75]
- Configuring SSL for SAP HANA datastore on Windows [page 74]

6.6.2 Configuring SSL for SAP HANA datastore on Windows

This topic contains steps to configure SSL encryption for an SAP HANA database datastore on a Windows operation system.

Before you perform these steps, verify your SSL encryption type (SAPCrypto or OpenSSL).

1. Open Microsoft Management Console (MMC).
2. Select to import the SAP HANA certificate file to Data Services trusted root certification certificates folder. Close MMC.
   
3. Open the ODBC Data Source Administrator.
   
   You can access the ODBC Data Source Administrator either from the Datastore Editor in Data Services Designer, or open it directly from your Start menu.
4. In the ODBC Data Source Administrator, open the System DSN tab and click Add.
5. Select the driver (HDBODBC) and click Finish.
6. Enter the Data Source Name and a Description.
7. Enter the Server:Port information. Click Settings.
8. Select Connect using SSL, and Validate the SSL certificate in the SSL Connection group.
9. Make any other applicable settings and click OK.
10. Close the ODBC Data Source Administrator.
11. Create the SAP HANA datastore using the SSL DSN that you just created.

### 6.6.3 Configuring SSL for SAP HANA datastore on Unix

This topic contains steps to configure SSL encryption for an SAP HANA database datastore on a Unix operating system.

Before you perform these steps, verify your SSL encryption type (SAPCrypto or OpenSSL).

For this task, you run the Data Services Connection Manager (`DSConnectionManager.sh`) to create or edit the `odbc.ini` file in the computer on which the SAP HANA database resides. For information about using the Connection Manager, see Using the Connection Manager for UNIX systems [page 53].

1. Export `$ODBCINI` to a file in the same computer as the SAP HANA data source. For example:

   ```bash
   export ODBCINI=<dir_path>/odbc.ini
   touch $ODBCINI
   ```

2. Start Connection Manager by entering the following command:

   ```bash
   $LINK_DIR/bin/DSConnectionManager.sh
   ```

3. Click the Data Sources tab and click Add to display the list of database types.

4. On the Select Database Type window, select the SAP HANA database type and click OK.

   The Configuration for... window appears with some of the connection information automatically completed:
   - Absolute location of the `odbc.ini` file
   - Driver (for SAP HANA)
   - Driver Version

5. Complete the remaining applicable options including:
   - DSN Name
   - Driver
   - Server Name
   - Instance
   - User Name
   - Password

6. Select “Y” for Specify the SSL Encryption Option.

7. Complete the remaining SSL options based on the descriptions in the following table.
Table 15: SAP HANA DSN SSL connection options in Connection Manager

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Encryption Option (Y/N)</td>
<td>Set to “Y” so that the client server (Data Services) verifies the certificate from the database server before accepting it. If you set to “N”, the client server accepts the certificate without verifying it, which is less secure.</td>
</tr>
<tr>
<td>HANA SSL Provider (sapcrypto/openssl)</td>
<td>Specify the cryptographic provider for your SAP HANA SSL connectivity. Options are: ○ OpenSSL (.pem) ○ SAPCrypto (.pse)</td>
</tr>
<tr>
<td>SSL Certificate File</td>
<td>Enter the location and file name for the SSL certificate file.</td>
</tr>
<tr>
<td>SSL Key File</td>
<td>Enter the location and file name for the SSL key file.</td>
</tr>
</tbody>
</table>

8. If you choose OpenSSL (.pem) for the Specify the HANA SSL provider option, use the Data Services bundled OpenSSL and not your operating system OpenSSL. Data Services OpenSSL is located in `<LINK_DIR>/bin/openssl`. Make sure that you use the Data Services bundled OpenSSL:

a. Check your OpenSSL version and dependencies with the shared library (using `ldd` command).

For example, if your client operating system has OpenSSL version 0.9.8, run the following command. (If your OpenSSL version is different from version 0.9.8, make sure that you use your actual version number in the following command instead of version 0.9.8.)

```
Sample Code

    ldd /usr/bin/openssl
    linux-vdso.so.1 => (0x00007fff37d9f000)
    libssl.so.0.9.8 => /usr/lib64/libssl.so.0.9.8 (0x00007f0586e05000)
    libcrypto.so.0.9.8 => /usr/lib64/libcrypto.so.0.9.8 (0x00007f0586a65000)
    libdl.so.2 => /lib64/libdl.so.2 (0x00007f058682f000)
    libz.so.1 => /build/i311498/ds427/dataservices/bin/libz.so.1 (0x00007f058614000)
    libcrypto.so.0.9.8 => /lib64/libcrypto.so.0.9.8 (0x00007f058629c000)
    /lib64/ld-linux-x86-64.so.2 (0x00007f058705c000)
```

b. Create a soft link in `<LINK_DIR>/bin` with the same version name but refer to the Data Services SSL libraries:

```
Sample Code

    ln -s libbodi_ssl.so.1.0.0 libssl.so.0.9.8
    ln -s libbodi_crypto.so.1.0.0 libcrypto.so.0.9.8
```

When you have completed the options, the utility automatically tests the connection.

After creating the SSL DSN, you can create an SAP HANA datastore in SAP Data Services Designer. Select the SSL DSN name that you just created in Data Services Connection Manager.
6.7 Enable MIT Kerberos for HP Vertica SSL protocol

SAP Data Services uses MIT Kerberos 5 authentication to securely access an HP Vertica database using SSL protocol.

An HP Vertica user with DBADMIN permissions must install MIT Kerberos 5 on the client machine. The client machine is where Data Services is installed. Additionally, the DBADMIN user must establish a Kerberos Key Distribution Center (KDC) server for authentication. The KDC server must support Kerberos 5 using the Generic Security Service (GSS) API. The GSS API also supports non-MIT Kerberos implementations, such as Java and Windows clients.

**Note**
This document focuses on enabling SSL protocol for the HP Vertica database datastore. However, specific Kerberos and HP Vertica database processes are required before you can enable SSL protocol in Data Services. For complete explanations and processes for security and authentication, consult your HP Vertica user documentation. Also consult the MIT Kerberos user documentation at [http://web.mit.edu/kerberos/](http://web.mit.edu/kerberos/).

MIT Kerberos authorizes connections to the HP Vertica database using a ticket system. The ticket system eliminates the need for users to enter a password.

**Edit configuration or initialization file**

After you install MIT Kerberos, define the specific Kerberos properties in the Kerberos configuration or initialization file and save it to your domain. For example, save krb5.ini to C:\Windows.

See the MIT Kerberos krb5.conf (.ini for Windows) documentation for complete information about completing the .conf or .ini file: [http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html](http://web.mit.edu/kerberos/krb5-current/doc/admin/conf_files/krb5_conf.html).

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default = &lt;value&gt;</td>
<td>The location for the Kerberos library log file, krb5libs.log. For example: default = FILE:/var/log/krb5libs.log</td>
</tr>
<tr>
<td>kdc = &lt;value&gt;</td>
<td>The location for the Kerberos Data Center log file, krb5kdc.log. For example: kdc = FILE:/var/log/krb5kdc.log</td>
</tr>
<tr>
<td>admin_server = &lt;value&gt;</td>
<td>The location for the administrator log file, kadmind.log. For example: admin_server = FILE:/var/log/kadmind.log</td>
</tr>
</tbody>
</table>
Table 17: [libdefaults] Settings used by the Kerberos 5 library

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_realm = &lt;value&gt;</td>
<td>The location of your domain. Example: default_realm = EXAMPLE.COM</td>
</tr>
<tr>
<td></td>
<td>Domain must be in all capital letters.</td>
</tr>
<tr>
<td>dns_lookup_realm = &lt;value&gt;</td>
<td>Set to False: dns_lookup_realm = false</td>
</tr>
<tr>
<td>dns_lookup_kdc = &lt;value&gt;</td>
<td>Set to False: dns_lookup_kdc = false</td>
</tr>
<tr>
<td>ticket_lifetime = &lt;value&gt;</td>
<td>Set number of hours for the initial ticket request. For example: ticket_lifetime = 24h</td>
</tr>
<tr>
<td></td>
<td>The default is 24h.</td>
</tr>
<tr>
<td>renew_lifetime = &lt;value&gt;</td>
<td>Set number of days a ticket can be renewed after the ticket lifetime expiration. For example: renew_lifetime = 7d</td>
</tr>
<tr>
<td></td>
<td>The default is 0.</td>
</tr>
<tr>
<td>forwardable = &lt;value&gt;</td>
<td>Initial tickets can be forwarded when this value is set to True. For example: forwardable = true</td>
</tr>
</tbody>
</table>

Table 18: [realms] Value for each Kerberos realm

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;kerberos_realm&gt; = {&lt;subsection_property = value&gt;}</td>
<td>Location for each property of the Kerberos realm. For example:</td>
</tr>
<tr>
<td></td>
<td>EXAMPLE.COM = {kdc=&lt;location&gt;admin_server=&lt;location&gt;kpasswd_server=&lt;location&gt;}</td>
</tr>
<tr>
<td></td>
<td>Properties include:</td>
</tr>
<tr>
<td></td>
<td>• KDC location</td>
</tr>
<tr>
<td></td>
<td>• Admin Server location</td>
</tr>
<tr>
<td></td>
<td>• Kerberos Password Server location</td>
</tr>
</tbody>
</table>

Note: Host and server names are lowercase.

Table 19: [domain_realm]

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;server_host_name&gt;=&lt;kerberos_realm&gt;</td>
<td>Maps the server host name to the Kerberos realm name. If you use a domain name, prefix the name with a period (.)</td>
</tr>
</tbody>
</table>
**kinit command**

After you have updated the configuration or initialization file and saved it to the client domain, execute the `kinit` command to generate a secure key.

For example, enter the following command using your own information for the variables: `kinit <user_name>@<realm_name>`

The command should generate the following keys:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-k</code></td>
<td>Precedes the service name portion of the Kerberos principal. The default is <code>vertica</code>.</td>
</tr>
<tr>
<td><code>-K</code></td>
<td>Precedes the instance or host name portion of the Kerberos principal.</td>
</tr>
<tr>
<td><code>-h</code></td>
<td>Precedes the machine host name for the server.</td>
</tr>
<tr>
<td><code>-d</code></td>
<td>Precedes the HP Vertica database name that you want to connect to.</td>
</tr>
<tr>
<td><code>-U</code></td>
<td>Precedes the user name of the administrator user.</td>
</tr>
</tbody>
</table>

Table 20:

See the MIT Kerberos ticket management documentation for complete information about using the `kinit` command to obtain tickets: [http://web.mit.edu/kerberos/krb5-current/doc/user/tkt_mgmt.html](http://web.mit.edu/kerberos/krb5-current/doc/user/tkt_mgmt.html).

**Related Information**

*Creating a DSN for HP Vertica [page 79]*

**6.8 Creating a DSN for HP Vertica**

To enable SSL for HP Vertica database datastores, first create a data source name (DSN). Users select this DSN when they create the database datastore in Designer.

Only an HP Vertica user with DBADMIN permissions can log in to HP Vertica database. Therefore, only a DBADMIN user can create the DSN. Other, non-DBADMIN users, can access the HP Vertica database only when the user is associated with an authentication method through a GRANT statement.

This feature is available in SAP Data Services 4.2 Service Pack 7 Patch 1 (14.2.7.1) or later.

Before performing these steps, install MIT Kerberos 5 and perform all of the required steps for MIT Kerberos authentication for HP Vertica as documented in your HP Vertica documentation in the security and authentication sections.
1. Open the ODBC Data Source Administrator. You can access the ODBC Data Source Administrator either from the Datastore Editor in Data Services Designer or directly from your Start menu.

2. In the ODBC Data Source Administrator, open the System DSN tab and click Add.

3. Select the HP Vertica driver from the list and click Finish.

4. Open the Basic Settings tab and complete the following options:

   Table 21: HP Vertica ODBC DSN Configuration Basic Settings tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DSN</strong></td>
<td>Enter the HP Vertica data source name.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Optional. Enter a description for this data source.</td>
</tr>
<tr>
<td><strong>Database</strong></td>
<td>Enter the name of the database that is running on the server.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>Enter the server name.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the port number on which HP Vertica listens for ODBC connections. The default is 5433.</td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>Enter the database user name. This is the user with DBADM MIN permission, or a user who is associated with the authentication method through a GRANT statement.</td>
</tr>
</tbody>
</table>

5. Optional. Select Test Connection. When the connection test is successful, open the Client Settings tab.

6. Make the following settings In the Client Settings tab.

   Table 22: HP Vertica ODBC DSN Configuration Client Settings tab

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Kerberos Host Name</strong></td>
<td>Enter the name of the host computer where Kerberos is installed.</td>
</tr>
<tr>
<td><strong>Kerberos Service Name</strong></td>
<td>Enter the applicable value.</td>
</tr>
<tr>
<td><strong>SSL Mode</strong></td>
<td>Select Require.</td>
</tr>
<tr>
<td><strong>Address Family Preference</strong></td>
<td>Select None.</td>
</tr>
<tr>
<td><strong>Autocommit</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Driver String Conversions</strong></td>
<td>Select Output.</td>
</tr>
<tr>
<td><strong>Result Buffer Size (bytes)</strong></td>
<td>Enter the applicable value in bytes. Default is 131072.</td>
</tr>
<tr>
<td><strong>Three Part Naming</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>
### Option

| Log Level | Select No logging from the dropdown list. |

7. Select **Test Connection**. When the connection test is successful click **OK** and close the ODBC Data Source Administrator.

Now the HP Vertica DSN that you just created is available to choose from the DSN option in the datastore editor.

Create the HP Vertica database datastore in Data Services Designer.

**Related Information**

Enable MIT Kerberos for HP Vertica SSL protocol [page 77]

### 6.9 Using the ODBC Driver Selector on Windows for server name connections

Run the Data Services ODBC Driver Selector on Windows to configure the ODBC driver library required for a database using server name (also known as DSN-less) connections for the Data Services repository or as a source or target database in a Data Services job.

1. Invoke the ODBC Driver Selector by opening a Command Prompt window and entering the following command:
   ```
   %LINK_DIR%/bin/ODBCDriversSelector.exe
   ```

2. Go to the database type and version in the column **Database version**, and click the cell under the column **ODBC Drivers** to display a list of existing drivers that Data Services detected and the current state of the driver.

   **Note**

   The list of drivers in the ODBC Driver Selector is the same as the list in the Windows ODBC Data Source Administrator for data sources using DSN connections. The state in the ODBC Driver Selector will have a state of “Installed” for these drivers. However, if you uninstall a driver, the ODBC Driver Selector state is “Not Installed”.

3. Select the ODBC Driver for your database type and click **OK**.

### 6.10 Using the Repository Manager

Use the Repository Manager to check the version, to upgrade, or to create a repository after installation.
Caution

It’s recommended that you do not use database tools to attempt to quickly replicate additional repositories. By using the Repository Manager to create and seed multiple repositories individually, you can avoid potential issues related to the configuration of repository objects.

1. On Windows, choose Start ➤ Programs ➤ SAP Data Services 4.2 ➤ Data Services Repository Manager to open the Repository Manager.
   You can also access the Repository Manager from the command line on both Windows and UNIX platforms. For more information, see the command-line reference appendix.
2. If you are creating a new repository, ensure that you created a database for the new repository to use.
3. In the Repository Manager window, select the database type and version of your repository.
4. For a DB2, MySQL or SAP HANA database, the default connection type is DSN-less (the Use data source name (DSN) checkbox is not selected).
   ○ If you want to use a DSN-less connection, type in the Database server name, Database name (for DB2 and MySQL) and Port.
   ○ If you want to use a DSN connection, select the check box for Use data source name (DSN) and enter the Data source name.
5. For an Oracle database, the default connection type is TNS-less (the Use TNS name checkbox is not selected).
   ○ If you want to use a TNS-less connection, type in the Hostname, SID, and Port
   ○ If you want to use a TNS connection, select the check box for Use TNS name and enter the TNS name.
6. For other database types, complete the information.
7. Enter the user name and password that you want to use for your repository.
8. Select one of the following repository types:

<table>
<thead>
<tr>
<th>Repository type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>(Default) Stores definitions of objects in your local repository.</td>
</tr>
<tr>
<td>Central</td>
<td>Stores definitions of objects in a central repository for multiple-user users.</td>
</tr>
<tr>
<td>Profiler</td>
<td>Stores information generated by the Data Profiler for determining the quality of your data.</td>
</tr>
</tbody>
</table>
9. If you are creating a new repository, click Create. If you are upgrading an existing repository, click Upgrade.
10. If you want to create or upgrade another repository, repeat steps 1 through 6.
11. When you finish creating or upgrading repositories, click Close.

Note

Before you can access the repository, you must associate it with a Job Server and register it in the Central Management Console (CMC)
6.11 Using the License Manager

See License Manager [page 149] for information.

6.12 Using the Server Manager on Windows

Use the Server Manager for many tasks such as to create, edit, or delete Job Servers and Access Servers after installation.

To open the Server Manager in Windows, choose Start ➤ Programs ➤ SAP Data Services 4.2 ➤ Data Services Server Manager.

The Server Manager utility window opens. The user interface consists of several tabbed windows for viewing, adding, and editing various aspects of your environment related to Data Services. The Server Manager has the following tabs:

- Job Server
- Access Server
- SSL (Secure Socket Layer)
- Run-Time
- NCS (Native Component Supportability) library
- SLD (System Landscape Directory)

When you have finished making settings in the Server Manager, click Close and Restart to restart the services.

Related Information

Server Manager (Windows) [page 156]

6.12.1 Configuring Job Servers

1. Open the Server Manager, click the Job Server tab and click Edit.
2. Decide which configuration task to perform:
   ○ To add a new Job Server, click Add. Continue to the remaining configuration steps.
   ○ To edit an existing Job Server, select the Job Server and click Edit. Continue to the remaining configuration steps.
   ○ To remove an existing Job Server, select the Job Server and click Delete. No additional configuration steps are required.

   **Note**
   If the Job Server has associated repositories, you must first delete those and then click OK before you can delete the Job Server.

3. In the Job Server Properties window, enter configuration information for the Job Server.
4. In the Associated Repositories section, configure any local or profiler repositories that you want to associate with the Job Server. Each Job Server must be associated with at least one local repository.
   a. If you want to use a DSN-less connection (for DB2, MySQL, SQL Anywhere, or SAP HANA database types), clear the Use data source name (DSN) checkbox.
   b. If you want to use a TNS-less connection for an Oracle database type, clear the Use TNS name checkbox.
   c. When you have finished configuring associated repositories, including one default, click OK.
5. Click OK to return to the Server Manager window.
6. Click Restart to restart the services with any updated configurations.

### 6.12.1.1 Job Server properties

Table 24:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Server name</td>
<td>Specifies a name that uniquely identifies the Job Server.</td>
</tr>
<tr>
<td>Job Server port</td>
<td>Specifies the TCP/IP port that the Job Server uses to receive commands from the Designer and the Access Server. If a computer hosts multiple Job Servers, each Job Server must have a unique port number. Additionally, the post number must not be used by another process on the computer. If you are unsure of which port number to use, use the default port number and increment it for each additional Job Server that you configure.</td>
</tr>
<tr>
<td>Support adapter and message broker communication</td>
<td>Enables communication between the Job Server and adapters. Each computer that hosts adapters must have exactly one Job Server designated to manage them.</td>
</tr>
<tr>
<td>Use SSL protocol for adapter, message broke and communication</td>
<td>Enables SSL security on the communication paths between the Job Server and any adapters or message brokers.</td>
</tr>
<tr>
<td>Communication port</td>
<td>Specifies the TCP/IP port number that the Job Server uses for communicating with adapters. The default port is 4001.</td>
</tr>
</tbody>
</table>
6.12.1.2 Configuring associated repositories

Each Job Server must be associated with at least one local repository, and can be associated with other local and profiler repositories. Configure associated repositories in the Associated Repositories section of the Job Server Properties window in the Server Manager.

To add an associated repository

1. Click Add to associate a new local or profiler repository with the Job Server.
2. Enter the required connection information for your repository database. The details required vary depending on the database type.
3. Enter the user name and password that you want to use for your repository.
4. Check Default repository if this is the default repository for the Job Server. You must specify exactly one default repository.
   
   Note
   Do not check Default repository if you are adding a profiler repository.

5. Click Apply to save your entries and associate the repository with the Job Server.

The associated repository entry updates with the Job Server's computer name and port number.

To edit an associated repository

1. Select the repository you want to change and click Edit.
2. Under Repository Information, enter the password.
3. Check or uncheck Default repository, indicating whether this is the default repository for the Job Server.
4. Click Apply to save the changes to the Job Server configuration.

   Note
   You can change only whether an associated repository is the default for the Job Server. If you need to make other changes, delete the existing associated repository and add a new one with the updated configuration information.

To delete an associated repository

1. Select the repository you want to delete and click Delete.
2. Under Repository Information, enter the password.
3. Click Apply to remove the associated repository from the Job Server configuration.
6.12.1.3 Resynchronizing associated repositories

Situations when you must resynchronize the Job Server and the local repository include:

- The Job Server information is not available or not correct in the local repository.
- You have uninstalled Data Services and are reinstalling the same version without creating a new local repository.
- You created a new local repository using the Repository Manager after creating a repository and Job Server when you installed Data Services.

To resynchronize Job Servers:

1. In the Job Server Configuration Editor window, select the name of your Job Server.
2. Click Resync with Repository.
3. In the Job Server Properties window, select an associated local repository.
4. Click Resync.
5. When asked whether to update this associated repository with this local machine information, click OK.
6. Under Repository Information, enter the local repository password.
7. Click Apply.
8. Click OK on the Job Server Properties window.

6.12.2 Configuring run-time resources

1. In the Server Manager window, click the Run-time resources tab.
2. For the Specify a directory with enough disk space for pageable cache option, accept the default directory (\<DS_COMMON_DIR>\Log\PCache) or click the ellipses button to browse to a different directory.

**Note**

For memory-intensive operations such as Group By, Order By, and Detailed profiling, specify a pageable cache directory that fulfills the following criteria:

- The directory contains enough disk space for your data. To estimate the amount of space required for pageable cache, consider factors such as:
  - Number of concurrently running jobs or data flows.
  - Amount of pageable cache required for each concurrent data flow.
- The directory exists on a separate disk or file system from the SAP Data Services system and operating system (such as the C:\ drive on Windows, or the root file system on UNIX systems).
- The directory limits the disk space that data flows consume. The pageable cache uses all available disk space on the file system that contains the pageable cache directory. So, to limit the disk space that data flows consume, create a file system (or partition on Windows) with a limited size. Use the new file system (partition on Windows) as the pageable cache directory.

The software uses this directory in the following situations:

- For pageable caching, which is the default cache type for data flows.
- When selecting a file transfer type and Automatic is specified in the Data_Transfer transform.
3. In the **Peer-to-peer options** area, change the values for **Start port** and **End port** to restrict the number of ports used by the software. The default values for **Start port** and **End port** are 1025 and 32767, respectively. The software uses these ports for peer-to-peer communications when sending data between data flows or sub data flows.

   **Note**
   If you want to enable SSL security on the communication paths between data flows and sub data flows, select **Use SSL protocol**.

4. Click **Apply** to save any configuration changes.

### 6.12.3 Configuring Access Servers

When you configure the location for an Access Server installation, SAP Data Services creates space for the Access Server log files.

1. Open the **Server Manager**, click the **Access Server** tab and click **Edit**.
2. Decide which configuration task to perform:
   - To add a new Access Server, click **Add**. Continue to the remaining configuration steps.
   - To edit an existing Access Server, select the Access Server and click **Edit**. Continue to the remaining configuration steps.
   - To remove an existing Access Server, select the Access Server and click **Delete**. No additional configuration steps are required.
3. In the **Access Server Properties** window, enter the Access Server configuration information and click **OK**.

   **Table 25:**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>Specifies the location of the log files for this instance of the Access Server. Click the ellipses button to browse to the Log directory under the directory where you installed the software. Do not change this value after the initial configuration.</td>
</tr>
<tr>
<td>Communication Port</td>
<td>Specifies the port on this computer that the Access Server uses to listen for incoming messages from clients. Make sure that this port number is unused and is unique for each Access Server.</td>
</tr>
</tbody>
</table>
### Property Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Specify any additional Access Server parameters.</td>
</tr>
<tr>
<td></td>
<td><strong>i Note</strong></td>
</tr>
<tr>
<td></td>
<td>Additional Access Server parameters can be viewed by typing AL_AccessServer at the command line. For more information, see “Real Time Performance” in the Management Console Guide.</td>
</tr>
<tr>
<td>Use SSL protocol</td>
<td>Enables SSL security for real-time messaging on this Access Server.</td>
</tr>
<tr>
<td>Enable Access Server</td>
<td>Controls whether the Access Server is automatically started when the Data Services service starts.</td>
</tr>
</tbody>
</table>

4. Click **OK** to return to the Server Manager window.
5. Click **Restart** to restart the services with the updated configuration.

### 6.12.4 Configuring SSL paths

Use the Server Manager to configure the paths to SSL certificates and keyfiles.

**i Note**

By default, the paths for the SSL certificate and keyfiles are automatically configured during installation. You do not need to change them unless you want to use your own certificates.

**i Note**

If you change the SSL certificate configuration, you must resync all repositories associated with the Job Server before you can run jobs successfully.

1. Open the Server Manager and click the SSL tab.
2. Specify the locations of the server certificate file, the server private key file, and the trusted certificates folder.

**i Note**

The server certificate must be in PEM format. Valid extensions for certificates in the trusted certificates folder include .pem, .crt, and .cer. Regardless of the file extension, all certificate file contents must be in PEM format.

3. If you want to specify a private key password file, select **Use server private key password file** and specify the location of the password file.
4. Click **Close and Restart** to close the Server Manager and restart any Data Services servers on the machine with the updated certificate information.
6.12.5 Verifying that Job and Access servers are running

To verify that Job Servers are running:

1. Check in the Windows Task Manager *Processes* tab for:
   - `al_jobservice.exe` (represents the SAP Data Services service)
   - `al_jobserver.exe` (one per Job Server)
   - `AL_AccessServer.exe` (one per Access Server)
2. If you do not see all the processes expected, check for error messages in the Job Server event log in 
   `<LINK_DIR>/log/<JobServer name>/server_eventlog.txt`.

**Note**

Access Server logs are in `<AccessServerPathName>/error_mm_dd_yyyy.log`

6.13 Using the Server Manager on UNIX systems

Use the Server Manager to create, edit, or delete Job Servers and Access Servers after installation.

The Server Manager displays the following:

**Job Server information**

Table 26:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>This name uniquely identifies the Job Server. The Job Server name cannot be changed.</td>
</tr>
<tr>
<td>TCP/IP port number</td>
<td>The port number is a TCP/IP port that the Job Server uses to receive commands from the Designer and an Access Server. If a computer hosts multiple Job Servers, each Job Server must have a unique port number. Choose a port number that is not used by another process on the computer. It's recommended that you use 3500. If you are unsure of which port number to use, use the default port number and increment it for each additional Job Server you configure.</td>
</tr>
</tbody>
</table>
Option Description
Supports adapter communication on port If this computer hosts adapters, you must designate one (and only one) Job Server to support them. Once a Job Server is set to support adapters (a port is entered and saved), it is marked on the Job Server Configuration screen with this label.

Run-time resource information

Table 27:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pageable cache directory</td>
<td>This directory contains the pageable cache that the software uses for memory-intensive operations and for file transfer types when Automatic is specified in the Data_Transfer transform.</td>
</tr>
<tr>
<td>Start port</td>
<td>The software uses this starting port number for peer-to-peer communication between data flows or sub data flows that are running on different Job Servers. The default is 1025.</td>
</tr>
</tbody>
</table>

Access Server information

Table 28:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server number</td>
<td>This sequence number uniquely identifies the Access Server on this machine. The Access Server number cannot be changed.</td>
</tr>
<tr>
<td>Directory</td>
<td>The directory containing Access Server information.</td>
</tr>
<tr>
<td>Communication port</td>
<td>This port number is used to communicate between the Access Server and the Administrator. The default is 4000.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Additional parameters used by the Access server. View Access Server parameters by typing AL_AccessServer at the command line. For more information about parameters, see &quot;Configuring an Access Server&quot; in the Management Console Guide.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enter Y to activate the Access Server.</td>
</tr>
</tbody>
</table>

Job service information

Table 29:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service executable path</td>
<td>The directory containing AL_JobService information.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the Data Services service:</td>
</tr>
<tr>
<td></td>
<td>● Running</td>
</tr>
<tr>
<td></td>
<td>● Not running</td>
</tr>
</tbody>
</table>

**SMTP Server information**

Table 30:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The name or IP address of the SMTP server (for example, mail.company.com).</td>
</tr>
<tr>
<td>Sender</td>
<td>The email address that will appear in the <em>From</em> field of the email.</td>
</tr>
</tbody>
</table>

### 6.13.1 Configuring Job Servers on UNIX

1. Ensure required environment variables are set, and run the Server Manager.

   ```
   $ cd $LINK_DIR/bin/
   $ . ./al_env.sh
   $ ./svrcfg
   ```

   The Server Manager main screen appears.

2. Enter **3** to configure a Job Server.
   The Job Server information screen appears.

**Note**

The repository information for each configured Job Server is displayed in one of the following formats:

- For a DSN or TNS connection:

   Table 31:

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Format of Repository String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>&lt;username&gt;@&lt;TNSname_user&gt;</td>
</tr>
<tr>
<td>SAP HANA</td>
<td>&lt;username&gt;@&lt;DSNname_user&gt;</td>
</tr>
<tr>
<td>DB2</td>
<td></td>
</tr>
<tr>
<td>MySQL</td>
<td></td>
</tr>
<tr>
<td>SQL Anywhere</td>
<td></td>
</tr>
</tbody>
</table>

- For a server name connection (also known as DSN-less or TNS-less connection):
Table 32:

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Format of Repository String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>&lt;username&gt;@&lt;server_SID_user&gt;</td>
</tr>
<tr>
<td>SAP HANA</td>
<td>&lt;username&gt;@&lt;server_port_user&gt;</td>
</tr>
<tr>
<td>MySQL</td>
<td>&lt;username&gt;@&lt;server_database_user&gt;</td>
</tr>
<tr>
<td>DB2</td>
<td></td>
</tr>
</tbody>
</table>

○ For SAP Sybase:
  <username>@<server_database_user>

3. Enter the command for the configuration task you want to perform:

<table>
<thead>
<tr>
<th>Command</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Add a new Job Server.</td>
</tr>
<tr>
<td>e</td>
<td>Edit an existing Job Server.</td>
</tr>
<tr>
<td>d</td>
<td>Delete an existing Job Server.</td>
</tr>
<tr>
<td>a</td>
<td>Add a repository connection to a Job Server.</td>
</tr>
<tr>
<td>u</td>
<td>Update a repository connection on a Job Server.</td>
</tr>
<tr>
<td>r</td>
<td>Remove a repository connection from a Job Server.</td>
</tr>
<tr>
<td>s</td>
<td>Set the default repository connection for a Job Server.</td>
</tr>
<tr>
<td>y</td>
<td>Resynchronize a Job Server configuration with a repository.</td>
</tr>
</tbody>
</table>

You must resynchronize your Job Server and repository when:
○ You have uninstalled Data Services and are reinstalling the same version without creating a new repository.
○ You have created a new repository using the Repository Manager after installing the software.

If you resynchronize your Job Server configuration with a repository, you must re-add a connection for this repository to the Administrator. For more information, see the Management Console Guide.

4. When you add or edit a Job Server, you must specify additional configuration details:
   a. Enter the name for the Job Server.
   b. Specify the TCP/IP port that the Job Server uses to receive commands from the Designer and the Access Server.

   ![Note]

   If a computer hosts multiple Job Servers, each Job Server must have a unique port number. Additionally, the port number must not be used by another process on the computer.

   If you are unsure of which port number to use, use the default port number and increment it for each additional Job Server that you configure.

   c. If you want to manage adapters with the Job Server, enter **Y**.
   d. If you want to manage adapter communication with the Job Server, specify the TCP/IP port number to use.
e. If you want to enable SSL on the adapter management communication paths used by the Job Server, enter `Y`.

5. When you add or edit a repository connection, you must specify the database connection information.
   a. If you want to use a DSN-less connection (for a DB2, MySQL, or SAP HANA database), enter `N` when the Server Manager asks you if you want to use an ODBC data source.
   b. If you want to use a TNS-less connection for an Oracle database, enter `N` when the Server Manager asks you if you want to use a TNS name.
   c. If you want to use a DSN or TNS connection, you must specify the following additional database connection information:

   Table 33:

<table>
<thead>
<tr>
<th>Database</th>
<th>Required information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>The TNSNAME specified in tnsnames.ora</td>
</tr>
<tr>
<td>MySQL</td>
<td>The DSN entry specified in odbc.ini</td>
</tr>
<tr>
<td>SAP HANA</td>
<td>The DSN entry specified in odbc.ini</td>
</tr>
<tr>
<td>DB2</td>
<td>The DB2 instance name</td>
</tr>
<tr>
<td>SQL Anywhere</td>
<td>The DSN entry specified in odbc.ini</td>
</tr>
</tbody>
</table>

   d. If your database type is SAP Sybase, specify the Sybase server name specified in the Interfaces file.

   **Note**

   The Server Manager for UNIX systems does not prompt for the repository password except when creating a Job Server or adding a repository. To update the repository password in the `<DS_COMMON_DIR>/conf/DSConfig.txt` file, enter `u`. All options use the updated password from DSConfig.txt file.

6. When you are satisfied with your configuration changes, enter `q` and then `x` to exit the Server Manager.

**Related Information**

[DSN-less and TNS-less connections](#) [page 20]

### 6.13.2 Configuring run-time resources

1. Ensure required environment variables are set, and run the Server Manager.

   ```
   $ cd $LINK_DIR/bin/
   $ . ./al_env.sh
   $ ./svrcfg
   ```

   The Server Manager main screen appears.

2. Enter 4 to configure run-time resources. The run-time resource information screen appears.
3. Enter e to edit the run-time resource configuration.
4. Accept the default Pageable Cache Directory, or specify a different location.

⚠️ Restriction

The Pageable Cache Directory path cannot exceed 70 characters.

ℹ️ Note

For memory-intensive operations such as Group By, Order By, and Detailed profiling, specify a pageable cache directory that fulfills the following criteria:
- The directory contains enough disk space for your data. To estimate the amount of space required, consider factors such as the number of concurrently running jobs or data flows and the amount of pageable cache required by each concurrent data flow.
- The directory exists on a separate disk or file system from the Data Services system and operating system.
- The directory limits the disk space that data flows consume. The pageable cache uses all available disk space on the file system that contains the pageable cache directory. To limit the disk space that data flows consume, create a file system with a limited size. Use the new file system as the pageable cache directory.

The software uses this directory in the following situations:
- For pageable caching, the default cache type for data flows. For more information, see the Performance Optimization Guide.
- When the software selects a file transfer type and Automatic is specified in the Data_Transfer transform.

5. Change the values for Start port and End port to restrict the number of ports used by the software for peer-to-peer communications. The default values are 1025 and 32767, respectively.

The software uses these ports for peer-to-peer communications when sending data between data flows or sub data flows that are running on different Job Servers.

6. Specify whether you want to use the SSL security protocol on the communication paths between data flows and sub data flows.

7. Enter q and then x to exit the Server Manager.

### 6.13.3 Configuring Access Servers

When you configure the location for an Access Server installation, SAP Data Services creates space for the Access Server log files.

1. Ensure required environment variables are set, and run the Server Manager.

   ```bash
   $ cd $LINK_DIR/bin/
   $ . ./al_env.sh
   $ ./svrcfg
   
   The Server Manager main screen appears.
   ```

2. Enter 4 to configure an Access Server.
The Access Server information screen appears.

3. Enter the command for the configuration task you want to perform:

<table>
<thead>
<tr>
<th>Command</th>
<th>Configuration task</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Create a new Access Server.</td>
</tr>
<tr>
<td>e</td>
<td>Edit an existing Access Server.</td>
</tr>
<tr>
<td>d</td>
<td>Delete an existing Access Server.</td>
</tr>
</tbody>
</table>

4. When you create or edit an Access Server, specify additional configuration details:
   a. If you are editing an existing Access Server, enter the number of the Access Server shown in the Access Server configuration information screen.
   b. Specify the directory for the Access Server.
   c. Specify the TCP/IP port that the Access Server should use for communication.

   **Note**
   You can configure more than one Access Server on the same computer, but each must have separate ports. If you enter a port number already in use, an error message appears.

   d. Specify any additional parameters for the Access Server.

   **Note**
   Additional Access Server parameters can be viewed by typing `AL_AccessServer` at the command line. For more information, see “Real Time Performance” in the Management Console Guide.

   e. Specify whether you want to use the SSL security for real-time messaging on this Access Server.
   f. Specify whether you want to enable the Access Server.

5. When you delete an Access Server, specify the number of the Access Server to delete.

   **Note**
   When you delete an Access Server, all Access Servers are stopped. When you exit the Server Manager, any remaining Access Servers restart.

6. When you are satisfied with your configuration changes, enter `q` and then `x` to exit the Server Manager.

### 6.13.4 Configuring SSL paths

Use the Server Manager to configure the paths to SSL certificates and keyfiles.

**Note**
By default, the paths for the SSL certificate and keyfiles are automatically configured during installation. You do not need to change them unless you want to use your own certificates.

1. Ensure required environment variables are set, and run the Server Manager.

   ```
   $ cd $LINK_DIR/bin/
   ```
The Server Manager main screen appears.

2. Enter 7 to configure SSL paths.
   The SSL configuration information screen appears.

3. Enter e to edit the SSL configuration.

4. Specify the SSL configuration information when prompted:
   a. The path to the server certificate file
   b. The path to the server private key file
   c. Whether you want to use a private key password file and the path to that file
   d. The directory where your trusted certificates are stored

   **Note**
   The server certificate must be in PEM format. Valid extensions for certificates in the trusted certificates folder include .pem, .crt, and .cer. Regardless of the file extension, all certificate file contents must be in PEM format.

5. When you are satisfied with your configuration changes, enter q and then x to exit the Server Manager.

The certificate information specified in the Server Manager applies to all Data Services servers running on that physical machine (for example, any Job Servers, Access Servers, and so on.)

### 6.13.5 Starting or stopping the service

The SAP Data Services service (*AL_JobService*) is a daemon associated with `$LINK_DIR` that starts locally-configured Job Servers and Access Servers and then monitors them and attempts to restart them if they are not running.

After you exit the Server Manager, *AL_JobService* automatically retrieves any changes made to Job Servers or Access Servers. You do not need to restart *AL_JobService*.

1. Run the Server Manager.

   ```
   $ cd $LINK_DIR/bin/
   $ ./al_env.sh
   $ ./svrcfg
   ```

   **Note**
   The second command sets required environment variables before ./svrcfg starts the Server Manager.

   The Server Manager main screen appears.

2. Enter 1 to control the service (Job service).

3. Start or stop the Job service.
   - Enter s to start the Job service.
   - Enter o to stop the Job service.
4. Enter `q` and then `x` to exit the Server Manager.

### 6.13.6 Configuring SMTP email

The Server Manager can be used to specify SMTP server settings for the `smtp_to` email function. For more information, see "Defining and enabling the smtp_to function" in the Reference Guide.

### 6.14 Configuring Metadata Browsing Service and View Data Service

The installation process of Data Services configures the following services (under the server `EIMAdaptiveProcessingServer`) with default settings.

- Metadata Browsing Service
- View Data Service

These services are used by Information Steward to connect and view data in profiling sources. You might want to change the configuration settings to more effectively integrate Information Steward with your hardware, software, and network configurations.

1. Go to the Servers management area of the CMC.
2. Expand Service Categories in the tree panel and select Enterprise Information Management Services.
3. Double-click `<computername.> EIMAdaptiveProcessingServer` in the list in the right pane.
4. On the Properties window, find the applicable service for which you want to change settings.
5. After making desired changes in the service, click Save or Save & Close.

**Note**

Not all changes occur immediately. If a setting cannot change immediately, the Properties window displays both the current setting (in red text) and the updated setting. When you return to the Servers management area, the server will be marked as Stale. When you restart the server, it will use the updated settings from the Properties dialog box and the Stale flag is removed from the server.

### Related Information

- Metadata Browsing Service configuration parameters [page 98]
- View Data Services configuration parameters [page 99]
### 6.14.1 Metadata Browsing Service configuration parameters

You can change the following properties of the Metadata Browsing Service.

Table 34:

<table>
<thead>
<tr>
<th>Server Configuration Parameter</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Name of the service configuration.</td>
<td>Alphanumeric string with a maximum length of 64. The Service Name cannot contain any spaces. Default value: MetadataBrowsing-Service</td>
</tr>
<tr>
<td>Maximum Data Source Connections</td>
<td>Maximum number of data source connections that can be opened at any time under a service instance.</td>
<td>integer. Default value: 200</td>
</tr>
<tr>
<td>Retry attempts to launch Service Provider</td>
<td>Maximum number of attempts to launch a new service provider when there is contention to access a shared service provider.</td>
<td>Default value: 1</td>
</tr>
<tr>
<td>Stateful Connection Timeout (seconds)</td>
<td>Maximum duration which a stateful connection is open. Stateful connections include SAP Applications and SAP BW Source.</td>
<td>Default value: 1200</td>
</tr>
<tr>
<td>Stateless Connection Timeout (seconds)</td>
<td>Maximum duration which a stateless connection is open. Stateless connections include all relational database sources.</td>
<td>Default value: 1200</td>
</tr>
<tr>
<td>Recycle Threshold</td>
<td>Maximum number of requests that will be processed by a service before the Data Services backend engine is recycled to free memory that was allocated for metadata browsing.</td>
<td>Default value: 50000</td>
</tr>
</tbody>
</table>
| Log Level | Level of logging of trace messages to the log file. | Information Steward logs:
- None: Logging disabled.
- Info: Logging disabled. (same as None)
- Finer: All traces, requests, and responses.

Data Services logs:
- None: Logging disabled.
- Info: All traces.
- Finer: All traces, requests, and responses.
Default level is Info. |
| Collect Connection Statistics | Enable or disable the collection of statistic information for each open connection. | Default is enabled. |

**Note**

If there is more than one instance of Metadata Browsing Service configured in the CMS, the same level of information is collected from all instances. The log level defined for the first running service is the level used.
### Server Configuration Parameters

<table>
<thead>
<tr>
<th>Server Configuration Parameter</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listener Port</td>
<td>Port number used to communicate with the Data Services backend engine.</td>
<td>Four-digit port number that is not currently in use. Default value: 4010</td>
</tr>
<tr>
<td></td>
<td>If you change the port number, you must restart the EIMAdaptiveProcessingServer for the change to take effect.</td>
<td></td>
</tr>
<tr>
<td>JMX Connector Port</td>
<td>Port number used for the JMX Connector.</td>
<td>Four-digit port number that is not currently in use. Default value: 4011</td>
</tr>
<tr>
<td></td>
<td>If you change the port number, you must restart the EIMAdaptiveProcessingServer for the change to take effect.</td>
<td></td>
</tr>
</tbody>
</table>

### 6.14.2 View Data Services Configuration Parameters

You can change the following properties of the View Data Service.

#### Table 35:

<table>
<thead>
<tr>
<th>Server Configuration Parameter</th>
<th>Description</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Name of the service configuration.</td>
<td>Alphanumeric string with a maximum length of 64. The Service Name cannot contain any spaces. Default value: ViewData</td>
</tr>
<tr>
<td>Listener Port</td>
<td>Port number used to communicate with the Data Services backend engine.</td>
<td>Four-digit integer. Default value: 4012</td>
</tr>
<tr>
<td></td>
<td>If you change the port number, you must restart the EIMAdaptiveProcessingServer for the change to take effect.</td>
<td></td>
</tr>
<tr>
<td>JMX Connector Port</td>
<td>Port number used for the JMX Connector.</td>
<td>Four-digit integer. Default value: 4013</td>
</tr>
<tr>
<td></td>
<td>If you change the port number, you must restart the EIMAdaptiveProcessingServer for the change to take effect.</td>
<td></td>
</tr>
<tr>
<td>Batch Size (kilobytes)</td>
<td>Size of the data to be stored in a view data response.</td>
<td>Minimum value: 1000 Maximum value: 5000 Default value: 1000</td>
</tr>
<tr>
<td>Minimum Shared Service Providers</td>
<td>Minimum number of shared Data Services backend engines that need to be launched at the startup time of the service.</td>
<td>Default value: 1</td>
</tr>
<tr>
<td>Server Configuration Parameter</td>
<td>Description</td>
<td>Possible Values</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maximum Shared Service Providers</td>
<td>Maximum number of shared Data Services backend engines that can be launched during the time to service the view data requests.</td>
<td>Default value: 5</td>
</tr>
<tr>
<td>Maximum Dedicated Service Providers</td>
<td>Maximum number of dedicated Data Services backend engines that can be launched at any instant of time.</td>
<td>Default value: 10</td>
</tr>
<tr>
<td>Recycle Threshold</td>
<td>Maximum number of requests that will be processed by a service before the Data Services backend engine is recycled to free memory that was allocated for viewing data.</td>
<td>Any integer. Default value: 200</td>
</tr>
<tr>
<td>Number of attempts to launch service provider</td>
<td>Number of attempts to be made to try launching the Data Services backend engine instance.</td>
<td>Default value: 1</td>
</tr>
<tr>
<td>Maximum idle time for shared service provider (minutes)</td>
<td>Maximum number of minutes that a Data Services backend engine can remain without processing any requests. After this time is exceeded, the Data Services backend engine is shut down.</td>
<td>Default value: 120</td>
</tr>
<tr>
<td>Log Level</td>
<td>Level of logging of trace messages to the log file.</td>
<td>Information Steward logs:</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>• None: Logging disabled.</td>
</tr>
<tr>
<td></td>
<td>If there is more than one instance of View Data Service configured in the CMS, the same level of information is collected from all instances. The log level defined for the first running service is the level used.</td>
<td>• Info: Logging disabled. (same as None)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Finer: All traces, requests, and responses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Services logs:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• None: Logging disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Info: All traces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Finer: All traces, requests, and responses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default level is Info.</td>
</tr>
</tbody>
</table>
### 6.15 Data Services CMC application settings

You can change the following settings for the Data Services Application on the Central Management Console (CMC).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>History Retention Period</strong></td>
<td>Number of days to retain the job execution history.</td>
</tr>
<tr>
<td></td>
<td>Default value: 30</td>
</tr>
<tr>
<td></td>
<td>• If you enter 0, then the software does not retain job history.</td>
</tr>
<tr>
<td></td>
<td>• If you enter a negative number, then the software retains job history indefinitely.</td>
</tr>
<tr>
<td><strong>Job Server Log Retention Period</strong></td>
<td>Number of days to retain the Job Server logs.</td>
</tr>
<tr>
<td></td>
<td>Default value: 30</td>
</tr>
<tr>
<td></td>
<td>• If you enter 0, then the software does not retain Job Server logs.</td>
</tr>
<tr>
<td></td>
<td>• If you enter a negative number, then the software retains Job Server logs indefinitely.</td>
</tr>
<tr>
<td><strong>Job History Cleanup Period</strong></td>
<td>Number of seconds from the job start time that the Data Services Management Console cleans up the bad or crashed job history.</td>
</tr>
<tr>
<td></td>
<td>With this setting, you can find jobs that are either running longer than the normal time, or jobs that have crashed abnormally.</td>
</tr>
<tr>
<td></td>
<td>A job that crashes for an abnormal reason fails to update the job history metadata tables or the local repository, and the software doesn’t register an end time. Therefore, even though the job crashed, the Management Console may show it as still running.</td>
</tr>
<tr>
<td></td>
<td>The default setting is 0.</td>
</tr>
<tr>
<td></td>
<td>• If you keep the default of 0, or set to a negative number, then the software does not clean up the bad or crashed job history.</td>
</tr>
<tr>
<td></td>
<td>• If you set to 1 or higher, then the software cleans up the bad or crashed job history in the set number of seconds from the job start time.</td>
</tr>
<tr>
<td></td>
<td>When you enter a positive number in this setting, enter a number that provides enough time for your longest running jobs to complete. After the time elapses, any jobs that do not have an end timestamp will be marked as failed. For these jobs, you can check the log files to discover if the job ended abnormally.</td>
</tr>
<tr>
<td></td>
<td>For example, if your longest-running job takes 30 minutes, set this option to 3600 seconds, so that, after an hour from the job start time, the status in the batch status page in the Management Console shows the job is no longer processing. That way, you can see a list of jobs that potentially crashed abnormally, without having to wait a long period of time.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Enable SSL communication for Metadata Browsing and View Data Services</strong></td>
<td>Specifies whether or not to use SSL communications for Metadata Browsing Service and View Data Service of the EIM Adaptive Processing Server. Other SAP software products, such as SAP Information Steward, use the Metadata Browsing Service and View Data Service service to browse and import metadata and to view the data in connections.</td>
</tr>
<tr>
<td><strong>Use Default SSL Settings</strong></td>
<td>Specifies whether or not to use the default SSL keystore and certificates. Default value: No If you specify No, then you must enter values in <strong>KeyStore File</strong>, <strong>KeyStore Password</strong>, and <strong>Key Password</strong>.</td>
</tr>
<tr>
<td><strong>KeyStore File</strong></td>
<td>File name of the keystore that contains the key and all the certificates that are part of the certificate chain involved in signing the key. Default value: <strong>DSJavaKeyStore.keystore</strong></td>
</tr>
<tr>
<td><strong>KeyStore Password</strong></td>
<td>Password to the keystore file.</td>
</tr>
<tr>
<td><strong>Key Password</strong></td>
<td>Password to the key inside the keystore file.</td>
</tr>
<tr>
<td><strong>Encryption passphrase</strong></td>
<td>Passphrase to use for encrypting passwords that are sent as part of requests to the Metadata Browsing Service and View Data Service. Other SAP software products, such as SAP HANA, use this Encryption passphrase to encrypt passwords when sending an open connection request. The backend engine will use this passphrase to decrypt the password and process the open connection request.</td>
</tr>
</tbody>
</table>
## 7 Monitoring

### 7.1 Monitoring jobs

Using the Administrator, you can monitor job execution of any batch job in a connected repository. You can monitor jobs that you run from the Administrator or from the Designer.

This section discusses how you can use the Administrator to view a batch job's overall status and statistics.

### 7.1.1 Viewing overall status of executed jobs

The *Batch Job Status* page lists each batch job execution. Use this list to view the overall status of each execution and to access more detailed statistics and log files.

1. Select ![Batch](<repository>).
   - To view jobs in all repositories from this page, select ![Batch](All Repositories). (The *All Repositories* option appears under the Batch Job node if more than one repository is connected to the Administrator.)
   - The *Batch Job Status* page shows each instance of job execution for the selected repository.

2. You can filter the list of batch jobs displayed by selecting a job name and/or when the job executed.
   - To filter by job, select the job name from the drop-down *Job name* list. Or type the name, or type part of the name and a wildcard character (\`\` or *), into the wildcard search string box and click *Search*. The Search field is not case sensitive and spaces are allowed.
   - To filter by when the job(s) executed, select one of the following options:
     - Show last execution of a job.
     - Show status relative to today—Select the number of previous days over which to view job executions.
     - Show status as a set period—Type the date range or select the dates by clicking the calendar icons.

3. Click *Search* to update the list.

4. To sort the values in each column in ascending or descending order, click the column heading.

5. Find the overall status of a batch job execution by examining the indicator in the *Status* column.

<table>
<thead>
<tr>
<th>Table 37:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indicator</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><img src="#" alt="Green" /></td>
<td>A green icon indicates that the batch job ran without error.</td>
</tr>
<tr>
<td><img src="#" alt="Yellow" /></td>
<td>A yellow icon indicates that the batch job has one or more warnings.</td>
</tr>
<tr>
<td><img src="#" alt="Red" /></td>
<td>A red icon indicates that the batch job experienced an error.</td>
</tr>
</tbody>
</table>

Check the End Time column to see if or when the job completed. If a job is running longer than usual, and there is no end time listed, there may be an issue with the job, or the job may have completed abnormally.
When a job completes abnormally, it does not update the job history metadata or the local repository, so there is no end time. To set a limit for how long these types of jobs display as still running, make sure to set the Data Services application setting `Job History Cleanup Period` in the Central Management Console. For more information about the `Job History Cleanup Period`, see [Data Services CMC application settings](#) [page 101].

6. If a batch job execution has a red status, examine the trace, monitor, and error logs for more information.

7. To view detailed information about a particular job execution, look at the data on the Batch Job Status page. If the job includes a server group icon in the Job Server column, this indicates that the job was executed by a server group. You can roll your cursor over the server group icon to view the name of the server group. The Job Server listed is the Job Server in the server group that executed the job.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>All jobs can be executed by an explicitly selected Job Server or by a server group. If you choose to execute a job using a server group, you can use this page to see which Job Server actually executed the job. If you explicitly select a Job Server to execute a job, then even if it is also part of a server group, the server group icon does not appear for the job in the Job Server column on this page.</td>
</tr>
</tbody>
</table>

### 7.1.2 Statistics

For each job execution, the Administrator shows statistics. Statistics quantify the activities of the components of the job. You can view the following types of statistics:

- Job statistics such as time spent in a given component of a job and the number of data rows that streamed through the component.
- Data flow object statistics such as the cache size used by a transform within a data flow.

#### 7.1.2.1 Viewing job statistics

To help tune the performance of a job, review job statistics.

1. Select `Batch` ➔ `<repository>` ➔

2. On the Batch Job Status page, find a job execution instance. Identify an instance using the page sub-title (which provides the name of the repository on which SAP Data Services stores the job) and the following column headings on this page:

<table>
<thead>
<tr>
<th>Table 38:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column</strong></td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Job Name</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>Name of a set of datastore configurations that the job uses to connect to source and target databases when it executes. Each value in this column is a link. Click the link to view the set of datastore configurations in the system configuration. To change the system configuration, click the Batch Job Configuration tab, then use the Execute, Add Schedule or Export Execution Command pages.</td>
</tr>
<tr>
<td>Job Server</td>
<td>The server that ran this job.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The date and time that the job execution instance started.</td>
</tr>
<tr>
<td>End Time</td>
<td>The date and time that this job execution instance stopped.</td>
</tr>
<tr>
<td>Duration</td>
<td>The time (in seconds) that the job took to complete.</td>
</tr>
<tr>
<td>Run #</td>
<td>The number of times that this instance ran before completing.</td>
</tr>
</tbody>
</table>

3. Under Job Information for an instance, click Monitor. The Administrator opens the Job Server Monitor Log Viewer page. This page shows several statistics about this instance of job execution starting with the name of the monitor log file.

After the file name, each line in the log provides the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Name</td>
<td>Indicates which object (step in a data flow) is executing.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates the run-time order of the processes in the execution of the transform object and the states of each process. These are not error status states. However, if a process state is Proceed and it never changes to Stop, this indicates the process ran with errors.</td>
</tr>
<tr>
<td>Initializing</td>
<td>Indicates that the job is initializing.</td>
</tr>
<tr>
<td>Optimizing</td>
<td>Indicates that the job is optimizing.</td>
</tr>
<tr>
<td>Proceed</td>
<td>Indicates that the process is executing.</td>
</tr>
<tr>
<td>Stop</td>
<td>Indicates that the process ended without error.</td>
</tr>
<tr>
<td>Row Count</td>
<td>Indicates the number of rows processed through this object. This value updates based on the Monitor sample rate (# of seconds) set as an execution option on the Execute Batch Job page.</td>
</tr>
<tr>
<td>Elapsed Time</td>
<td>Indicates the time (in seconds) since the object received its first row of data.</td>
</tr>
<tr>
<td>Absolute Time</td>
<td>Indicates the time (in seconds) since the execution of this entire data flow (including all of the transforms) began.</td>
</tr>
</tbody>
</table>

### Related Information

Viewing overall status of executed jobs [page 103]

### 7.1.2.2 Data flow statistics

To help tune the performance of a data flow, review data flow statistics.
7.1.3 Ignoring error status

The Batch Job Status page includes an option to Ignore Error Status. Use this option if you are working through jobs with warnings or errors on this page and you want to mark a row so that you know you are finished looking at its logs.

1. On the Batch Job Status page, select the job or jobs that you want to ignore.
2. Click the Ignore Error Status button.
   The page refreshes and the rows you selected now display a green status icon.

7.1.4 Deleting batch job history data

The Batch Job Status page includes an option to delete information about how a job ran.

If you want to manually delete rows from this page, select the rows that you want to delete, then select Delete. You can also manage this information by setting the Administrator’s log retention period.

```
<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>When you delete this batch job history data, the software also clears data validation statistics from Data Validation Metadata Reports. Additionally, many history and log files contain data cleanse statistics and other information required for regulatory reports. Delete these files with caution. If you are not sure what logs are deleted when you delete the batch job history data, make backup copies of the logs before you delete them.</td>
</tr>
</tbody>
</table>
```

Related Information

History retention and Job Server log retention [page 50]

7.1.5 Stopping a running job

The Batch Job Status page includes an option to abort batch jobs. If a batch job is running and you need to stop it, select the check box next to the job name and click Abort.

7.1.6 Deleting trace, monitor, and error logs for a batch job

You can view and delete trace, monitor, and error logs for job instances from the Batch Job Status page.

You can use the Delete button on the Batch Job Status page to delete a set of batch log history files from a Job Server computer and its corresponding repository. The corresponding Job Server must be up and running to view or delete these logs. You can set trace log options on the Execute Batch Job page.
Caution

When you delete trace, monitor, and error log files you may be deleting important files that the software needs to create regulatory or certified reports as well as statistical tables. Make sure that the log files you are deleting do not need to be used for reporting purposes. If you are not sure, make backup copies of the files that you need before you delete the batch job history.

1. Select `Batch <repository>`.
2. Select the job or jobs for which you want to delete logs.
   Alternately, you can click `Select All`.
3. Click `Delete`.
   The batch log history files are deleted from the Job Server computer and its corresponding repository.

Related Information

History retention and Job Server log retention [page 50]
Statistics [page 104]
8  Lifecycle management

8.1  Migration basics

About this section

Migration as it relates to SAP Data Services is the process of moving applications through multiple development phases into production. The software supports simple and complex application migration through all phases into production.

Related Information

Development phases [page 108]
Migration mechanisms and tools [page 110]

8.1.1  Development phases

The ETL application development process typically involves three distinct phases:

- Design phase
- Test phase
- Production phase

You can use SAP Data Services in all three phases. Because each phase might require a different repository to control environment differences, the software provides controlled mechanisms for moving objects from phase to phase.

Each phase could involve a different computer in a different environment with different security settings. For example, design and initial test may only require limited sample data and low security, while final testing may require a full emulation of the production environment including strict security.
8.1.1.1 Design phase

In this phase, you define objects and build diagrams that instruct SAP Data Services in your data movement requirements. The software stores these specifications so you can reuse them or modify them as your system evolves.

Design your project with migration to testing and final production in mind. Consider these basic guidelines as you design your project:

- Construct design steps as independent, testable modules.
- Use meaningful names for each step you construct.
- Make independent modules that can be used repeatedly to handle common operations.
- Use test data that reflects all the variations in your production data.

8.1.1.2 Test phase

In this phase, you use SAP Data Services to test the execution of your application. At this point, you can test for errors and trace the flow of execution without exposing production data to any risk. If you discover errors during this phase, return the application to the design phase for correction, then test the corrected application.

Testing has two parts:

- The first part includes designing the data movement using your local repository.
- The second part includes fully emulating your production environment, including data volume.

The software provides feedback through trace, error, and monitor logs during both parts of this phase.

The testing repository should emulate your production environment as closely as possible, including scheduling jobs rather than manually starting them.
8.1.1.3 Production phase

In this phase, you set up a schedule in SAP Data Services to run your application as a job. Evaluate results from production runs and when necessary, return to the design phase to optimize performance and refine your target requirements.

After moving the software into production, monitor it in the Administrator for performance and results. During production:

- Monitor your jobs and the time it takes for them to complete. The trace and monitoring logs provide information about each job as well as the work flows and data flows contained within the job. You can customize the log details. However, the more information you request in the logs, the longer the job runs. Balance job run-time against the information necessary to analyze job performance.
- Check the accuracy of your data.

To enhance or correct your jobs:

- Make changes in your design environment.
- Repeat the object testing.
- Move changed objects back into production.

8.1.2 Migration mechanisms and tools

SAP Data Services provides two migration mechanisms:

- Export/import migration works best with small to medium-sized projects where a small number of developers work on somewhat independent Data Services applications through all phases of development.
- Multi-user development works best in larger projects where two or more developers or multiple teams are working on interdependent parts of Data Services applications through all phases of development.

Regardless of which migration mechanism you choose, it is recommended that you prepare for migration using one or more tools that best fit your development environment. The mechanism and tools you use will depend on the needs of your development environment.

If your source data will come from multiple, homogeneous systems, it is recommended that you use Datastore and system configurations tools.

When migrating applications in a multi-user environment, it is strongly recommended that you use Naming conventions for migration.

Related Information

Export/import migration [page 111]
Preparing for migration [page 112]
Datashore and system configurations [page 116]
Naming conventions for migration [page 113]
8.1.2.1 Which mechanism is best?

Although SAP Data Services supports a multi-user environment, you may not need to implement this architecture on all projects. If your project is small to medium in size and only consists of one or two developers, then a Central Repository may not be a necessary solution to integrating the work of those developers.

For example, only two consultants worked on a certain HR data mart application. The Development system was designed so that while Consultant 1 managed the Master Repository, Consultant 2 worked on a new section within a complete copy of the Master Repository.

Consultant 2 then exported this new section back into the Master Repository using the export utility that allows objects to be 'Created', 'Replaced', or 'Ignored'. After updating the Master Repository, Consultant 2 took a new complete copy of the Master Repository, overwriting the previous copy.

Use the following matrix to help you determine which mechanism and tools would work best in your environment.

Table 40:

<table>
<thead>
<tr>
<th>Situation/requirements</th>
<th>Migration Mechanisms</th>
<th>Tools</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Export/import</td>
<td>Multi-user</td>
<td>Naming conventions</td>
</tr>
<tr>
<td>Small to medium-sized project</td>
<td>X</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Multiple-team project</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Source data from multiple, homogeneous systems</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Different source or target database among environments</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Need a “fast and easy” migration solution</td>
<td>O</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Optimal solution: X Compatible solution: O

8.1.2.2 Export/import migration

Export/import is the basic mechanism for migrating SAP Data Services applications between phases. First, you export jobs from the local repository to another local repository or to an intermediate file which you can then import into another local repository. For example, when moving from design repository to test repository, you export from the design repository to a file, then import the file to your test repository.
If you find application errors during testing, you can correct them in the development environment, then export the corrected version and import it back into the test repository for retesting.

**Related Information**

Export/Import [page 119]

### 8.1.2.3 Multi-user migration

You can also migrate SAP Data Services applications between phases in more complex development environments. Instead of exporting and importing applications, multi-user development provides a more secure check-in, check-out, and get mechanism, using a central repository to store the master copies of your application elements. Multi-user development includes other advanced features like labeling and filtering to provide you more flexibility and control in managing application objects.

### 8.2 Preparing for migration

**About this section**

Before you develop SAP Data Services applications, it is recommended that you first set up a comprehensive structure to facilitate the migration process between development phases.

This section discusses tools that can help you build your migration structure.

It is recommended that you implement standardized naming conventions for connectivity between computer systems. Add datastore and system configurations to more easily work with multiple homogeneous systems.
8.2.1 Naming conventions for migration

The best way to ensure fast and seamless migration is to use common naming conventions across all systems and phases of all your development environments.

Just as it is recommended that you standardize object prefixes, suffixes, and path name identifiers to simplify your projects internally, we also recommend the use of naming conventions externally for migration purposes.

To ease migration, use common naming conventions for:

- Connections to external datastores
- Directory locations
- Schema structures and owners

You want to make it as quick and easy as possible to migrate applications between users and between phases. This translates to significantly reducing or eliminating time spent reconfiguring your jobs to work in each specific environment.

While the actual data you are extracting, transforming, and loading usually differs by database, the essential structure of the data should be the same on every database with which you want the same applications to work. Therefore, it makes the most sense to standardize your database naming and structuring before starting the development process.
You can make connection names meaningful to a certain phase and specific computer system names (Test_DW, Dev_DW, Prod_DW), however if you choose this naming structure, it is recommended that you use datastore configurations for migration purposes.

Table 41:

<table>
<thead>
<tr>
<th>Development phase</th>
<th>Test phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name: Dev_DW</td>
<td>User name: Test_DW</td>
</tr>
<tr>
<td>Password: Dev_DW</td>
<td>Password: Test_DW</td>
</tr>
<tr>
<td>Host String: Dev_DW</td>
<td>Host String: Test_DW</td>
</tr>
</tbody>
</table>

For a job to run against Test and Development, it would have to use Test_DW and Dev_DW and this would require you to create different datastore configurations for when the job runs against the Test or the Dev instance, respectively.

Alternatively, you could call the connection string DW and regardless of what instance you ran the job against, it would run without users having to create multiple datastore configurations.

Table 42:

<table>
<thead>
<tr>
<th>Development Phase</th>
<th>Test Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database A</td>
<td>Database B</td>
</tr>
<tr>
<td>User name: DW</td>
<td>User name: DW</td>
</tr>
<tr>
<td>Password: DW</td>
<td>Password: DW</td>
</tr>
<tr>
<td>Host string: DW</td>
<td>Owner name: DW</td>
</tr>
</tbody>
</table>

Examples:
- There is one Oracle source system in your company that processes order entry data. Multiple instances of this system exist for development, test, and production purposes. Therefore, you name the connection string to your Oracle source system "ORDER_SYSTEM". Then in all phases, you configure that name to point to the correct (phase-specific) instance of the system.
- Name the connection string to your target data warehouse "DW" then point it to different databases depending on whether you are in the development, test, or production environment.

When you use this generic, cross-phase naming method, you cannot access both dev and test from the same computer (since the connection string maps only to one instance). If you require access to both, use multiple datastore configurations.

Related Information

Export/Import [page 119]
8.2.1.2 Directory locations

It is recommended that you use logical directory names (for example, \x\) or point to common local drives to standardize directory location. For example, since every computer has a \c:\ drive, pointing to the directory location, \c:\temp would be a safe, reproducible standard.

8.2.1.3 Schema structures and owners

To further facilitate a seamless structure between development phases, give all your database instances the same owner name for the same schema structures from which you are reading and to which you are loading. Regardless of name, the owner of each schema structure can vary and the software will reconcile them.
8.2.2 Datastore and system configurations

Datastore and system configurations are powerful tools for reducing the configurations required to execute the same logic against different datastore environments. With configurations, migration between development phases becomes faster and more simplified.

Related Information

Datastore configurations and migration [page 116]
Multiple configurations in multi-user environments [page 118]

8.2.2.1 Datastore configurations and migration

Without multiple configuration datastores, each time you export/import from one repository to another, you may need to spend time reconfiguring datastore connections to work with the new repository (and sometimes new host computer).

Without multiple configurations, each job in a repository can run only against one datastore configuration.

With multiple configurations, instead of a separate datastore (and datastore configuration) for each database instance, you can associate multiple datastore configurations with a single datastore definition.
Each system configuration defines a set of datastore configurations that you want to use together when running a job. You must create datastore configurations for the datastores in your repository before you can create system configurations.

All objects you want to import into a multiple configurations datastore must share the same owner.
8.2.2.2 Multiple configurations in multi-user environments

SAP Data Services also supports a multi-user development environment. A team can work together on an application during development, testing, and production phases. Further, different teams can work on the different phases simultaneously.

Individual users work on an application in their unique local repositories. The team uses a central repository to store, check in, and check out objects that belong to the application master copy. The central repository preserves all versions of an application's objects, allowing you to revert to a previous version if needed.

The easiest way to set up your environment to work with multi-user functionality is by establishing the exact same environment naming standards among your developers. In each developer's environment, the configuration would be different. For example a database connection string would point to their local database. However, if implementing these naming standards is not possible, you can still save time and streamline your multi-user environment by using multiple-configuration datastores.

For example, if your developers use databases with the same metadata structure but different database instances and owners, you can define a datastore configuration for each developer on your design team, mapping different owners to a common set of aliases used by all. This way, they can share and contribute to the same projects.
without having to set up their datastore connection information each time they check out a project from the central repository.

8.3 Export/Import

Overview of export/import

The simplest type of migration in Data Services is called export/import. This section discusses the export/import method in SAP Data Services Designer.

8.3.1 Exporting/importing objects

The export feature gives you the flexibility to manage and migrate projects involving multiple developers and different execution environments. When you export a job from a development repository to a production repository, you can change the properties of objects being exported to match your production environment. In particular, you can change datastore definitions—application and database locations and login information—to reflect production sources and targets.

You can export objects to another repository or a flat file (.atl or .xml). If the destination is another repository, you must be able to connect to and have write permission for that repository, and your repository versions must match.

You cannot export read-only transform configurations.

Related Information

The Designer Export editor [page 119]
Exporting objects to another repository [page 121]
Exporting objects to a file [page 122]
Exporting a repository to a file [page 123]
Importing from a file [page 124]
Export and import options [page 166]

8.3.1.1 The Designer Export editor

In the Designer Export editor, you specify the objects you want to export and an export location. In Designer, choose Tools → Export or select an object and right-click Export to open the Export editor.
To specify an object to export, drag the object from the object library into the *Objects to Export* window.

The Object to Export window shows the final list of objects to be exported. When you drag any object from the object library, the datastores, file formats, custom functions, and transform configurations included in the object definition are automatically added to the other export sections. Each object in an export window opens to show objects called by this object.

You can control which associated objects to exclude or include. For example, you can export a work flow and all tables contained in the work flow without exporting an associated data flow.

To control which objects to export, either select an object, right-click, and choose a shortcut menu option, or select the white space in the Export editor, right-click, and choose a shortcut menu option:

<table>
<thead>
<tr>
<th>Table 43:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Export</td>
<td>Starts the export process.</td>
</tr>
<tr>
<td>Exclude</td>
<td>Removes only the selected object from the list of objects to be exported. The object remains in the list, but its exclusion is indicated by a red &quot;x&quot; on the object icon. All occurrences of the object are excluded. When you export the list, excluded objects are not copied to the destination. Objects called by this object are not removed from the list of objects to be exported, unless they are specifically excluded.</td>
</tr>
<tr>
<td>Include</td>
<td>Adds an excluded object to the export plan. The red &quot;x&quot; on the icon disappears. All occurrences of the object are included. When you export, the included objects are copied to the destination.</td>
</tr>
<tr>
<td>Exclude Tree</td>
<td>Removes the selected object and all objects called by this object from the export. The objects remain in the list, but their exclusion is indicated by a red &quot;x&quot; on the icons—the selected object and any objects it calls are excluded. When you export the list, the excluded objects are not copied to the destination.</td>
</tr>
<tr>
<td>Include Tree</td>
<td>Adds the selected excluded object and the objects it calls to the export list. The red &quot;x&quot; on the selected object and dependents disappears. When you export the list, the included objects are copied to the destination.</td>
</tr>
</tbody>
</table>

Note

You cannot export read-only transform configurations, so they are automatically excluded.
8.3.1.2 Exporting objects to another repository

You can export objects from the current repository to another repository. However, the other repository must be the same version as the current one. The export process allows you to change environment-specific information defined in datastores and file formats to match the new environment.

1. In the object library, choose an object to export. Right-click and choose Export.
   The Export editor opens in the workspace. To add more objects to the list of objects to export, drag the objects from the object library into the Objects to Export section of the editor.
2. Refine the list of objects to export.
   You can use the options available in the right-click menu for each object to include or exclude the object from the export list.
3. When your list is complete, right-click and choose Export.
4. In the Export to repository window, enter your user credentials for the Central Management Server (CMS).

   Table 44:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Specify the server name and optionally the port for the CMS.</td>
</tr>
<tr>
<td>User name</td>
<td>Specify the user name to use to log into CMS.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify the password to use to log into the CMS.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Specify the authentication type used by the CMS.</td>
</tr>
</tbody>
</table>

5. Click Log on.
The software attempts to connect to the CMS using the specified information. When you log in successfully, the list of local repositories that are available to you is displayed.

6. Select the repository you want to use as the export target.
7. Click Next to continue exporting to the selected repository.
8. In Export Confirmation window, verify the components to export.

The Destination status column shows the status of the component in the target database and the proposed action.

Table 45:

<table>
<thead>
<tr>
<th>Destination Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does not exist</td>
<td>Create/Exclude</td>
</tr>
<tr>
<td>Exists</td>
<td>Replace/Exclude</td>
</tr>
</tbody>
</table>

To edit an action, select any number of objects (using the SHIFT and CTRL keys) and select either Create, Exclude, or Replace from the Target Status list box.

9. Click Next.
10. In the Datastore Export Options window, select the datastore, change the owner of a table or the connection properties of the datastore as necessary, and click Advanced.
11. Change the database connection information as required by the target database and click Next.
12. In the File Format Mapping dialog, select a file and change the Destination Root Path, if necessary.

You can change the Destination Root Path for any file formats to match the new destination.
13. Click Finish.

SAP Data Services copies objects in the Export editor to the target destination. When copying is complete, the objects display in the Output window. The Output window shows the number of objects exported as well as a list of any errors.

**8.3.1.3 Exporting objects to a file**

You can also export objects to a file. If you choose a file as the export destination, Data Services does not provide options to change environment-specific information.

1. Right-click an object in the object library, and click Export.
   The Export editor opens in the workspace. To add more objects to the list of objects to export, drag the object from the object library into the Objects to Export section of the editor.
2. Refine the list of objects to export.
   You can use the options available in the right-click menu for each object to include or exclude the object from the export list.
3. When your list is complete, right-click the editor and click Export to ATL file or Export to XML file, depending on the type of file format that you want to export.

**Tip**

ATL is the software’s proprietary format. Using XML might make repository content easier for you to read. XML can also be used with the object creation XML toolkit. For more information, see the Integrator Guide.
By default, non-executable elements are excluded from exported XML files to improve readability. For example, the exact arrangement of transforms within a data flow would not be maintained, and the transforms would be arranged automatically when imported back into the software.

If you want to include these elements, deselect **Exclude non-executable elements from exported XML document.** This option is available in the Designer > General group in the Tools > Options menu.

4. Specify the location for the exported file.

5. Enter the case-sensitive passphrase to use to encrypt any passwords that are stored in the objects you are exporting and click **OK.**

![Note]
You must enter the same passphrase when you import the file back into a repository. If you use an incorrect passphrase, the software will still import the objects, but any stored passwords will be removed.

This option (**Export to XML file**) allows SAP Data Quality Management SDK developer to configure Data Quality transforms within the Data Services Designer and export the settings to XML files for use with the Data Quality Management SDK.

However, if you employ Data Services as a configuration tool for the Data Quality Management SDK, Data Services does not support the creation of a change log for changes to the configuration. You can employ the Data Services central repository concept to manage changes to the Data Quality transforms, but no change log is created.

### 8.3.1.4 Exporting a repository to a file

You can also export an entire repository to a file. When you export or import a repository, jobs and their schedules (created in SAP Data Services) are automatically exported or imported as well. Schedules cannot be exported or imported without an associated job and its repository.

If you choose a file as the export destination, the software does not provide options to change environment-specific information.

1. From the object library, right-click and choose Repository > Export To File.

   A window opens to prompt you for the destination of the export file. You can browse the directory to change the location, set the file type (XML or ATL), and enter a name for the file.

2. Click **Save.**

3. Enter the case-sensitive passphrase to use to encrypt any passwords that are stored in the repository and click **Export.**

![Note]
You must enter the same passphrase when you import the file back into a repository. If you use an incorrect passphrase, the software will still import the objects, but any stored passwords will be removed.

The repository is exported to the file.
8.3.1.5 Importing from a file

Importing objects or an entire repository from a file overwrites existing objects with the same names in the destination repository.

1. There are two ways to import repository files into another repository. Use Tools ➤ Import from file, or in the object library, right-click and choose Repository ➤ Import from File.

   A window opens for you to specify the file to import. You can import individual files or the whole repository using either an ATL, XML, DMT, or FMT file type. (ATL is the software’s internal scripting language. DMT and FMT are files exported from the SAP Data Quality Management or IQ8 products.)

2. Select a file to import and click Open.

3. When importing an ATL or XML file, a list of objects displays in the Import Plan window.

   Highlight objects and use the buttons at the bottom of the window to include or exclude them during import. You can also right-click on an object to access these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude</td>
<td>Removes only the selected object from the list of objects to be imported. The object remains in the list, but its exclusion is indicated by a red “x” on the object icon. All occurrences of the object are excluded. When you import the list, excluded objects are not copied to the destination. Objects called by this object are not removed from the list of objects to be imported, unless they are specifically excluded.</td>
</tr>
<tr>
<td>Exclude Tree</td>
<td>Removes the selected object and all objects called by this object from the import. The objects remain in the list, but their exclusion is indicated by a red “x” on the icons—the selected object and any objects it calls are excluded. When you import the list, the excluded objects are not copied to the destination.</td>
</tr>
<tr>
<td>Include</td>
<td>Adds an excluded object to the import plan. The red “x” on the icon disappears. All occurrences of the object are included. When you import, the included objects are copied to the destination.</td>
</tr>
<tr>
<td>Include Tree</td>
<td>Adds the selected excluded object and the objects it calls to the import list. The red “x” on the selected object and dependents disappears. When you import the list, the included objects are copied to the destination.</td>
</tr>
<tr>
<td>Import</td>
<td>Starts the import process.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the import process.</td>
</tr>
<tr>
<td>Select All</td>
<td>Selects all the objects.</td>
</tr>
</tbody>
</table>

4. Enter the passphrase that was used to encrypt passwords when the file was exported and click Import.

   **Note**

   If the passphrase does not match the passphrase you used to export the file, the import will continue, but any passwords will be emptied and need to be reset manually.
5. Perform any additional steps that may vary depending on the type of the file you are importing.

- If you attempt to import an ATL file saved from an earlier version of SAP Data Services, a warning displays indicating that the version of the ATL file is lower than the repository version and that the ATL file you are about to import might contain objects that do not make optimal use of your upgraded repository. For example, new options for some features might not be available. To update an ATL file, import it into a repository of the same version then upgrade that repository. To abort the import, click No. To continue with the import, click Yes.
- If you attempt to import an ATL file saved from a repository that is later than your current version, an error message displays indicating that the version of the ATL file is higher than the repository version and cannot be imported. Click OK.
- If you attempt to import a DMT or FMT file, the software displays the File Format Editor which allows you to complete missing values for the properties of the file. Also, because DMT and FMT formats support field names longer than 60 characters, you must uniquely rename any field names longer than 60 characters prior to importing the file.

8.3.2 Backing up repositories

Use your DBMS utilities to back up your repositories regularly. For information, refer to your DBMS documentation.

8.3.3 Maintaining Job Server performance

If you are designing jobs, typically you might use the same computer for your Designer, repository, and Job Server. In addition, you might use the same datastore for both your repository and your target database.

However, when you migrate your jobs into a test environment, the Job Server could move to a separate computer (typically from a Windows to a UNIX platform). The SAP Data Services Job Server computer uses source, target, and repository database client libraries to extract, transform, and load data according to a job’s design. Therefore, the Job Server computer must have a database client installed for each database you are using to run a job. In addition, you can localize source and target databases using locale and code page settings.

When migrating jobs between different Job Servers verify that the code page used by each source and target database is the same as the code page set for the corresponding database client on the Job Server’s computer.

The database client code page used by a Job Server on a Windows might be different from the one used on UNIX. For example, the Oracle client code page MS1252 on Windows should be changed to the ISO88591 code page on UNIX.

The software allows different code pages to be used in sources and targets. Mismatched locale settings do not cause errors and the software attempts to treat equivalent settings without any transcoding. However, mismatches may result in performance degradation from transcoding done by the software during job execution.

If your jobs do not require the use of different locales, you can increase performance by ensuring that default locales are not mismatched. After migration, if you notice a significant difference between the speed of design and test environments, check locale settings. In the Designer, check to see that datastore code pages for sources and targets match client code pages on the Job Server computer.
8.4 The Enhanced Change and Transport System (CTS+)

The Change and Transport System (CTS) in SAP Solution Manager or SAP NetWeaver is used to transport ABAP objects from source system to target system for lifecycle management. Enhanced CTS, or CTS+, is CTS with the ability to transport non-ABAP objects.

We refer to the CTS that is enabled to transport non-ABAP objects as Enhanced CTS or CTS+. However, for simplicity, we use the term CTS in this section to mean one of two things:

- The system where the transport landscapes are configured.
- The system that transports ABAP and non-ABAP objects.

If you do not need a transport management system (TMS) with SAP Solution Manager or SAP NetWeaver, you can continue to use Object Promotion in Data Services to transport objects over secure FTP, or you can continue to use a shared folder.

If you already use CTS in your SAP Solution Manager or SAP NetWeaver system to transport ABAP objects, you can save time and be more efficient by installing the CTS plug-in and set your system to transport non-ABAP Data Services objects.

You must be using the specified versions of Solution Manager or NetWeaver, which either have the CTS plug-in included in the installation, or require you to download the CTS plug-in from the SAP Service Marketplace. You also must install or upgrade to Data Services 4.2 Support Pack 6 patch 1 or later to use CTS. See the Configuration Guide for CTS+ for version requirements.

Transport the following Data Services objects, and their dependents, using CTS:

- Projects
- Jobs
- Workflows
- Dataflows
- File formats
- Functions
- Datastores (as top-level object only)

⚠️ Restriction

**Datastores** You can transport datastores and their dependents, however datastores are not exported as part of an object dependency. Additionally, for security reasons, the datastore password is not exported with the datastore. The datastore in development or test should be different from the one in production. To avoid errors, export a datastore object separate from other Data Services objects. After you import the datastore to production, an administrator must reconfigure the datastore. This behavior prevents users from overwriting existing jobs that use the datastore.

For complete information about using Data Services with CTS, see the Configuration Guide for CTS+ that is included with the Data Services documentation, available on the SAP Customer Portal at [http://help.sap.com/bods](http://help.sap.com/bods)
8.5 Data Services Object Promotion Management

8.5.1 About object promotion

8.5.2 Overview of Data Services Object Promotion Management

The Object Promotion tool in the Data Services Administrator enables you to move one or more Data Services objects from a development environment to a QA environment, or directly to a production environment.

To ensure security, these environments typically do not have direct access to one another. Object promotion in Data Services is accomplished over secure FTP or over a shared directory that only an Administrator or a user with an account assigned to the Data Services Administrator group can configure for this purpose, maintaining security in both source and target environments.

Users with View access to a repository can export its objects from a development environment to a shared directory created by authorized users. Users who have Full Control access to the repository can import objects after an Administrator or a user with an account assigned to the Data Services Administrator group has granted them the new Manage Object Promotion Import user application right.

The user who starts the Server Intelligence Agent (SIA) on the server that has access to the shared directories that are used for exporting and importing promoted objects, must have full read and write access to those shared directories. If the server is started by a user who does not have full access to the shared directory, all configurations for export and import operations for that shared directory will fail validation, and the configurations cannot be completed until the issue is resolved. To validate this, an authorized user or the administrator can validate the configuration by testing the connection or re-saving the configuration to check. If another user without full read write privileges to the shared directory starts SIA after a configuration has been successfully validated, all export and import operations from that configuration will fail until SIA is restarted by a user with the required credentials.

If objects with the same name and types are selected for import, the objects are imported sequentially based on the date of export. When you view the list of exported objects in the Import Configuration page in the Administrator, the exported objects are grouped together with objects of the same type and object name, listed in order by the date they were exported. If the same object and types are exported multiple times, depending on the export date, you can import the same objects, and these objects are imported sequentially, based on the export date.

8.5.3 Requirements for object promotion

The following table describes requirements that apply when using the SAP Data Services Object Promotion Management tool in the Administrator in Management Console to promote Data Services objects.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source and target must have the same Data Services version</td>
<td>The source and target repositories must both be running the same version of Data Services before attempting to promote objects to or from them.</td>
</tr>
</tbody>
</table>
| Full read and write access to shared directories  | The user who starts the Server Intelligence Agent (SIA) on the server that has access to the shared directories that are used for exporting and importing promoted objects must have full read and write access to those shared directories.  
  If the server is started by a user who does not have full access to the shared directory, all configurations for export and import operations for that shared directory will fail validation, and the configurations cannot be completed until the issue is resolved. To validate this, go to configuration page and click Test, or try to save the configuration again.  
  If another user without full read write privileges to the shared directory starts the SIA on the server after export and import configurations have been successfully validated and saved, all of those export and import configurations will fail to successfully run until the SIA is restarted by a user with the required credentials. |
<p>| All dependent objects are promoted exept for datastores | When you promote a Data Services object, all of its dependent objects are also promoted, with the exception of its datastores. Typically, datastores in a development environment contain data that is used only for testing, and that data is not typically used in a production environment. If you need to promote a datastore from a development environment to a production environment, the datastore must be promoted separately. |
| Datastore passwords are not included in the import or export | When a datastore is promoted, its password is not included in the import or export operation, so the password field for the promoted datastore is left blank. This is intentional and provides a safeguard to prevent the unintended use of a development or QA datastore in a production environment. It also provides another level of security, because only the owner of a datastore should know its password. |</p>
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconfigure datastore after promotion</td>
<td>After a datastore promotion completes, you reconfigure the datastore under <em>Administration &gt; Management &gt; Datastore</em> in SAP Data Services Management Console. Set a password for the promoted datastore in its new location, and if needed, modify the location of the database it uses. If the datastore used in the production environment is different from the one used in development or QA, be sure to update them. If a valid datastore password is not entered after the datastore has been imported into another environment, all of the jobs that depend on that datastore will fail to run until you enter the password.</td>
</tr>
<tr>
<td>User’s account must be assigned to Administrator group account</td>
<td>Only a user whose account is assigned to the Data Services Administrator group account can create and edit the configurations used for exporting or importing objects. An Administrator, or a user who is assigned to the Data Services Administrator group, can assign rights to another user who is not part of that group, the Manage Object Promotion Configurations right to allow the user (who is not part of that group) the rights to modify the configurations through the Administrator in the Master Console.</td>
</tr>
<tr>
<td>Only users with at least View access to repository can export objects</td>
<td>Only users with, at a minimum, View access to a repository can export its objects to the shared directory configured by an Administrator or a Data Services Administrator group user.</td>
</tr>
<tr>
<td>Only Data Services Administrator group users can import objects into a repository</td>
<td>An Administrator or a user whose account is a member of the Data Services Administrator group can assign another user who is not part of that group the right to Manage Object Promotion Import, which grants that user the authorization to import objects into a repository. That user must also have Full Control access to the repository to be able to import its objects.</td>
</tr>
<tr>
<td>Each top-level object import is run sequentially</td>
<td>If one object fails to import, it will revert back, then the import continues to the next top-level object.</td>
</tr>
</tbody>
</table>

**Related Information**

Managing application rights for a group [page 41]
8.5.3.1 User rights for object promotion management stages

The following table summarizes the required user rights for each stage of the Object Promotion Management process.

Table 48:

<table>
<thead>
<tr>
<th>Type of user</th>
<th>Configure export and import</th>
<th>Export objects from repository (source)</th>
<th>Import objects from shared directory (target)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Services Administrator group</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Regular Data Services user, without additional rights</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Must also have, at minimum, View access to export objects from the repository</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regular Data Services user, with Manage Object Promotion Configurations right</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Must also have, at minimum, View access to export objects from the repository</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regular Data Services user, with Manage Object Promotion Import right</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Must also have the required Full Control access to the shared directory</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Information

Managing application rights for a group [page 41]

8.5.4 Object promotion user interface

The Data Services Object Promotion Management tool is found in the Management Console under the Administrator. To view the choices, select or expand the Object Promotion menu.

When you select the title for the Object Promotion menu, the Object Promotion page appears, with choices to access and run existing export and import configurations. The following table describes each option.
Table 49:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Export objects</strong></td>
<td>Manages the export of specific object types from specific repositories. After you select a repository and object type, and select Next, a table appears with details for each object of the selected type that resides on that repository and is available to export.</td>
</tr>
<tr>
<td><strong>Export Substitution Parameters</strong></td>
<td>Manages the export of one or more substitution parameters, which are listed by the repository in which they reside. After you select a substitution parameter and select Next, a table appears with details for each substitution parameter.</td>
</tr>
<tr>
<td><strong>Export System Configurations</strong></td>
<td>Manages the export of one or more individual system configurations from the local repository. After you select a system configuration and select Next, a table appears with details for each system configuration.</td>
</tr>
<tr>
<td><strong>Import</strong></td>
<td>Displays details for objects that have been exported from the repository and are available to import. A search tool provides a way to narrow the displayed list. From the displayed results, you can select one or more objects to import.</td>
</tr>
</tbody>
</table>

Each of the pages displayed for these choices include an indication of whether an export or import has ever been run on the displayed object(s).

Table 50:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value = Yes</th>
<th>Value = No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exported</td>
<td>One or more export operations have been run on this repository object. The status of these operations could be success or failure.</td>
<td>No export operations have ever been run on this repository object.</td>
</tr>
<tr>
<td>Imported</td>
<td>One or more import operations have been run on this repository object. The status of these operations could be success or failure.</td>
<td>No import operations have ever been run on this repository object.</td>
</tr>
</tbody>
</table>

8.5.4.1 Object Promotion menu choices

When you expand the Object Promotion menu, there are two choices explained in the following table.

Table 51:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Configuration</td>
<td>Lists all of the export configurations that have been created by authorized users.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Import Configuration</td>
<td>Lists all of the import configurations that have been created by authorized users.</td>
</tr>
</tbody>
</table>

The export and import configurations are displayed and are available for selection in the list on the **Object Promotion** page, which is displayed when you select either choice.

**i Note**

Users whose accounts are not members of the Data Services Administrator group or who have not been granted specific permissions by a member of that group cannot create or edit export and import configurations, nor can they run the import configurations created by an authorized user.

- To edit an export or import configuration, users outside the Data Services Administrator group must be granted the **Manage Object Promotion Configurations** right.
- To run an import configuration to import objects, users outside the Data Services Administrator group must be granted the **Manage Object Promotion Import** right, and they must also have **Full Control** access to the repository.

### 8.5.5 Configuring object promotion

#### 8.5.5.1 Set up export configuration

The following specific requirements and recommendations apply when setting up an export configuration:

- Only a user whose account is assigned to the Data Services Administrator group account can create and edit the configurations used for exporting or importing objects. An administrator, or a user who is assigned to the Data Services Administrator group, can assign to another user, who is not part of that group, the right to modify the configurations (**Manage Object Promotion Configurations** rights) through the Administrator in Master Console.
- For security reasons, only a system administrator can create a shared directory to which objects can be exported to or imported from. If a shared directory has not yet been created but you have been granted permission to configure exports and imports, the only available transport option you will see for your configuration is FTP.
- If you are configuring an export to use FTP to promote objects to a UNIX system, be sure to configure the FTP server to have full read and write access to the shared directory that was set up to receive exported objects.
- If you need to clear space on the shared directory, you can safely delete the exported .ATL and .manifest files after you have finished importing them. If you create a separate export configuration for each release, it is easier to identify the groups of files you can safely archive or delete.
- A repository can be associated with multiple, different export configurations.
8.5.5.1.1 Setting up an export configuration

Use object promotion to create a configuration that can be used to export an object and its dependent objects over secure FTP or directly to a shared directory:

1. Open Data Services Management Console and select Object Promotion > Export Configuration.
2. In the Export Configuration page, click Add.
3. Create either an export configuration to transport objects over FTP or an export configuration to transport objects directly to an existing shared directory

   To create an export configuration to transport objects over FTP:
   a. On the FTP tab, enter information in each of the required fields.
   b. Choose to enable Secure FTP.
   c. Select one or more entries in the Available Repositories list to associate with this configuration.
   d. Optional. Click Test to ensure that the configuration can access the repositories and the Target Directory that you associated with this configuration.
   e. Save the configuration.

   To create an export configuration to transport objects directly to an existing shared directory:
   a. On the Shared Directory tab, enter a name for the configuration and a target directory to which the objects should be exported on the shared directory.
   b. Select one or more entries in the Available Repositories list to associate with this configuration. You can only export objects from the repositories that are selected for the Associated Repositories list.
   c. Save the configuration.

When you test or save the configuration, the Object Promotion Management tool validates whether the SIA service can save (read and write) content to the shared directory. If the configuration can access the repositories with which it has been associated and the SIA service validates access to the shared directory, the configuration is saved with the name you specified. After it is saved, the named configuration will appear as a choice on the Export Configuration page, and as an Object Name choice when you choose Export Objects, Export System Configuration, or Export Substitution Parameters.

To modify an export configuration, return to the Export Configuration and select the Object Name of the configuration you want to modify.

To remove an export configuration, select it in the Export Configuration and click Remove.

Related Information

Requirements for object promotion [page 127]
Exporting an object [page 135]
8.5.5.2 Set up import configuration

The following specific requirements apply when setting up an import configuration:

- The object and all of its dependent objects must have already been exported before you run the import configuration.
- An import configuration can be associated with only one repository.
- A target repository must be configured to a shared directory where ATL files have been exported.
- Only a user whose account is assigned to the Data Services Administrator group account can create and edit the configurations used for exporting or importing objects. An administrator, or a user who is assigned to the Data Services Administrator group, can assign to another user who is not part of that group, the right to modify the configurations (Manage Object Promotion Configurations rights) through the Administrator in Master Console.

Related Information

Requirements for object promotion [page 127]
Importing an object [page 138]

8.5.5.2.1 Setting up an import configuration

You use object promotion to create a configuration than can be used to import an object and its dependent objects from a shared directory:

1. In Data Services Management Console, expand the Object Promotion menu, then select Import Configuration.
2. On the Import Configuration page, click Add.
3. Select the Repository from which the objects were configured to be exported, and in the Source Directory field, enter the directory path to where the export configuration deposited the objects.
   After you configure the Repository, it cannot be configured with a different path, because that repository will no longer show up in the list of choices.
4. Save the configuration.

If the import configuration can access the shared directory to where the objects are exported, the configuration is saved with the name of the target repository. The configuration will appear as a choice on the Import Configuration page, and as an Object Name choice when you choose Import.

To modify an import configuration, return to the Import Configuration page and select the Object Name of the configuration you want to modify.

To remove an import configuration, select it in the Import Configuration and click Remove.

If you imported a datastore, after it is imported you must reconfigure the datastore under Administration > Management > Datastore in SAP Data Services Management Console and assign it a password.

After you import a collection of substitution parameters, if needed, you can update the paths for the substitution parameters after they are imported to their new location.
**8.5.6 Promoting objects**

**8.5.6.1 Export an object**

Specific requirements when exporting an object.

- The source and target repositories must be running the same version of SAP Data Services.
- You can export from a local repository or a central repository.
- If a datastore is a dependent object of the object you are exporting, the datastore must be exported separately.
- When a datastore is promoted, its password is not included in the import or export operation, so the password field for the promoted datastore is left blank. This is intentional and provides a safeguard to prevent the unintended use of a development or QA datastore in a production environment.

**Note**

After a datastore promotion is completed, be sure to reconfigure the datastore under *Administration > Management > Datastore* in SAP Data Services Management Console. Set a password for the promoted datastore in its new location, and if needed, modify the location of the database it uses.

- The repository from which you are exporting objects must be associated with an export configuration.

**Related Information**

Exporting an object [page 135]

**8.5.6.1.1 Exporting an object**

Use object promotion to export objects.

You can use object promotion to export the following types of objects from their current repository to a shared directory:

- Project
- Job
- Work flow
- Data flow
1. In Data Services Management Console, select **Object Promotion**.
2. Select one of the following choices in the **Objects** list, then click **Next**.
   - Export objects
   - Export system configurations
   - Export substitution parameters
3. Select a repository (local or central) and if you chose **Export objects**, choose an object type, then click **Next**.
   The **Export** page appears, with a list of the latest version of all the objects you specified that are available in your chosen repository.
   
   There are 23 entries listed on each page. You can include up to 23 of the entries listed on a given **Export** page in a single export operation. Click the page links to view any subsequent pages of available objects.
4. If you chose **Export system configurations** or **Export substitution parameters** in the **Objects** list, narrow the list to display only the objects you want to export.
   
   To narrow the list, use the **Search** field to look for objects that completely or partially match the export configuration for the objects you want to export. The **Search** field supports wildcards.
5. If you chose **Export objects** in the **Objects** list, narrow the list to display only the objects you want to export using a filter. To filter the list:
   a. Enter specific text to search for what appears in the **Object name** field. You can use an asterisk as a wildcard to expand your search to objects that partially match or are part of a common naming scheme.
   b. If the selected **Object Type** is **Job**, select a specific **Project** (the default is **All Projects**).
   c. If you are exporting from the central repository, additional filter choices are available.
      If the selected **Object Type** is **Project**, select a different version in the **Get** list (the default is **Latest Version**).
      When you submit the query, it matches the parent object’s label with the associated version. If the label for a child of an object does not match with the specified label, when a parent object is exported, the latest version of the child object will be exported.
      
      d. Click **Search** to use your selections to search for objects that match your choices.
6. Individually choose up to 23 **Object Name** entries displayed on the current page, or choose **Select All** to import all 23 objects on the currently displayed page.
7. Choose the export method.
8. Click **Export** to start exporting the objects you selected.

For each object, an ATL file and a manifest file are written to the **Target Directory** specified in the export configuration.
A Confirmation page displays progress for the export, and the Status is automatically refreshed every five seconds. When the export is completed, the automatic refresh ends, the ending Status information is displayed (success or failure), and log information is stored in the repository under the AL_EXPORT_HISTORY table. To view the log information while you have the Confirmation page open, select view log under the Status column of the displayed report. Details about the job are on the Trace tab. If there were any issues with the export, messages are recorded to the Error tab.

A unique confirmation ID is assigned to each export attempt. The confirmation ID is used for a unique ID in the AL_EXPORT_HISTORY table. The confirmation ID is used to pass information when you import the exported objects. The confirmation ID contains the following information:

<Timestamp-in-milliseconds>-<six-digit random number>-<number of export attempts>

To convert the time stamp that is displayed in milliseconds to date format, copy the integers displayed next to Confirmation# up to the first dash, and paste them into any available conversion tool.

**i Note**

Make a note of the unique confirmation number displayed on the Confirmation page, and copy any information from the log that you want to preserve. You cannot return to this Confirmation page after you dismiss it. A copy of the log is also written to the repository under the AL_EXPORT_HISTORY table, so you can query the table to find the log information later.

If you exported a datastore, and after it is imported, you must reconfigure the datastore under Administration > Management > Datastore in SAP Data Services Management Console and assign it a password.

If you exported substitution parameters, you can update the paths for the substitution parameters after they are imported to their new location. To edit substitution parameters, you must either be an administrator, or your account is a member of the Data Services Administrator group, or you are granted the rights by either an administrator or a member of the Administrator group to Manage datastore and substitution param configurations.

**Related Information**

Requirements for object promotion [page 127]
Setting up an export configuration [page 133]
Managing application rights for a group [page 41]

**8.5.6.2 Import an object**

Specific requirements when importing an object to another repository.

- The source and target repositories must be running the same version of SAP Data Services.
- Your user account must be a member of the Data Services Administrator group, or a member of that group must have granted your user account the Manage Object Promotion Import right and you have Full Control permissions for the repository.
- You can only import objects to a local repository.
When a datastore is promoted, its password is not included in the import or export operation, so the password field for the promoted datastore is left blank. This is intentional and provides a safeguard to prevent the unintended use of a development or QA datastore in a production environment.

After a datastore promotion is completed, be sure to reconfigure the datastore under Administration > Management > Datastore in SAP Data Services Management Console. Set a password for the promoted datastore in its new location, and if needed, modify the location of the database it uses.

Related Information

Importing an object [page 138]

**8.5.6.2.1 Importing an object**

The software securely imports objects using object promotion.

Use object promotion to securely import objects into a production environment from the source directory for the import configuration.

1. In Data Services Management Console, select Object Promotion.
2. Select a target repository from which to import objects, then click Next.
   The Import page appears with a list of exported objects that are available in the target repository. These entries contain information about objects that are associated with a corresponding export configuration, and they contain information about where to find the exported objects.

   There are 23 entries listed on each page. You can include up to 23 of the entries listed on a given Import page in a single import operation. Click the page links to view any subsequent pages of available objects.

3. To narrow the list to display only the objects you want to import, use the Filter choices to filter the displayed entries in the list or search for objects that completely or partially match the export configuration for the objects you want to import. The Search field supports wildcards.

4. Individually choose up to 23 entries displayed on the current page, or choose Select All to import all 23 objects displayed on the current page.

5. Click Import to start importing the selected objects.

The Confirmation page displays progress for the import, and the Status is automatically refreshed every five seconds. When the import is completed, the automatic refresh ends, the ending Status information is displayed (success or failure), and log information is stored in the repository under the AL_IMPORT_HISTORY table.

To view the log information while you have the Confirmation page open, select view log under the Status column of the displayed report. Details about the job are on the Trace tab. If there were any issues with the export, messages are recorded to the Error tab.

A unique confirmation ID is assigned to each import attempt. The confirmation ID is used for a unique ID in the AL_IMPORT_HISTORY table. The confirmation ID contains the following information:

<Timestamp-in-milliseconds>-<six-digit random number>-<number of import attempts>

To convert the time stamp that is displayed in milliseconds to date format, copy the integers displayed next to Confirmation# up to the first dash, and paste them into any available conversion tool.

138
Note

Make a note of the unique confirmation number displayed on the Confirmation page, and copy any information from the log that you want to preserve. You cannot return to this Confirmation page after you dismiss it. A copy of the log is also written to the repository under the AL_IMPORT_HISTORY table, so you can query the table to find the log information later.

If you imported a datastore, after it is imported you must reconfigure the datastore under Administration > Management > Datastore in SAP Data Services Management Console and assign it a password.

If you imported substitution parameters, you can update the paths for the substitution parameters after they are imported to their new location. To edit substitution parameters, you must either be an administrator, or your account is a member of the Data Services Administrator group, or you are granted the rights by either an administrator or a member of the Administrator group to Manage datastore and substitution param configurations.

Related Information

Requirements for object promotion [page 127]
Setting up an import configuration [page 134]
Managing application rights for a group [page 41]
9 Integration with SAP and SAP Solution Manager

9.1 Integration overview

Data Services can be integrated into a number of SAP solutions to take advantage of their features.

The System Landscape Directory and Solution Manager Diagnostics products help you manage, monitor, and maintain your Data Services deployment.

9.1.1 SAP System Landscape Directory (SLD)

The system landscape directory of SAP NetWeaver is the central source of system landscape information relevant for the management of your software life-cycle.

By providing a directory comprising information about all installable software available from SAP and automatically updated data about systems already installed in a landscape, you get the foundation for tool support to plan software life-cycle tasks in your system landscape.

The SAP Data Services installation program registers the vendor and product names and versions with the SLD, as well as server and front-end component names, versions, and location.

9.1.2 Solution Manager Diagnostics (SMD)

Analyze and monitor a complete landscape.

The SMD component of SAP Solution Manager provides all functionality to centrally analyze and monitor a complete system landscape. The SMD server can monitor Data Services if an SMD Agent is installed. The SMD Agent gathers information for the SMD server which can then be used for root cause analysis.

Data Services provides support for this performance monitoring through CA/Wily Introscope in Solution Manager Diagnostics through an integration with the NCS library. The NCS library is installed automatically with Data Services.

9.2 SLD and SAP Solution Manager integration checklist

The following table summarizes what components are required to enable SLD and SAP Solution Manager to provide support for Data Services.
### 9.3 Managing System Landscape Directory registration

#### 9.3.1 Data Services registration in the SLD

The System Landscape Directory (SLD) is a central repository of system landscape information that is relevant for the management of the software lifecycle. The SLD contains a description of the system landscape—the systems and software components that are currently installed.

SLD data suppliers (SLDReg) register the systems on the SLD server and keep the information up-to-date. Management and business applications access the information stored in the SLD to perform tasks in a collaborative computing environment.

SLDReg is installed when you install the SAPHOSTAGENT. Once SLDReg has been installed, you need to create a `slddest.cfg` and `slddest.cfg.key` file to enable it to connect to the SLD server.

The SLDReg data supplier is provided for every installation of Data Services to report on the following components:

- Server components (job server, access server)
- Services deployed on the Business Intelligence Platform (RFC Server, View Data and Metadata Browsing Service, Administrator Service)
- Web applications deployed on an application server (Management Console)

#### Note

SAP NetWeaver has a built-in SLD-DS supplier that registers the NetWeaver application server as well as hosted web applications and services. This SLD-DS is relevant for Data Services deployments that are integrated within an SAP NetWeaver environment.
During the installation of Data Services, information required for registering Data Services is stored in a configuration file. This file contains information used by the SLDReg to connect to the Data Services database.

For information on how to configure the specific data supplier for WebSphere, see the SAP Web Application Deployment Guide.

### 9.3.2 Configuring SLD in Server Manager (Windows)

Use the Data Services Server Manager utility to create or edit System Landscape Directory (SLD) registration information.

1. Select \<LINK_DIR>\Data Services <version>\bin \AWServerConfig.exe \.
   
The Data Services Server Manager opens.
2. Click the SLD tab to open the SLD settings.
3. Make the following settings as applicable:
   - SLD Server Host
   - SLD Server Port
   - SLD Server Username
   - SLD Server Password
   - Connection type
   - System ID
   - Central Host
   - Virtual Hostname
4. Click Close and Restart.
   
The utility restarts the Job Service.

#### Related Information

- SAP System Landscape Directory (SLD) [page 140]
- SLD and SAP Solution Manager integration checklist [page 140]
- Creating a slddest.cfg.key file for the SLDReg [page 142]

### 9.3.3 Creating a slddest.cfg.key file for the SLDReg

Before creating a slddest.cfg.key file for the SLD data supplier, you need to download and install the SAPHOSTAGENT.

#### Note

If you selected to add SLD during the Data Services installation, you do not need to create this file. If you are choosing to activate SLD after installing Data Services, follow this procedure.
The `slddest.cfg.key` file is required for SLD registration with the data supplier that reports on Data Services servers.

**Note**

This procedure creates both the `slddest.cfg` and the `slddest.cfg.key` file. Both of these files are required for SLD integration to work.

1. Open a command line console.
2. Navigate to the default SAPHOSTAGENT install path.
   - On Windows: `Program Files\SAP\hostctrl\exe`
   - On UNIX: `/usr/sap/hostctrl/exe`
3. Run the following command:
   
   ```bash
   sldreg -configure slddest.cfg
   ```
4. Enter the following configuration details:
   - User name
   - Password
   - Host
   - Port number
   - Specify to use HTTP

   The `sldreg` tool will create the `slddest.cfg.key` file that will automatically be used by the data supplier to push information to the SLD server.

**Tip**

For SLD integration to work, SLDReg must be running in the `<LINK_DIR>/sldreg` directory, or these files need to be manually copied to this directory.

### 9.3.4 Configuring SLD in Server Manager (Unix)

Use the Data Services Server Manager utility to create or edit System Landscape Directory (SLD) registration information.

1. Open a command line and type: `$ cd $LINK_DIR/BIN/svrcfg` to open Server Manager.
2. Enter the corresponding value based on the information that appears in Server Manager. Select 8 to configure system landscape directory registration.

   The software displays your current SLD configuration information.
3. Enter `e` to edit the SLD registration configuration.
4. Enter `E` to enable the SLD registration.
5. Specify the SLD configuration information when prompted:
   - SLD Server Host
   - SLDServer Port
   - SLD Server Username
6. Enter Y to save your changes.

The software creates the slddest.cfg and key file for SLDReg. Then it shows a list of your new SLD registration settings. A message appears telling you to restart the Job Service to complete the SLD registration.

7. Restart the Job Service using `net start "SAP Data Services"`.

8. Enter q when you are finished.

### Related Information

[Configuring SLD in Server Manager (Windows) [page 142]

### 9.3.5 When is SLD registration triggered?

The Data Services service invokes SLDReg (the data supplier for Data Services) to handle SLD registration.

### 9.4 Performance and availability monitoring

#### 9.4.1 Solution Manager Diagnostics (SMD) overview

The Solution Manager Diagnostics (SMD) component of SAP Solution Manager provides all functionality to centrally analyze and monitor a complete system landscape. Data Services can be monitored by the SMD server if an SMD Agent is installed. The SMD Agent gathers information for the SMD which can then be used for root cause analysis. Information collected and sent to the SMD server includes back-end server configurations and the location of server log files.

Data Services provides support for performance and availability monitoring through CA Wily Introscope in Solution Manager Diagnostics through an integration with the NCS library. The NCS library is installed automatically with Data Services.

The following table describes the components of SMD.
Table 53: Components of SMD

<table>
<thead>
<tr>
<th>Component</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Solution Manager</td>
<td>You must have Solution Manager 7.01 SP26 or later installed. For more information, see <a href="https://support.sap.com/solution-manager.html">https://support.sap.com/solution-manager.html</a>.</td>
</tr>
<tr>
<td>SMD Agent</td>
<td>A local agent (DIAGNOSTICS.AGENT) that collects and sends the information to the SMD server. This agent must be downloaded and installed on each Job Server that you want to monitor. The Data Services installation does not install this agent for you. Information about installing and configuring the agent is available at: <a href="https://support.sap.com">https://support.sap.com</a>.</td>
</tr>
<tr>
<td>CA Wily Introscope</td>
<td>An application performance management framework. Introscope Enterprise Server is part of Solution Manager. There is no need to perform a separate installation. For more information, see <a href="https://support.sap.com">https://support.sap.com</a>.</td>
</tr>
<tr>
<td>SAPOSCOL</td>
<td>The SAP Operating System Collector provides operating system data to the SMD and Introscope.</td>
</tr>
</tbody>
</table>

All of these components are available for download from http://support.sap.com/swdc.

9.4.2 SMD agent guidelines

The SMD Agent is a local agent (DIAGNOSTICS.AGENT) that collects and sends the information to the SMD server.

All of these components are available for download from http://support.sap.com/swdc.

The following are provided as guidelines for using SMD agents to monitor Data Services:

- The installation order of the monitored system and agent is not critical. You can install the SMD Agent before or after installing and deploying Data Services.
- If the servers are deployed on a distributed system, you should install an SMD Agent on every machine hosting a server.

Related Information

http://wiki.sdn.sap.com/wiki/display/TechOps/RCA_Home
9.4.3 Configure your system for SMD

There are a few settings and files to configure to get SMD working properly on your system.

- You must enable the feature in the Server Manager for each of the Job Servers for which you want to get performance metrics.
- If you have problems, you can edit the `ncs.conf` file. This file controls the information sent to the SMD Agent.

**Note**

Normally, you can keep the default settings. The file contains descriptions of the options. The file is located in the `<LINK_DIR>\bin` directory of your Data Services installation.

- Configure the following SMD Agent files to provide information to the Solution Manager server.
  - `SapAgentConfig.xml`
  - `IntroscopeSapAgent.profile`

  These files are located in your SMD Agent installation location.

9.4.4 Enabling performance instrumentation on Windows

You must enable the Job Server before you can monitor its performance. To enable the Job Server:

1. Open the Data Services Server Manager. (Start > Programs > SAP Data Services)
2. Click the Native Component Supportability NCS tab.
3. Select `Enable instrumentation in NCS (Native Component Supportability) library`.

In most circumstances, you can leave the default settings for the rest of the options.

Related Information

Native Component Supportability tab options [page 146]

9.4.4.1 Native Component Supportability tab options

Table that describes all of the options in the Native Component Supportability tab of the Server Manager.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Tracing level threshold** | Indicates the tracing level under which the instrumented code needs to go to produce a trace:  
   • 0: Use the value from ncs.conf configuration file  
   • 1-5: No tracing (NONE)  
   • 6-10: Tracing major points (MAJOR)  
   • 11-15: Tracing minor points (MINOR)  
   • 16-20: Tracing fine details (FINE)  
   • >20: Max details (FINEST)                                                                |
| **Execution interval**     | Indicates execution interval for CPU usage/process memory metrics to be sent to Wily Enterprise Manager in seconds. 0 = The default NCS scheduler will be used. |
| **Execution time offset**  | Indicates execution time offset with regard to the interval in seconds.  
   For example, if the interval is 3600 (every one hour) and the offset is 1800 (every half an hour), the information will be sent to SMD agent at 3:30, 4:30, 5:30, and so on. If the interval is smaller than the NCS library scheduler interval defined in parameter "datasending_interval", the offset parameter will be bypassed. |
| **Tracing level**          | This option is not currently used.                                                                                                           |
| **Application passport**   | This option is not currently used.                                                                                                           |

Related Information

Enabling performance instrumentation on Windows [page 146]

9.4.5 Enabling performance instrumentation on UNIX and Linux

If you are running Data Services on a UNIX or Linux platform, you will need to edit the DSConfig.txt file to enable instrumentation.

1. Navigate to <DS_COMMON_DIR>/conf.
2. Open the DSConfig.txt file.
3. Set the Wily_instrumentation parameter to True.

The other parameters (found in the Engine section) can be left with the default values.
Wily_instrumentation=TRUE
Wily_instrumentation_Level_Threshold=0
Wily_instrumentation_Interval=0
Wily_instrumentation_Offset=
Wily_instrumentation_TraceLevel=3487
Wily_instrumentation_App_Passport=

9.4.6 Heartbeat monitoring

Availability monitoring (heartbeat) lets you use the SAP Solution Manager to check whether a component such as a Job Server or Access Server is up and running. You can also get information about real-time services for Access Servers.

From CA Wily Introscope under the Status node, you can view each monitored Job Server or Access Server’s status. For heartbeat, a value of 1 indicates the server is running; 0 indicates it is not.

In addition, you can view an Access Server’s real-time service status. The status indicators are:

Table 55:

<table>
<thead>
<tr>
<th>Value</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>not running</td>
</tr>
<tr>
<td>1</td>
<td>starting</td>
</tr>
<tr>
<td>2</td>
<td>started</td>
</tr>
<tr>
<td>3</td>
<td>shutting down</td>
</tr>
<tr>
<td>4</td>
<td>warning</td>
</tr>
<tr>
<td>5</td>
<td>error</td>
</tr>
<tr>
<td>9</td>
<td>disabled</td>
</tr>
</tbody>
</table>

9.4.7 Alert monitoring

Alerts let you view critical errors in the SAP Solution Manager. From Data Services, Job Servers send alerts when a job fails.

From CA Wily Introscope under the Status node, you can view each monitored Job Server’s status. For alerts, a value of 1 indicates a job has failed in that Job Server’s repository.
10 Command line administration

10.1 Command lines overview

This section lists the command-line options that control the behavior of each Data Services component. Throughout this section, values provided in square brackets [ ] are optional.

**Note**
The following tables list the supported command-line options. Data Services components use a number of internal options that are not listed in these tables. These internal options should not be modified.

10.2 License Manager

License Manager can be used only in command-line mode. You can use it to manage your product activation keycodes—the alphanumeric codes that are referred to each time that you run certain software. By using License Manager, you can view, add, and remove product activation keycodes for SAP solution portfolio software (such as SAP Data Services) that require them.

**Note**
License Manager accesses keycodes on the local system only; you cannot access the keycodes from a remote system. When updating keycodes, make the changes on all SAP Data Services computers by launching License Manager on each computer, including Designer and Job Server computers.

**Note**
If you are running a Windows operating system, you will not be able to add or remove license keycodes unless you have Administrator privileges. For those with non-administrator privileges, only the -v and --view parameters are available for use.

**Syntax**

```
LicenseManager [-v | -a <keycode> | -r <keycode> [-l <location>]]
```
Table 56:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-v or --view</td>
<td>Displays the stored product activation keycodes. For example:</td>
</tr>
<tr>
<td></td>
<td>Keycode: 00000-0000000-0000000-0000</td>
</tr>
<tr>
<td></td>
<td>Trial Option: Yes</td>
</tr>
<tr>
<td></td>
<td>Expired: No</td>
</tr>
<tr>
<td></td>
<td>Days Remaining: 54</td>
</tr>
<tr>
<td>-a or --add &lt;keycode&gt;</td>
<td>Adds the specified license keycode, and displays the stored keycodes. Returns status messages for the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• An internal error occurred.</td>
</tr>
<tr>
<td></td>
<td>• Successfully added the keycode.</td>
</tr>
<tr>
<td></td>
<td>• Successfully added the keycode and replaced a trial version.</td>
</tr>
<tr>
<td></td>
<td>• Keycode not added because it is invalid.</td>
</tr>
<tr>
<td></td>
<td>• Keycode not added because it is a duplicate.</td>
</tr>
<tr>
<td>-r or --remove &lt;keycode&gt; [-l &lt;location&gt;]</td>
<td>Removes the specified product activation keycode, and displays the stored keycodes. If &lt;location&gt; is specified, the removal is restricted to that node. Returns status messages for the following conditions:</td>
</tr>
<tr>
<td></td>
<td>• An internal error occurred.</td>
</tr>
<tr>
<td></td>
<td>• Removed one keycode.</td>
</tr>
<tr>
<td></td>
<td>• Removed multiple keycodes.</td>
</tr>
<tr>
<td></td>
<td>• Keycode not removed because it is invalid.</td>
</tr>
<tr>
<td></td>
<td>• Keycode not removed because it was not found.</td>
</tr>
</tbody>
</table>

10.2.1 Configuring License Manager on Unix

Before you can use License Manager on UNIX platforms, you need to set the environment variable BOE_REGISTRYHOME. If you've already configured the SAP Data Services environment by running al_env.sh script, the BOE_REGISTRYHOME variable should already be set. If the variable has not been set, manually add it to your .profile, .login, or .cshrc file.

If you use Bourne shell, add product entries to your .profile or .login file.

```bash
BOE_REGISTRYHOME=$LINK_DIR/registry ; export BOE_REGISTRYHOME
```

If you use C shell (Berkeley), add product entries to your .cshrc file.

```bash
setenv BOE_REGISTRYHOME $LINK_DIR/registry
```

10.2.2 Starting License Manager

You can run License Manager after the SAP Data Services installation has completed.
On Windows

Choose Start Programs SAP Data Services 4.2 SAP License Manager Run as administrator.

A command line window opens displaying License Manager command line options.

On UNIX

Run LicenseManager from the command line without specifying any options:

$ cd $LINK_DIR/bin
$ ./LicenseManager

10.3 Connection Manager (Unix)

The Connection Manager (DSConnectionManager) is a graphical interface used to configure ODBC databases and ODBC drivers that you want to use for Data Services repositories, sources and targets after installation on Unix platforms. The Connection Manager includes a command-line mode that you can use if you do not want to use the graphical interface, or need to troubleshoot errors.

To use DSConnectionManager.sh from the command line, use the -c parameter which must be the first parameter.

If an error occurs when using the Connection Manager, use the -d option to show details in the log

For example:

$LINK_DIR/bin/DSConnectionManager.sh -c -d

10.4 Repository Manager (Windows)

Use RepoManBatch.exe to create or update repositories from the command line on Windows platforms.

By default, RepoManBatch.exe is installed to the <LINK_DIR>/bin directory.

Specify parameters using a command prompt.

C:\Program Files\SAP BusinessObjects\Data Services\bin>RepoManBatch.exe

Usage:

-<User> Repository login user
-P<Password> Repository login password
-s Use Server name based connection
-S<Server> Repository server name
-p<PortNo> Repository server port number
-N<DatabaseType> Repository database type
-Q<Database> Repository database
-V<Database_version> Repository database server version
-g Repository using Windows Authentication (Microsoft SQL Server only)
-t<Type> Repository type: local, central, profiler
-c Repository create
-u Repository upgrade
-v Repository version
-d Show details
-a Repository security

**Example**

RepoManBatch -Usa -P -NMicroSoft_SQL_Server -SServer -QJake -c -tcnentral -d

or

RepoManBatch -UJake -PJake -NOOracle -Sdbsvr -v

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-U</td>
<td>Repository login user. This parameter is required for all database types.</td>
</tr>
<tr>
<td>-P</td>
<td>Repository login password. This parameter is required for all database types.</td>
</tr>
<tr>
<td>-s</td>
<td>Specify this parameter to use a server name (also know as DSN-less or TNS-less) connection to the repository. If you specify this parameter, you must specify the -p and -V parameters.</td>
</tr>
<tr>
<td>Flag</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -S   | Repository server name:  
  - For DB2: Data source  
  - For MySQL: ODBC data source name  
  - For Oracle: TNSNAME defined in tnsnames.ora  
  - For SAP HANA: ODBC data source name  
  - For SAP Sybase SQL Anywhere: ODBC data source name  
  - For SAP ASE: Server  
  This parameter is required for all database types. |
| -p   | Repository database port number.  
  This parameter is required if you specified -s for a server name connection. |
| -N   | Repository database type:  
  - DB2  
  - HANA  
  - MySQL  
  - Oracle  
  - SQL_Anywhere  
  - Sybase  
  This parameter is required for all database types. |
| -Q   | Repository database name.  
  This parameter is required only for SAP ASE. |
| -V   | Repository database version.  
  This parameter is required if you specified -s for a server name connection. |
| -t   | Repository type:  
  - local  
  - central  
  - profiler |
| -c   | Operation mode: Creates repository. |
| -u   | Operation mode: Upgrades repository. |
| -v   | Operation mode: Gets repository version. |
| -d   | Operation mode: Shows details. |
### 10.5 Repository Manager (Unix)

You can use the executable called `repoman` to create or update repositories from the command line on Unix platforms. By default, `repoman` is installed to the `<LINK_DIR>/bin` directory.

Specify parameters using a command prompt.

```
$ ./repoman
```

**Usage:**

- `-U<User>` : Repository login user
- `-P<Password>` : Repository login password
- `-S<Server>` : Repository server name
- `-N<DatabaseType>` : Repository database type: SQL_Anywhere, Sybase, MySQL, HANA, DB2, Oracle
- `-Q<Database>` : Repository database
- `-s` : Connect Repository database by DSN-less (ODBC) or TNS-less for Oracle
- `-V<databaseVersion>` : Repository database version (only available with `-s`):
  - MYSQL 5.0, MYSQL 5.1 (default)
  - HANA 1.X (default)
  - DB2 UDB 9.X
  - ORACLE 11G, ORACLE 10G
  - SQL Anywhere 12.X
- `-p<port>` : Repository database port
- `-t<Type>` : Repository type: local, central, profiler
- `-b` : Check database connectivity
- `-c` : Repository create
- `-u` : Repository upgrade
- `-v` : Repository version
- `-d` : Show details
- `-a` : Repository security
- `-l` : Create log file
- `-z` : Create error file

**For example:**

```
./repoman -Usa -P -NDB2 -SServer -QJake -c -tcentral -d
```

or

```
./repoman -UJake -PJake -NOracle -Ssrvr -v
```

**Usage:**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Central repository security.</td>
</tr>
<tr>
<td>-o</td>
<td>Overwrite existing repository.</td>
</tr>
</tbody>
</table>
Table 58:

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
</table>
| -U   | Repository login user  
This parameter is required for all database types. |
| -P   | Repository login password  
This parameter is required for all database types. |
| -s   | Specify this parameter to use a server name (also known as DSN-less or TNS-less) connection to the repository. If you specify this parameter, you must specify the -p and -V parameters. |
| -S   | Repository server name:  
- For DB2: data source  
- For MySQL: ODBC data source name  
- For Oracle: TNSNAME defined in tnsnames.ora  
- For SAP HANA: ODBC data source name  
- For SAP Sybase SQL Anywhere: ODBC data source name  
- For SAP ASE: server  
This parameter is required for all database types. |
| -p   | Repository database port number  
This parameter is required if you specified -s for a server name connection. |
| -N   | Repository database type:  
- DB2  
- HANA  
- MySQL  
- Oracle  
- SQL Anywhere  
- Sybase  
This parameter is required for all database types. |
| -Q   | Repository database name  
This parameter is required only for SAP ASE. |
| -V   | Repository database version  
This parameter is required if you specified -s for a server name connection. |
| -t   | Repository type:  
- local  
- central  
- profiler  
This parameter is required if you specified -s for a server name connection. |
<p>| -c   | Operation mode: Creates repository |
| -u   | Operation mode: Upgrades repository |
| -v   | Operation mode: Gets repository version |
| -d   | Operation mode: Shows details |</p>
<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a</td>
<td>Central repository security</td>
</tr>
<tr>
<td>-o</td>
<td>Overwrite existing repository</td>
</tr>
</tbody>
</table>

10.6 Server Manager (Windows)

The Server Manager (`AWServerConfig.exe`) is used to create, edit, or delete Job Servers and Access Servers after installation on Windows platforms. In addition to the default graphical user interface, `AWServerConfig.exe` also supports command-line parameters for several tasks:

- Adding a Job Server
- Adding an Access Server
- Adding run-time resources
- Configuring SSL
- Enabling and setting NCS library
- Adding and editing SLD registration information for Data Services

**Note**

On Windows platforms, there is no command-line option to start or stop the Data Services service using `AWServerConfig.exe` because it is installed as a Windows service. The Data Services service can be started and stopped using the standard `net` command.

**Example**

**Start Data Services services**

```
net start "SAP Data Services"
```

**Example**

**Stop Data Services services**

```
net stop "SAP Data Services"
```

10.6.1 Adding an Access Server

To use `AWServerConfig.exe` to add an Access Server from the command line, use the `-n` parameter, along with additional Access Server-specific parameters. `-n` must be the first argument.
Access Server parameters

Table 60:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-R&lt;access_server_dir&gt;</td>
<td>Specifies the directory path for the Access Server. Replace &lt;access_server_dir&gt; with the Access Server directory path.</td>
</tr>
<tr>
<td>-A&lt;port&gt;</td>
<td>Specifies the port assigned to the Access Server. Replace &lt;port&gt; with the desired port number. The port number may have a value between 1024 and 49151, and must be unique and not in use.</td>
</tr>
<tr>
<td>-E</td>
<td>Indicates that the Access Server should be enabled. If not specified, the Access Server is created but not enabled.</td>
</tr>
<tr>
<td>-T&lt;param&gt;</td>
<td>Specifies a parameter for the Access Server. Replace &lt;param&gt; with the desired parameter.</td>
</tr>
</tbody>
</table>

Example

Create and enable an Access Server on port 4000

AWServerConfig.exe -n -RC:\DataServices\AccessServer -A4000 -E

10.6.2 Adding a Job Server

To use AWServerConfig.exe to add a Job Server from the command line, use the -n parameter, along with additional Job Server-specific parameters. -n must be the first parameter.

Job Server parameters

Table 61:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-J&lt;server_name&gt;</td>
<td>Specifies the name of the Job Server. Replace &lt;server_name&gt; with the desired name for the Job Server. The specified name may not contain @@ and must be unique.</td>
</tr>
<tr>
<td>-P&lt;port_number&gt;</td>
<td>Specifies the listening port for the Job Server. Replace &lt;port_number&gt; with the desired port number. The port number may have a value between 1024 and 49151, and must be unique and not in use.</td>
</tr>
<tr>
<td>~a</td>
<td>Indicates that the Job Server will manage an adapter. If not specified, the new Job Server will not manage adapters.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-B&lt;broker_port&gt;</td>
<td>Specifies the adapter manager port. Replace &lt;broker_port&gt; with the desired port number. The port number may have a value between 1024 and 49151, and must be unique and not in use.</td>
</tr>
<tr>
<td>-s</td>
<td>Indicates that SNMP is enabled for the Job Server. If not specified, SNMP is disabled.</td>
</tr>
<tr>
<td>-d</td>
<td>Indicates that this is the default repository for the Job Server.</td>
</tr>
<tr>
<td>-U&lt;username&gt;</td>
<td>Specifies the username used to connect to the repository. Replace &lt;username&gt; with the repository username.</td>
</tr>
<tr>
<td>-W&lt;password&gt;</td>
<td>Specifies the password used to connect to the repository. Replace &lt;password&gt; with the repository password.</td>
</tr>
<tr>
<td>-N&lt;db_type&gt;</td>
<td>Specifies the type of database used for the repository. Replace &lt;db_type&gt; with a valid value: * DB2 * Microsoft_SQL_Server * MySQL * Oracle * SQL_Anywhere * Sybase</td>
</tr>
<tr>
<td>-S&lt;server_name&gt;</td>
<td>Specifies the database service name or server name used to connect to the repository. Replace &lt;server_name&gt; with the appropriate information for the database type: * For Oracle, the database service name as specified in tnsnames.ora. * For DB2, the database instance name. * For Microsoft SQL Server, the database server name. * For Sybase, the database server name. * For MySQL, the database source name as specified in the system DSN. * For SAP Sybase SQL Anywhere, the database server name.</td>
</tr>
<tr>
<td>-Q&lt;database_name&gt;</td>
<td>Specifies the database name for the repository. Replace &lt;database_name&gt; with the name of the repository database.</td>
</tr>
</tbody>
</table>

**Note**

This parameter is required only for repositories on Sybase and Microsoft SQL Server.
Table 62: Run-time resource parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-C&lt;cache_dir&gt;</td>
<td>Specifies the directory for the pageable cache. Replace &lt;cache_dir&gt; with the desired directory.</td>
</tr>
<tr>
<td>-PF&lt;from_port&gt;</td>
<td>Specifies the starting port number. Replace &lt;from_port&gt; with the desired port number. The port number may have a value between 1025 and 32766, and must be unique and not in use.</td>
</tr>
<tr>
<td>-PT&lt;to_port&gt;</td>
<td>Specifies the ending port number. Replace &lt;to_port&gt; with the desired port number. The port number may have a value between 1026 and 32767, and must be unique and not in use. The ending port value must be greater than the starting port value.</td>
</tr>
</tbody>
</table>

Example

**Add a pageable cache resource on ports 2000-2550**

AWServerConfig.exe -n -C "%LINK_DIR%\log\Pcache" -PF2000 -PT2550
10.7 Server Manager (Unix)

The Server Manager (svrcfg) is used to create, edit, or delete Job Servers and Access Servers after installation on Unix platforms. In addition to the console-based interface, svrcfg also supports command-line parameters for several tasks:

- Adding a Job Server
- Adding an Access Server
- Adding run-time resources
- Starting Data Services services
- Stopping Data Services services

Common parameters

svrcfg supports one common parameter for all operations. Other available parameters depend on the operation.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -T<task>  | Specifies the configuration task to perform. Available values for <task> include:  
  - JS - Add a Job Server  
  - AS - Add an Access Server  
  - R - Add run-time resources  
  - START - Start services  
  - STOP - Stop services |

**Note**

When starting or stopping the Data Services services, svrcfg requires no additional parameters.

**Example**

Start Data Services services

```
svrcfg -TSTART
```

**Example**

Stop Data Services services

```
svrcfg -TSTOP
```
Output

When using svrcfg to perform tasks from the command line, output is directed to the console (or stdout). The last line of the output indicates whether the task execution succeeded or failed. Possible statuses include:

- Success
- Failure

10.7.1 Adding an Access Server

To use svrcfg to add an Access Server from the command line, use the -TAS parameter, along with additional Access Server-specific parameters.

Access Server parameters

Table 64:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-A&lt;path&gt;</td>
<td>Specifies the path for the access server. Replace &lt;path&gt; with the desired path.</td>
</tr>
<tr>
<td>-O&lt;port&gt;</td>
<td>Specifies the port assigned to the Access Server. Replace &lt;port&gt; with the desired port number. The port number may have a value between 1024 and 49151, and must be unique and not in use.</td>
</tr>
<tr>
<td>-R&lt;param&gt;</td>
<td>Specifies a parameter for the Access Server. Replace &lt;param&gt; with the desired parameter.</td>
</tr>
<tr>
<td>-E</td>
<td>Indicates that the Access Server should be enabled. If not specified, the Access Server is created but not enabled.</td>
</tr>
</tbody>
</table>

Example

Create and enable an Access Server on port 4000

svrcfg -TAS -A/home/bods/AStest -O4000 -E

10.7.2 Adding a Job Server

To use svrcfg to add a Job Server from the command line, use the -TJS parameter, along with additional Job Server-specific parameters.
# Job Server parameters

Table 65:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-J&lt;server_name&gt;</td>
<td>Specifies the name of the Job Server. Replace &lt;server_name&gt; with the desired name for the Job Server. The specified name may not contain @ and must be unique.</td>
</tr>
<tr>
<td>-p&lt;port_number&gt;</td>
<td>Specifies the listening port for the Job Server. Replace &lt;port_number&gt; with the desired port number. The port number may have a value between 1024 and 49151, and must be unique and not in use.</td>
</tr>
<tr>
<td>-a</td>
<td>Indicates that the Job Server will manage an adapter. If not specified, the new Job Server will not manage adapters.</td>
</tr>
<tr>
<td>-b&lt;broker_port&gt;</td>
<td>Specifies the adapter manager port. Replace &lt;broker_port&gt; with the desired port number. The port number may have a value between 1024 and 49151, and must be unique and not in use.</td>
</tr>
<tr>
<td>-e</td>
<td>Indicates that SNMP is enabled for the Job Server. If not specified, SNMP is disabled.</td>
</tr>
<tr>
<td>-D&lt;db_type&gt;</td>
<td>Specifies the type of database used for the repository. Replace &lt;db_type&gt; with a valid value:</td>
</tr>
<tr>
<td></td>
<td>● DB2</td>
</tr>
<tr>
<td></td>
<td>● HANA</td>
</tr>
<tr>
<td></td>
<td>● MySQL</td>
</tr>
<tr>
<td></td>
<td>● Oracle</td>
</tr>
<tr>
<td></td>
<td>● SQL_Anywhere</td>
</tr>
<tr>
<td></td>
<td>● SYBASE</td>
</tr>
<tr>
<td>-C&lt;connect_string&gt;</td>
<td>Specifies the connection string to use to connect to the repository. Replace &lt;connect_string&gt; with appropriate information for the database type:</td>
</tr>
<tr>
<td></td>
<td>● For DB2, the database instance name.</td>
</tr>
<tr>
<td></td>
<td>● For MySQL, the data source name as specified in the odbc.ini file referenced by $ODBCINI.</td>
</tr>
<tr>
<td></td>
<td>● For Oracle, the service name as specified in tnsnames.ora.</td>
</tr>
<tr>
<td></td>
<td>● For SAP HANA, the data source name as specified in the odbc.ini file referenced by $ODBCINI.</td>
</tr>
<tr>
<td></td>
<td>● For SAP Sybase SQL Anywhere, the database server name.</td>
</tr>
<tr>
<td></td>
<td>● For Sybase, the database server name.</td>
</tr>
</tbody>
</table>
### Parameter Description

- **-d <database>**
  Specifies the database name for the repository.
  Replace `<database>` with the name of the repository database.

  **Note**
  This parameter is required only for repositories on Sybase.

- **-U <username>**
  Specifies the username used to connect to the repository.
  Replace `<username>` with the repository username.

- **-P <password>**
  Specifies the password used to connect to the repository.
  Replace `<password>` with the repository password.

---

**Example**

Add a Job Server with an Oracle repository

```
svrcfg -TJS -JJobServer_1 -p3500 -DOracle -CORCL -Uuser -Ppassword
```

---

### 10.7.3 Adding run-time resources

To use `svrcfg` to add run-time resources from the command line, use the `-TR` parameter, along with additional run-time resource-specific parameters.

---

#### Run-time resource parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-i &lt;cache_dir&gt;</code></td>
<td>Specifies the directory for the pageable cache. Replace <code>&lt;cache_dir&gt;</code> with the desired directory.</td>
</tr>
<tr>
<td><code>-t &lt;port&gt;</code></td>
<td>Specifies the starting port number. Replace <code>&lt;port&gt;</code> with the desired port number. The port number may have a value between 1025 and 32766, and must be unique and not in use.</td>
</tr>
<tr>
<td><code>-n &lt;port&gt;</code></td>
<td>Specifies the ending port number. Replace <code>&lt;port&gt;</code> with the desired port number. The port number may have a value between 1026 and 32767, and must be unique and not in use. The ending port value must be greater than the starting port value.</td>
</tr>
</tbody>
</table>
### 10.8 Password encryption

You can use `al_encrypt` to encrypt a password by using either an encryption key or a passphrase.

Additionally, you can use `al_encrypt` to return the base64 encoding of any text. This may be useful if you need to modify a command line that contains global variable or substitution variable data, which must be encoded in base64 form.

By default, `al_encrypt` is installed to the `<LINK_DIR>/bin` directory.

#### Syntax

```
al_encrypt -e <plain_password> [-k <key string> | -p <passphrase>]
```

```
al_encrypt "<text to encode>"
```

#### Table 67:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-e &lt;password&gt;</code></td>
<td>Specifies the plain-text password to encrypt.</td>
</tr>
<tr>
<td><code>-k &lt;key string&gt;</code></td>
<td>Specifies the encryption key to use to encrypt the password.</td>
</tr>
<tr>
<td><code>-p &lt;passphrase&gt;</code></td>
<td>Specifies the passphrase to use to encrypt the password.</td>
</tr>
<tr>
<td><code>&lt;text to encode&gt;</code></td>
<td>When you run <code>al_encrypt</code> with no parameters, it returns the base64 encoding of any following optionally-quoted text.</td>
</tr>
</tbody>
</table>

#### Example

**Encrypt a password using a passphrase**

```
al_encrypt -e mypassword -p thepassphrase > +01000000012030300803E83F55088B0C987CD715006C02938825530E8691DFD9DB4198AFFC5C194CD8CE6D338FDE470E2
```

**Encode text using base64 encoding**

```
 al_encrypt "encode this as base64" > ZW5jb2RlIHRoaXMgYXMgYmFzZTY0
```
10.9 al_engine

al_engine is a core Data Services process. It is responsible for executing jobs, importing and exporting repository objects, and so on.

Common options

al_engine supports options that are common to many different operations.

Table 68:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-U &lt;Username&gt;</td>
<td>Specifies the username used to log into the repository.</td>
</tr>
<tr>
<td>-P &lt;Password&gt;</td>
<td>Specifies the password used to log into the repository.</td>
</tr>
<tr>
<td>-S &lt;ServerName&gt;</td>
<td>Specifies the repository server name. For a DSN connection to a DB2, SAP HANA SAP Sybase, or SAP Sybase SQL Anywhere repository, use ODBC connection name.</td>
</tr>
<tr>
<td>-N &lt;DatabaseType&gt;</td>
<td>Specifies the repository database type. Acceptable values include:</td>
</tr>
<tr>
<td></td>
<td>● Oracle</td>
</tr>
<tr>
<td></td>
<td>● Microsoft_SQL_Server</td>
</tr>
<tr>
<td></td>
<td>● DB2</td>
</tr>
<tr>
<td></td>
<td>● MySQL</td>
</tr>
<tr>
<td></td>
<td>● Sybase</td>
</tr>
<tr>
<td></td>
<td>● HANA</td>
</tr>
<tr>
<td></td>
<td>● SQL_Anywhere</td>
</tr>
<tr>
<td>-Q &lt;DatabaseName_or_SID&gt;</td>
<td>Specifies the repository database name or SID (for Oracle). For a DSN-less connection to a DB2, SAP Sybase, or SAP Sybase SQL Anywhere repository, use database name.</td>
</tr>
<tr>
<td>-Kserver</td>
<td>Specify this parameter to use a server name (also known as DSN-less or TNS-less) connection to the repository. If you specify this parameter, you must specify the -Kport and -Kversion parameters.</td>
</tr>
<tr>
<td>-Kport &lt;PortNumber&gt;</td>
<td>Repository port number for server name connection. This parameter is required if you specified -Kserver for a server name connection.</td>
</tr>
<tr>
<td>-Kversion &lt;VersionNumber&gt;</td>
<td>Repository database server version for server name connection. This parameter is required if you specified -Kserver for a server name connection. For example, -Kversion&quot;MySQL 5.1&quot;</td>
</tr>
<tr>
<td>-g</td>
<td>Specifies Windows Authentication as the repository connection type. This parameter is valid only for repositories on Microsoft SQL Server.</td>
</tr>
<tr>
<td>-v</td>
<td>Returns the version number of the Data Services engine.</td>
</tr>
</tbody>
</table>
### 10.9.1 Export and import options

`al_engine` supports options that are used only for export and import operations. `al_engine` can import and export repository information in two formats: XML and ATL, the software’s internal scripting language.

#### Table 69: Export and import options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-X</code></td>
<td>Exports the entire repository in ATL format to <code>repo_export.atl</code>.</td>
</tr>
<tr>
<td><code>-XKserver</code></td>
<td>Exports repository server name connection (for MySQL, SAP HANA, ORACLE, and DB2).</td>
</tr>
<tr>
<td><code>-XKport&lt;PortNumber&gt;</code></td>
<td>Exports repository port number for server name connection. This parameter must be used with <code>-XKserver</code> parameter.</td>
</tr>
<tr>
<td><code>-XKversion&lt;VersionNumber&gt;</code></td>
<td>Exports repository database server version for server name connection. This parameter must be used with the <code>-XKserver</code> parameter. For example, <code>-XKversion&quot;MySQL 5.1&quot;</code></td>
</tr>
<tr>
<td><code>-Xp&lt;ObjectType&gt;@&lt;FileName&gt;</code></td>
<td>Exports all repository objects of the specified type to the specified file in ATL format.</td>
</tr>
<tr>
<td><code>-Xp&lt;ObjectType&gt;@&lt;FileName&gt;@&lt;ObjectName&gt;</code></td>
<td>Exports the specified repository object to the specified file in ATL format.</td>
</tr>
<tr>
<td><code>-Xp&lt;ObjectType&gt;@&lt;FileName&gt;@&lt;ObjectName&gt;@DE</code></td>
<td>Exports the specified repository object and its dependents to the specified file in ATL format, including datastore information.</td>
</tr>
<tr>
<td><code>-Xp&lt;ObjectType&gt;@&lt;FileName&gt;@&lt;ObjectName&gt;@D</code></td>
<td>Exports the specified repository object and its dependents to the specified file in ATL format, excluding datastore information.</td>
</tr>
<tr>
<td><code>-XX[L]</code></td>
<td>Exports the entire repository in XML format to <code>export.xml</code>.</td>
</tr>
<tr>
<td><code>-XX[L]@&lt;ObjectType&gt;@&lt;FileName&gt;</code></td>
<td>Exports all repository objects of the specified type to the specified file in XML format.</td>
</tr>
<tr>
<td><code>-XX[L]@&lt;ObjectType&gt;@&lt;FileName&gt;@&lt;ObjectName&gt;</code></td>
<td>Exports the specified repository object to the specified file in XML format.</td>
</tr>
<tr>
<td><code>-XX[L]@&lt;ObjectType&gt;@&lt;FileName&gt;@&lt;ObjectName&gt;@DE</code></td>
<td>Exports the specified repository object and its dependents to the specified file in XML format, including datastore information.</td>
</tr>
<tr>
<td><code>-XX[L]@&lt;ObjectType&gt;@&lt;FileName&gt;@&lt;ObjectName&gt;@D</code></td>
<td>Exports the specified repository object and its dependents to the specified file in XML format, excluding datastore information.</td>
</tr>
<tr>
<td><code>-f&lt;filename.atl&gt;</code></td>
<td>Imports information from <code>&lt;filename.atl&gt;</code> into the repository.</td>
</tr>
<tr>
<td><code>-XI&lt;filename.xml&gt;</code></td>
<td>Imports information from <code>&lt;filename.xml&gt;</code> into the repository.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--passphrase &lt;passphrase&gt;</code></td>
<td>Specifies a plain-text passphrase to use to encrypt any passwords when exporting objects or decrypt any passwords when importing objects.</td>
</tr>
<tr>
<td><code>--epassphrase &lt;passphrase&gt;</code></td>
<td>Specifies a base64-encoded passphrase to use to encrypt any passwords when exporting objects or decrypt any passwords when importing objects. This parameter can be used to use a passphrase that contains special characters.</td>
</tr>
</tbody>
</table>

**Note**
You must transcode the passphrase to the UTF8 character set before encoding it into base64.

### Note

For all `--xx` parameters, the optional addition `[L]` specifies a lean XML format for export. The lean XML format excludes all non-executable elements from the exported XML to improve readability. For example, the exact arrangement of transforms within a data flow in the Designer workspace area would not be maintained. When imported back into the software, the transforms would be arranged automatically.

**Note**
When you export objects, you must specify a passphrase with either the `--passphrase` parameter or the `--epassphrase` parameter. When you import objects, the passphrase is optional. However, if you do not specify a passphrase, or the specified passphrase is incorrect, any encrypted passwords in the imported objects will be removed.

### Available object type codes

Table 70:

<table>
<thead>
<tr>
<th>Code</th>
<th>Object type</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Projects</td>
</tr>
<tr>
<td>J</td>
<td>Jobs</td>
</tr>
<tr>
<td>W</td>
<td>work flows</td>
</tr>
<tr>
<td>D</td>
<td>data flows</td>
</tr>
<tr>
<td>T</td>
<td>Idocs</td>
</tr>
<tr>
<td>F</td>
<td>User-defined file formats</td>
</tr>
<tr>
<td>X</td>
<td>XML and DTD message formats</td>
</tr>
<tr>
<td>S</td>
<td>Datastores</td>
</tr>
<tr>
<td>C</td>
<td>Custom functions</td>
</tr>
<tr>
<td>B</td>
<td>COBOL Copybooks</td>
</tr>
<tr>
<td>Code</td>
<td>Object type</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>E</td>
<td>Excel workbooks</td>
</tr>
<tr>
<td>p</td>
<td>System profiles</td>
</tr>
<tr>
<td>v</td>
<td>Substitution parameter configurations</td>
</tr>
<tr>
<td>K</td>
<td>SDK-type transform configurations</td>
</tr>
</tbody>
</table>

### Example

**Export all data flows in lean XML format**

```
al_engine -Uuser -Ppassword -Slocalhost -NMySQL -QTheRepository -XXL@D@exported_dataflows.xml -passphraseMypassphrase
```
Important Disclaimers and Legal Information

Coding Samples
Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility
The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language
As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with “you”, or a gender-neutral noun (such as “sales person” or “working days”) is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks
The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).