IBM InfoSphere Information Server
Version 9 Release 1

Administration Guide

IBM
Before using this information and the product that it supports, read the information in "Notices and trademarks" on page 345.
## Contents

### Chapter 1. Administration overview . . . 1
- IBM InfoSphere DataStage administration . . . 4
- IBM WebSphere Application Server administration . 5

### Chapter 2. Opening the consoles . . . . 7
- Opening the IBM InfoSphere Information Server console . . . . 7
- Opening the IBM InfoSphere Information Server web console . . . . 8
  - Determining the URL for the IBM InfoSphere Information Server Web console . . . 8
  - Configuring your Web browser to work with the IBM InfoSphere Information Server Web console . . . 9
  - Navigating to the IBM InfoSphere Information Server Web console . . . . 11
- Logging in to the IBM WebSphere Application Server administrative console . . . . 11

### Chapter 3. IBM InfoSphere Information Server console overview . . . . 13
- Main areas of the console . . . . 13
  - My Home workspace . . . . 13
  - Workspace Navigator . . . . 15
  - Project menu . . . . 16
  - Palettes . . . . 17
  - Project dashboard . . . . 19
  - Status bar . . . . 19
  - Shortcuts . . . . 20
  - Notes . . . . 20
- Basic task flow in the workspaces . . . . 20
  - Select a task menu from the Workspace Navigator . . . . 21
  - Select the task that you want to perform from the task menu . . . . 21
  - Select objects and a task in the workspace . . . . 22
  - Work in a task pane . . . . 23
- Reporting, scheduling, and logging in the console . . . . 24
  - Reporting . . . . 24
  - Scheduling . . . . 24
  - Logging . . . . 25
- Online help . . . . 25

### Chapter 4. Working with projects in the IBM InfoSphere Information Server console . . . . . 27
- Setting up a project in the IBM InfoSphere Information Server console . . . . 27
  - Creating a project . . . . 27
  - Modifying project properties . . . . 27
  - Customizing the project dashboard . . . . 28
- Opening an existing project in the IBM InfoSphere Information Server console . . . . 28

### Chapter 5. Customizing the consoles . . . . . 29
- Customizing the IBM InfoSphere Information Server console . . . . . 29
  - Customizing the My Home workspace . . . . 29
  - Modifying user preferences . . . . 29
  - Creating shortcuts . . . . 29
  - Working with palettes . . . . 30
  - Creating notes . . . . 31
  - Refreshing an object list . . . . 31
  - Changing your password . . . . 31
- Customizing the IBM InfoSphere Information Server Web console . . . . . 32
  - Customizing the Home tab . . . . 32
  - Changing your password . . . . 32

### Chapter 6. Managing security . . . . . 33
- Security setup . . . . 33
  - User registry configuration . . . . 34
  - User and group creation . . . . 54
  - Assigning user roles . . . . 64
  - Engine security configuration . . . . 77
- Configuring WebSphere Application Server for non-root administration (Linux, UNIX) . . . . 87
- Starting IBM InfoSphere Information Server node agents as a non-root user . . . . . 95
- Audit logging configuration . . . . 97
- Administrator account password changing . . . . 110
  - Changing an IBM InfoSphere Information Server administrator password . . . . 110
  - IBM WebSphere Application Server administrator password changing . . . . 112
  - Metadata repository database owner password changing . . . . . 115
  - Changing the analysis database owner account credentials . . . . . 117
  - Changing IBM DB2 passwords . . . . 118
- Administration commands and tools . . . . 118
  - AppServerAdmin command . . . . 119
  - DirectoryAdmin tool . . . . 122
  - DirectoryCommand tool . . . . 133
  - Encrypt command . . . . 143

### Chapter 7. Activating entitled IBM InfoSphere DataStage editions and feature packs . . . . . 149
- Viewing a list of activated IBM InfoSphere DataStage editions and feature packs . . . . 150
- Activating and deactivating IBM InfoSphere DataStage editions and feature packs . . . . 151
- LicensingServiceAdmin command reference . . . . 153

### Chapter 8. Managing active sessions . . . . 157
- Viewing all active sessions . . . . 157
- Setting session limits . . . . 157

© Copyright IBM Corp. 2007, 2013
<table>
<thead>
<tr>
<th>Chapter 9. Managing repositories</th>
<th>161</th>
</tr>
</thead>
<tbody>
<tr>
<td>RepositoryAdmin tool reference</td>
<td>161</td>
</tr>
<tr>
<td>List and display options</td>
<td>163</td>
</tr>
<tr>
<td>The option to save SQL scripts</td>
<td>167</td>
</tr>
<tr>
<td>Registration options</td>
<td>167</td>
</tr>
<tr>
<td>Update options</td>
<td>169</td>
</tr>
<tr>
<td>Unregistration options</td>
<td>171</td>
</tr>
<tr>
<td>The option to test a repository connection</td>
<td>171</td>
</tr>
<tr>
<td>Example: Changing connection properties</td>
<td>171</td>
</tr>
<tr>
<td>Example: Manually registering a repository</td>
<td>172</td>
</tr>
<tr>
<td>Example: Relocating a repository</td>
<td>174</td>
</tr>
<tr>
<td>Example: Upgrading the schema of an existing repository</td>
<td>176</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 10. Managing clusters and high availability configurations</th>
<th>179</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active-passive configuration administration</td>
<td>179</td>
</tr>
<tr>
<td>Administering an active-passive configuration based on Tivoli System Automation for Multiplatforms</td>
<td>179</td>
</tr>
<tr>
<td>WebSphere Application Server cluster administration</td>
<td>179</td>
</tr>
<tr>
<td>WebSphere Application Server cluster administration tools</td>
<td>179</td>
</tr>
<tr>
<td>Propagating the plugin-cfg.xml file to the front-end Web server</td>
<td>181</td>
</tr>
<tr>
<td>Adding a new cluster member</td>
<td>183</td>
</tr>
<tr>
<td>Adding a new managed node</td>
<td>183</td>
</tr>
<tr>
<td>Synchronizing nodes after changing the master repository configuration</td>
<td>185</td>
</tr>
<tr>
<td>Restarting application server processes</td>
<td>186</td>
</tr>
<tr>
<td>Setting up HTTP session database persistence</td>
<td>188</td>
</tr>
<tr>
<td>IBM DB2 high availability configuration administration</td>
<td>188</td>
</tr>
<tr>
<td>Failover in an IBM DB2 HADR configuration</td>
<td>188</td>
</tr>
<tr>
<td>Recovering from a failover in a DB2 clustered configuration</td>
<td>190</td>
</tr>
<tr>
<td>Engine tier failover recovery</td>
<td>190</td>
</tr>
<tr>
<td>Recovering from an engine tier failover</td>
<td>191</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 11. Managing logs</th>
<th>195</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging</td>
<td>195</td>
</tr>
<tr>
<td>Logging components</td>
<td>195</td>
</tr>
<tr>
<td>Logging configurations</td>
<td>195</td>
</tr>
<tr>
<td>Severity levels</td>
<td>196</td>
</tr>
<tr>
<td>Views of logged events</td>
<td>196</td>
</tr>
<tr>
<td>Shared and private views</td>
<td>196</td>
</tr>
<tr>
<td>Managing logging views in the console</td>
<td>197</td>
</tr>
<tr>
<td>Creating a view of logged events in the console</td>
<td>197</td>
</tr>
<tr>
<td>Viewing logged events</td>
<td>197</td>
</tr>
<tr>
<td>Editing a log view</td>
<td>198</td>
</tr>
<tr>
<td>Copying a log view</td>
<td>198</td>
</tr>
<tr>
<td>Purging logged messages</td>
<td>198</td>
</tr>
<tr>
<td>Managing logging views in the IBM InfoSphere Information Server Web console</td>
<td>199</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 12. Managing schedules</th>
<th>205</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria for schedule views</td>
<td>205</td>
</tr>
<tr>
<td>Shared and private views</td>
<td>206</td>
</tr>
<tr>
<td>Creating a schedule view</td>
<td>206</td>
</tr>
<tr>
<td>Creating a schedule view from a copy</td>
<td>206</td>
</tr>
<tr>
<td>Viewing the schedules that are captured by a schedule view</td>
<td>207</td>
</tr>
<tr>
<td>Pausing all the schedules in a view</td>
<td>207</td>
</tr>
<tr>
<td>Resuming all the schedules in a view</td>
<td>207</td>
</tr>
<tr>
<td>Purging the history for all the schedules in a view</td>
<td>208</td>
</tr>
<tr>
<td>Working with the scheduled tasks in a view</td>
<td>208</td>
</tr>
<tr>
<td>Stopping a scheduled task</td>
<td>208</td>
</tr>
<tr>
<td>Purging the history of a scheduled task</td>
<td>208</td>
</tr>
<tr>
<td>Viewing a list of completed schedules</td>
<td>209</td>
</tr>
<tr>
<td>Viewing a list of running schedules</td>
<td>209</td>
</tr>
<tr>
<td>Viewing a list of upcoming scheduled tasks</td>
<td>209</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 13. Backing up and restoring IBM InfoSphere Information Server</th>
<th>211</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verifying system and disk space requirements</td>
<td>211</td>
</tr>
<tr>
<td>Credential information</td>
<td>212</td>
</tr>
<tr>
<td>Backing up IBM InfoSphere Information Server components</td>
<td>213</td>
</tr>
<tr>
<td>Restoring IBM InfoSphere Information Server components</td>
<td>216</td>
</tr>
<tr>
<td>Back up and restore scenarios</td>
<td>218</td>
</tr>
<tr>
<td>Back up and restore scenarios for the metadata repository</td>
<td>218</td>
</tr>
<tr>
<td>Back up and restore scenarios for the engine tier and InfoSphere DataStage</td>
<td>220</td>
</tr>
<tr>
<td>Back up and restore scenarios for the InfoSphere Information Analyzer analysis database</td>
<td>220</td>
</tr>
<tr>
<td>Back up and restore scenarios for the user registry</td>
<td>221</td>
</tr>
<tr>
<td>InfoSphere DataStage project folder options</td>
<td>221</td>
</tr>
<tr>
<td>Additional files to back up</td>
<td>222</td>
</tr>
<tr>
<td>Back up and restore commands for the recovery tool</td>
<td>223</td>
</tr>
<tr>
<td>Response command</td>
<td>223</td>
</tr>
<tr>
<td>Restart command</td>
<td>224</td>
</tr>
<tr>
<td>Version command</td>
<td>225</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 14. Administering IBM InfoSphere Information Server and IBM WebSphere Application Server services</th>
<th>227</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance mode</td>
<td>228</td>
</tr>
</tbody>
</table>
Shutting down services (Windows) .... 230
    Stopping IBM WebSphere Application Server
    (Windows) ............................................. 231
Shutting down services (Linux, UNIX) .... 232
    Stopping IBM WebSphere Application Server
    (Linux, UNIX) ........................................ 233
Starting services (Windows) ........ 235
    Starting IBM WebSphere Application Server
    (Windows) ............................................ 235
Starting services (Linux, UNIX) .... 237
    Starting IBM WebSphere Application Server
    (Linux, UNIX) ........................................ 238
IBM WebSphere Application Server process status checking .... 241
    Checking the status of IBM WebSphere
    Application Server (stand-alone installation) .... 241
    Checking the status of IBM WebSphere
    Application Server startup (stand-alone
    installation) ........................................... 242
    Checking the status of IBM WebSphere
    Application Server startup (clustered
    installation) ............................................ 243
    Checking the status of IBM WebSphere
    Application Server cluster members ........ 244
    Checking the status of IBM WebSphere
    Application Server node agents ........ 244
    Checking the status of the IBM WebSphere
    Application Server Deployment Manager .... 245
IBM WebSphere Application Server system log files ...... 245

Chapter 15. Managing assets by using
the command line ................................ 247
Using the istool command line .... 247
    Location of the istool command line .... 247
    Commands and common parameters for istool .... 248
    Command modes for istool ...................... 251
Asset interchange ................................ 252
    Common asset-interchange scenarios .......... 255
InfoSphere Business Glossary assets .......... 256
    Export command for business glossary assets .... 256
    Import command for business glossary assets .... 258
    Generating business glossary content from other
    sources .................................................. 260
InfoSphere FastTrack assets ........ 272
    Asset IDs .............................................. 273
    Export command for InfoSphere FastTrack
    assets ................................................. 274
    Import command for InfoSphere FastTrack
    assets ................................................ 275
InfoSphere Information Analyzer assets .... 278
    Export command for InfoSphere Information
    Analyzer assets ........................................ 278
    Import command for InfoSphere Information
    Analyzer assets ........................................ 280
InfoSphere DataStage and QualityStage assets ...... 281
    Build package command ......................... 282
    Deploy package command ....................... 283
    Send package command ............................ 285
    Export command for InfoSphere DataStage and
    QualityStage assets .................................. 286
    Import command for InfoSphere DataStage
    and QualityStage assets ............................ 292
    Delete command for InfoSphere DataStage
    assets .................................................. 294
InfoSphere Streams assets .......... 296
    Export command for InfoSphere Streams assets .... 296
    Import command for InfoSphere Streams assets .... 297
Common metadata assets ........ 298
    Common metadata asset types and identity
    strings for the command line .................... 299
    Importing and exporting common metadata
    assets by using the command line ............... 307
    Querying and deleting assets by using the
    command line ........................................... 318
    Delete command for disconnected assets ....... 324
Reporting assets ................ 325
    Export command for reporting assets ......... 325
    Import command for reporting assets .......... 328
Security assets ................ 330
    Export command for security assets .......... 330
    Import command for security assets .......... 333

Appendix A. Product accessibility ........ 337
Appendix B. Reading command-line
syntax .................................................. 339
Appendix C. Contacting IBM ........ 341
Appendix D. Accessing and providing
feedback on the product
documentation ........................................ 343
Notices and trademarks .......... 345
Index ................................................. 349
Chapter 1. Administration overview

With IBM® InfoSphere® Information Server, you can administer security, entitlements, clusters and high availability configurations, logs, schedules, and services, and back up data. Both the IBM InfoSphere Information Server console and the IBM InfoSphere Information Server Web console provide administration capabilities.

Security administration

As part of InfoSphere Information Server administration, you set up and manage suite security. Security administration includes the following tasks:

- Configuring and administering the user registry
  The user registry holds user account information, such as user names and passwords, that can be accessed during authentication. You choose a user registry for the suite to use. You can choose the internal InfoSphere Information Server user registry, or an external local operating system or lightweight directory access protocol (LDAP) user registry. Depending on the registry you choose and the topology of your installation, you might also have to map credentials from one user registry to another.

- Controlling access
  You create user accounts and groups. You assign roles to users and groups to specify which features users can use and which projects a user can access. User roles can be defined at several levels that build on one another.

- Auditing security-related events
  Security-related events include all activities that set or modify security-related settings and all user authentications and application access attempts. You configure which events to log and how much information to include. You monitor and analyze the log information to help prevent unauthorized access to sensitive data.

- Administering account passwords
  You periodically change administrator account passwords to comply with your security policies.

- Managing active user sessions
  You view current active sessions, and manage session limits. If necessary, you can force one user or all users to disconnect.

Entitled IBM InfoSphere DataStage® edition and feature pack administration

As part of InfoSphere Information Server administrator, you control activation of InfoSphere DataStage editions and feature packs to comply with your Proof of Entitlement from IBM. Administration includes the following tasks:

- Initial edition and feature pack activation
  When you install InfoSphere DataStage, the InfoSphere Information Server installation program prompts you to select the InfoSphere DataStage editions and feature packs to install and activate. Select the items for which you have a valid Proof of Entitlement from IBM. The installation program activates the features that are associated with the items that you select. Any other editions or feature packs are deactivated and cannot be used.
Maintaining the list of activated items
If you later acquire entitlements for an additional InfoSphere DataStage edition or feature pack, you must activate the item within InfoSphere Information Server. If you no longer have entitlement for an item, you must deactivate it. When you deactivate the edition or feature pack, the features within the item are no longer available for use.

Clusters and high availability configuration and administration
If a portion of your installation is set up in a clustered or high availability configuration, you administer the cluster. Administration includes the following tasks:

- Administering an active-passive configuration administration
  If one or more software tiers in your installation is set up in an active-passive configuration, you monitor and manage the server pair. If a hardware or network error causes a failover to the passive server, you recover projects and restart any interrupted jobs. You can also force a failover to free the active server for maintenance or upgrade tasks.

- Administering an application server cluster
  If the InfoSphere Information Server services tier is implemented in an IBM WebSphere® Application Server cluster, you administer and maintain the cluster. Tasks include adding cluster members, adding managed nodes, synchronizing information between nodes, and restarting processes.

- Administering an IBM DB2® high availability configuration
  If the metadata repository tier is implemented in a DB2 cluster or high availability disaster recovery (HADR) configuration, you monitor the cluster. If a failover occurs, you recover from a failover and restore service.

Log administration
You can manage logs across all of the InfoSphere Information Server product modules. Logs are stored in the metadata repository. Log administration includes the following tasks:

- Configuring logging
  You specify which logging categories and severity levels of logging events are stored in the metadata repository.

- Querying logs
  You create log views in the IBM InfoSphere Information Server console and IBM InfoSphere Information Server Web console. You use the views to retrieve and query the logged events that are stored in the metadata repository.

Scheduling administration
Many of the product modules use scheduling capabilities. For example, a report run and an analysis job in IBM InfoSphere Information Analyzer are scheduled tasks. Scheduling administration includes the following tasks:

- Creating, updating, and managing schedules
  Schedule management is done within the product module. For example, you create a schedule for a column analysis job to run weekly in an InfoSphere Information Analyzer project in the console.

- Viewing schedules
You can obtain a global view of all the scheduled activities for all product modules. With this data, you can ensure that enough resources are available to process the schedules. You can monitor who schedules tasks and how often.

- Querying schedules
  You can query all the schedules that are defined across all product modules. You can check their status, history, and forecast. You can also do maintenance tasks such as purging the scheduled execution history. You can stop or start existing schedules to prevent system overload.

### Backup administration

To prevent the loss of data and to prepare for disaster recovery, you administer regular backups. Backup administration includes the following tasks:

- Backing up InfoSphere Information Server components
  You schedule and perform regular backups of all databases, profiles, libraries, and other data.

- Restoring components
  To recover your data in the event of a hardware failure or other disaster, you can restore the data that you have backed up.

### Service administration

You administer InfoSphere Information Server services and WebSphere Application Server services. Administration includes the following tasks:

- Placing InfoSphere Information Server in and out of maintenance mode
  You can place InfoSphere Information Server in maintenance mode to prevent non-administrator users from logging in while you run maintenance tasks.

- Stopping and restarting services
  Many maintenance and administration tasks require that you stop and restart various InfoSphere Information Server services or WebSphere Application Server services.

- Checking the status of services
  You can determine the status of services for troubleshooting or other maintenance tasks.

### Asset administration

Assets include projects, templates, configuration specifications, parameter sets, and all other information that is produced within the InfoSphere Information Server product modules. The assets are stored in the metadata repository. Administration includes the following tasks:

- Importing and exporting assets
  To move assets from one InfoSphere Information Server installation to another, you export the assets from one installation and import them into another. For example, if you have a development system, a test system, and a production system, you move assets between the systems.

- Querying and deleting assets
  You can query certain assets and delete them as necessary.
Administration tools

To administer InfoSphere Information Server, you use the following software tools:

- IBM InfoSphere Information Server console
  The IBM InfoSphere Information Server console ("the console") is a rich client-based interface for activities such as profiling data and developing service-oriented applications. In the console, you can complete administration tasks, reporting tasks, and the tasks that are associated with IBM InfoSphere Information Analyzer and IBM InfoSphere Information Services Director.

- IBM InfoSphere Information Server Web console
  The IBM InfoSphere Information Server Web console ("the Web console") is a browser-based interface for administrative activities such as managing security and creating views of scheduled tasks. In the Web console, you can perform administration tasks, reporting tasks, and the tasks that are associated with IBM InfoSphere Business Glossary and the Information Services catalog.

For certain tasks, you also use the WebSphere Application Server administrative console.

To administer assets, you use the istool command line.

IBM InfoSphere DataStage administration

For detailed IBM InfoSphere DataStage administration information, refer to InfoSphere DataStage administration guides.

Table 1. InfoSphere DataStage administration guides

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Client Guide</td>
<td>Describes the IBM InfoSphere DataStage and QualityStage® Administrator client and provides instructions about performing setup, routine maintenance operations, and administration on the IBM InfoSphere Information Server engine.</td>
</tr>
<tr>
<td>Designer Client Guide</td>
<td>Describes the IBM InfoSphere DataStage and QualityStage Designer client and gives a general description of how to create, design, and develop an InfoSphere DataStage and QualityStage application.</td>
</tr>
<tr>
<td>Director Client Guide</td>
<td>Describes the IBM InfoSphere DataStage and QualityStage Director client and explains how to validate, schedule, run, and monitor parallel jobs and server jobs.</td>
</tr>
<tr>
<td>Globalization Guide</td>
<td>Contains information about using the national language support (NLS) features that are available in InfoSphere DataStage and QualityStage when NLS is installed.</td>
</tr>
</tbody>
</table>

By default, the documentation is installed on your system:

- **Windows**
  To access a list of the documentation on your system, click **Start > All Programs > IBM InfoSphere Information Server > Documentation**.

- **Linux**
  The PDF documentation for the suite is installed in `\IBM\InformationServer\Documentation`. 
A complete set of the PDF documentation for the suite is on the IBM InfoSphere Information Server PDF CD that is included with the installation software.

**IBM WebSphere Application Server administration**

While you can perform most administration tasks in the IBM InfoSphere Information Server console or IBM InfoSphere Information Server Web console, you might need to change the user registry configuration, troubleshoot the application, tune the performance, and perform other configuration tasks directly in IBM WebSphere Application Server.

You can find information about WebSphere Application Server at the following locations:

- Version 8.5: publib.boulder.ibm.com/infocenter/wasinfo/v8r5/index.jsp
- Version 8.0: publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

For detailed WebSphere Application Server administration information, refer to the following administration topics.

*Table 2. WebSphere Application Server administration topics*

<table>
<thead>
<tr>
<th>Task</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task</td>
<td>Link</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring bidirectional language support for IBM InfoSphere Business Glossary</td>
<td>See the topic about bidirectional language support in the IBM InfoSphere Business Glossary Administrator’s and Author’s Guide</td>
</tr>
</tbody>
</table>
Chapter 2. Opening the consoles

To administer IBM InfoSphere Information Server, you can use the IBM InfoSphere Information Server console, IBM InfoSphere Information Server Web console, and the IBM WebSphere Application Server administrative console.

Opening the IBM InfoSphere Information Server console

To set up security, manage projects, analyze data, enable information services, or run reports, use the IBM InfoSphere Information Server console. The console is a rich-client-based interface.

About this task

Use the console for the following administrative activities:

- Create and manage projects.
- Set project-level security.
- Analyze data with IBM InfoSphere Information Analyzer.
- Enable information services with IBM InfoSphere Information Services Director.
- Run reports.

Procedure

1. From the Microsoft Windows start menu, select Start > All Programs > IBM InfoSphere Information Server > IBM InfoSphere Information Server Console.
2. In the User Name field, type your user name.
3. In the Password field, type your password.
4. In the Server menu, type or select a host name and port. The host name and port depend on whether WebSphere Application Server clustering is set up for your services tier configuration and whether secure HTTP (HTTPS) is set up.

<table>
<thead>
<tr>
<th>IBM WebSphere Application Server configuration</th>
<th>Host value</th>
<th>Port value (HTTP protocol)</th>
<th>Port value (HTTPS protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server clustering is set up</td>
<td>The host name or IP address of the front-end dispatcher (either the Web server or the load balancer). Do not use the host name of a particular cluster member.</td>
<td>HTTP port of the front-end dispatcher (for example, 80). Do not use the port number of a particular cluster member.</td>
<td>HTTPS secure port of the front-end dispatcher (for example, 443). Do not use the port number of a particular cluster member.</td>
</tr>
<tr>
<td>Clustering is not set up</td>
<td>The host name or IP address of the computer where WebSphere Application Server is installed.</td>
<td>HTTP transport port (configured as WC_defaulthost in WebSphere Application Server). Default: 9080</td>
<td>HTTPS transport secure port (configured as WC_defaulthost_secure in WebSphere Application Server). Default: 9443</td>
</tr>
</tbody>
</table>

5. Click Login.
Opening the IBM InfoSphere Information Server web console

To manage security, view scheduled tasks, work with reports, or perform tasks that are related to IBM InfoSphere Business Glossary or the Information Services catalog, use the InfoSphere Information Server Web console.

Use the web console for the following administrative activities:

- Managing security.
- Creating views of scheduled tasks.
- Reporting.
- Tasks that are associated with IBM InfoSphere Business Glossary.
- Tasks that are associated with the Information Services catalog.

To access the web console, determine the URL to use, configure your browser, and navigate to the console window.

Determining the URL for the IBM InfoSphere Information Server Web console

The URL for the IBM InfoSphere Information Server Web console differs depending upon the IBM WebSphere Application Server communication protocol and configuration.

**Procedure**

The syntax of the URL is as follows:

```
protocol://host:port/ibm/iis/console
```

*protocol* is the communication protocol: either http or https.

*host* and *port* differ depending upon the communication protocol and WebSphere Application Server configuration (clustered or non-clustered):

<table>
<thead>
<tr>
<th>IBM WebSphere Application Server configuration</th>
<th>Host value</th>
<th>Port value (HTTP protocol)</th>
<th>Port value (HTTPS protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebSphere Application Server clustering is set up</td>
<td>The host name or IP address of the front-end dispatcher (either the Web server or the load balancer). Do not use the host name of a particular cluster member.</td>
<td>HTTP port of the front-end dispatcher (for example, 80). Do not use the port number of a particular cluster member.</td>
<td>HTTPS secure port of the front-end dispatcher (for example, 443). Do not use the port number of a particular cluster member.</td>
</tr>
<tr>
<td>Clustering is not set up</td>
<td>The host name or IP address of the computer where WebSphere Application Server is installed.</td>
<td>HTTP transport port (configured as WC_defaulthost in WebSphere Application Server). Default: 9080</td>
<td>HTTPS transport secure port (configured as WC_defaulthost_secure in WebSphere Application Server). Default: 9443</td>
</tr>
</tbody>
</table>

For example, in a configuration where clustering is not set up, the HTTPS URL might be:

```
https://myhost.example.com:9443/ibm/iis/console
```
Configuring your Web browser to work with the IBM InfoSphere Information Server Web console

The IBM InfoSphere Information Server Web console is supported with both Microsoft Internet Explorer and Mozilla Firefox. You must do these steps in your preferred Web browser before you use the IBM InfoSphere Information Server Web console.

Before you begin

- Make sure that your browser is supported by InfoSphere Information Server. For information about supported browsers, see the InfoSphere Information Server system requirements at [www.ibm.com/software/data/integration/info_server/overview/requirements.html](http://www.ibm.com/software/data/integration/info_server/overview/requirements.html).
- Determine the URL to use to access the web console. See [http://publib.boulder.ibm.com/infocenter/iisinfsv/v9r1/topic/com.ibm.swg.im.iis.found.admin.common.doc/topics/t_admin_determining_url.html](http://publib.boulder.ibm.com/infocenter/iisinfsv/v9r1/topic/com.ibm.swg.im.iis.found.admin.common.doc/topics/t_admin_determining_url.html). The host name and port differ depending upon the IBM WebSphere Application Server communication protocol and configuration in use.
- If HTTPS is enabled, then the first time that you access the Web console, a message about a security certificate is displayed if the certificate from the server is not trusted. If you receive such a message, follow the browser prompts to accept the certificate and proceed to the login page.

Configuring Microsoft Internet Explorer to work with the IBM InfoSphere Information Server Web console

You can enable Microsoft Internet Explorer to work with the IBM InfoSphere Information Server Web console.

Procedure

1. Enable JavaScript:
   a. Click Tools > Internet Options. On the Security tab, click Custom Level.
   b. In the Security Settings window, select Scripting > Active Scripting > Enable.
2. Set the browser to accept cookies for the InfoSphere Information Server host site:
   a. Click Tools > Internet Options.
   b. On the Privacy tab, click Sites.
   c. In the Address of Web site field, enter the InfoSphere Information Server host name.
   d. Click Allow.
   e. Click OK.
3. Enable pop-up windows for the URL of the IBM InfoSphere Information Server Web console:
   a. Click Tools > Pop-up Blocker > Pop-up Blocker Settings or turn off the pop-up window blocker.
   b. If you selected the settings, type the URL and click Add.

   **Note:** To enable pop-up windows for the site, you might also need to disable or configure pop-up blockers.
4. Specify that the pages are refreshed every time you visit the site:
a. Click **Tools > Internet Options** and on the General tab, click **Settings**. Select **Settings** in the Browsing history section.
b. Select **Every time I visit to the webpage** or **Automatically** and click **OK**.

5. Optional: Disable the display of friendly HTTP error messages:
   a. Click **Tools > Internet Options**.
   b. On the **Advanced** tab, clear **Browsing > Show friendly HTTP error messages**.

### Configuring Internet Explorer to work with the IBM InfoSphere Information Server Web console on Microsoft Windows Server 2008

In Microsoft Windows Server 2008, you might need to add the InfoSphere Information Server web console URL to the trusted sites zones in Internet Explorer.

#### About this task

If you are browsing to an IBM InfoSphere Information Server Web console by using its host name, such as http://hostname:9080/ibm/iis/console, you must add the URL (http://hostname) to the trusted site zones in Internet Explorer.

You do not have to add the URL to the trusted sites zones if your client computer is also your server and you are browsing to the server by using the URL http://localhost:9080/ibm/iis/console, or if you are using Mozilla Firefox.

#### Procedure

1. In Microsoft Internet Explorer, choose **Tools > Internet Options**.
2. In the **Security** tab, select the **Trusted Sites zone**.
3. Click **Sites**.
4. In the Trusted Sites window, enter the URL and click **Add**.

### Configuring Mozilla Firefox to work with the IBM InfoSphere Information Server Web console

You can configure Mozilla Firefox to work with the IBM InfoSphere Information Server Web console.

#### Procedure

1. Enable JavaScript:
   a. Click **Tools > Options**, and on the Content tab, click **Enable JavaScript**.
2. Set the browser to accept cookies for the InfoSphere Information Server host site.
   a. Click **Tools > Options**.
   b. On the **Privacy** tab, click the **Accept cookies from sites** option or click **Exceptions** and add the site to the allowed site list by entering the host name and clicking **Allow**.
3. Enable pop-up windows for the URL of the web console:
   a. Click **Tools > Options**.
   b. Select the **Contents** tab and either clear the **Block pop-up windows** option or click **Exceptions** and add the site to the allowed list by entering the host name and clicking **Allow**.
**Viewing report results in a Web browser**
Set additional security options to ensure that report results open correctly in Microsoft Internet Explorer.

**Procedure**
1. In the Internet Explorer toolbar, click **Tools > Internet Options**.
2. On the **Security** tab, click the zone in which the services tier is located, such as **Local intranet**.
3. On the **Security** tab, click **Custom Level**.
4. In the Security Settings window, scroll to **Automatic prompting for file downloads** under **Downloads** and select **Enable**.
5. Click **OK**.
6. Click **OK**.

**Navigating to the IBM InfoSphere Information Server Web console**
The IBM InfoSphere Information Server Web console ("the web console") is a browser-based interface for administrative activities.

**Before you begin**
- Make sure that your browser is supported by IBM InfoSphere Information Server. For information about supported browsers, see the InfoSphere Information Server system requirements at [www.ibm.com/software/data/integration/info_server/overview/requirements.html](http://www.ibm.com/software/data/integration/info_server/overview/requirements.html).
- Determine the URL to use to access the web console. See “Determining the URL for the IBM InfoSphere Information Server Web console” on page 8.
- Configure your browser as described in “Configuring your Web browser to work with the IBM InfoSphere Information Server Web console” on page 9.

**Procedure**
1. Open a web browser, and navigate to the console. The URL to use depends upon the IBM WebSphere Application Server communication protocol and configuration in use. See “Determining the URL for the IBM InfoSphere Information Server Web console” on page 8.
2. If HTTPS is enabled, then the first time that you access the web console, a message about a security certificate is displayed if the certificate from the server is not trusted. Follow the browser prompts to accept the certificate and proceed to the login page.
3. Type your user name and password.
4. Click **OK** to open the Home tab.

**Logging in to the IBM WebSphere Application Server administrative console**
Because IBM InfoSphere Information Server server-side processes run on WebSphere Application Server, you do certain administrative tasks by using the WebSphere Application Server administrative console.
Before you begin

To perform various tasks in the WebSphere Application Server administrative console, you must have sufficient authority. The authority level that you require differs from task to task.

Procedure

1. Open a Web browser, and navigate to the WebSphere Application Server administrative console. The URL is in the following form:

   https://hostname:port/ibm/console

   Specify hostname and port in the following manner:

   • If WebSphere Application Server clustering is set up for your services tier configuration, specify the host name (or IP address) and port of the computer that hosts the Deployment Manager. The default port number is 9043.

   • If clustering is not set up, specify the host name or IP address of the computer where WebSphere Application Server is installed. Specify the port number that is assigned to the WebSphere Application Server administrative console. The default port number is 9043.

2. Log in to the WebSphere Application Server administrative console.
Chapter 3. IBM InfoSphere Information Server console overview

The IBM InfoSphere Information Server console is a rich-client-based interface for activities such as creating and managing projects, setting project-level security, analyzing data with IBM InfoSphere Information Analyzer, enabling information services with IBM InfoSphere Information Services Director, and running reports.

From the IBM InfoSphere Information Server console, you can complete the following tasks:
- Create a project
- Set up project-level security
- Analyze information
  - Columns
  - Primary keys and foreign keys
  - Across multiple data sources
- Enable information services
  - Connect to providers
  - Develop projects, applications, services, and operations
  - Deploy services
- Run reports
- Create views of scheduled tasks and logged messages
- Troubleshoot jobs

Main areas of the console

The IBM InfoSphere Information Server console provides workspaces that you use to investigate data, deploy applications and Web services, and monitor schedules and logs.

In the following topics, both IBM InfoSphere Information Analyzer and IBM InfoSphere Information Services Director were installed. Some features might not be available if you have only one product module installed.

My Home workspace

When you open the IBM InfoSphere Information Server console, the My Home workspace is shown. In this workspace, you can access getting started information and you can access projects.

The following figure shows the My Home workspace. You can customize the sections that appear in the workspace.
This workspace contains the following sections:

**Getting Started pane**

The Getting Started describes how to work in a product module, such as how to work in IBM InfoSphere Information Analyzer. The information that is displayed corresponds to the product modules that you have installed.
Many topics in the Getting Started pane have a link that opens the related task and a link that opens the information center for more information (the “Learn more” link).

**Projects pane**

In the Projects pane, you can select a project to open. Multiple users can contribute to and work on a project in the console. This pane shows a list of all of the projects that you have access to.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Created</th>
<th>Last Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indem</td>
<td>Indem</td>
<td>Information Services</td>
<td>8/15/2007 5:44:02</td>
<td>8/15/2007 5:44:02</td>
</tr>
</tbody>
</table>

If you select an InfoSphere Information Analyzer project from the Projects pane, you can see the status of that project in the project details section.

**Workspace Navigator**

The primary means of navigating through the workspaces is the Workspace Navigator. The Workspace Navigator is a series of menus that you use to move through workspaces.

The Workspace Navigator consists of five navigation menus. Each navigation menu contains links to workspaces that you use to complete tasks. The workspaces that are available depend on the product module that you are working in. Some navigation menus might be empty if a particular component has not been installed.

Each workspace corresponds to a navigation menu. For example, if you open the project properties workspace, the Overview navigation menu is highlighted. You
can view all open workspaces that are associated with the current navigation menu that is selected. You cannot view any open workspaces that are associated with a navigation menu that is not selected.

When you select a link and open a workspace, the number on the navigation menu indicates how many workspaces are open per menu. For example, if the dashboard workspace and the project properties workspace are open, the number 2 is displayed on the Overview navigation menu.

![Workspace Navigator on the IBM InfoSphere Information Server console toolbar](image)

Figure 4. The Workspace Navigator on the IBM InfoSphere Information Server console toolbar

The types of tasks that are available depend on the product module and project that you are working with. The following list describes the type of tasks that are available in each of the menus.

**Home navigation menu**
Contains configuration and metadata tasks. For example, if you have IBM InfoSphere Information Services Director installed, you can set up connections to available information providers in the Information Services Connection workspace.

**Overview navigation menu**
Contains the project dashboard and Project Properties workspace. For example, you specify project details in the Project Properties workspace.

**Investigate navigation menu**
Contains information discovery and data profiling tasks. For example, if you have IBM InfoSphere Information Analyzer installed, you can run a column analysis job in the Column Analysis workspace.

**Develop navigation menu**
Contains data transformation and information services enablement tasks. For example, if you have InfoSphere Information Services Director installed, you design, create, and develop applications in the Information Services Application workspace.

**Operate navigation menu**
Contains job scheduling tasks, logging tasks, and information services application tasks. For example, you create views of logged messages in the Log View workspace.

**Project menu**
Above the Workspace Navigator, you can access the project menu to open a project, move between open projects, and create projects.
To open the project menu, click the drop-down menu.

Figure 5. The Project menu above the Workspace Navigator

You can perform configuration and administrative tasks, such as logging, scheduling, and reporting, outside of the context of a project in the console.

To perform product module tasks, such as information analysis or services enablement, you must first open a project. A project is a logical container for all of the tasks that can be performed in a product module.

**Palettes**

You can use the palettes to view a history of your activities and to open workspaces, access shortcuts, and manage notes. You can dock, float, or anchor the palettes. By default, the palettes are located on the left side of the console.

To open the palettes, click one of the tabs.
Notes  Use this palette to view the notes that are associated with an object. Notes are only available for some product modules.

Shortcuts  Use this palette to go to workspaces or panes for which you previously created shortcuts.

History  Use this palette to view a list of the workspaces you visited. The current or most recently visited workspace is at the top of the list.

Open Workspaces  This palette shows all open workspaces. Project-specific workspaces are grouped by project.

To hide the palettes, click outside of the pane.
Project dashboard

When you open a project, the project dashboard is displayed.

IBM InfoSphere Information Analyzer and IBM InfoSphere Information Services Director projects both contain a dashboard. The following figure shows an example of the InfoSphere Information Analyzer dashboard.

Use the Dashboard tab to learn more about the task workflow and, for some product modules, to view the current status of the project. You can customize the dashboard in the console to add or remove content panes. For some product modules, you can also configure the dashboard to show a set of charts and graphs that are based on underlying project information.

Status bar

After you submit a job that requires processing, the status bar is displayed at the bottom of the workspace.

The status bar shows the progress of activities, error messages, and warnings. You use the status bar to monitor any jobs or activities that you initiated.

The status bar can be in one of the following states:

Closed
When no activities are running, the status bar is closed.

Activity in progress
When an activity or job is running, the status bar remains closed and displays a green status indicator that moves across the length of the bar.
Notification
When you initiate an activity or when an activity is completed, the status bar opens briefly and shows details about the status of the activity. When an activity is running, you can view more information about the status of the activity by rolling your cursor over the status bar to open the status pane. The status pane contains a larger progress bar, summary information about the activity, and a Details button. You can roll over the status bar at any time to view the status of the jobs or activities that you initiated.

Details
To view information about the status of an activity, click the Details button in the status pane. You can view details such as the time that the activity started running and whether there are any system warnings or errors. The Details state lists all the activities and jobs that you initiated.

Shortcuts
To quickly return to a task at a later time, you can create a shortcut.

To create a shortcut to the open task, click the Shortcut button.

After you create the shortcut, you can click the Shortcuts tab to return to the task.

![Image of the Shortcuts tab]

Figure 8. The Shortcuts tab

Notes
You can use notes to comment on objects, provide information to other users, and identify issues for further investigation. Notes are available depending on the suite component that you are working in.

You can create or view notes by using the notes palette or clicking on a note icon. Note icons are located at the top of task panes.

Basic task flow in the workspaces
Even though you perform different types of tasks in an IBM InfoSphere Information Analyzer project and an IBM InfoSphere Information Services Director project, the basic task flow is the same.

The following topics describe the basic task flow in the workspaces. This example shows the task flow in the context of creating a column analysis job with
InfoSphere Information Analyzer. The types of tasks and options that are available will vary between InfoSphere Information Analyzer projects and InfoSphere Information Services Director projects.

**Select a task menu from the Workspace Navigator**

After you open a project, the first step is to select a task menu from the Workspace Navigator.

**About this task**

The Workspace Navigator consists of five navigation menus. Each navigation menu contains links to workspaces that you use to complete tasks. The workspaces that are available depend on the suite component that you are working in. Some navigation menus might be empty if a particular component has not been installed.

Select the menu that corresponds with the type of task you want to perform.

![Image of Workspace Navigator](image)

*Figure 9. In this example, the user selects the Investigate task menu*

**Select the task that you want to perform from the task menu**

Next, you select the task that you want to perform from the task menu.

**About this task**

Each navigation menu contains a list of high-level tasks that you can perform. Select the task to open the workspace that is associated with that high-level task.
Select objects and a task in the workspace

In the workspace, you select an item to work with from the objects lists and then select a task to perform from the Tasks list.

About this task

The object list contains the items that you perform the tasks on, such as data sources, applications and services, or log views. The object list can also contain status information, such as the completion of analysis or the creation date of a log view.

The Tasks list contains the tasks that you can perform on the selected objects.

Select an object to work with in the objects list, as shown in the following figure.

Figure 10. In this example, the user selects Column Analysis to open the Column Analysis workspace

Figure 11. Example of data sources selected in the Column Analysis workspace’s object list
And then, select the task that you want to perform from the Tasks list.

Tasks might be unavailable if you have not yet selected an object, or if there is a prerequisite task.

**Work in a task pane**

After you select a task from the Tasks lists, a task pane opens. In the task pane, you can select options and provide details to complete the task.

**About this task**

Note that when the task pane opens, the object list and Tasks list are collapsed at the top of the workspace. The following figure shows the Run Column Analysis task pane.

*Figure 12. Example of selecting task from the Tasks list in the Column Analysis workspace.*

*Figure 13. The Run Column Analysis task pane*
The content of each task pane differs. Many task panes require that you select options and provide additional details. You can also schedule certain tasks to run at specified times or intervals. The asterisk (*) indicates a required field.

When you have completed the task, click **Save** or **Submit**.

After you submit a job that requires processing, the status bar is displayed at the bottom of the workspace.

---

### Reporting, scheduling, and logging in the console

The IBM InfoSphere Information Server console also gives you access to common administrative tasks, such as reporting, scheduling, and logging.

#### Reporting

You can use the reports workspace to create, edit, or view a report. A report shows the details of an activity that has been completed in the suite.

To create a report, you select a report template and then specify the project that you want to associate with the report. You then type parameters for the report and choose the format that you want the report to be created in such as PDF, XML, or DHTML. The report templates that are available correspond to the components in the suite.

To edit a report, you select the report that you want to modify and then create a copy of it. You make any changes in the copy.

Reports can be saved in the metadata repository and can be accessed by you or by other authorized users. You or other users can use the information in the reports to complete other tasks in the product modules.

You can also use the reports workspace to view saved reports that were generated in the suite and to select certain reports as your favorites. To find a report, you can filter the list of available reports by the names of the projects that they are associated with or by the dates on which the reports were created. If you select a report as a favorite, the report is accessible in the report favorites pane in the My Home workspace.

#### Scheduling

You create schedule views to query the schedules that you created elsewhere in the suite.

You create a schedule to define when an activity will run in the suite component that you are working in. A schedule contains details about when the activity will run, such as a specific time or day. Schedules can be configured to run at any time or on any date that you specify. You can also configure schedules to run repeatedly or at different intervals.

A schedule view shows information such as a list of available schedules in the suite, a history of the scheduled tasks that have completed, and a forecast of the
schedules that will run at a specific time. You can create a query in multiple ways: by selecting the name of a schedule that you want to view, the user who created the schedule, the date on which the schedule will run, or the date on which the schedule was created or updated. You can also query schedules by the suite component that they were created in. You can view only the schedules that you created. A suite administrator can view all schedules in the suite.

You can make a schedule view private to restrict users from accessing it. Schedule views that are marked as private are available only to the user who created them. If you want to make a schedule view available to all users, you can mark it as shared. A shared schedule view can only be edited by the user who created the schedule view or by the suite administrator.

Logging

You can configure log views to manage the log messages that are generated when activities run in the suite.

You create log views to query log messages. Log messages show details about the activities that run in the suite. After you create a log view, you use filters to restrict the information in the log view. Only a suite administrator can delete log messages. If you want to delete log messages, you select the log view that contains the information that you want to remove.

You can restrict access to a log view by making the log view private. Private log views are available only to the user who created the log view. If you want a log view to be available to all users, you can share the log view. Shared log views can be edited only by the user who created the shared log view or by a suite administrator.

Online help

If you need help when you are working on a task, press F1 to access context-sensitive help, open the information center, or find specific information about the task in the instruction pane.

Context-sensitive help

When you need assistance while you work, press F1 to open context-sensitive help. For example, from the project properties workspace, press F1 to open the project properties documentation in the information center.

Information center

The information center is this Web-based help system and knowledge base, in which you can find conceptual and task-based information about the suite, the console, and the tasks that you can complete in the IBM InfoSphere Information Server console. You can also access information about all the products that you have installed.

Instruction panes

You can find information about the task in the instruction pane. An instruction pane button appears at the top of most panes and tabs. Most panes contain instructional text.
Figure 15. The instruction icon highlighted

To show the instructional text, click (instruction pane).

To hide the instructional text, click the instruction icon again.
Chapter 4. Working with projects in the IBM InfoSphere Information Server console

In the IBM InfoSphere Information Server console, a project is a logical container for all of the tasks that can be performed in a product module. Multiple users can contribute to a project and view the status of a project over time.

Setting up a project in the IBM InfoSphere Information Server console

To set up a project, you first create a project and provide basic project details.

Creating a project

You must first create a project. A project is a logical container for all of the tasks that can be performed in a product module.

Before you begin

You must have permissions to create a project. If you do not, all project creation menus and tasks are disabled.

Procedure

2. In the New Project window, select the type of project that you want to create. The Type field is displayed only if more than one product module is installed.
3. Type a name for the project.
4. Click OK to open the Project Properties workspace.

What to do next

- "Modifying project properties"
- "Assigning users to a project and assigning roles" on page 74

Modifying project properties

You can view and modify the properties of your project.

Before you begin

You must have project administrator authority.

Procedure

1. On the Overview navigator menu in the IBM InfoSphere Information Server console, select Project Properties.
2. Specify information about the project.
3. Click Save All.
Customizing the project dashboard

You can customize the Dashboard workspace in the IBM InfoSphere Information Server console to add or remove content panes. For some product modules, you can also configure the dashboard to show a set of charts and graphs that are based on underlying project information.

Procedure

1. On the Overview navigator menu in the IBM InfoSphere Information Server console, select Dashboard.
2. In the Dashboard workspace, click Configure.
3. Optional: Click Add to add content panes to the Content list. The available content panes depend on the product modules that are installed.
4. In the Configure Dashboard window, select the content pane that you want to modify.
5. For each content pane, you can modify the label of the pane and select whether it is displayed on the workspace. Some content panes have additional configuration properties.
6. Click OK to save your changes.

Opening an existing project in the IBM InfoSphere Information Server console

You can open an existing project to perform tasks that are associated with the project's product module, such as information analysis or information services enablement.

Before you begin

You or your administrator must create and set up a project.

Procedure

1. In the Projects pane of the My Home workspace, select a project from the list.
2. Click Open Project to open the Dashboard workspace.
Chapter 5. Customizing the consoles

You can customize both the IBM InfoSphere Information Server console and the IBM InfoSphere Information Server Web console.

Customizing the IBM InfoSphere Information Server console

The IBM InfoSphere Information Server console integrates multiple product modules into a unified user interface. To customize the IBM InfoSphere Information Server console, you can set user preferences, create shortcuts, create notes, and change your password.

Customizing the My Home workspace

You can customize the My Home workspace to show or remove information in the Getting Started pane, project information, and favorite reports. You can also add or remove content panes for the product modules that are installed.

Procedure

1. On the Home navigator menu, select My Home.
2. In the My Home workspace, click Configure.
3. In the Configure My Home window, select the content pane that you want to modify.
4. Optional: Click Add to add content panes to the Content list. The content panes that are available depend on the product modules that are installed. Product module panes might have additional configurable details.
5. For each content pane, you can modify the label of the pane and specify whether it is displayed on the My Home workspace.
6. Click OK to close the window.

Modifying user preferences

You can modify user preferences for startup, to change the behavior of panes, and to customize the status bar.

Procedure

1. Select Edit > Preferences.
2. In the User Preferences window, select the type of preferences that you want to modify.
3. Modify the available options.
4. Click OK to close the window and save your changes.

Creating shortcuts

You can create shortcuts to quickly access frequently used workspaces or tasks.

Procedure

1. On the workspace or task, click Add Shortcut.
2. In the Add to Shortcuts window, type a name for the shortcut.
3. Optional: Click **New Folder** to create a folder to organize your shortcuts.

4. Optional: Select a folder to add your shortcut to. You can also drag folders around in the list to reorder them or to nest them.

5. Click **OK** to save your changes.

**What to do next**

You can now access your shortcut on the Shortcuts palette.

**Working with palettes**

Palettes are containers for IBM InfoSphere Information Server console shortcuts, workspace history, open workspaces, and notes. You can dock, float, and anchor the palettes.

**About this task**

By default, the palettes are docked on the left side of the IBM InfoSphere Information Server console. When docked, the palettes display as a set of vertical tabs.

**Procedure**

To open a palette, click the tab. You can click a workspace to hide the palettes again.

**What to do next**

To pin the palette to stay open, click the pin image.

To reposition a palette, right-click the tab or the top bar of the palette.

**Floating the palettes**

You can float the palettes to move them as a separate pane in the IBM InfoSphere Information Server console. You can float an individual palette or you can float the palettes as a group.

**Procedure**

To float the palettes as a group, select the top bar of the palettes and drag it to a new location in the console. You can also select and drag an individual tab in the palettes to just float that tab.

**What to do next**

Floated palettes can be docked by clicking **Dock**, or anchored by clicking **Anchor**.

**Anchoring the palettes**

You can anchor the palettes to one side of the workspace. You can anchor an individual palette or you can anchor the palettes in groups.
Procedure
To anchor a palette, drag the palette to the opposite edge of the workspace. Anchored palettes can be stacked vertically or grouped together in one or more sets.

What to do next
Anchored palettes can be docked by clicking Dock, or floated by clicking Float.

To switch the side of the window that the palettes are docked or anchored to, select the top bar of the docked palettes and drag it to the other side of the workspace.

Creating notes
In some product modules, you can create notes to comment on an object, provide information to other users, and flag issues for further investigation.

Procedure
1. On the pane or table that you want to add the note, click Note.
2. On the Notes palette, click New. New notes are saved when you create them.
3. In the table, specify information for the note. Any changes you make to a note are automatically saved.
4. In the Notes palette, click Close.

What to do next
After you create the note, you and other users can access the note by clicking Note.

Refreshing an object list
You can refresh an object list to view changes made by other users.

Procedure
To refresh an object list, click Refresh or right-click the header above the object list.

Changing your password
You can change the password that you use to log in to the server. If IBM InfoSphere Information Server is configured to authenticate against an external directory, passwords cannot be changed.

Procedure
To change your password, click File > Change Password.
Customizing the IBM InfoSphere Information Server Web console

You can access suite administration and reporting tasks, information about deployed information services, and glossaries of information assets in the IBM InfoSphere Information Server console. To customize the IBM InfoSphere Information Server console, you can customize the Home tab and change your password.

Customizing the Home tab

You can customize the Home tab. For example, you can show a list of the latest report results.

Procedure

1. On the Home tab, select Customize My Home.
2. In the Customize My Home dialog box, select the components that you want to display on the left and right sides of the Home tab.
3. Click Save to close the dialog box.

Changing your password

You can change the password that you use to log in to the IBM InfoSphere Information Server Web console.

Procedure

To change your password, click Change Password in the top right corner of the Web console window and type the required information.
Chapter 6. Managing security

To set up security, you configure the user registry, control access levels, create or update users and groups, and configure audit logging. After security is set up, you can change user names and passwords and perform other administrative tasks by using IBM InfoSphere Information Server administration commands and tools.

If you enabled Secure Sockets Layer (SSL) for IBM WebSphere Application Server, refer to the IBM InfoSphere Information Server Planning, Installation, and Configuration Guide for information about administering SSL for InfoSphere Information Server.

Security setup

Setting up a secure environment in IBM InfoSphere Information Server involves configuring the user registry, creating users, and assigning security roles to those users.

In InfoSphere Information Server, to set up a secure environment you complete the following tasks:

1. Choose a user registry and configure it for InfoSphere Information Server.
   - A user registry contains valid user names and passwords. To log in to InfoSphere Information Server, a user must have a user name and password in the user registry. The installation program configures InfoSphere Information Server to use its internal user registry. As part of security setup, you can configure InfoSphere Information Server to use an external user registry such as a local operating system user registry or lightweight directory access protocol (LDAP) user registry.

2. Create users and groups.
   - Create users and groups in the user registry. If InfoSphere Information Server is configured to use the internal user registry, create users and groups by using the InfoSphere Information Server console or the InfoSphere Information Server Web console. If InfoSphere Information Server is configured to use an external user registry, use standard operating system utilities or user registry utilities to create users and groups.

3. Assign security roles to users and groups.
   - To configure which suite components a user or a group has access to and what level of access that user or group has in the suite component, assign security roles to the user or group.

   - The InfoSphere Information Server engine performs user authentication separately from other InfoSphere Information Server components. Depending on your user registry configuration, you might have to map credentials between the InfoSphere Information Server user registry and the local operating system user registry on the computer where the engine is installed.

5. Assign project roles to users.
   - Some suite components require that you assign project-specific roles to users.

Optionally, you can also complete the following setup tasks:

- Configure IBM WebSphere Application Server for non-root administration.
By default, WebSphere Application Server runs as root. However, it can also be run by using a non-root user ID. You can configure and set appropriate file system permissions for WebSphere Application Server to "run-as" a non-root user ID.

- **Configure InfoSphere Information Server agents for non-root administration**
  By default, the InfoSphere Information Server agents (such as the ASB and logging agents) run as root. However, they can also be run by using a non-root user ID. You can configure and set appropriate file system permissions for the agents to "run-as" a non-root user ID.

- **Configure the Auditing service.**
  The Auditing service creates an audit trail of security-related events. The trail includes all activities that set or modify security-related settings and all user authentications and application logins. You can configure which audit events to log and how much information to include based on your auditing requirements.

**User registry configuration**

A user registry holds user account information, such as a user name and password, that is accessed during authentication. To log in to IBM InfoSphere Information Server, a user must have a user name and password in the user registry.

During installation, the InfoSphere Information Server installation program configures InfoSphere Information Server to use an internal user registry. The internal user registry is located in the metadata repository. After you install InfoSphere Information Server, you can continue to use the internal user registry. Alternatively, you can set up InfoSphere Information Server to use a local operating system user registry or a Lightweight Directory Access Protocol (LDAP) compliant user registry.

If you choose to change registries, complete the change immediately after the installation finishes. For best results, do not change user registries after the system has been in production. If you must change the user registry after the system has been in production, consider migrating to a new installation to avoid security issues and risks. Otherwise, there a mismatch might occur between the users of the old and new user registries.

**Internal user registry overview**

By default, IBM InfoSphere Information Server stores user information in the internal user registry in the metadata repository.

The following figure shows an InfoSphere Information Server topology where the services tier and metadata repository tier are on one computer. InfoSphere Information Server and IBM WebSphere Application Server are both configured to use the internal user registry provided by InfoSphere Information Server. The internal user registry is stored in the metadata repository.
As shown in the figure, the InfoSphere Information Server directory service communicates with the internal user registry. WebSphere Application Server also communicates with the internal user registry. WebSphere Application Server performs the underlying InfoSphere Information Server user authentication.

When you use the internal user registry, you create users directly through the InfoSphere Information Server console or the InfoSphere Information Server Web console. You can also create groups and assign users to those groups. The credentials are stored in the internal user registry. The group membership information and the associations between users and their security roles are also stored in the internal user registry. E-mail addresses and business addresses are also stored here.

The internal user registry stores only digested (one-way encryption) passwords for increased security. User names and group IDs can contain any letters or digits, and the following special characters:

- Underscore (_)
- Hyphen (-)
- Comma (,)
- Backslash (\)
- Equal sign (=)
- Dollar sign ($)
The InfoSphere Information Server engine performs user authentication separately from other InfoSphere Information Server components, and cannot use the internal user registry. Instead, the InfoSphere Information Server engine uses the operating system user registry to perform user authentication. If you configure InfoSphere Information Server to use the internal user registry, you must map credentials between the InfoSphere Information Server user registry and the local operating system user registry on the computer where the engine is installed.

**External user registry overview**

You can configure IBM InfoSphere Information Server to authenticate users based on an existing external user registry, such as a local operating system user registry or a Lightweight Directory Access Protocol (LDAP) user registry.

InfoSphere Information Server supports all external registries that are supported by IBM WebSphere Application Server Network Deployment. For more information about user registries that WebSphere Application Server supports, see the WebSphere Application Server documentation:

- IBM WebSphere Application Server Network Deployment 8.5:  

- IBM WebSphere Application Server Network Deployment 8.0:  

The following figures show an InfoSphere Information Server topology where the services tier and metadata repository tier are located on one computer. In the first figure, InfoSphere Information Server and IBM WebSphere Application Server are both configured to use the local operating system user registry. In the second figure, InfoSphere Information Server and IBM WebSphere Application Server are both configured to use an external LDAP user registry.
Figure 17. Example of an InfoSphere Information Server architecture that uses the local operating system user registry.
When you use an external user registry, WebSphere Application Server communicates with that user registry. The InfoSphere Information Server directory service communicates with the WebSphere Application Server user registry. It does not communicate with the external user registry directly. By going through WebSphere Application Server to access the external user registry, InfoSphere Information Server takes advantage of the capabilities in WebSphere Application Server for handling various kinds of external user registries.

When you use an external user registry, you create users and groups through the administration tools for that user registry. InfoSphere Information Server looks to the external user registry for user names, passwords, group definitions, and group memberships. Password restrictions are imposed by the user registry.

If you are configuring WebSphere Application Server clustering for scalability or high-availability, you cannot configure InfoSphere Information Server to use the local operating system user registry. Instead, configure an LDAP user registry or the internal user registry.

Even when you configure InfoSphere Information Server to use an external user registry, certain user information is still maintained in the internal user registry. Specifically, the internal user registry always stores the security roles that are assigned to users and groups, as well as attributes that are not passed through by WebSphere Application Server, such as e-mail addresses and business addresses. The internal user registry is always available and working in the background.
User registry considerations
Choose your user registry configuration based on the scale of your installation and
the experience of your administrators.

The supported user registry configurations differ in the following areas:
• Ease of installation and setup.
• Ease of maintenance of users and groups, and the level of authentication
  required.
• The number of sets of credentials that you must maintain.
• How the credentials are stored.
• Feature support.
• Engine security considerations. The IBM InfoSphere Information Server engine
  performs user authentication separately from other InfoSphere Information
  Server components. Depending on your topology and the user registry that you
  choose, you might have to map credentials between the InfoSphere Information
  Server user registry and the local operating system user registry on the
  computer where the engine is installed.

Internal user registry: Least complex, suitable for small-scale installations
Consider the following information when determining whether to use the
internal user registry:
• The internal user registry is set up by the installation program.
  InfoSphere Information Server is configured to use this user registry by
default.
• To manage users and groups, you use the InfoSphere Information Server
  console or Web console. With other user registry configurations, you
  must have administrative access to the user registry.
• Because the internal user registry is separate from other user registries, it
  requires that you maintain an independent set of credentials for each
  InfoSphere Information Server user that are unrelated to any other user
  registry that is maintained for other business applications.
• User credentials are stored in the InfoSphere Information Server
  metadata repository database. User credential information is one-way
  encrypted in the database.
• The internal user registry has no support for password policies, length,
or expiration dates.
• The InfoSphere Information Server engine cannot use the internal user
  registry for authentication. You must map credentials between the
  InfoSphere Information Server user registry and the local operating
  system user registry on the computer where the engine is installed. If the
  user names or passwords are changed in the local operating system user
  registry, an administrator must update the mapping. The administrator
  can use the InfoSphere Information Server console for this task.
• The mapped user credentials are also stored in the InfoSphere
  Information Server metadata repository database. User credential
  information is strongly encrypted in the database.

Local operating system user registry: Suitable for small and self-contained
installations, if the internal user registry is unsuitable
Consider the following information when determining whether to use a
local operating system user registry:
Windows
You might experience major performance issues if you use a local operating system user registry configuration on a Microsoft Windows computer when the computer is registered in a Windows domain.

To use a local operating system user registry configuration, you must perform additional configuration steps after software installation is complete.

To manage users and groups, you use standard operating system utilities. For this reason, you must have administrative access.

Unlike the internal user registry configuration, with this configuration you can maintain a single set of credentials for each user.

The local operating system user registry has support for features such as password policies, length, and expiration dates.

Linux
IBM WebSphere Application Server must be run as root, because the application server authenticates passwords.

If you plan to create a WebSphere Application Server cluster for scalability or high-availability, you cannot use a local operating system user registry configuration because it is not supported.

If the services tier and engine tier are installed on the same computer, you can configure both InfoSphere Information Server and the engine to share the local operating system user registry. In this case, credential mapping is not required. If the services tier and engine tier are installed on separate computers, you must map credentials between the InfoSphere Information Server user registry and the local operating system user registry on the computer where the engine is installed.

Lightweight Directory Access Protocol (LDAP) user registry: Most powerful, but most complex

To use an LDAP user registry configuration, you must perform additional configuration steps after the software installation is complete.

Setup and administration of an LDAP user registry is more technically complex than with the other user registry configurations.

An LDAP user registry has better performance than the other user registry configurations, and is more scalable.

Unlike the internal user registry configuration, with this configuration you can maintain a single set of credentials for each user.

An LDAP user registry has support for features such as password policies, length, and expiration dates.

To manage users and groups, you use utilities that are specific to the LDAP server. You must have LDAP server administrative access.

You can configure both InfoSphere Information Server and the engine to use the LDAP user registry. In this case, credential mapping is not required. However, in IBM AIX®, Solaris, HP-UX, and Linux installations, you must configure Pluggable Authentication Module (PAM) support on the engine tier computer.

Switching to the local operating system user registry (IBM WebSphere Application Server Network Deployment)
After you install IBM InfoSphere Information Server, you can configure the suite to use the local operating system user registry. Follow this procedure if your installation includes IBM WebSphere Application Server Network Deployment 8.0 or 8.5.
Before you begin

If you have implemented WebSphere Application Server clustering for your installation, use of the local operating system user registry is not supported.

WebSphere Application Server has a number of restrictions regarding local operating system user registries on both UNIX and Microsoft Windows. For example:

- **Linux** **UNIX**: WebSphere Application Server processes must be run as root.
- **Linux** **UNIX**: The network information service (NIS) protocol is not supported.
- **Windows**: The use of domain accounts imposes access rights on users who run WebSphere Application Server processes.

See the WebSphere Application Server documentation for more information:

- Version 8.0: publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.nd.doc/info/ae/tsec_localos.html

Procedure

1. Create a user account on the local computer to use for the WebSphere Application Server administration account. Alternatively, select an existing account. As part of the switch to the local operating system user registry, you direct WebSphere Application Server to use this account for the administrator role.

   **Note**: This account can be the same as the account that owns the WebSphere Application Server installation. Alternatively, the account can be the same as the account that runs the WebSphere Application Server processes. Alternatively, it can be a different account.

2. Log in to the WebSphere Application Server administrative console.
3. In the console, click **Security > Global Security**. The Global Security page appears.
4. Ensure that the **Use realm-qualified user names** option is not selected.
5. In the User account repository section on the right side of the page, click the **Available realm definitions** list and select **Local operating system**.
6. Click **Configure**.
7. In the **Primary administrative user name** field, type the name of the user account that you created in step 1.
8. Click **Apply**.
9. Select **Server identity that is stored in the repository**.
10. In the **Server user ID or administrator user on a Version 6.0.x node** field, type the short name of the user account that you created in step 1.
11. In the **Server user password** field, type the password of the user account that you created in step 1.
12. Click **OK**.
13. Click the **Save** link at the top of the page, and click the **Save** button.
14. On the Global Security page, ensure that LTPA is selected for the Active authentication mechanism setting.

15. In the Available realm definitions list, select Local operating system, and click Set as current. If an error occurs, the application server is unable to authenticate with the local operating system by using the credentials that you provided.

16. Click the Save link, and click the Save button.

17. Stop WebSphere Application Server.

18. Log in to the services tier computer.

19. From the command line, run the AppServerAdmin command. This command propagates the WebSphere Application Server administrator user name and password to WebSphere Application Server.

   ```
   /opt/IBM/InformationServer/ASBServer/bin/AppServerAdmin.sh -was 
   -user was_admin_user_id -password was_admin_password
   ```

   ```
   C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -was 
   -user was_admin_user_id -password was_admin_password
   ```

   In the command, was_admin_user_id and was_admin_password must match the credentials that you provided in the WebSphere Application Server administrative console.

   **Tip:** The -password parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command.

20. If you are switching the user registry for a system that has been used for a while by multiple users, clean up the users and groups that are related to the security configuration. See “Switching the user registry configuration for a system in use” on page 53.


   After WebSphere Application Server is restarted, during the InfoSphere Information Server initialization, the WebSphere Application Server user registry configuration is checked and the InfoSphere Information Server user registry configuration is automatically adjusted if needed. The default WebSphere Application Server administrator user is also automatically configured as the initial new InfoSphere Information Server default administrator user.

**What to do next**

After you change the user registry, you can open the InfoSphere Information Server Web console and grant suite administrator access to additional users as needed.

**Configuring IBM InfoSphere Information Server to use PAM (Linux, UNIX)**

Pluggable Authentication Module (PAM) is currently supported on IBM AIX, Oracle Solaris, HP-UX, and Linux platforms. You can configure the services tier, engine tier, or both, to use PAM. If you choose to use PAM on the engine tier and you also want to use an LDAP user registry, you must configure PAM on the engine tier before setting up IBM InfoSphere Information Server to use an LDAP user registry.
Configuring the IBM InfoSphere Information Server services tier to use PAM (Linux, UNIX):

Configuring PAM for the services tier is optional. Configure PAM only if you want the services tier to use PAM for authentication. Unlike the engine tier, the services tier can authenticate through LDAP without PAM.

Before you begin

To complete these tasks, you must have a working knowledge of PAM and the authentication modules and strategies.

About this task

Consider these reasons why you might configure PAM on the services tier:

• Multiple PAM modules can be configured to allow fallback authentication options. For example, you can configure an LDAP server as the primary user registry for authentication and also configure a fallback to local operating system authentication in case the LDAP authentication fails. Such a configuration allows you to combine multiple user registries.

• PAM is a way to customize local operating system authentication. For example, PAM can be used to delegate a local operating system authentication to an LDAP server.

PAM provides authentication support only (verification of the user ID and password). InfoSphere Information Server also requires user and group membership information to determine the roles assigned to a user used for authorization decisions. PAM does not provide user and group membership support. InfoSphere Information Server determines user and group membership by using two possible mechanisms:

1. By default, it looks in the /etc/passwd and /etc/group files.
2. You can specify the user and group files to use as PAM registry configuration options.

Restrictions:

• If you configure PAM for use with InfoSphere Information Server, it is strongly recommended that you not run IBM WebSphere Application Server in a clustered environment. Because PAM relies on local files to determine user and group memberships, you would need to ensure that the user and group files are in sync across the nodes. Unexpected results can occur if the files become out of sync.

• The PAM user registry is supported as a stand-alone user registry and is not supported when using a WebSphere federated user registry.

• When a local operating system PAM module is used in the PAM configuration, IBM WebSphere Application Server must be run as root. When a local operating system PAM module is not configured, IBM WebSphere Application Server can be run as a non-root user. This restriction is true for all supported operating systems.

Perform this task on the computer that hosts the services tier. PAM support is specific to each platform.
Procedure
1. Add to or create the PAM configuration file on your platform.
2. Configure IBM WebSphere Application Server
   a. Log in to the IBM WebSphere Application Server Administrative console.
   b. Navigate to the security section of the IBM WebSphere Application Server
      Administrative console. Select **Security > Global Security**.
   c. In the User account repository section, select Standalone custom registry
      from the **Available realm definitions** field and click **Configure**.
   d. In the **Primary administrative user name** field, type the administrator user
      name, which is a valid PAM user ID.
   e. Select the server identity that is stored in the repository. Enter the valid
      PAM user ID and password.
   f. Ensure that the custom registry class name is the following string:
      `com.ibm.is.isf.j2ee.impl.was.security.WASExtendedCustomUserRegistry`. Click
      **Apply**.
   g. Complete this step only if you want to use files other than the local
      operating system authentication files. In the Custom Properties section,
      select **New**, define the following properties and values, and click **OK**.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.ibm.is.isf.j2ee.impl.was.security.\</td>
<td>The file where the user information is stored. The information in the file must be stored in the same manner as it would in the /etc/passwd file. If this property is not specified, the default user registry file /etc/passwd is used.</td>
</tr>
<tr>
<td>WASExtendedCustomUserRegistry.usersFile</td>
<td></td>
</tr>
<tr>
<td>com.ibm.is.isf.j2ee.impl.was.security.\</td>
<td>The file where the group information is stored. The information in the file must be stored in the same manner as it would in the /etc/groups file. If this property is not specified, the default group registry file /etc/groups is used.</td>
</tr>
<tr>
<td>WASExtendedCustomUserRegistry.groupsFile</td>
<td></td>
</tr>
<tr>
<td>com.ibm.is.isf.j2ee.impl.was.security.\</td>
<td>You can configure multiple PAM modules with different names on the same computer. Choose the one that you want to specify for this configuration. If this property is not specified, then the default value isf pam is chosen and a module with that file name is expected to be in the pam.d configuration directory.</td>
</tr>
<tr>
<td>WASExtendedCustomUserRegistry.moduleName</td>
<td></td>
</tr>
</tbody>
</table>

h. Test your configuration. In the Standalone Custom Registry section, click
   **Set as current**. If an error occurs, the application server is unable to
   authenticate with the internal user registry by using the credentials that you
   provided. Recheck your configuration.

   i. Click **Apply**, click **Save**, and log out of the console.

3. Stop the application server.
Attention:

- When stopping the application server processes, use the old user name and password, that is, the credentials of the application server administrator from the previous user registry.
- It is recommended that you not configure PAM in a clustered installation.
  However, if you do, first stop the application servers and the node agents, and then stop the Deployment Manager.

4. Log in to the computer on which the AppServerAdmin tool is installed. This tool is on the same computer as the services tier, in the IS_install_dir/ASBServer/bin directory.

5. From the command line, run the AppServerAdmin command. This command propagates the administrator user name and password to the application server. Specify the same user ID and password specified in the Administrative console in step 2d on page 44.

   IS_install_dir/ASBServer/bin/AppServerAdmin.sh -was
   -user was_admin_user_id -password was_admin_password

   Tip: The -password parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command.

6. Restart the application server. In a clustered installation, start the Deployment Manager, the node agents, and then the application servers. If one of the node agents does not start, the node agent cannot be restarted because the user registry configuration at the Deployment Manager and node levels do not match. To fix this problem, run the application server syncNode command to synchronize the node with the Deployment manager.

   a. Log in to the node.
   b. Run the syncNode command.

   WAS_install_dir/AppServer/profiles/custom_profile/bin/syncNode.sh
   dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password

   dmgr_hostname
   The host name of the computer on which the Deployment Manager is running.

   dmgr_port
   The port number of the Deployment Manager. (The default is 8879.)

   was_admin_username and was_admin_password
   The administrator user name and password for the application server.

7. Check the application server log files to ensure that no errors occurred.
8. Verify the configuration by logging in to the IBM InfoSphere Information Server Web console with the new user ID and password.

Configuring the IBM InfoSphere Information Server engine tier to use PAM (Linux, UNIX):

Configuring PAM on the engine tier is optional. Configure PAM on the engine tier only if you want the engine tier to authenticate through an LDAP server.

Before you begin

To complete these tasks, you must have a working knowledge of PAM and the authentication modules and strategies.
About this task

Perform this task on the computer that hosts the engine tier.

To configure PAM on IBM AIX, see the Configuring DataStage to use PAM Authentication on AIX support document [http://www.ibm.com/support/docview.wss?rs=14&uid=swg21398309](http://www.ibm.com/support/docview.wss?rs=14&uid=swg21398309).

Use the following procedure to configure PAM on Linux and UNIX.

Procedure

1. Add to or create the PAM configuration file on your platform.
2. Stop the InfoSphere Information Server engine by running the following command:
   ```bash
   $DSHOME/bin/uv -admin -stop
   ```
3. Edit the uvconfig file in the DSHOME directory to change the setting of the AUTHENTICATION tunable to 1. The following example shows the AUTHENTICATION tunable set to 1.
   ```
   # AUTHENTICATION - Specifies the method by which UNIX user authentication is done. Currently, the following methods are supported:
   #   0) Standard O/S Authentication (default)
   #   1) Pluggable Authentication Module (PAM)
   # This value should only be changed with a full understanding of the implications, as improper setting of this value can lead to the environment being unusable.
   AUTHENTICATION 1
   ```
4. Add the PAM service entry, dsepam, to the PAM configuration file. The name and the location of the PAM configuration file are platform-dependent.
5. Regenerate the InfoSphere Information Server engine configuration file by running the following command:
   ```bash
   $DSHOME/bin/uv -admin -regen
   ```
6. Restart the InfoSphere Information Server engine by running the following command:
   ```bash
   $DSHOME/bin/uv -admin -start
   ```

What to do next

Set up the InfoSphere Information Server engine tier to use the Lightweight Directory Access Protocol (LDAP) user registry.

If you have configured PAM for both the engine and services tier by using an LDAP user registry, you can share the user registry with the tiers that you configured for PAM. Both PAM configurations must point to the same user registry by using the same set of PAM modules. For more information, see “Shared user registry overview” on page 78.

Examples of PAM configuration files (Linux, UNIX):

Some example PAM configuration files for various operating systems are shown.

On a Linux system, you must create a file named dsepam in the /etc/pam.d directory. The following example shows the possible contents of the dsepam file on a 64-bit Linux system:
For IBM AIX, see the Configuring DataStage to use PAM Authentication on AIX support document [http://www.ibm.com/support/docview.wss?rs=14&uid=swg21398309] for an example PAM configuration file on AIX.

The following example is for SUSE Linux on System z® and on 64 bit platforms:

```bash
#%PAM-1.0
auth  required /lib64/security/pam_stack.so service=system-auth
password required /lib64/security/pam_stack.so service=system-auth
account required /lib64/security/pam_stack.so service=system-auth
```

On a Solaris system, you must edit the existing `pam.conf` file in the `/etc` directory and add an entry like the following example:

```bash
dsepd auth required /usr/lib/security/pam_unix.so.1
```

**Switching to an LDAP user registry**


**Before you begin**

- The InfoSphere Information Server engine performs user authentication separately from other InfoSphere Information Server components. You can configure the engine to use the LDAP user registry that you set up. For IBM AIX, Solaris, HP-UX, and Linux platforms, you can optionally configure Pluggable Authentication Module (PAM) support before you switch the user registry. For more information, see "Configuring IBM InfoSphere Information Server to use PAM (Linux, UNIX)" on page 42.
- In an IBM WebSphere Application Server stand-alone installation, WebSphere Application Server must be running.
- In a clustered installation, the Deployment Manager and all node agents must be running.

**About this task**

InfoSphere Information Server supports any LDAP-compliant user registry that IBM WebSphere Application Server Network Deployment supports. For more information about supported LDAP servers, see the IBM WebSphere Application Server Network Deployment system requirements:

- IBM WebSphere Application Server Network Deployment 8.5: [http://www-01.ibm.com/support/docview.wss?uid=swg27023941]
- IBM WebSphere Application Server Network Deployment 8.0: [http://www.ibm.com/support/docview.wss?uid=swg27021246]

**Procedure**

1. Do the procedures in the WebSphere Application Server documentation for configuring LDAP user registries.

   Procedures for configuring LDAP user registries within WebSphere Application Server can be found in the WebSphere Application Server information center:
2. In a clustered installation, synchronize the configuration files on the nodes in the cluster:
   a. In the **System administration > Nodes**.
   b. Select the check boxes beside all nodes.
   c. Click **Synchronize**.
   d. Log out of the console.

3. Stop WebSphere Application Server. In a clustered installation, stop the application servers and the node agents, and then stop the Deployment Manager.

   **Important:** When stopping the WebSphere Application Server processes, use the credentials of the WebSphere Application Server administrator from the previous user registry.

4. Log in to the computer on which the **AppServerAdmin** tool is installed:
   - If you have implemented WebSphere Application Server clustering within your installation, log in to the computer that hosts the WebSphere Application Server Deployment Manager.
   - If you have not implemented clustering, log in to the services tier computer.

5. From the command line, run the **AppServerAdmin** command. This command propagates the WebSphere Application Server administrator user name and password to WebSphere Application Server.

   **Linux**
   ```bash
   /opt/IBM/Information/server/ASBServer/bin/AppServerAdmin.sh -was
   -user was_admin_user_id -password was_admin_password
   ```

   **Windows**
   ```bash
   C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -was
   -user was_admin_user_id -password was_admin_password
   ```

   In the command, **was_admin_user_id** and **was_admin_password** must match the new WebSphere Application Server administrator credentials that you provided in the WebSphere Application Server administrative console.

   **Tip:** The **-password** parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command.

6. If you are switching the user registry for a system that has been used for a while by multiple users, clean up the users and groups that are related to the security configuration. See “Switching the user registry configuration for a system in use” on page 53.

7. Restart WebSphere Application Server. In a clustered installation, start the Deployment Manager, and then the node agents and application servers.

   After WebSphere Application Server is restarted, during the InfoSphere Information Server initialization, the WebSphere Application Server user registry configuration is checked and the InfoSphere Information Server user registry configuration is automatically adjusted if needed. The default
WebSphere Application Server administrator user is also automatically configured as the initial new InfoSphere Information Server default administrator user.

8. If one of the node agents was not running when you did the previous steps, the node agent cannot be restarted because the user registry configuration at the Deployment Manager and node levels do not match. To fix this problem, run the WebSphere Application Server `syncNode` command to synchronize the node with the Deployment manager. To run the `syncNode` command:
   a. Log in to the node.
   b. Run the `syncNode` command.

   ```
   /opt/IBM/WebSphere/AppServer/profiles/custom_profile/bin/syncNode.sh
   dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password
   ```

   ```
   C:\IBM\WebSphere\AppServer\profiles\custom_profile\bin\syncNode
   dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password
   ```

   In the command:
   • `dmgr_hostname` is the host name of the computer where the Deployment Manager is running.
   • `dmgr_port` is the port number of the Deployment Manager (the default is 8879).
   • `was_admin_username` is the user name of the WebSphere Application Server administrator.
   • `was_admin_password` is the administrator password.
   c. Restart the node agent. See “Starting IBM WebSphere Application Server (Windows)” on page 235 or “Starting IBM WebSphere Application Server (Linux, UNIX)” on page 238.

What to do next

After you change the user registry, you can use the WebSphere Application Server administrator user name and password to log in to the InfoSphere Information Server Web console. In the console, grant suite administrator access to additional users as needed. The WebSphere Application Server administrator is granted InfoSphere Information Server administrator privileges by default.

LDAP distinguished name (DN) determination:

To configure IBM InfoSphere Information Server to use a lightweight directory access protocol (LDAP) user registry, you might need the full LDAP distinguished name (DN) of the suite administrator. If you cannot get the LDAP DN from your LDAP administrator, you can use these procedures to determine the LDAP DN.

Determining an LDAP distinguished name (DN) by using the IBM WebSphere Application Server Administrative Console:

You can determine a full LDAP distinguished name (DN) by using the WebSphere Application Server administrative console.

Procedure
1. Log in to the IBM WebSphere Application Server administrative console.
2. From the console, select **Applications > Application Types > WebSphere enterprise applications**.
3. Click an application name.
4. Under Detail properties, click **Security role to user/group mapping**.
5. Select a role and click **Map Users**.
6. In the **Search String** field, enter an asterisk (*) and click **Search**.

Determining an LDAP distinguished name (DN) by using Active Directory search (Windows):

If you have access to a Microsoft Windows computer that is registered with a Windows Active Directory domain, you can use the user search feature to determine a Windows Active Directory distinguished name.

**Procedure**
1. On the computer, click **Start > Run**.
2. In the window, type `compmgmt.msc` and press Enter.
3. Expand Local Users and Groups.
4. Open the **Groups** folder and double-click one of the groups.
5. In the Properties window, click **Add**.
6. In the Select Users window, click **Advanced**.
7. In the Select Users window, search for the IBM WebSphere Application Server user name. You must select the X500 name in the attributes to display the full distinguished name. The search returns the full distinguished name.

**Switching back to the internal user registry**

If necessary, after configuring the IBM InfoSphere Information Server suite to use an external user registry, you can switch back to the internal user registry. The internal user registry is the user registry that was configured during the initial installation of InfoSphere Information Server.

**Before you begin**
- In an IBM WebSphere Application Server stand-alone installation, WebSphere Application Server must be running.
- In a clustered installation, the Deployment Manager and all node agents must be running.
- See the WebSphere Application Server documentation for more information:

**Procedure**

The internal user registry is an IBM WebSphere Application Server custom user registry.

1. Log in to the computer on which the **DirectoryAdmin** tool is installed:
   - If you have implemented WebSphere Application Server clustering for your installation, log in to the computer that hosts the WebSphere Application Server Deployment Manager.
If you have not implemented clustering, log in to the services tier computer.

2. From the command line, run the following command to create the WebSphere Application Server default administrator in the internal user registry:

   Linux
   /opt/IBM/InformationServer/ASBServer/bin/DirectoryAdmin.sh -user
   -userid was_admin_username -password was_admin_password -admin

   Windows
   C:\IBM\InformationServer\ASBServer\bin\DirectoryAdmin.bat -user
   -userid was_admin_username -password was_admin_password -admin

   In the command, was_admin_username and was_admin_password are the user name and password of the new WebSphere Application Server administrator. This account is the administrator from the newly configured internal user registry.

3. Log in to the WebSphere Application Server administrative console.

4. In the console, click Security > Secure administration, applications, and infrastructure.
   In WebSphere Application Server, click Security > Global Security.

5. Ensure that the Use domain-qualified user names option is not selected.

6. In the User account repository section, click the Available realm definitions list and select Standalone custom registry.

7. Click Configure.

8. In the Primary administrative user name field, enter the administrator username that you specified in the command in step 2.

9. Ensure that the custom registry class name is the following string:
   com.ibm.is.isf.j2ee.impl.was.security.WASCustomUserRegistry

10. Click Apply.

11. Select Server identity that is stored in the repository.

12. In the Server user ID or administrative user on a Version 6.0.x node field, type the short name of the user account that you created in step 2.

13. In the Password field, type the password of the user account that you specified in the command in step 2.

14. Click OK.

15. In the User account repository section, click the Available realm definitions list and select Standalone custom registry.

16. Click Set as current. If an error occurs, the application server is unable to authenticate with the internal user registry by using the credentials that you provided.

17. Click Apply and then click Save.

18. Log out of the console.

19. Stop WebSphere Application Server. In a clustered installation, stop the application servers and the node agents, and then stop the Deployment Manager.

   **Important**: When stopping the WebSphere Application Server processes, use the credentials of the WebSphere Application Server administrator from the previous user registry.

20. Log in to the computer on which the AppServerAdmin tool is installed. This tool is on the same computer as the DirectoryAdmin tool.
21. From the command line, run the **AppServerAdmin** command. This command propagates the WebSphere Application Server administrator user name and password to WebSphere Application Server.

   **Linux**
   /opt/IBM/Information/server/ASBServer/bin/AppServerAdmin.sh -was
   -user was_admin_user_id -password was_admin_password

   **Windows**
   C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -was
   -user was_admin_user_id -password was_admin_password

   In the command, **was_admin_user_id** and **was_admin_password** must match the credentials that you provided in the WebSphere Application Server Administrative Console.

   **Tip:** The **-password** parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command.

22. If you are switching the user registry for a system that has been used for a while by multiple users, clean up the users and groups that are related to the security configuration. See “Switching the user registry configuration for a system in use” on page 53.

23. Restart WebSphere Application Server. In a clustered installation, start the Deployment Manager, and then the node agents and application servers.

24. If one of the node agents was not running when you did the previous steps, the node agent cannot be restarted. The user registry configuration at the Deployment Manager and node levels do not match. To fix this problem, run the WebSphere Application Server **syncNode** command to synchronize the node with the Deployment manager. To run the **syncNode** command:
   a. Log in to the node.
   b. Run the **syncNode** command.

   **Linux**
   /opt/IBM/WebSphere/AppServer/profiles/custom_profile/bin/syncNode.sh
   dmgr_hostname dmgr_port -user was_admin_username -password
   was_admin_password

   **Windows**
   C:\IBM\WebSphere\AppServer\profiles\custom_profile\bin\syncNode
   dmgr_hostname dmgr_port -user was_admin_username -password
   was_admin_password

   In the command:
   • **dmgr_hostname** is the host name of the computer where the Deployment Manager is running.
   • **dmgr_port** is the port number of the Deployment Manager (default is 8879).
   • **was_admin_username** is the user name of the WebSphere Application Server administrator.
   • **was_admin_password** is the administrator password.

   c. Restart the node agent. See “Starting IBM WebSphere Application Server (Windows)” on page 235 and “Starting IBM WebSphere Application Server (Linux, UNIX)” on page 238.

25. Check the WebSphere Application Server log files to ensure that there are no errors.
What to do next

The administrator account is also automatically configured as the initial new InfoSphere Information Server default administrator.

After the user registry configuration change, you can open the InfoSphere Information Server Web console, create new users, and grant them roles.

Switching the user registry configuration for a system in use

If you switch the user registry after the system has been used for a while by multiple users, you must clean up the security repository as part of the user registry change. If you switch the user registry immediately after installation, you do not have to do this procedure.

About this task

If you must switch the user registry, do the registry switch immediately after installing the software if possible, before you do any additional security configuration tasks. If you must switch the user registry at a later time, do this procedure to clean up all previous security configuration settings. Settings include role assignments, credential mappings, and access rights. These settings are deleted from the repository. You must configure the settings again manually for the new users of the new registry.

If you must change the user registry after the system has been in production, consider instead migrating to a new installation to avoid any security issues and risks. Otherwise, a mismatch might occur between the users of the old and new user registries.

Procedure

1. Perform the procedure to switch the user registry. Stop the procedure at the point where you are directed back to this procedure. For user registry switching procedures, see “User registry configuration” on page 34.

2. Log in to the computer on which the DirectoryAdmin tool is installed:
   - If you have implemented WebSphere Application Server clustering within your installation, log in to the computer that hosts the WebSphere Application Server Deployment Manager.
   - If you have not implemented clustering, log in to the services tier computer.

3. From the command line, run the following command to clean up all of the groups that are related to the security configuration:

   Windows
   C:\IBM\InformationServer\ASBServer\bin\DirectoryAdmin.bat -delete_groups

   Linux
   /opt/IBM/InformationServer/ASBServer/bin/DirectoryAdmin.sh -delete_groups

4. From the command line, run the following command to clean up all of the users related to the security configuration:

   Windows
   C:\IBM\InformationServer\ASBServer\bin\DirectoryAdmin.bat -delete_users

   Linux
   /opt/IBM/InformationServer/ASBServer/bin/DirectoryAdmin.sh -delete_users

5. If you switch to the InfoSphere Information Server internal user registry, run the following command from the command line again:
Windows
C:\IBM\InformationServer\ASBServer\bin\DirectoryAdmin.bat -user -userid was_admin_username -password was_admin_password

Linux
/opt/IBM/InformationServer/ASBServer/bin/DirectoryAdmin.sh -user -userid was_admin_username -password was_admin_password

You can provide the password as plain text or as a string that has been encrypted with the encrypt command.

6. Complete the remainder of the user registry switching procedure.

User and group creation

Create users as the first level of security. You must create a user for each person who will log in to IBM InfoSphere Information Server.

If the InfoSphere Information Server internal user registry is used, you can create users and groups by using the InfoSphere Information Server console or the InfoSphere Information Server Web console. The InfoSphere Information Server console is available with IBM InfoSphere Information Analyzer and InfoSphere Information Services Director. The InfoSphere Information Server Web console is available to all InfoSphere Information Server users with the SuiteUser role.

If you are using an external user registry, such as the local operating system user registry or Lightweight Directory Access Protocol (LDAP), you must create users and groups by using the user registry administration tools. You cannot create users and groups in external user registries by using the InfoSphere Information Server consoles.

Default and preconfigured users

In addition to users that you create, several default or preconfigured users are created by you or for you during the installation process.

Accounts must be created for the administrator users for IBM InfoSphere Information Server and IBM WebSphere Application Server. These users are typically called "isadmin" and "wasadmin." You can choose to create them during installation. The accounts must be created in the user registry that is used by WebSphere Application Server.

<table>
<thead>
<tr>
<th>Sample user name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isadmin</td>
<td>InfoSphere Information Server administrator</td>
</tr>
<tr>
<td>wasadmin</td>
<td>WebSphere Application Server administrator and InfoSphere Information Server administrator</td>
</tr>
</tbody>
</table>

Table 5. Services tier users

There must be at least one user account for the engine. This user ID is typically called “dsadm.” You can choose to create this account during installation. It must be created in the user registry that is used by the engine. This user registry can be the local operating system user registry. Alternatively, the user registry can be an external user registry. This external user registry must be configured through Pluggable Authentication Modules (PAM). PAM must run on the operating system of the computer that is hosting the engine.
Table 6. Engine tier users

<table>
<thead>
<tr>
<th>Sample user name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsadm</td>
<td>IBM InfoSphere DataStage administrator</td>
</tr>
</tbody>
</table>

There are several other users that you must define. The following users must be local operating system users where the metadata repository tier is installed. You can choose to create these accounts during installation:

- If you use IBM DB2 for the metadata repository:
  - You must have a DB2 instance owner. This user is the owner of the DB2 database management system. This user is typically called "db2admin" in Microsoft Windows installations, and "dasusr1" in Linux and UNIX installations.
  - You must have a non-fenced instance user. This user is typically called "db2inst1".
  - You must have a fenced user. This user is typically called "db2fenc1".
- All installations must have an owner for the metadata repository database within the database management system. This account is typically called "xmeta."
- IBM InfoSphere Information Analyzer installations must have an owner for the information analysis database within the database management system. This account is typically called "iauser."

Table 7. Additional users

<table>
<thead>
<tr>
<th>Sample user name (Windows)</th>
<th>Sample user name (Linux, UNIX)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db2admin</td>
<td>dasusr1</td>
<td>DB2 instance owner (only required if you are using DB2 to host the metadata repository database or analysis database)</td>
</tr>
<tr>
<td>N/A</td>
<td>db2inst1</td>
<td>DB2 non-fenced instance user (only required if you are using DB2 to host the metadata repository database or analysis database)</td>
</tr>
<tr>
<td>N/A</td>
<td>db2fenc1</td>
<td>DB2 fenced user (only required if you are using DB2 to host the metadata repository database or analysis database)</td>
</tr>
<tr>
<td>xmeta</td>
<td>xmeta</td>
<td>Metadata repository database owner</td>
</tr>
<tr>
<td>iauuser</td>
<td>iauuser</td>
<td>Information analysis database owner</td>
</tr>
</tbody>
</table>

Creating users in the IBM InfoSphere Information Server console

If the IBM InfoSphere Information Server internal user registry is used, you can create users as the first level of security. You must create a user for each person that needs to log in to InfoSphere Information Server.

Before you begin

- You must have IBM InfoSphere Information Analyzer or InfoSphere Information Services Director installed.
- You must have Administrator authority.
Procedure
1. On the **Home** navigator menu, select **Configuration** > **Users**.
2. In the Tasks pane, click **New User**.
3. In the New User pane, specify information about the user. The **User Name**, **Password**, **Confirm Password**, **First Name (Given Name)**, and **Last Name (Family Name)** fields are required.
4. In the Suite pane, specify the rights for the user.
5. In the Suite Component pane, select whether the user has any suite component roles. You must add at least one suite component role for each suite component that you want the user to access. For example, if you are creating a user that will access IBM InfoSphere Information Analyzer, you must assign the Information Analyzer Project Administrator, Data Administrator, or User role.
6. Optional: In the Groups pane, click **Browse** to add the user to a group.
   a. In the Add Groups window, select the group that you want to add the user to.
   b. Click **Add**.
   c. Click **OK** to close the window.
7. Click **Save** > **Save and Close**.

What to do next

After you create users, you can add the users to new or existing projects.

Creating groups in the IBM InfoSphere Information Server console

If the IBM InfoSphere Information Server internal user registry is used, you can create user groups and assign security settings and roles to the groups. All users that belong to a group automatically inherit the security settings and roles that are assigned to the group.

Before you begin

- You must have IBM InfoSphere Information Analyzer or InfoSphere Information Services Director installed.
- You must have Administrator authority.

Procedure
1. On the **Home** navigator menu, select **Configuration** > **Groups**.
2. On the Groups workspace, click **New Group** on the Tasks pane.
3. Specify information about the group. The **ID** and the **Group Name** fields are required.
4. In the Suite pane, specify the rights for the group.
5. In the Suite Component pane, select whether the group has any suite component roles. You must add at least one suite component role for each suite component that you want the group of users to access. For example, if you are creating a group that will access IBM InfoSphere Information Analyzer, you must assign the Information Analyzer Project Administrator, Data Administrator, or User role.
6. Optional: In the Users pane, click **Browse** to add users to the group.
   a. In the Add Users window, select the user that you want to add to the group.
   b. Click **Add**.
c. Click OK to close the window.
7. Click Save > Save and Close.

What to do next

After you create groups, you can add the groups to new or existing projects.

Adding users to a group in the IBM InfoSphere Information Server console

If the IBM InfoSphere Information Server internal user registry is used, you can add users to a group to quickly assign and reassign user roles.

Before you begin

You must have IBM InfoSphere Information Analyzer or InfoSphere Information Services Director installed.

Procedure

1. On the Home navigator menu, select Configuration > Groups.
2. In the Groups workspace, select a group.
3. In the Task pane, click Open.
4. In the Users pane, click Browse.
5. In the Add Users window, select the users that you want to add to the group.
6. Click Add.
7. Click OK to save your choices and to close the Add Users window.
8. Click Save > Save and Close to save the assignments.

Creating users in the IBM InfoSphere Information Server Web console

If the IBM InfoSphere Information Server internal user registry is used, you can create users as the first level of security. You must create a user for each person that needs to log in to InfoSphere Information Server.

Before you begin

You must have suite administrator authority.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Users and Groups > Users.
3. In the Users pane, click New User.
4. In the Create New User pane, provide information about the user.
5. In the Roles pane, specify whether the user is an administrator and user of the suite or a user of the suite.
6. In the Suite Component pane, select whether the user has any suite component roles. To log in to any of the product modules, a user must have the suite user role. Also add at least one suite component role for each suite component that you want the user to access. For example, if you are creating a user that will access IBM InfoSphere Information Analyzer, you must assign the suite user role, and also the Information Analyzer Project Administrator, Data Administrator, or User role.
7. Click **Save and Close** to save the user information in the metadata repository.

**Creating groups in the IBM InfoSphere Information Server Web console**

If the IBM InfoSphere Information Server internal user registry is used, you can create user groups and assign security settings and roles to the groups. All users that belong to a group automatically inherit the security settings and roles that are assigned to the group.

**Before you begin**

You must have suite administrator authority.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Users and Groups > Groups**.
3. In the Groups pane, click **New Group**.
4. In the Create New Group pane, provide information for the group.
5. Optional: In the Roles pane, specify whether the group has administrator and user privileges in the suite or user privileges in the suite.
6. Optional: In the Suite Component pane, select whether the group has any suite component roles. You must add at least one suite component role for each suite component that you want the users in the group to access. For example, if you are creating a group for users that are to access IBM InfoSphere Information Analyzer, you must assign the Information Analyzer Project Administrator, Data Administrator, or User role.
7. Assign users to the group.
   a. In the Users pane, click **Browse**.
   b. In the Search for Users window, type a name in the search fields and click **Filter**. To view all users, click **Clear Filter**.
   c. Select the users that you want to assign to the group.
   d. Click **OK** to save your choices and close the Search for Users window.
8. Click **Save and Close** to save the group.

**Adding users to a group in the IBM InfoSphere Information Server Web console**

If the IBM InfoSphere Information Server internal user registry is used, you can add users to a group to quickly assign and reassign user roles.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Users and Groups > Groups**.
3. In the Groups pane, select a group and click **Open Group**.
4. In the Users pane, click **Browse**.
5. In the Search for Users window, locate the users that you want to add to the group.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To search for a user by name:</td>
<td>Type a name in the search fields and click Filter.</td>
</tr>
<tr>
<td>To view all users:</td>
<td>Do not enter any text in the fields and click Clear Filter.</td>
</tr>
</tbody>
</table>

6. Select the users that you want to assign to the group.
7. Click OK to save your choices and close the Search for Users window.
8. Click Save and Close to save the assignments.

Permissions and groups configuration (Windows Server 2008)

After you install IBM InfoSphere Information Server on Microsoft Windows 2008 Server, you must perform an additional task to configure users.

About this task

Which task you use depends on whether Microsoft Windows Server 2008 is configured to be a domain controller.

The first time that a user of an InfoSphere Information Server client, such as the IBM InfoSphere DataStage client or the IBM InfoSphere Information Server console, successfully logs in to the InfoSphere Information Server services tier, the server is added to the registered-servers.xml file. This file is located in the C:\IBM\InformationServer\ASBNode\eclipse\plugins\com.ibm.isf.client. directory by default.

When logging in to the services tier for the first time, the operating system user on the client must have write permission to the registered-servers.xml file on the client so that it can be updated. If the user does not have the required permission, the login fails.

System administrators can limit access to specific InfoSphere Information Server services tiers from any client by removing the file system write permission to the registered-servers.xml file. The administrator, or anyone who has write permission, can log in ahead of time to each server that the client user will access. The administrator can then distribute the prepopulated registered-servers.xml file to the remaining clients in their network. To set or remove file system write permission, see “Configuring write permission to the registered-servers.xml file” on page 62.

Configuring permissions and groups (Windows Server 2008):

You must complete these tasks to configure users and groups to access to IBM InfoSphere Information Server. This configuration is required only for the engine tier computer. This configuration is only applicable to the users of the operating system where the engine tier components are installed.

Procedure
2. Create a group.
   a. Click Start > Control Panel > Administrative Tools > Computer Management.
   b. In the Computer Management window, expand System Tools > Local Users and Groups > Groups.
c. Click **Action > New Group**.

d. In the New Group window, type **DataStage** as the name for the group, click **Create**, and click **Close**.

3. Configure users and the DataStage group to log in.
   a. Click **Start > Control Panel > Administrative Tools > Local Security Policy**.
   b. In the Local Security Settings window, expand **Local Policies > User Rights Assignment** to display the policies.
   c. In the Local Security window, click the **Allow log on Locally** policy and click **Actions > Properties**.
   d. In the Allow log on Locally Properties window, click **Add User or Group**.
   e. In the Select Users or Groups window, click **Locations**, click the name of your local computer, and click **OK**.
   f. In the Select Users or Groups window, click **Advanced** and click **Find Now**.
   g. In the search results, select **Authenticated Users** and **DataStage** and click **OK** three times to save the results and to return to the Local Security window.
   h. In the Local Security window, click the **Log on as a Batch Job** policy and click **Actions > Properties**.
   i. In the Log on as a Batch Job window, click **Add User or Group**.
   j. In the Select Users or Groups window, click **Locations**, click the name of your local computer, and click **OK**.
   k. In the Select Users or Groups window, click **Advanced**, and then click **Find Now**.
   l. In the search results, select **DataStage** and click **OK** three times to save the results and to return to the Local Security window.
   m. Close the Local Security Policy window.

4. Add users to the group.
   a. From the Computer Management window, click **Groups**.
   b. Click the name of the group that you want to add users to (DataStage).
   c. Click **Action > Add to Group**.
   d. In the User Properties window, click **Add**.
   e. In the Select Users or Groups window, click **Location**.
   f. Click the name of your local computer, and then click **OK**.
   g. In the Select Users window, click **Advanced**.
   h. In the window that opens, click **Find Now**.
   i. Click the names of users that you want to include in the group, and click **OK**. At a minimum, include all authenticated users.
   j. Click **OK** three times to return to the Computer Management window.
   k. Close the Computer Management window.

5. Set permissions for the following folders:
   - C:\IBM\InformationServer\Server
   - C:\Program Files\MKS Toolkit\fifos
   - C:\Windows\%TEMP%
   - C:\tmp

Complete the following steps for each of the listed folders.
   a. Select the folder and click **File > Properties**.
b. In the Properties window, click the **Security** tab, and click **Edit**.

c. In the Permissions window, click **Add**.

d. In the Select Users or Groups window, click **Locations**.

e. Click the name of the local computer, and click **OK**.

f. In the Select Users or Groups window, click **Advanced**.

  g. In the window that opens, click **Find Now**.

h. Click the name of the group that you want to set permissions for (DataStage).

  i. Click **OK** twice.

  j. In the Permissions list, select to allow Modify, Read & execute, List folder contents, Read, and Write Permissions. Click **OK**.

  k. If you receive a message that asks you to confirm the changes, click **Apply changes to this folder, subfolders and files**.

**Configuring permissions and groups (Windows Server 2008 domain controller):**

If Microsoft Windows Server 2008 is a domain controller, you must complete these tasks to configure users and groups to access IBM InfoSphere Information Server. This configuration is required only for the engine tier computer and is only applicable to the users of the operating system where the engine tier components are installed.

**Procedure**

Because you cannot add the built-in authenticated users group to a group that you create in steps b and c, you might prefer to skip steps b and c and use the authenticated users group directly.


2. Create a group.

   a. Click **Start > Control Panel > Administrative Tools > Active Directory and Computers**.

   b. In the Active Directory and Computers window, click **Users** in the current domain.

   c. In the window that opens, click **Action > New Group**.

   d. In the New Group window, type **DataStage** as the name for the group.

   e. Leave **Group scope** as **Global** and **Group type** as **Security**.

   f. Click **OK**

3. Configure the server to allow local users and the DataStage group to log in.

   a. Click **Start > Control Panel > Administrative Tools > Domain Security Policy**.

   b. In the Domain Security Policy window, expand **Local Policies > User Rights Assignment** to display the policies.

   c. In the Domain Security window, click the **Allow log on Locally** policy, and click **Actions > Properties**.

   d. In the Allow log on Locally Properties window, click **Add User or Group**.

   e. Click **Browse**.

   f. In the Select Users, Computers, or Groups window, click **Advanced** and then click **Find Now**.

   g. In the search results, click **Authenticated Users** and **DataStage**, and then click **OK** three times to return to the Domain Security Policy window.
In the Domain Security window, click the **Log on as a Batch Job** policy, and click **Actions > Properties**.

In the Log on as a Batch Job window, click **Add User or Group**.

Click **Browse**.

In the Select Users, Computers, or Groups window, click **Advanced** and then click **Find Now**.

In the search results, click **DataStage** and click **OK** three times to return to the Domain Security Policy window.

Close the Domain Security Policy window.

### Add users to the group.

a. In the Users in the current domain window, click the name of the group that you want to add users to (DataStage), and click **OK**. Authenticated users are not available.

b. Click **Action > Properties**.

c. In the Properties window, click the **Members** tab, and then click **Add**.

d. In the window that opens, click **Advanced**, and then click **Find Now**.

e. Click the names of users that you want to add to the group, and then click **OK**. Authenticated users are not available.

f. Click **OK** two times to save your results and to return to the Active Directory and Computers window.

g. Close the Active Directory and Computers window.

### Set permissions for the following folders:

- C:\IBM\InformationServer\Server
- C:\Program Files\MKS Toolkit\fifos
- C:\Windows\%TEMP%
- C:\tmp

Complete the following steps for each of the listed folders.

a. Select the folder and click **File > Properties**.

b. In the Properties window, click the **Security** tab, and click **Edit**.

c. In the Permissions window, click **Add**.

d. In the Select Users, Computers, or Groups window, click **Locations**.

e. In the window that opens, click **Advanced**, and then click **Find Now**.

f. Click the name of the group that you want to set permissions for (DataStage).

g. Click **OK** twice.

h. In the Permissions list, select to allow Modify, Read & execute, List folder contents, Read, and Write Permissions. Click **OK**.

i. If you receive a message to confirm your changes, confirm by clicking **Apply changes to this folder, subfolders and files**.

### Configuring write permission to the registered-servers.xml file:

The first time that a given services tier is accessed from a given client system, the user that is currently logged into the operating system must have write permission to the **registered-servers.xml** file to allow the application to add the host name and port of the client system to the file. Once the information is added, any subsequent login by any user by any InfoSphere Information Server application on the client system only requires read access to the file.
About this task

When an InfoSphere Information Server client application logs into a services tier for the first time, the application adds the services tier host name and port to the local registered-servers.xml file. This file contains the list of services tiers to be displayed as choices for subsequent client logins.

By default, administrators have write permission to the registered-servers.xml file. Write permission for the Users group must also be added for the application to access the file.

Procedure

To give the Users group write permission to the file:

- **Windows XP**
  1. In Microsoft Windows Explorer, locate the registered-servers.xml file. By default, this file is located in the following directory: C:\IBM\InformationServer\ASBNode\eclipse\plugins\com.ibm.isf.client
  2. Right-click the file and select **Properties**
  3. In the Properties window, click the **Security** tab.
  4. Click **Add**.
  5. In the Select Users or Groups window, click **Locations**.
  6. Select the name of your local computer and click **OK**.
  7. In the Select Users or Groups window, click **Advanced**.
  8. Click **Find Now** and select the Users group.
  9. Click **OK** twice.
  10. With the Users group selected, click **Allow** for the Write permission, and click **OK**.
  11. If you receive a message to confirm your changes, confirm by clicking **Apply changes to this folder, subfolders and files**.

- **Windows 2008 and Windows 7**
  1. In Microsoft Windows Explorer, locate the registered-servers.xml file. By default, this file is located in the following directory: C:\IBM\InformationServer\ASBNode\eclipse\plugins\com.ibm.isf.client
  2. Right-click the file and select **Properties**
  3. In the Properties window, click the **Security** tab.
  4. Click **Edit**.
  5. In the Permissions window, click **Add**.
  6. In the Select window, click **Locations**.
  7. Select the name of your local computer and click **OK**.
  8. In the Select window, click **Advanced**.
  9. Click **Find Now** and select the Users group.
  10. Click **OK** twice.
  11. With the Users group selected, click **Allow** for the Write permission, and click **OK**.
  12. If you receive a message to confirm your changes, confirm by clicking **Apply changes to this folder, subfolders and files**.
Assigning user roles

IBM InfoSphere Information Server supports role-based access control. User roles determine which features users can use. For some suite components, user roles also determine which projects a user can access.

User roles can be defined at several levels that build on one another. Users derive authority from the combination of their role in InfoSphere Information Server (their suite roles), their role in the suite component (for example, IBM InfoSphere Information Analyzer or IBM InfoSphere FastTrack), and the permissions they have to work in a given project (their project roles).

Suite

Suite-level roles are the basic roles that users need to access any part of InfoSphere Information Server. Users who are not Suite Users cannot authenticate with InfoSphere Information Server. All InfoSphere Information Server users must have the Suite User role. A suite user can also have the Suite Administrator role to complete administration tasks. Users with the Suite Administrator role must also have the Suite User role assigned to their user names.

The common metadata component roles are also suite-level roles. These roles have certain authority over metadata in the metadata repository.

Component

Component-level roles provide access to the features of a specific product module. Users can be users or administrators of a product module. For example, you can be an InfoSphere Information Analyzer user and an IBM InfoSphere DataStage administrator.

Project

Project-level roles are defined in the product module and by the product module. For example, in an information analysis project in the IBM InfoSphere Information Server console, you can assign a user the Information Analyzer Data Steward role for that project.

Assigning user roles

Typically, an InfoSphere Information Server administrator assigns suite-level roles and component-level roles. Both roles are assigned by using the IBM InfoSphere Information Server console or IBM InfoSphere Information Server Web console. The InfoSphere Information Server console is available with IBM InfoSphere Information Analyzer and InfoSphere Information Services Director. The InfoSphere Information Server Web console is available to all InfoSphere Information Server users with the SuiteUser role.

After the security roles are configured, the administrator of each product module further defines the project-level roles in the IBM InfoSphere Information Server console or the IBM InfoSphere DataStage and QualityStage Administrator client. To perform the actions of a particular project-level role, a user must also have suite-level access and access to the product module that owns the project. For example, to be an InfoSphere DataStage developer, a user must be assigned the roles of suite user and component-level InfoSphere DataStage, as well as the InfoSphere DataStage developer project role.
Security role overview
IBM InfoSphere Information Server supports role-based access control. Users derive authority from the union of their roles in InfoSphere Information Server (the suite roles), their roles in the suite component, such as IBM InfoSphere Information Analyzer (the suite component roles), and the projects that they work with (the project roles).

Security configuration is performed by two levels of administrators:

**InfoSphere Information Server administrators**
These administrators are in charge of assigning the suite and suite component roles to users. These roles determine which suite components the user can access and whether the user has component administrator or component user access in those suite components. InfoSphere Information Server administrators can also configure credential mappings for InfoSphere Information Analyzer, IBM InfoSphere DataStage, and IBM InfoSphere QualityStage users. InfoSphere Information Server administrators must have, at least, the Suite Administrator and Suite User role assigned to their user names. During installation, a default InfoSphere Information Server administrator is created to perform the initial installation tasks and configure the user registry. The default IBM WebSphere Application Server administrator is always automatically configured as an InfoSphere Information Server administrator when you restart IBM WebSphere Application Server.

**InfoSphere Information Server suite component administrators**
These administrators are in charge of assigning the component project roles to the users that were configured by the InfoSphere Information Server administrator. These assignments are configured in the suite component. For example, the InfoSphere Information Server component administrator can assign the Information Analyzer Business Analyst role to a user in the information analysis screens of the console. For InfoSphere DataStage projects, these role assignments are configured in the InfoSphere DataStage Administrator client. The InfoSphere DataStage and QualityStage administrators can also use the IBM InfoSphere Information Server Web console to configure credential mappings.

**Suite roles**

**Suite User**
Identifies which users in the user registry have general access to InfoSphere Information Server and the suite components. A user must have this role to authenticate with InfoSphere Information Server or any of the suite components.

**Suite Administrator**
Provides InfoSphere Information Server administration privileges to the user. The Suite Administrator role includes additional permissions; however, the Suite User role must also be assigned to the user for it to authenticate.

The common metadata roles are also suite roles. See “Common metadata roles” on page 69.

The following figure shows the InfoSphere Information Server security roles.
IBM InfoSphere FastTrack roles:

For IBM InfoSphere FastTrack, administrators can further define user authority by assigning suite component roles to InfoSphere FastTrack users.

Suite component roles

FastTrack Project Administrator
The InfoSphere FastTrack Project Administrator can create and manage projects, and manage user and group access to projects.

FastTrack User
An InfoSphere FastTrack User can use InfoSphere FastTrack functions. Users must be authorized to projects before they can use functions for creating, managing, and viewing mapping specifications.

IBM InfoSphere Metadata Workbench roles:

The suite administrator assigns roles that define the tasks that users of IBM InfoSphere Metadata Workbench can perform.

IBM InfoSphere Metadata Workbench has the following roles:

Metadata Workbench Administrator
Runs the automated and manual analysis services, publishes queries, and explores metadata models. Performs all tasks that IBM InfoSphere Metadata Workbench users can perform.
The Metadata Workbench administrator must be familiar with the enterprise database metadata and data file metadata that is imported into the repository. The administrator must also be familiar with the metadata that is used in jobs.

**Metadata Workbench User**
Finds and explores information assets, runs analysis reports, and creates, saves, and runs queries.

**IBM InfoSphere Business Glossary roles:**
For IBM InfoSphere Business Glossary, administrators can further define user authority by assigning suite component roles to InfoSphere Business Glossary users.

**Suite component roles**

**Business Glossary Administrator**
Can set up and administer the glossary so that other users can find and analyze the information that they need. Can also create stewards from users and groups.

**Business Glossary Author**
Can create and edit terms and categories, including assigning assets in the metadata repository to terms.

**Business Glossary User**
Can examine the terms and categories in the glossary, and the assets in the metadata repository.

**Business Glossary Basic User**
Can examine the terms and categories in the glossary, but cannot examine the assets in the metadata repository.

**Business Glossary Asset Assigner**
Assigns assets in the metadata repository to glossary terms and categories from other products in the InfoSphere Information Server suite.

**IBM InfoSphere DataStage and IBM InfoSphere QualityStage roles:**
For InfoSphere DataStage and InfoSphere QualityStage, administrators can further define user authority by assigning suite component and project roles to InfoSphere DataStage and InfoSphere QualityStage users.

You can assign suite component roles in the console or the Web console. Project roles can be assigned only in the Permissions page of the IBM InfoSphere DataStage Administrator client.

**Suite component roles**

**DataStage and QualityStage Administrator**
Can perform the following tasks:
- Assign project roles to InfoSphere DataStage suite users in the InfoSphere DataStage Administrator client
- Use the Administrator client to create, delete, and configure projects
- Mark projects as protected
- Unprotect protected projects
- Issue server engine commands
• Use the Designer client to create and edit jobs and other objects
• Use the Director client to run and schedule jobs
• View the entire job log messages
• Import objects into protected projects

With this role, the user cannot edit jobs or other objects in protected projects.

DataStage and QualityStage User
Provides access to InfoSphere DataStage and InfoSphere QualityStage. Additionally, this role is used to filter the lists of users and groups that are shown in the InfoSphere DataStage Administrator client. If an IBM InfoSphere Information Server user does not have this role, that user cannot access any of the InfoSphere DataStage or InfoSphere QualityStage product modules, even if that user has InfoSphere DataStage or InfoSphere QualityStage project roles assigned to the user name.

Project roles

DataStage Developer
Can perform the following tasks:
• Use the Designer client to create and edit jobs and other objects
• Use the Director client to run and schedule jobs
• View entire job log messages

With this role, the user can also use the Administrator client to perform limited tasks including changing project NLS settings and changing project properties (not protect/unprotect).

With this role, the user cannot edit jobs or other objects in protected projects, create, delete, or configure projects (can perform limited configuration tasks), mark existing projects as protected, unprotect protected projects, assign project roles to InfoSphere DataStage suite users in the Administrator client, or import objects into protected projects.

DataStage Production Manager
Can perform the following tasks:
• Mark existing projects as protected
• Unprotect protected projects
• Use the Designer client to create and edit jobs and other objects
• Use the Director client to run and schedule jobs
• View entire job log messages
• Import objects into protected projects

With this role, users can also use the InfoSphere DataStage Administrator client to perform limited tasks including changing the project NLS settings, issuing server engine commands, and changing project properties.

With this role, users cannot edit jobs or other objects in protected projects. In addition, the role cannot create, delete, or configure projects (except for limited configuration tasks), or assign project roles to InfoSphere DataStage suite users in the Administrator client.

DataStage Operator
Can perform the following tasks:
• Use the Director client to run and schedule jobs
• View entire job log messages (unless set to read first line only by InfoSphere DataStage Administrator)

With this role, users can also use the Administrator client to perform limited tasks including changing project NLS settings and changing project properties (not protect/unprotect).

DataStage Super Operator

Can perform the following tasks:
• Use the Director client to run and schedule jobs
• View entire job log messages
• Use the Designer client to view jobs and view objects

This role can also use the Administrator client to perform limited tasks including changing project NLS settings and changing project properties (not protect/unprotect).

With this role, users cannot use the Designer client to create and edit jobs and other objects, edit jobs or other objects in protected projects, create, delete or configure projects, mark existing projects as protected, unprotect protected projects, assign project roles to InfoSphere DataStage suite users in the Administrator client, or import objects into protected projects.

For more information, see the IBM InfoSphere DataStage and QualityStage Administrator Client Guide.

Operational metadata roles:

You can assign operational metadata component roles to a user.

Suite component roles

Operational Metadata Administrator

Can import operational metadata into the repository. You can assign this role to a suite user and edit the runimporter.cfg file to include the user name and password of that user. When you run the runimporter file, it uses those credentials to allow the user to import operational metadata into the repository.

Operational Metadata Analyst

Can create and run reports on operational metadata in the Reporting tab of the Web console.

Operational Metadata User

Can view reports on operational metadata.

Common metadata roles:

You can assign common metadata component roles to a user.

Suite component roles

Common Metadata User

Uses the Repository Management tab of InfoSphere Metadata Asset Manager to browse, search for, and inspect assets that are in the metadata repository.

Common Metadata Importer

On the Import tab of InfoSphere Metadata Asset Manager, creates import areas, imports to the staging area, analyzes, previews, and shares imports.
to the metadata repository and performs all other tasks. Views and works in only those import areas that this user creates. Uses the Repository Management tab to browse, search for, and inspect assets that are in the metadata repository.

**Common Metadata Administrator**

On the Administration tab of InfoSphere Metadata Asset Manager, specifies import policies and configures metadata interchange servers. On the Import tab, creates import areas, imports to the staging area, analyzes, previews, and imports to the metadata repository. Can view and work in all import areas. On the Repository Management tab, merges and deletes assets and sets implementation relationships. Additionally, has all the privileges of the Common Metadata User and the Common Metadata Importer.

On the istool command line, exports, imports, and deletes common metadata assets.

**Common data rule roles:**

You can assign data rule roles to a user.

**Suite component roles**

**Rule Administrator**

Sets up and administers who can access and run data rules and rule sets, so that other users can find and run data rules and rule sets for projects.

**Rule Author**

Provides the ability to author data rule definitions and rule set definitions.

**Rule Manager**

Manages the creation and organization of data rules and rule sets. This role manages who can create data rule definitions, rule set definitions, and metrics, as well as who can run data rules, rule sets, and metrics.

**Rule User**

Provides the ability to run data rules and rule sets.

**IBM InfoSphere Information Analyzer roles:**

For IBM InfoSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to InfoSphere Information Analyzer users.

You can assign suite component roles in the IBM InfoSphere Information Server console or the IBM InfoSphere Information Server Web console. Project roles can be assigned only in the Project Properties workspace of the console.

**Suite component roles**

**Information Analyzer Data Administrator**

Can import metadata, modify analysis settings, and add and modify system sources.

**Information Analyzer Project Administrator**

Can administer projects by creating, deleting, and modifying information analysis projects.
Information Analyzer User
Can log on to InfoSphere Information Analyzer, view the dashboard, and open a project.

Project roles

Information Analyzer Business Analyst
Reviews analysis results. With this role, users can set baselines and checkpoints for baseline analysis, publish analysis results, delete analysis results, and view the results of analysis jobs.

Information Analyzer Data Operator
Manages data analyses and logs. With this role, users can run or schedule all analysis jobs.

Information Analyzer Data Steward
Provides read-only views of analysis results. With this role, users can also view the results of all analysis jobs.

Information Analyzer DrillDown User
Provides the ability to drill down into source data if drill down security is enabled.

IBM InfoSphere Information Services Director roles:

For IBM InfoSphere Information Services Director, administrators can further define user authority by assigning suite component roles and project roles to InfoSphere Information Services Director users.

Suite component roles

Information Services Director Catalog Manager
Provides full access to the Information Services Catalog tab including the ability to manage and modify services categories, services, and custom attributes. The InfoSphere Information Services Director Administrator is automatically granted Information Services Catalog Manager authority.

Information Services Director Administrator
Provides access to all of the InfoSphere Information Services Director functions.

Information Services Director Consumer
Provides ability to invoke secured services.

Information Services Director Operator
Provides access to the InfoSphere Information Services Director runtime functions. An operator can add and remove providers as well as configure runtime parameters of a deployed application, service and operation. In addition, an operator can deploy applications from the design time view.

Information Services Director User
Provides access to view a list of applications in the runtime environment and view information on the Information Services Catalog tab. This user can browse deployed applications, services, operations, and providers.

Project roles

Information Services Director Designer
With the Information Services Director Designer role, users can access only projects that it is authorized for at design time. At the project level at design time, the ISD Designer can:
• View project details and the list of projects
• View the list of applications
• Update applications
• Export applications
• Import services into an existing application
• View, add, or remove services.

At run time, the Information Services Director Designer can view the list of applications.

**Information Services Director Project Administrator**

Provides access to create and delete applications, add and remove users and groups to projects, and edit project properties.

**IBM InfoSphere Data Quality Console roles:**

InfoSphere Information Server administrators define user authority by assigning suite component roles to IBM InfoSphere Data Quality Console users. The user role determines the tasks that a user can complete and what the user sees on each page of the data quality console.

You can assign suite component roles in the IBM InfoSphere Information Server console or the IBM InfoSphere Information Server Web console.

**Suite component roles**

**Administrator**

Administrators ensure that exception information is collected and shown in the data quality console. They also maintain the activity log.

**Review manager**

Review managers track all of the exception descriptors in the data quality console and assign exception descriptors to reviewers.

**Reviewer**

Reviewers track the exceptions that are associated with the exception descriptors that are assigned to them.

**Business steward**

Business stewards view exceptions to track the data quality of business entities such as implemented data resources.

**Assigning security roles in the IBM InfoSphere Information Server console**

To create a secure project environment, you can define a security policy that is based on user authentication and role identification. Users derive authority from the union of their individual and group roles.

**Before you begin**

You must have IBM InfoSphere Information Analyzer or InfoSphere Information Services Director installed to use the InfoSphere Information Server console.

**About this task**

In the InfoSphere Information Server console, you can specify which roles users can perform in the suite. You can further define which suite components the users have access to and what their roles are in those suite components.
Assigning security roles to a user in the IBM InfoSphere Information Server console:

All users require authorization to access components and features of the IBM InfoSphere Information Server. You can assign one or more suite and suite component roles to a user.

Before you begin

You must have suite administrator authority.

About this task

Changing the roles that are assigned to a user does not affect any currently active sessions for that user. The new role assignments will only be available the next time the user logs in. You can use session administration to disconnect the user and force the user to log in again.

Procedure

1. On the Home navigator menu, select Configuration > Users.
2. In the Users workspace, select a user.
3. In the Task pane, click Assign Roles.
4. In the Roles pane, select a suite role to assign to the user.
5. In the Suite Component pane, select one or more suite component roles to assign to the user.
6. Click Save > Save and Close to save the authorizations in the metadata repository.

What to do next

Certain suite components, such as IBM InfoSphere DataStage and IBM InfoSphere Information Analyzer, also require that you assign additional user roles in the clients or projects.

Assigning security roles to a group in the IBM InfoSphere Information Server console:

You can assign one or more suite and suite component roles to a group of users.

Before you begin

You must have suite administrator authority.

About this task

Changing the roles that are assigned to a group does not affect any currently active sessions for the users in that group. The new role assignments will only be available the next time the users log in. You can use session administration to disconnect the users and force the users to log in again.

Procedure

1. On the Home navigator menu, select Configuration > Groups.
2. In the Groups workspace, select a group.
3. In the Task pane, click Assign Roles.
4. In the Roles pane, select a suite role to assign to the group.
5. In the Suite Component pane, select one or more suite component roles to assign to the group.
6. Click Save > Save and Close to save the authorizations in the metadata repository.

**Viewing the roles that are assigned to a user or a group:**

In the IBM InfoSphere Information Server console, you can view the suite and suite component roles that are assigned to a user or group. If an administrator assigned project roles to the user or group, you can also view the project roles.

**Before you begin**

You must have suite administrator authority.

**Procedure**

1. On the Home navigator menu, select Configuration > Users, or select Configuration > Groups.
2. Select a user or group and click Open.
3. In the Roles pane, view the list of assigned suite, suite component, or assigned project roles. Project roles are assigned in the context of a project in IBM InfoSphere DataStage, or in the IBM InfoSphere Information Server console.

**Assigning users to a project and assigning roles**

When you create a project, you can specify which users can access that project. You can also specify which actions users can perform in that project.

**About this task**

To add users to a project and assign roles, you use different tools. The tool you use depends upon the product module in which you are working:

- For IBM InfoSphere Information Analyzer and IBM InfoSphere Information Services Director, use the IBM InfoSphere Information Server console as described in this procedure.
- For IBM InfoSphere DataStage and IBM InfoSphere QualityStage, use the IBM InfoSphere DataStage and QualityStage Administrator. See the IBM InfoSphere DataStage and QualityStage Administrator Client Guide.
- For IBM InfoSphere FastTrack, use the IBM InfoSphere FastTrack console. See the IBM InfoSphere FastTrack Tutorial.

**Procedure**

1. In the IBM InfoSphere Information Server console, open the project that you want to assign users and roles to.
2. On the Overview navigator menu in the IBM InfoSphere Information Server console, select Project Properties.
3. On the Project Properties workspace, select the Users tab.
4. In the Users pane, click Browse to add users to the project.
5. On the Add Users window, select the users that you want to add to the project, click Add, then click OK.
6. On the Project Roles pane, select a project role to assign to the selected user. A user can be assigned one or more roles in a project.
7. Click **Save All**.

**Assigning groups to a project and specifying roles**

When you create a project, you can specify which groups can access that project. You can also specify which actions they can perform in that project.

**About this task**

To assign groups to a project and select roles, you use different tools. The tool you use depends on the product module in which you are working:

- For IBM InfoSphere Information Analyzer and IBM InfoSphere Information Services Director, use the IBM InfoSphere Information Server console as described in this procedure.
- For IBM InfoSphere DataStage and IBM InfoSphere QualityStage, use the IBM InfoSphere DataStage and QualityStage Administrator. See the **IBM InfoSphere DataStage and QualityStage Administrator Client Guide**.
- For IBM InfoSphere FastTrack, use the IBM InfoSphere FastTrack console. See the IBM InfoSphere FastTrack Tutorial.

**Procedure**

1. In the IBM InfoSphere Information Server console, open the project that you want to assign groups to.
2. On the **Overview** navigator menu in the IBM InfoSphere Information Server console, select **Project Properties**.
3. On the Project Properties workspace, select the **Groups** tab.
4. In the Groups pane, click **Browse** to add groups to the project.
5. On the Add Groups window, select the groups that you want to add to the project, click **Add**, then click **OK**.
6. On the Project Roles pane, select a role to assign to the selected group. A group can be assigned one or more roles in a project.
7. Click **Save All**.

**Assigning security roles in the IBM InfoSphere Information Server Web console**

To create a secure project environment, you define a security policy that is based on user authentication and roles. Users derive authority from the union of their individual and group roles.

**About this task**

In the IBM InfoSphere Information Server Web console, you can specify which roles users can perform in the suite. You can further define which suite components the users have access to and what their roles are in those suite components.

**Assigning security roles to a user in the IBM InfoSphere Information Server Web console:**

All users require authorization to access components and features of IBM InfoSphere Information Server. You can assign one or more suite and suite component roles to a user.
Before you begin

You must have suite administrator authority.

About this task

Changing the roles that are assigned to a user does not affect any currently active sessions for that user. The new role assignments will only be available the next time the user logs in. You can use session administration to disconnect the user and force the user to log in again.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Users and Groups > Users**.
3. In the Users pane, select a user and click **Open User**.

   **Note:** You can assign roles to more than one user at a time by clicking **Add Roles to Multiple Users**.

4. In the Roles pane, select a suite role to assign to the user.
5. In the Suite Component pane, select one or more suite component roles to assign to the user.
6. Click **Save and Close** to save the authorizations in the metadata repository.

What to do next

Certain suite components, such as IBM InfoSphere DataStage and IBM InfoSphere Information Analyzer, also require that you assign additional user roles in the clients or projects.

Assigning security roles to a group in the IBM InfoSphere Information Server Web console:

You can assign one or more suite and suite component roles to a group of users.

Before you begin

You must have suite administrator authority.

About this task

Changing the roles that are assigned to a group does not affect any currently active sessions for the users in that group. The new role assignments will only be available the next time the users log in. You can use session administration to disconnect the users and force the users to log in again.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Users and Groups > Groups**.
3. In the Users pane, select a group and click **Open Group**.

   **Note:** To assign roles to more than one group at a time, click **Add Roles to Multiple Groups**.
4. In the Roles pane, select a suite role to assign to the group.
5. In the Suite Component pane, select one or more suite component roles to
assign to the group.
6. Click Save and Close to save the authorizations in the metadata repository.

What to do next

Certain suite components, such as IBM InfoSphere DataStage and IBM InfoSphere
Information Analyzer, also require that you assign additional group roles in the
clients or projects.

Viewing the roles that are assigned to a user or a group:

You can view the suite and suite component roles that are assigned to a user or
group. If an administrator assigned project roles to the user or group, you can also
view the project roles.

Before you begin

You must have suite administrator authority.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the
   Administration tab.
2. In the Navigation pane
   • Select Users and Groups > Users.
   • Or, select Users and Groups > Groups.
3. Select a user or group.
4. Click Open User or Open Group.
5. In the Roles pane, view the list of assigned suites, suite component, or project
   roles. Project roles are assigned in the context of a project in IBM InfoSphere
   DataStage or in the IBM InfoSphere Information Server console.

Engine security configuration

The IBM InfoSphere Information Server engine performs user authentication
separately from other InfoSphere Information Server components. Depending upon
your user registry configuration, you might have to map credentials between the
InfoSphere Information Server user registry and the local operating system user
registry on the computer where the engine is installed.

IBM InfoSphere DataStage, IBM InfoSphere QualityStage, and IBM InfoSphere
Information Analyzer require access to the engine and require that engine
credentials be configured.

The InfoSphere Information Server engine requires valid user credentials for each
InfoSphere Information Server user that needs to access the engine. User
credentials are stored in a user registry.

If the InfoSphere Information Server engine can share the user registry that
InfoSphere Information Server uses, the user credentials for both InfoSphere
Information Server and the engine can come from this user registry. If the user
registry cannot be shared, you must create a mapping between credentials in the
user registry that InfoSphere Information Server uses and valid user credentials that exist in the local operating system user registry on the computer where the engine is installed.

The services tier and the engine can share a local operating system user registry if they are installed on the same computer. If they are installed on separate computers, they can share an external user registry such as a Lightweight Directory Access Protocol (LDAP) or Windows Active Directory user registry. The services tier and the engine cannot share the InfoSphere Information Server internal user registry.

In an installation with more than one InfoSphere Information Server engine, you choose the authentication method on a per InfoSphere Information Server engine basis.

**Credential mapping overview**
If IBM InfoSphere Information Server and the InfoSphere Information Server engine do not share the user registry, you must create a mapping between credentials in the user registry that InfoSphere Information Server uses and user credentials that exist in the local operating system user registry on the engine tier computer.

After you have configured the shared user registry, use the IBM InfoSphere Information Server Web console to indicate the new configuration to InfoSphere Information Server.

Do these tasks to map credentials.

After you share the user registry or define credential mappings, you must give your users access to IBM InfoSphere DataStage and IBM InfoSphere QualityStage.

**Shared user registry overview**
If you configure IBM InfoSphere Information Server to use an external user registry, you might be able to share the user registry between InfoSphere Information Server and the InfoSphere Information Server engine.

Sharing the user registry allows IBM WebSphere Application Server, InfoSphere Information Server, and the InfoSphere Information Server engine to access the same user names, passwords, and group definitions. When the user registry is shared, authentication to the engine occurs silently by using the same credentials (user ID and password) that the user uses to authenticate with InfoSphere Information Server. In this mode, no credential mapping is required.

You can share the user registry in any of the following scenarios:

- The engine tier and the services tier are installed on the same computer, and InfoSphere Information Server is configured to use the local operating system user registry. In this case, they can share the local operating system user registry.

**Note:** Sharing of the local operating system user registry is not supported in installations that include WebSphere Application Server clustering.

- The engine tier and the services tier are installed on separate computers, but both use the same Lightweight Directory Access Protocol (LDAP) user registry for authentication. In this scenario, you must configure Pluggable Authentication Module (PAM) on the engine tier computer.
The engine tier and the services tier are installed on separate computers, but both use the same Microsoft Windows Active Directory user registry (which is an LDAP user registry) for authentication.

The engine tier and the services tier are installed on separate computers, but the computers are within the same domain. This configuration may have performance issues, and is not recommended.

**Note:** This configuration is not supported in installations that include WebSphere Application Server clustering.

If the engine tier and services tier cannot share a user registry, you must create a mapping between credentials in the user registry that InfoSphere Information Server is using and valid user credentials that exist in the local operating system user registry on the computer where the engine is installed.

The engine tier cannot use the InfoSphere Information Server internal user registry. If InfoSphere Information Server is configured to use the internal user registry, you must configure credential mapping.

The following figure shows a configuration in which the engine tier and services tier are installed on the same computer. They both share the local operating system user registry. Specifically, the InfoSphere Information Server engine is configured to use the local operating system user registry. InfoSphere Information Server is configured to use the WebSphere Application Server user registry and then access the same operating system user registry.
The following figure shows a configuration in which the engine tier and services tier are installed on separate UNIX computers. They both share a common LDAP user registry. Specifically, the InfoSphere Information Server engine is configured to use the LDAP user registry. InfoSphere Information Server is configured to use the WebSphere Application Server user registry and then access the LDAP user registry. To provide the interface between the engine and the LDAP user registry, Pluggable Authentication Module (PAM) is configured on the engine tier computer.

Figure 20. Example of architecture that uses a shared local operating system user registry

The following figure shows a configuration in which the engine tier and services tier are installed on separate UNIX computers. They both share a common LDAP user registry. Specifically, the InfoSphere Information Server engine is configured to use the LDAP user registry. InfoSphere Information Server is configured to use the WebSphere Application Server user registry and then access the LDAP user registry. To provide the interface between the engine and the LDAP user registry, Pluggable Authentication Module (PAM) is configured on the engine tier computer.
After you share the user registry, you must still grant the engine tier operating system users the required permissions. See Permissions and groups configuration.

**Credential mapping overview**

If IBM InfoSphere Information Server and the InfoSphere Information Server engine do not share the user registry, you must create a mapping between credentials in the user registry that InfoSphere Information Server uses and user credentials that exist in the local operating system user registry on the engine tier computer.

You must use credential mapping in the following scenarios:

- InfoSphere Information Server is configured to use the internal user registry. The InfoSphere Information Server engine cannot use the internal user registry.
- Linux UNIX The services tier and engine tier are installed on separate computers. They do not share a user registry.
- Windows The services tier and engine tier are installed on separate computers. The computers are not in the same domain.

The credential mappings are stored with the internal user registry in the metadata repository. The passwords are strongly encrypted for increased security.

You can create individual user mappings, so that each InfoSphere Information Server user is associated with exactly one engine user. You also can create a default user mapping, so that all InfoSphere Information Server users who do not have individual credential mappings can access the engine through a shared user name.
In the following figure, the services tier and engine tier are installed on the same computer. However, InfoSphere Information Server is configured to use the internal user registry. Because the engine tier computer cannot use this user registry, credential mapping is configured between the internal user registry and the local operating system user registry.

In the following figure, the services tier and engine tier are installed on separate computers. InfoSphere Information Server is configured to use the local operating system user registry. Since the engine tier computer cannot share this user registry, credential mapping is configured between the local operating system user registry on the services tier computer and the local operating system user registry on the engine tier computer.
Indicating to InfoSphere Information Server that the user registry is shared

After you have configured the shared user registry, use the IBM InfoSphere Information Server Web console to indicate the new configuration to InfoSphere Information Server.

Before you begin

- You must have suite administrator authority.
- You must ensure that the user registry that you are sharing is the same for both the services tier and the engine tier, and that no credential mapping is required.

Procedure

1. In the InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Domain Management > Engine Credentials.
3. Select the InfoSphere Information Server engine that you have configured to use the same user registry as InfoSphere Information Server.
4. Click Open Configuration.
5. In the configuration pane, select **Share User Registry between InfoSphere Information Server and its engine**.

6. Click **Save and Close**.

**What to do next**

Grant your users access to IBM InfoSphere DataStage and IBM InfoSphere QualityStage. After you indicate to InfoSphere Information Server that the user registry is shared, all credential mapping menus are disabled and you do not need to define any additional mappings. The same user name and password that is used to log in to InfoSphere Information Server is used to run data integration jobs in the engine.

**Credential mapping**

Do these tasks to map credentials.

An administrator can perform credential mappings for a group of users. Alternatively, users can map their own credentials. The following table describes the credential mapping-related tasks that different types of users can complete:

*Table 8. Credential mapping-related tasks for different user types*

<table>
<thead>
<tr>
<th>User type</th>
<th>Permitted credential mapping-related tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoSphere Information Server suite administrators, IBM InfoSphere DataStage administrators, and IBM InfoSphere QualityStage administrators</td>
<td>These users can define default engine tier operating system credentials to use for all users that are trying to connect to InfoSphere Information Server engine and that do not have a specific credential mapping defined. For each individual InfoSphere Information Server user, these administrators can define specific engine tier operating system credentials to map to the InfoSphere Information Server user credentials.</td>
</tr>
<tr>
<td>InfoSphere DataStage and InfoSphere QualityStage users</td>
<td>These users can define their own credential mappings in the Web console. Users can only define credentials for their user names.</td>
</tr>
</tbody>
</table>

**Defining default credentials:**

You can define a default user name and password for the suite to map to each user’s engine tier operating system user credentials.

**Before you begin**

You must have suite administrator authority or IBM InfoSphere DataStage and IBM InfoSphere QualityStage administrator authority.

**About this task**

The default credentials are used for any users who do not have their own credential mappings. If you do not want users who do not have mapped credentials to access the server, do not add default mapping credentials.
Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigator pane, select Domain Management > Engine Credentials.
3. Select the InfoSphere Information Server engine for which you want to specify the default credentials.
4. Click Open Configuration.
5. In the User Name field, type the user name to be used by all InfoSphere Information Server users for whom a specific mapping is not defined.
6. In the Password field, type the corresponding password. The user name and password that you provide must be a valid user name and password for the operating system where the engine tier components are installed.
7. Confirm the password.
8. Click Save and Close.

Configuring your credentials:
As a suite administrator or suite user, you can map the credentials for your own user account.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Domain Management > Engine Credentials.
3. Select the InfoSphere Information Server engine that you want to configure.
4. Click Open My Credentials.
5. Type the user name and password that you want to use to connect to the IBM InfoSphere Information Server engine. The user name and password that you provide must be a valid user name and password for the operating system where the engine tier components are installed.
6. Click Save and Close.

Mapping user credentials:
You can map one or more user credentials to engine tier operating system user credentials.

About this task
If you use the IBM InfoSphere Information Server user registry, you must create credential mappings before you can use IBM InfoSphere DataStage and IBM InfoSphere QualityStage clients. Create users and groups in the Web console before you begin this task.

Suite users can configure their own credential mappings.

Procedure
1. Log in to the IBM InfoSphere Information Server Web console by using Administrator credentials.
2. On the Administration tab, expand the Domain Management section and click Engine Credentials.
3. Select the InfoSphere Information Server engine for which you want to map user credentials.

4. Click **Open User Credentials**.

5. Click **Browse** to search for suite users.

6. Optional: Specify additional search criteria, and click **Filter** to display a list of users.

7. From the search results, select the suite users that you want to map to the engine tier operating system local credentials and click **OK**.

8. On the Map User Credentials pane, select one or more users to map to the credentials. If you want to map some suite users to one user and map other suite users to a different user, select one subset of users and continue.

9. In the Assign User Credentials pane, specify the local operating system user credentials. The user name and password that you provide must be a valid user name and password for the operating system where the engine tier components are installed. If you want to preserve credential mappings that users have already configured, select the **Apply Only to Users without Credentials** check box.

10. Click **Apply**.

11. To map credentials for additional suite users, do one of the following:
   - Repeat steps 8 through 10 to map credentials for additional users displayed in the Map User Credentials pane.
   - Repeat steps 5 through 10 to select from a new filtered list of users and map credentials for those users.

**What to do next**

After you map the credentials, any suite user or group that is assigned an IBM InfoSphere DataStage and QualityStage user or administrator security role can log in to an InfoSphere DataStage and QualityStage client.

**Granting access to IBM InfoSphere DataStage and QualityStage users**

After you share the user registry or define credential mappings, you must give your users access to IBM InfoSphere DataStage and IBM InfoSphere QualityStage.

**Procedure**

1. Ensure that the operating system user has the proper file access permissions to InfoSphere DataStage, InfoSphere QualityStage, and the relevant files.

   When you create, compile, or import a job in InfoSphere DataStage, files are created using the operating system user on the engine that the InfoSphere Information Server user is mapped to. The InfoSphere DataStage engine processes are run with a umask set to 002; therefore, files are created with write permission to the primary group of the operating system user. If you later need to update, compile, or re-import the job with another user, it will fail if the operating system user that the user is mapped to is not in the same primary group as the last operating system user that updated the job. Therefore, all credential-mapped operating system users to be used to update or import jobs should belong to the same primary group.

2. Grant the required suite and suite component roles to the user in the Web console.

   a. Using a role that has administrative privileges, log in to the IBM InfoSphere Information Server Web console.
b. Select the Administration tab.
c. In the Navigation pane, select Users and Groups > Users.
d. Select the user that you want to grant access to and click Open User.
e. In the Roles pane, assign the following roles to the user.

**Suite User**
Required for all users in order to log in to any of the suite components.

**DataStage and QualityStage User**
Required for any user in order log in to any of the InfoSphere DataStage and InfoSphere QualityStage product modules.

**DataStage and QualityStage Administrator**
Optional. Grants full access to all projects and the administrative capability of InfoSphere DataStage and InfoSphere QualityStage.

3. If you did not grant the DataStage and QualityStage Administrator authority, you must use the IBM InfoSphere DataStage and QualityStage Administrator client to grant project level roles to the user. If the user has only the DataStage and QualityStage user role and no specific project roles, that user cannot log in to the InfoSphere DataStage clients.

**Configuring WebSphere Application Server for non-root administration (Linux, UNIX)**

By default, the IBM WebSphere Application Server runs as root. However, it can also be run by using a non-root user ID. The following instructions describe the steps required to configure and set appropriate file system permissions for WebSphere Application Server to run as a non-root user ID.

You must rerun the post-installation steps (go to “Running post-installation commands to enable non-root administration (Linux, UNIX)” on page 89) after either of the following actions:

- You install any add-on components, fix packs, or patches to the services tier. Certain installations might have changed permissions.
- If any of the application servers were restarted as the root user and you want them to be started again as the non-root user. Certain files might now have root ownership and must be changed.

**Restrictions**

- If you are using the local operating system as the user registry, WebSphere Application Server must be run as root. WebSphere Application Server must be run as root in this case, because of system permissions that are required for credential checking.
- If the IBM InfoSphere Information Server services tier is configured to use PAM authentication and a local operating system PAM module is used in the PAM configuration, such as the /etc/passwd and /etc/group files, then WebSphere Application Server must be run as root. When a local operating system PAM module is not configured, WebSphere Application Server can be run as non-root as long as the non-root user has read permission on the configured files.
- WebSphere Application Server must be run as root when installing patches, fix packs, and upgrades. When running the installation program or Update Installer, make sure to first restart WebSphere Application Server to run as root. When preparing to run an installation process, if WebSphere Application Server is running as a non-root user, you might need to first stop WebSphere Application Server.
Server while logged in as that non-root user. You can then log in as root, start WebSphere Application Server as root, and then start the installation program or Update Installer.

- The task of starting and stopping WebSphere Application Server must be designated to one non-root user only.

  The user who starts WebSphere Application Server must also be the user who stops WebSphere Application Server. Therefore, as preparation for any installations, after WebSphere has already been configured for running as a non-root user and is started by that non-root user, you must first stop WebSphere Application Server while logged in as the configured non-root user. When WebSphere Application Server is stopped, log in as root and restart WebSphere Application Server before starting any InfoSphere Information Server installations.

- Avoid assigning the dsadm user to manage WebSphere Application Server. Using the dsadm user to manage WebSphere Application Server might cause overwrite issues for the InfoSphere Information Server environment settings. The non-root user selected for running WebSphere must not source dsenv.

Setting up a new non-root user for WebSphere Application Server (Linux, UNIX)

If you have IBM InfoSphere Information Server installed, you can create a user who can manage WebSphere Application Server processes. These steps need to be completed only once.

Before you begin

Make sure to read the restrictions in "Configuring WebSphere Application Server for non-root administration (Linux, UNIX)" on page 87.

Important: Before you begin this task, back up your system so that the backup can be used to restore the original state if necessary. See Chapter 13, “Backing up and restoring IBM InfoSphere Information Server,” on page 211.

About this task

The general purpose in these instructions is to transfer the ownership of some of the files under WebSphere Application Server and InfoSphere Information Server to the new non-root user, at which point the new user would be able to take over the management of the WebSphere Application Server process. This one-time setup task describes the steps for creating the user. The post installation instructions describe the steps that must be performed after every installation action.

These steps use wasadmin as the new non-root user. However, this is just an example user name; you can use any user name that you want, or use an existing user.

You must be a system administrator with root access.

Procedure

1. Create the wasadmin user by running the command:
   ```
   useradd -m -d /home/wasadmin wasadmin
   ```

   Note: If you are using an existing user, replace instances of wasadmin with your selected user name.

2. Set the umask of this user to 0022 by typing: umask 0022
What to do next

Proceed to the post-installation tasks for either a stand-alone environment or cluster environment to configure the settings in InfoSphere Information Server for the non-root user: "(Stand-alone environment) Running post-installation commands to enable non-root administration (Linux, UNIX)" or "(Cluster environment) Running post-installation commands to enable non-root administration (Linux, UNIX)" on page 91.

Running post-installation commands to enable non-root administration (Linux, UNIX)

After installing IBM InfoSphere Information Server or adding components, patches, or fix packs, run these commands to enable non-root administration. The steps differ depending upon whether IBM WebSphere Application Server is set up in a clustered configuration or stand-alone configuration.

(Stand-alone environment) Running post-installation commands to enable non-root administration (Linux, UNIX):

You must run these tasks every time you install IBM InfoSphere Information Server where IBM WebSphere Application Server is set up in a stand-alone configuration. You must also run these tasks after you install any new add-on components, patches, or fix packs in this configuration. If you are installing an InfoSphere Information Server engine or client patch, the following instructions do not apply. You must also run these tasks any time the application server is restarted as the root user and you now want to start it again as the non-root user.

Before you begin

- If you have more than one patch or add-on InfoSphere Information Server product to install, install all the patches and add-on products before you begin these steps. When running the installation program or Update Installer, make sure to first restart IBM WebSphere Application Server to be running under root.
- If WebSphere Application Server was previously configured for non-root administration and is running under the non-root user, you might need to first stop WebSphere Application Server while logged in as the non-root user. You can then log in as root and start WebSphere Application Server under root before starting the installation.
- Stop all InfoSphere Information Server processes, including WebSphere Application Server, the server engine, JobMonApp, logging, and ASB agents. See “Shutting down services (Linux, UNIX)” on page 232.
  - The applications should be stopped while logged in as the user who started the application.
  - If WebSphere Application Server is already running as a non-root user, you must log in as that non-root user to stop WebSphere Application Server.
  - If the ASB and logging agents are started as root, you must log in as root to stop the agents.

About this task

- These steps apply to stand-alone (non-cluster) environments only. If you have a cluster configuration, see "(Cluster environment) Running post-installation commands to enable non-root administration (Linux, UNIX)" on page 91.
The non-root user name, wasadmin, is an example that is used throughout the documentation. If you have a different non-root user name, make sure to use that one instead and replace every instance of wasadmin in the commands that you run.

Procedure

1. Remove *.jar and *.lck files from the temporary directory by running the commands:

   Note: The operating system-defined temporary directory, tmp, is either /tmp or /var/tmp. Change the file path below accordingly.

   ```
   rm /tmp/*.jar
   rm /tmp/*.lck
   ```

2. If WB_vrdata or BG_vrdata exist in the temporary directory, run the following commands:

   Note: The OS-defined temporary directory, tmp, is either /tmp or /var/tmp. Change the file path below accordingly.

   ```
   rm -rf /tmp/WB__vrdata
   rm -rf /tmp/BG__vrdata
   ```

3. Either wasadmin must be a member of the group assigned to the Reporting workspace directories and below with rwx permission, or you must set wasadmin as the owner of the Reporting workspace directories and below.

   Note: If you relocated the Reporting workspace directory as described in the technote http://www.ibm.com/support/docview.wss?rs=14&uid=swg21317914 assign appropriate permissions to that directory instead.

   Run the commands to set the wasadmin user as the owner of the Reporting workspace directories:

   ```
   cd /tmp
   chown -R wasadmin informationServer
   ```

   Note: Where the temporary directory, tmp, is either /tmp or /var/tmp as defined by the operating system.

   Note: If your system was configured to relocate the temporary directory used by IBM InfoSphere Business Glossary or IBM InfoSphere Metadata Workbench as described in the following technote, follow the instructions in the following technote to assure that appropriate permissions are assigned to the WB__vrdata and BG__vrdata directories: http://www.ibm.com/support/docview.wss?rs=3291&uid=swg21413637

4. Run the commands to set wasadmin as the owner of the InfoSphere Information Server profile of WebSphere Application Server:

   ```
   cd WAS_installation_path/profiles
   chown -R wasadmin InfoSphere
   ```

   Note: Where WAS_installation_path is the path where WebSphere Application Server is installed. The default installation path is /opt/IBM/WebSphere/AppServer. InfoSphere is the default name for the InfoSphere Information Server
profile installed under WebSphere Application Server. If you installed InfoSphere Information Server to a profile name other than InfoSphere, use that profile name instead.

5. Run the commands below to enable the non-root user to successfully run MetadataServer.sh to start WebSphere Application Server.

```
cd IS_installation_path/ASBServer
chmod 755 bin

cd bin

# if the log doesn't exist, create it
touch startMetadataServer.log

chown wasadmin startMetadataServer.log

cd ../conf
chown wasadmin MetadataServer.info
```

6. Start the WebSphere Application Server process as wasadmin and start all InfoSphere Information Server processes. See "Starting services (Linux, UNIX)" on page 237.

**Important:** When you restart InfoSphere Information Server processes, LoggingAgent and ASBAgent are started as root. To configure these agents as the non-root user, you must complete the following procedure: "Starting IBM InfoSphere Information Server node agents as a non-root user" on page 95.

If the agents are ever started by root and then are started by a non-root user, you must delete the process output files, such as *.out and *.err files that are located in the IS_installation_path/ASBNode and IS_installation_path/ASBNode/bin folders, to allow the new owners of the agent processes to regenerate those output files. This could have occurred during an installation process if the agents also had been configured to run under a non-root user and were restarted as root during the installation.

What to do next

Now, you can configure WebSphere Application Server to start as the non-root user during a system restart. See "Configuring WebSphere Application Server to start as the non-root user during a system restart (Linux, UNIX)" on page 94.

(Cluster environment) Running post-installation commands to enable non-root administration (Linux, UNIX):

You must run these tasks every time you install IBM InfoSphere Information Server and after you install any new add-on components, patches, or fix packs. If you are installing an InfoSphere Information Server engine or client patch, the following instructions do not apply. You must also run these tasks any time the application server, nodeagent, or deployment manager is restarted as the root user and you now want to start it again as the non-root user.

**Before you begin**

- If you have more than one patch or add-on InfoSphere Information Server product to install, install all the patches and add-on products before you begin these steps. When running the installation program or Update Installer, make sure to first restart all IBM WebSphere Application Server processes to be running under root. If WebSphere Application Server was previously configured for non-root administration and is running under the non-root user, you might need to first stop all WebSphere Application Server processes while logged in as
the non-root user. You can then log in as root and start all WebSphere Application Server processes under root before starting the installation.

- Stop all InfoSphere Information Server processes, including WebSphere Application Server, the server engine, JobMonApp, logging, and ASB agents. See “Shutting down services (Linux, UNIX)” on page 232.
  - The applications should be stopped while logged in as the user who started the application.
  - If WebSphere Application Server is already running as a non-root user, you must log in as that non-root user to stop WebSphere Application Server.
  - If the ASB and logging agents are started as root, you must log in as root to stop the agents.

About this task
- These steps apply to cluster environments only. If you have a stand-alone (non-clustered) configuration, see “(Stand-alone environment) Running post-installation commands to enable non-root administration (Linux, UNIX)” on page 89.
- The non-root user name, wasadmin, is an example that is used throughout the documentation. If you have a different non-root user name, make sure to use that one instead and replace every instance of wasadmin in the commands that you run.
- This procedure must be repeated on all systems where IBM WebSphere Application Server Network Deployment is installed. This includes the computer that hosts the Deployment Manager and the computers that host the various managed nodes.

Procedure
1. Remove *.jar and *.lck files from the temporary directory by running the commands:

   **Note:** The operating system-defined temporary directory, tmp, is either /tmp or /var/tmp. Change the file path below accordingly.

   ```
   rm /tmp/*.jar
   rm /tmp/*.lck
   ```

2. If WB_vrdata or BG_vrdata exist in the temporary directory, run the following commands:

   **Note:** The operating system-defined temporary directory, tmp, is either /tmp or /var/tmp. Change the file path below accordingly.

   ```
   rm -rf /tmp/WB_vrdata
   rm -rf /tmp/BG_vrdata
   ```

3. Either wasadmin must be a member of the group assigned to the Reporting workspace directories and below with rwx permission, or you must set wasadmin as the owner of the Reporting workspace directories and below.

   **Note:** If you relocated the Reporting workspace directory as described in the technote [http://www.ibm.com/support/docview.wss?rs=14&uid=swg21317914](http://www.ibm.com/support/docview.wss?rs=14&uid=swg21317914)
assign appropriate permissions to that directory instead.

Run the commands to set the non-root user as the owner of the Reporting workspace directories:

```
  cd /tmp
  chown -R wasadmin informationServer
```

**Note:** The tmp temporary directory is either /tmp or /var/tmp, as defined by the operating system.

**Note:** If your system was configured to relocate the temporary directory used by IBM InfoSphere Business Glossary or IBM InfoSphere Metadata Workbench as described in the following technote, follow the instructions in the following technote to assure that appropriate permissions are assigned to the WB__vrdata and BG__vrdata directories: [http://www.ibm.com/support/docview.wss?rs=3291&uid=swg21413637](http://www.ibm.com/support/docview.wss?rs=3291&uid=swg21413637)

4. Assign wasadmin ownership to all WebSphere Application Server profiles participating in the InfoSphere Information Server cluster.

**Note:** There are multiple WebSphere Application Server profiles potentially on different machines.

a. For each profile in the cluster, run the following command to change ownership to the non-root user.

```
  cd WAS_installation_path/profiles
  chown -R wasadmin Custom01
```

*WAS_installation_path* is the path where WebSphere Application Server is installed. The default installation path is /opt/IBM/WebSphere/AppServer. *Custom01* is the default name for the InfoSphere Information Server profile installed under WebSphere Application Server. If you installed InfoSphere Information Server to a profile name other than Custom01, use that profile name instead.

Repeat this step on each custom profile. (A custom profile is a WebSphere Application Server profile that hosts a managed node.)

b. Run the commands to assign ownership to the non-root user of the Deployment Manager profile. In this example, the profile is named *Dmgr01*, but you can specify a different name.

```
  cd WAS_installation_path/profiles
  chown -R wasadmin Dmgr01
```

*WAS_installation_path* is the path where WebSphere Application Server is installed. The default installation path is /opt/IBM/WebSphere/AppServer. *Dmgr01* is the default profile name for the Deployment Manager profile.

5. Start all WebSphere Application Server processes as wasadmin user and start all InfoSphere Information Server processes. See “Starting services (Linux, UNIX)” on page 237.

**Important:** When you restart InfoSphere Information Server processes, LoggingAgent and ASBAgent are started as root. To configure these agents as the non-root user, you must follow the procedure in “Starting IBM InfoSphere Information Server node agents as a non-root user” on page 95.

If the agents are ever launched by root and then are started by a non-root user, you must delete the process output files, such as *.out* and *.err* files that are located in the IS_installation_path/ASBNode and IS_installation_path/ASBNode/bin folders, to allow the new owners of the agent processes to regenerate those output files. The situation could have occurred during an
installation process if the agents also had been configured to run under a non-root user and were restarted as root during the installation.

**Configuring WebSphere Application Server to start as the non-root user during a system restart (Linux, UNIX)**

You can configure IBM WebSphere Application Server to start as the non-root user when a system restart occurs. To set up WebSphere Application Server in this manner, locate and change the content of the ISFServer files.

**About this task**

Do this task after you have done the post-configuration steps for the first time. After you do the following steps, it is unnecessary to repeat them after new installation activities.

**Note:** This task applies to stand-alone (non-clustered) installations only.

**Procedure**

1. Find the ISFServer files that must be modified:
   - For the HP-UX operating system, use the command:
     ```
     cd /sbin
     find . -name *ISFServer*
     ```
   - For all other operating systems, use the command:
     ```
     cd /etc
     find . -name *ISFServer*
     ```

   This might return multiple files with various prefixes in the name. Some files might be links to other files and could reflect the change you made in the original file without needing to edit each file that was found. If you have multiple instances of WebSphere Application Server installed, there might be unique files for each WebSphere Application Server instance. You only have to modify the files that reference the instances of WebSphere Application Server that you have configured to start as non-root.

2. Identify the files to modify.
3. Change and save the content of these files.

**Note:** This step assumes that InfoSphere Information Server has been installed under the default installation path, /opt/IBM/InformationServer. Your actual installation path might differ.

Change the following content:

```bash
#!/bin/sh
# chkconfig: 2345 85 60
# description: Information Services Framework server.
IS_INIT_D=true;export IS_INIT_D
"/opt/IBM/InformationServer/ASBServers/bin/MetadataServer.sh" "$*
```

Change as follows:

```bash
#!/bin/sh
# chkconfig: 2345 85 60
# description: Information Services Framework server.
IS_INIT_D=true;export IS_INIT_D
/usr/bin/su - wasadmin -c "!/opt/IBM/InformationServer/ASBServers/bin/MetadataServer.sh $*"
```

**Note:** The location of your MetadataServer.sh file might be different and should reflect the location of your IBM InfoSphere Information Server installation directory.
Starting IBM InfoSphere Information Server node agents as a non-root user

The node agents (the ASB and logging agents) can be started as the IBM InfoSphere DataStage administrator user. Do this procedure after you create an installation of InfoSphere Information Server. Repeat this procedure after you add additional product modules or fix packs. You must also rerun steps 6-13 any time you have restarted the node agents as the root user and you now want to start them again as the non-root InfoSphere DataStage administrator user.

Before you begin

Before doing these steps, back up your system so that you can restore the original state if necessary. See Chapter 13, “Backing up and restoring IBM InfoSphere Information Server,” on page 211.

About this task

Do these steps on all engine tier computers. You must be a system administrator who has root access.

Instructions in this procedure use the default InfoSphere Information Server installation locations. Your path varies if you installed InfoSphere Information Server in a different location.

The following directory is the default InfoSphere Information Server installation location: /opt/IBM/InformationServer

Procedure

1. If you added additional product modules or fix packs to an existing InfoSphere Information Server installation, skip to step 6 on page 96. If you are modifying a fresh installation, continue with step 2.

2. Verify that the InfoSphere DataStage administrator account that originally installed the engine tier exists. Verify that it belongs to the InfoSphere DataStage primary group. The InfoSphere DataStage administrator account is typically named dsadm. The InfoSphere DataStage primary group is typically named dstage.

   Note: If you did not install InfoSphere DataStage or IBM InfoSphere Information Analyzer, you can choose any trusted user.

3. Make sure that the stack_hard variable in the /etc/security/limits file is set to -1 for the user that was selected in step 2.

4. Make sure that the user can write to the temporary directory.

5. Configure the node agents to start as the non-root user when a computer restarts. To do so, locate and change the content of the ISFAgents files on the engine tier computers.

   Note: The location and file name are different for each operating system, but the content of the file is the same.

   a. Find the ISFAgents file that must be modified.

      • Run this command: cd /sbin

      • Run this command: cd /etc

   b. Run the command: find . -name "*ISFAgents*"
c. Change the content of the file. The file contains information such as these lines:

```bash
#!/bin/sh
# chkconfig: 2345 85 60
# description: Information Services Framework server.
IS_INIT_D=true; export IS_INIT_D
"/opt/IBM/InformationServer/ASBNode/bin/NodeAgents.sh" "$@"
```

Change as follows:

```bash
#!/bin/sh
# chkconfig: 2345 85 60
# description: Information Services Framework server.
IS_INIT_D=true; export IS_INIT_D
/usr/bin/su - dsadm -c "/opt/IBM/InformationServer/ASBNode/bin/NodeAgents.sh $*"
```

Note: If you did not install InfoSphere DataStage or InfoSphere Information Analyzer, in place of `dsadm` in the file, specify the alternate user that was selected in step 2 on page 95.

6. Log in as a system administrator with root access.
7. Change to the `/opt/IBM/InformationServer/ASBNode/bin` directory.
8. Run this command to stop the node agents:

   ```bash
   ./NodeAgents.sh stop
   ```

   Note: If you use IBM InfoSphere Information Services Director, verify that all related jobs are stopped. Typically, stopping the node agents stops all InfoSphere Information Services Director jobs.

9. Remove any remaining root-owned *.out, *.err, and *.pid files from the `/opt/IBM/InformationServer/ASBNode` and `/opt/IBM/InformationServer/ASBNode/bin` directories. You must always complete this step before you first start the node agents as a non-root user, if you previously started the node agents as root.

10. Change the ownership of the `/opt/IBM/InformationServer/ASBNode` directory to the trusted user that was selected in step 2 on page 95. To change the ownership, run this command:

    ```bash
    chown -R user /opt/IBM/InformationServer/ASBNode
    ```

    where `user` is the trusted user.

11. Log in as dsadm or as the user that you selected in step 2 on page 95.
12. Change to the following directory:

    `/opt/IBM/InformationServer/ASBNode/bin`

13. Run the following command to start the node agents:

    ```bash
    ./NodeAgents.sh start
    ```

**What to do next**

To ensure that your system is configured correctly, run the following commands. If the commands succeed, restart your system. Then run the commands again to make sure that the startup scripts were correctly modified.

- If the default ports for logging and ASB agents are 31531 and 31533, as specified during the initial installation, run this command:

  ```bash
  netstat -a | grep 3153
  ```
If the agents are not running, you must stop and start the node agents again.

- Run the following command to verify that the agents are up and running as the specified user:
  
  ```bash
  ps -ef | grep Agent
  ```

**Audit logging configuration**

The Auditing service creates an audit trail of security-related events. These events include all security-related settings changes and user login and logout operations. You can configure which audit events to log and how much information to include based on your auditing requirements.

The auditing configuration is controlled by a properties file. You can restrict access to this properties file by using file system permission settings. This allows you to restrict the role of auditing configuration to select users or groups. Security auditing trails assist in the detection of access to controlled information and application usage. Monitoring and analysis of the logged audit information can lead to improvements in the control of data access and the prevention of malicious or careless unauthorized access to sensitive data or configuration settings. The monitoring of application and individual user access, including system administration actions, provides an historic record of activity. This information allows you to adjust user or group security roles to enable or prevent access to application features. This information can also assist in showing compliance with corporate security policies.

The following events log audit records:

- Creation and removal of users and groups
- Assignment or removal of a user from a group
- User password changes (does not log the password)
- Changes to security roles assigned to users or groups
- Changes to user or group permissions on a project and the associated project-level security roles that are assigned
- Changes to mapped engine credentials
- User login
- User logout
- Session termination
- Session timeout
- Changes to audit logging configuration settings

See “Types of audit events” on page 98 for more information about these events.

**Configuration file**

An auditing configuration file (ISAuditing.properties) is installed in the classes directory of the IBM InfoSphere Information Server profile in IBM WebSphere Application Server. The default location is WebSphere\AppServer\profiles\InfoSphere\classes. This file is where you configure which audit events are logged and how much information to retain. You can keep the auditing configuration file in its default location or you can move it to another directory. You can set file system write permissions on the file or its folder to restrict who can change the auditing configuration settings.
Audit log files

The default values in the auditing configuration file causes the audit log files to be created in the logs directory of the InfoSphere Information Server profile in IBM WebSphere Application Server. The default location is Websphere\AppServer\profiles\InfoSphere\logs with the name ISAuditLog_0.log. If the logs directory does not exist, the audit log file is created in the directory of the application server where InfoSphere Information Server is installed.

Refer to “Audit logs” on page 106 for more information about the log files.

Types of audit events

The Auditing service provides groups of events that log audit records.

The following groups of audit events are logged:

• User and group management
• User, group, and project security role assignments
• Engine credential mapping
• User session management
• Audit configuration

User and group management events:

User and group management consists of the following events: creation and removal of users and groups, user group membership changes, and user credential changes.

User and group management events can be logged only if the User Registry Configuration is set to InfoSphere Information Server User Registry. These events cannot be logged when the User Registry Configuration is set to Application Server Registry such as when configured to use LDAP or the local operating system for user authentication. Those configurations manage users and groups through external tools so that IBM InfoSphere Information Server is not involved in the management of these resources and is not aware when changes are made.

The following event messages are logged with parameters that describe the subjects that are changed or created. The (caller) indicated in each message is the user ID of the caller to this event method:

ADD_USER (caller): UserID="xxx", LastName="xxx", FirstName="xxx"

Logged when a new user is created in the InfoSphere Information Server console, Web console, or DirectoryCommand command line tool. New users created through the DirectoryAdmin command line tool on the server do not log an audit event. However, these users cannot log in to InfoSphere Information Server until they are assigned at least the SuiteUser Security Role through the InfoSphere Information Server console or Web console. This security assignment is audited. The DirectoryAdmin command line tool is available on the server side installation that has restricted access. This command cannot be executed on a client side installation.
ADD_GROUP (caller): GroupID="xxx", GroupName="xxx"
Logged when a group is created in the InfoSphere Information Server console, Web console, or DirectoryCommand command line tool.

DELETE_USERS (caller): UserIDs="xxx, yyy"
Logged when users are deleted through the InfoSphere Information Server console or Web console. Deleting ALL USERS through the DirectoryAdmin command line tool on the server does not log an audit event. This is not a typical action and is used only in a recovery type operation.

DELETE_GROUPS (caller): GroupIDs="xxx, yyy"
Logged when groups are deleted through the InfoSphere Information Server console or Web console. Deleting ALL GROUPS through the DirectoryAdmin command line tool on the server does not log an audit event. This is not a typical action and is used only in a recovery type operation.

ADD_USERS_TO_GROUPS (caller): UserIDs="xxx, yyy", GroupIDs="xxx, yyy"
Logged when users are added to groups in the InfoSphere Information Server console, Web console, or DirectoryCommand command line tool.

DELETE_USERS_FROM_GROUPS (caller): UserIDs="xxx, yyy", GroupIDs="xxx, yyy"
Logged when users are removed from groups in the InfoSphere Information Server console or Web console.

CHANGE_PASSWORD (caller): UserID="xxx"
Logged when the Change Password action is used in the InfoSphere Information Server console or Web console to change the password of the user who is currently logged in.

SET_CREDENTIAL (caller): UserID="xxx"
Logged when a password is changed for any user by an administrator in the InfoSphere Information Server console or Web console. Changing a user's password through the DirectoryAdmin command line tool on the server does not log an audit event.

REMOVE_CREDENTIAL (caller): UserIDs="xxx, yyy"
Logged when a password is cleared for one or more users.

User, group, and project security role assignment events:

The user, group, and project security role assignments consist of the following events: creation or deletion of a security role, assignment and removal of security roles to users or groups, and assignment or removal of users or groups and roles to a project.

The following event messages are logged with parameters that describe the subjects that are changed or created. The (caller) indicated in each message is the user ID of the caller to this event method:

ADD_ROLE (caller): RoleID="xxx"
Logged when a new security role is created. Because security roles are internally created by IBM InfoSphere Information Server, these audit events can occur only during a maintenance release installation that includes new roles, if any.

DELETE.Roles (caller): RoleIDs="xxx, yyy"
Logged when a security role is deleted. This audit event does not occur because there is no user interface to delete a security role.
ASSIGN GROUP_ROLES *(caller)*: GroupIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when security roles are assigned to groups in the InfoSphere Information Server console, Web console, or DirectoryCommand command line tool.

ASSIGN USER_ROLES *(caller)*: UserIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when security roles are assigned to users in the InfoSphere Information Server console, Web console, or DirectoryCommand command line tool.

REVOKE GROUP_ROLES *(caller)*: GroupIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when security roles are deleted from groups in the InfoSphere Information Server console or Web console.

REVOKE USER_ROLES *(caller)*: UserIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when security roles are deleted from users in the InfoSphere Information Server console or Web console.

ASSIGN PROJECT USER_ROLES *(caller)*: Project="xxx", UserIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when users and associated project security roles are assigned to project permissions in the IBM InfoSphere DataStage Administrator, InfoSphere Information Server console, or IBM InfoSphere FastTrack client.

ASSIGN PROJECT GROUP_ROLES *(caller)*: Project="xxx", GroupIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when groups and associated project security roles are assigned to project permissions in the InfoSphere DataStage Administrator, InfoSphere Information Server console, or IBM InfoSphere FastTrack client.

REVOKE PROJECT USER_ROLES *(caller)*: Project="xxx", UserIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when project security roles are changed for a user or when users are removed from a project's permissions in the InfoSphere DataStage Administrator, InfoSphere Information Server console, or IBM InfoSphere FastTrack client.

REVOKE PROJECT GROUP_ROLES *(caller)*: Project="xxx", GroupIDs="xxx, yyy", RoleIDs="xxx, yyy"
Logged when project security roles are changed for a group or when groups are removed from a project's permissions in the InfoSphere DataStage Administrator, Information Server console, or IBM InfoSphere FastTrack client.

REVOKE PROJECT ALL ROLES *(caller)*: Project="xxx"
Logged when all security roles assigned to a project are removed.

Engine credential mapping events:

The engine credential mapping consists of the following events: assignment and removal of credentials to IBM InfoSphere DataStage suite users and assignment of default credentials for an IBM InfoSphere Information Server engine when mapping credentials using the Engine Credentials panel of the IBM InfoSphere Information Server Web console.

The following event messages are logged with parameters that describe the subjects that are changed or created. The *(caller)* indicated in each message is the user ID of the caller to this event method:
ADD_DATASTAGE_CREDENTIAL (caller): UserID="xxx, yyy", DSServer="xxx", Username="xxx"
	Logged when a mapped credential is set for one or more suite users in the IBM InfoSphere Information Server Web console.

SET_DEFAULT_DATASTAGE_CREDENTIAL (caller): DSServers="xxx, yyy", Username="xxx"
	Logged when default engine credentials are set in the Engine Configuration in the IBM InfoSphere Information Server Web console.

REMOVE_DATASTAGE_CREDENTIAL (caller): UserID="xxx, yyy", DSServer="xxx"
	Logged when a mapped credential is cleared for one or more suite users in the IBM InfoSphere Information Server Web console.

REMOVE_DEFAULT_DATASTAGE_CREDENTIAL (caller): DSServers="xxx, yyy"
	Logged when default engine credentials are cleared in the Engine Configuration in the IBM InfoSphere Information Server Web console.

DATASTAGE_CREDENTIAL_MAPPING_DISABLED (caller): DSServer="xxx"
	Logged when Share User Registry is selected in the Engine Configuration in the IBM InfoSphere Information Server Web console. With this setting, InfoSphere DataStage users are authenticated to the operating system of the server engine using the same credentials they used to log in to the InfoSphere DataStage client application.

DATASTAGE_CREDENTIAL_MAPPING_ENABLED (caller): DSServer="xxx"
	Logged when Share User Registry is cleared in the Engine Configuration in the IBM InfoSphere Information Server Web console. This restores the use of the mapped credentials for InfoSphere Information Server engine authentication.

User session management events:

User session management consists of the following events: user login and logout, direct session termination, and session expiration.

The following event messages are logged with parameters that describe the subjects that are involved. The (caller) indicated in each message is the user ID of the caller to this event method:

LOGIN (caller): UserID="xxx", Client="xxx", Origin="xxx", SessionID="xxx"
Logged when a user logs in to an IBM InfoSphere Information Server client application or command line tool or when an internal process logs in to InfoSphere Information Server to perform an operation. This action creates an InfoSphere Information Server session. UserID is the userid used to authenticate with the server. In some cases, this userid value indicates a special trusted userid reserved for use by InfoSphere Information Server. This type of login is for performing some scheduled or system-initiated operation. Client indicates the type of application that initiated the login. Origin indicates the host name of the system from which the login originated. SessionID is a unique alphanumeric value that unambiguously associates this login session with a LOGOUT, SESSION_TERMINATED, or SESSION_EXPIRED audit event, or with log messages associated with this session in other diagnostic logs. If this event is configured for LOG LEVEL=INFO, the system user login events are filtered out and not logged. These types of log ins are for InfoSphere Information Server internal operations performed for various tasks. An example of a system user login event is a LOGIN event with a UserID=InformationServerSystemUser. These events...
events typically occur every 30 minutes as part of a scheduler activity but can occur for other operations at other times.


Logged when a user or process explicitly logs out of an active InfoSphere Information Server session. This event might not occur when an application abnormally terminates, such as when the Web browser is closed with an active InfoSphere Information Server Web console or when a session is terminated by an administrator or times out (in which case a SESSION_TERMINATED or SESSION_EXPIRED event is logged). **UserID** is the authenticated userid that initially created this session. **Client** indicates the type of application that uses this session. **Origin** indicates the host name of the system from which the login originated. **SessionID** is the same value that was logged with the corresponding LOGIN event to uniquely identify this session. If this event is configured for LOG LEVEL=INFO, then logouts from system user sessions are filtered out and not logged. These types of log outs are for InfoSphere Information Server internal operations performed for various tasks.


Logged when an InfoSphere Information Server session is disconnected by an administrator in the IBM InfoSphere Information Server Web console. If Disconnect All is selected, or multiple sessions are selected, each disconnected session is logged as a separate audit event. Only active sessions that are terminated log an audit event. Sessions that have already expired are ignored because they have been previously logged with a SESSION_EXPIRED audit event. **UserID** is the authenticated userid that initially created this session. **Client** indicates the type of application that uses this session. **Origin** indicates the host name of the system from which the login originated. **SessionID** is the same value that was logged with the corresponding LOGIN event to uniquely identify this session.

**SESSION_EXPIRED: SessionID=“xxx”**

Logged when an idle InfoSphere Information Server session times out and is terminated. The timeout is based on the Inactive Session Timeout value configured in Global Session Properties of Session Management in the IBM InfoSphere Information Server Web console. **SessionID** is the same value that was logged with the corresponding LOGIN event to uniquely identify this session. Additional information about this session is not available at this time to be logged. To determine the actual client application and userid associated with this session, find the corresponding LOGIN event with the same **SessionID** value.

**Audit configuration events:**

Auditing configuration consists of the following events: auditing properties file location, audit file configuration settings, and audit event settings.

The following event messages are logged with parameters that describe the audit configuration settings used. These messages are logged when the application server starts and the auditing service is initialized.

**AUDITING_Configuration_FILE: Path=“xxx”**

Logged when IBM WebSphere Application Server starts and the Auditing Service is initialized. **Path** indicates the location and name of the auditing configuration file that is used to initialize and configure auditing support.
Logged when WebSphere Application Server starts and the Auditing Service is initialized. Path indicates the location where audit log files are created. Name is the pattern configured for the log file name. MaxSize is the maximum size in bytes that each log file can grow to. Count is the maximum number of files created before recycling. Format is the format of the audit log file. Append indicates whether new records are appended or a new file is created when the Auditing service is initialized.

AUDITING EVENT_SETTINGS: xxx=“yyy”, xxx=“yyy”
Logged when WebSphere Application Server starts and the Auditing Service is initialized. This event message includes a comma delimited list of all auditing event types and the current log level setting for each where xxx is the event type and yyy is the log level. Typical log levels are ALL, INFO, or OFF. ALL indicates that all events of this type are always logged. OFF indicates that no events of this type will be logged. Any other value will filter which messages are logged for that event type. Each message is assigned a specific log level by IBM InfoSphere Information Server. Only INFO and FINE levels are currently assigned to messages. Messages assigned at a lower level than INFO, which includes messages assigned a log level of FINE, are not logged if the event type is configured for INFO. The only event types that currently have FINE level log messages are LOGIN and LOGOUT events. Refer to “User session management events” on page 101 for more information about which messages are assigned which log levels.

Configuring the audit configuration file
Use the ISauditing.properties file to configure which audit events are logged and to configure the audit log file itself such as the location, name, maximum size, and number of cycled files to keep. By default, the file is located in the classes directory of the IBM InfoSphere Information Server profile in IBM WebSphere Application Server. The default location is WebSphere/AppServer/profiles/InfoSphere/classes. The file is read during the Auditing service initialization when the application server starts up, so changes to the configuration settings take effect only after the application server restarts.

Audit configuration values
The ISauditing.properties file contains the following default settings. The default values are used if the properties file is missing, if a value from the properties file is missing, or if an invalid value is configured.

auditing.enable = true
    Enables or disables auditing. Setting this value to false disables all further logging and ignores all other settings in the configuration file.

audit.file.path = logs
    Location where to create the audit log file. The WebSphere Application Server process owner must have write access to this directory. A relative path is considered to be off the InfoSphere Information Server profile directory of WebSphere Application Server. Use the forward slash (/) as the path separator.

audit.file.name = ISauditLog_%g.log
    Audit file name. A pattern consisting of a string that includes the following special components that will be replaced at run time:
• %g - Generation number to distinguish rotated logs. This is replaced by a numeric value with 0 being the latest log file (the one currently being written to) and then sequential values increasing with each additional log file created as the file reaches the maximum size. The larger the number, the older the log file.

• %% - Translates to a single percent sign (%).

**audit.file.size = 1000000**

Maximum size of each audit log file in bytes. If this value is equal to zero, there is no limit to the size of the log file. All audit records continue to be logged to the same file. Use 0 with caution. When a logged audit record causes the file size to exceed this configured size, the log file cycles, and a new log file is created.

**audit.file.count = 5**

Maximum number of audit log files to rotate through. If this value is greater than 1 and the %g generation parameter is not included in the audit file name (audit.file.name), a numeric value preceded by a period is added to the end of the file name. Existing audit files are renamed when a new file is created. The higher the generation number, the older the log file. The count includes the 0 generation file. For example,

    **audit.file.count = 5** allows the creation of file name ISauditLog_0.log through ISauditLog_4.log.

**audit.file.format = Simple**

Format of the audit file. Possible values are Simple, XML, or both. If configured as both, the file name extension specified in audit.file.name will be replaced with .xml for the XML log files or added to the end of the file name if no extension is specified.

**audit.file.append = true**

Audit file append setting. Setting this value to false, forces the creation of a new 0 generation log file each time WebSphere Application Server restarts. Setting this value to true continues appending to the existing 0 generation file until the maximum size is reached. If the **audit.file.format = XML**, set the value to false to prevent multiple XML file headers from being written to the file.

The following list shows the valid audit event types and the log level setting for each:

- **audit.event.ADD_USER = ALL**
- **audit.event.ADD_GROUP = ALL**
- **audit.event.DELETE_USERS = ALL**
- **audit.event.DELETE_GROUPS = ALL**
- **audit.event.ADD_USERS_TO_GROUPS = ALL**
- **audit.event.DELETE_USERS_FROM_GROUPS = ALL**
- **audit.event.CHANGE_PASSWORD = ALL**
- **audit.event_SET_CREDENTIAL = ALL**
- **audit.event.REMOVE_CREDENTIAL = ALL**
- **audit.event.ADD_ROLE = ALL**
- **audit.event.DELETE_ROLES = ALL**
- **audit.event.ASSIGN_GROUP_ROLES = ALL**
- **audit.event.ASSIGN_USER_ROLES = ALL**
- **audit.event.REVOKE_GROUP_ROLES = ALL**
- **audit.event.REVOKE_USER_ROLES = ALL**
- **audit.event.ASSIGN_PROJECT_USER_ROLES = ALL**
- **audit.event.ASSIGN_PROJECT_GROUP_ROLES = ALL**
Enables the audit events to be included in the logs. Set the desired log level for each audit event to ALL, INFO, or OFF.

- **ALL** enables logging of all audit records produced by the system for the configured event type. If an `audit.event` type is missing from the configuration file or is configured for an invalid log level, it defaults to a log level of **ALL**.

- **INFO** filters which audit records get logged by ignoring requests to log all audit records defined with a log level lower than **INFO**. The only audit records produced with a log level lower than **INFO** are **LOGIN** and **LOGOUT** event records for System User logins and logouts. These system user events are not initiated by a user but are from internal operations within InfoSphere Information Server. Setting `audit.event.LOGIN=INFO` suppresses logging of the system user login events.

- **OFF** suppresses logging of all audit records produced by the system for the configured event type.

**Audit configuration security**

The Audit service creates an audit trail of security-related events. You can secure the audit configuration and logs to prevent unauthorized tampering.

Set the path where audit files are located in the `ISauditing.properties` configuration file. If configured as a relative path, the specified directory must exist off the IBM InfoSphere Information Server profile directory under IBM WebSphere Application Server. If configured in another location, the full path must be specified and you must ensure that the WebSphere Application Server process owner has file system write permission to that directory.

By default, the location of the `ISauditing.properties` configuration file is in the InfoSphere Information Server profile of WebSphere Application Server in the `classes` directory. This is the same location as the `isfconfig.properties` file. A new key is added to the `isfconfig.properties` file to indicate the location of the `ISauditing.properties` file. This key and default value are: `auditing.config.file = classes/ISauditing.properties`.

To ensure additional secure access to the auditing configuration settings, you can relocate the `ISauditing.properties` configuration file to another location and update the `audit.config.file` value in the `isfconfig.properties` file to specify the full path and auditing property file name of the new location. A relative path assumes a root of the InfoSphere Information Server Profile directory under
WebSphere Application Server. Use the forward slash (/) for the path separator. The WebSphere Application Server process owner must have read access to the file wherever it is relocated. However, write access can be restricted to individuals who have the authority to modify the auditing configuration. To detect any attempt to spoof the official configuration, the location of the audit configuration file used is logged as an audit event in the audit file at WebSphere Application Server startup. If someone with write access to the isfconfig.properties file changes the location or name of the auditing configuration file, this information is logged.

The absence of the configured auditing properties file or a pointer to an invalid or partial file defaults to logging events using the default audit configuration settings. A missing property key or an invalid value for a key results in the default value being used for that property key. These precautions are in place to prevent an unauthorized circumvention of audit logging.

**Auditing in a clustered environment**

There are information and auditing considerations that are specific to a clustered IBM WebSphere Application Server configuration.

In a clustered configuration, a separate set of audit log files are created on each managed node, each containing the specific events processed by that node. You must gather and collate these files to sort events by timestamp if you want a single, chronological audit trail.

If a managed node in the cluster is configured with multiple application servers, each application server creates and manages its own audit log files. Because all application servers on a single managed node share the same auditing configuration settings, it is not possible to configure different file names or locations for each application server. The first application server that is initialized uses (or creates) the 0 generation audit file by the configured log file name. Subsequent application servers initialized on that same managed node create a 0 generation audit file by the same name, but with a period and a sequential number appended to the end of the file name.

For clustered configurations that include multiple managed nodes, any changes to the auditing configuration settings must be made to the ISAuditing.properties file in the classes directory of each node's profile. If this properties file has been relocated or renamed, the appropriate changes must be made to the isfconfig.properties file on each managed node denoting the path and file name of the custom auditing configuration file.

**Audit logs**

The audit log file can be created in simple text format or in XML format. The size of each audit record varies depending on the event, the string length, and the number of parameters associated with the audit event and the format selected.

Audit events are recorded in the audit log file on the IBM InfoSphere Information Server Services tier. Logging in to or out of any InfoSphere Information Server client application or command-line tool logs events. Audit events are logged for managing the users, groups, or security roles in the InfoSphere Information Server console, InfoSphere Information Server Web console, the IBM InfoSphere FastTrack client, and the InfoSphere DataStage Administrator client. DirectoryCommand and other command-line tools also log events.
Log file sizing

The log file size and the number of log files to keep are based on the settings in the audit configuration file. With the default values of `audit.file.size=10000000` and `audit.file.count=5`, when the file grows to approximately 10 million bytes, it is renamed to `ISauditLog_1.log`. A new `ISauditLog_0.log` file is created to hold the most recent audit events. Up to five files can be created, at which time, when the current `ISauditLog_0.log` file exceeds the size limit of 10 million bytes, the oldest log is deleted, the other files are renamed, and a new file with generation number 0 is created. The higher the generation number of the file, the older the audit events.

Log file formats

The simple text format allows easy viewing and the XML format is convenient for formatting or parsing the logs with custom applications. Both file formats can be created at the same time. The XML format produces larger audit records and thus fewer events per file than the simple text format. When XML format is used, the Java™ logger creates the XML file and adds the XML file header. The logger is initialized on each startup of IBM WebSphere Application Server at which time the XML header is written to the file. If the logger is configured for `audit.file.append=true`, the XML header is written to the current end of the file causing multiple XML file header elements to appear in the log file making the XML malformed. Configure `audit.file.append` as `false` when configured for `audit.file.format=xml` or `both`. However, `audit.file.append=false` means the current 0 generation log file is renamed to generation 1 and a new generation 0 log file is created each time IBM WebSphere Application Server restarts. So certain log files might not be the full maximum size in length when you use `audit.file.append=false`.

Example: Simple text format:

You can create the audit log in a simple text format.

Sample audit log

The following example is an excerpt from an audit log in simple text format. For illustration purposes, this example shows each event on more than one line. In an actual audit log file, each event is logged to a single line.

```

2009-04-04 04:01:50.154 EST INFO: ADD_USER (admin): UserID="ppds1", LastName="PersonDS1", FirstName="Project"

2009-04-04 04:01:50.387 EST INFO: SET_CREDENTIAL (admin): UserID="ppds1"

2009-04-04 04:01:50.654 EST INFO: ASSIGN_USER_ROLES (admin): UserIDs="ppds1", RoleIDs="SuiteUser, DataStageAdmin, DataStageUser"

2009-04-04 04:11:41.325 EST INFO: ADD_GROUP (admin): GroupID="regPeeps", GroupName="Regular People"

2009-04-04 04:11:42.895 EST INFO: ASSIGN_GROUP_ROLES (admin): GroupIDs="regPeeps", RoleIDs="SuiteUser"

2009-04-04 04:12:01.343 EST INFO: ASSIGN_GROUP_ROLES (admin): GroupIDs="regPeeps", RoleIDs="DataStageUser"

2009-04-04 04:12:12.784 EST INFO: LOGIN (admin): UserID="admin",
```
You can create the audit log in XML format.

Sample audit log

The following example is an excerpt from an audit log in an XML format:

```xml
<?xml version="1.0" encoding="windows-1252" standalone="no"?>
<!DOCTYPE log SYSTEM "logger.dtd">
<log>
  <record>
    <date>2009-05-21T00:00:00</date>
    <millis>1242878400161</millis>
    <sequence>323</sequence>
    <logger>com.ibm.is.auditing</logger>
    <level>FINE</level>
    <thread>51</thread>
  </record>
  <record>
    <date>2009-05-21T00:00:04</date>
    <millis>1242878404458</millis>
    <sequence>324</sequence>
    <logger>com.ibm.is.auditing</logger>
    <level>FINE</level>
    <thread>51</thread>
  </record>
  <record>
    <date>2009-05-21T16:24:50</date>
    <millis>1242937490614</millis>
    <sequence>351</sequence>
    <logger>com.ibm.is.auditing</logger>
    <level>INFO</level>
    <thread>46</thread>
    <message>LOGIN (admin): UserID="admin", Client="Web Console", Origin="localhost", SessionID="1CB85C6D-2698-490F-B817-788D93681B09"</message>
  </record>
</log>
```
Chapter 6. Managing security

<catalog>com.ascential.acs.auditing.server.impl.resources.StringData</catalog>
<param>admin</param>
<param>admin</param>
<param>Web Console</param>
<param>localhost</param>
<param>1C5D5CFD-298E-400F-81B7-7B8F93681B09</param>
</record>
<record>
<date>2009-05-21T16:27:24</date>
<millis>1242937644348</millis>
<sequence>370</sequence>
<logger>com.ibm.is.auditing</logger>
<level>INFO</level>
<thread>46</thread>
<message>ADD_USER (admin): UserID="ppds1", LastName="PersonDS1", FirstName="Project"</message>
</record>
<record>
<date>2009-05-21T16:27:24</date>
<millis>1242937644645</millis>
<sequence>371</sequence>
<logger>com.ibm.is.auditing</logger>
<level>INFO</level>
<thread>46</thread>
<message>ASSIGN_USER_ROLES (admin): UserIDs="ppds1", RoleIDs="SuiteUser"</message>
</record>
<record>
<date>2009-05-21T16:27:24</date>
<millis>1242937644801</millis>
<sequence>372</sequence>
<logger>com.ibm.is.auditing</logger>
<level>INFO</level>
<thread>46</thread>
<message>ASSIGN_USER_ROLES (admin): UserIDs="ppds1", RoleIDs="DataStageAdmin, DataStageUser"</message>
</record>
<record>
<date>2009-05-21T16:27:24</date>
<millis>1242937644973</millis>
<sequence>373</sequence>
<logger>com.ibm.is.auditing</logger>
<level>INFO</level>
<thread>46</thread>
<message>SET_CREDENTIAL (admin): UserID="ppds1"</message>
</record>
Administrator account password changing

After running the installation program, you can change the passwords for administrator accounts that you created during installation.

You can change the following administrator account passwords:
- An IBM InfoSphere Information Server administrator password.
- An IBM WebSphere Application Server administrator password.
- IBM InfoSphere Information Analyzer analysis database owner account credentials.
- IBM DB2 passwords.

Changing an IBM InfoSphere Information Server administrator password

You can change an InfoSphere Information Server administrator account password after installation.

About this task

InfoSphere Information Server administrator accounts are the main administration accounts for InfoSphere Information Server.

You can create as many InfoSphere Information Server administrator accounts as you need. Any users with the suite administrator role assigned to them are InfoSphere Information Server administrators. The IBM WebSphere Application Server default administrator account also has this role.

Procedure

1. Change the password. Use the method that matches your user registry setup:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If your system uses the operating system user registry</td>
<td>Change the password by using standard operating system utilities.</td>
</tr>
<tr>
<td>If your system uses a Lightweight Directory Access Protocol (LDAP) user registry</td>
<td>Change the password by using LDAP utilities.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>If your system uses the internal user registry</td>
<td>Change the password by using the InfoSphere Information Server Web console. See “Changing passwords by using the IBM InfoSphere Information Server Web console.”</td>
</tr>
</tbody>
</table>

2. If the credentials that you change are also the WebSphere Application Server or IBM DB2 administrator credentials, run the `AppServerAdmin` command to propagate the new password across your configuration. See “IBM WebSphere Application Server administrator password changing” on page 112 and “Metadata repository database owner password changing” on page 115.

**Changing passwords by using the IBM InfoSphere Information Server Web console**

If your system is configured to use the internal user registry, change passwords by using the IBM InfoSphere Information Server Web console.

**Before you begin**

To change a suite administrator or suite component user password, you need suite-level administrator authority.

**About this task**

Use this procedure to change passwords if all of the following statements are true:

- Your system is configured to use the internal user registry.

  If your system is configured to use the local operating system user registry, do not use this procedure. Instead, change passwords by using standard operating system utilities.

  If your system uses a Lightweight Directory Access Protocol (LDAP) user registry, do not use this procedure. Instead, change passwords by using LDAP utilities.

- If your installation includes a stand-alone implementation of IBM WebSphere Application Server, you are changing a password other than the WebSphere Application Server administrator password.

  If you are changing the WebSphere Application Server administrator password in a stand-alone implementation, do not use this procedure. Instead, follow the procedure in “IBM WebSphere Application Server administrator password changing” on page 112.

- You can log in to the IBM InfoSphere Information Server Web console.

  If you cannot log in to the Web console, use the `DirectoryAdmin` tool as described in “DirectoryAdmin tool” on page 122 to change passwords.

Individual users can also change their passwords by logging in to the IBM InfoSphere Information Server Web console and clicking the Change Password link.

**Procedure**

1. Log in to the IBM InfoSphere Information Server Web console. Use an account with administrator access.
2. In the Web console, click the Administration tab.
3. In the navigation pane, select Users and Groups > Users.
4. In the Users pane, select the check box for the WebSphere Application Server administrator.
5. In the right pane, click Open User.
6. In the Password field, type the new password.
7. In the Confirm Password field, retype the new password.
8. In the lower right corner of the page, click Save and Close.

IBM WebSphere Application Server administrator password changing

The procedure for changing the WebSphere Application Server administrator password differs depending on whether WebSphere Application Server clustering is implemented within your installation.

Changing the IBM WebSphere Application Server administrator password in a stand-alone installation

You can change the WebSphere Application Server administrator password after installation. Follow this procedure if your implementation includes a stand-alone installation of WebSphere Application Server.

Procedure

1. Stop WebSphere Application Server. See “Stopping IBM WebSphere Application Server (Windows)” on page 231 or “Stopping IBM WebSphere Application Server (Linux, UNIX)” on page 233.
2. Log in to the services tier computer. Use an account with administrator credentials.

   Linux      UNIX
   The account must have execution permission for the tools in the ASBServer/bin directory within the InfoSphere Information Server installation directory.
3. Change the password:

   • If your system is configured to use the internal user registry, change the password by using the DirectoryAdmin command:

     Windows
     
     C:\IBM\InformationServer\ASBServer\bin\DirectoryAdmin.bat -user
     -userid wasadmin -password password

     Linux      UNIX
     /opt/IBM/InformationServer/ASBServer/bin/DirectoryAdmin.sh -user
     -userid wasadmin -password password

     In the command, wasadmin is the WebSphere Application Server administrator user name, and password as the new password.

     Tip: The value for the -password parameter can be either plain text or an encrypted string that has been created with the encrypt command.
     Do not use the IBM InfoSphere Information Server Web console to change the WebSphere Application Server administrator password.

   • If your system uses an operating system user registry, change the password by using standard operating system utilities.

   • If your system uses a Lightweight Directory Access Protocol (LDAP) user registry, change the password by using LDAP utilities.
4. Run the AppServerAdmin command with the -was option to update the credentials across your configuration.
For example, to update your configuration with user name wasadmin1 and password mypassword, run the following command:

- **Linux**
  ```bash
  /opt/IBM/InformationServer/ASBServer/bin/AppServerAdmin.sh -was
  -user wasadmin1 -password mypassword
  ```

- **Windows**
  ```bash
  C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -was
  -user wasadmin1 -password mypassword
  ```

**Tip:** The -password parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command. This command updates the WebSphere Application Server user registry configuration. You do not have to use the WebSphere Application Server administrative console.

5. Restart WebSphere Application Server. See "Starting IBM WebSphere Application Server (Linux, UNIX)" on page 238 or "Starting IBM WebSphere Application Server (Windows)" on page 235.

6. When restarting WebSphere Application Server, regardless of the method that you use, the startup method returns before the application server is fully started. To verify that WebSphere Application Server has started, monitor the log files. See "Checking the status of IBM WebSphere Application Server startup (stand-alone installation)" on page 242.

## Changing the IBM WebSphere Application Server administrator password in a clustered installation

You can change the WebSphere Application Server administrator password after installation. Follow this procedure if WebSphere Application Server clustering is implemented for your installation.

**Procedure**

1. Make sure that all node agents are running. See "Checking the status of IBM WebSphere Application Server node agents".

2. Change the user password:
   - If your system uses the internal user registry, change the password by using the IBM InfoSphere Information Server Web console. See "Changing passwords by using the IBM InfoSphere Information Server Web console" on page 111.
   - If your system uses a Lightweight Directory Access Protocol (LDAP) user registry, change the password by using LDAP utilities.

3. Log in to the computer that hosts the WebSphere Application Server Deployment Manager.
   - **Linux**
     Log in as root.
   - **Windows**
     Use an account with administrator privileges.

4. Make sure that all node agents are still running after the password change. See "Checking the status of IBM WebSphere Application Server node agents" on page 244.

5. Stop the Deployment Manager. See "Stopping the IBM WebSphere Application Server Deployment Manager (Windows)" on page 232 or "Stopping the IBM WebSphere Application Server Deployment Manager (Linux, UNIX)" on page 234. Do not stop the node agents.
6. On the computer that hosts the WebSphere Application Server Deployment Manager, run the `AppServerAdmin` command with the `-was` option to update the credentials across your configuration.

For example, to update your configuration with user name `wasadmin1` and password `mypassword`, run the following command:

```
Linux
/opt/IBM/InformationServer/ASBServer/bin/AppServerAdmin.sh -was
-user wasadmin1 -password mypassword

To run this command, use an account that has execution permission for the tools in the ASBServer/bin directory.
```

```
Windows
C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -was
-user wasadmin1 -password mypassword
```

**Tip:** The `-password` parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command.

This command updates the WebSphere Application Server user registry configuration. You do not have to use the WebSphere Application Server administrative console.

7. Restart the Deployment Manager. See “Starting the IBM WebSphere Application Server Deployment Manager (Windows)” on page 236 or “Starting the IBM WebSphere Application Server Deployment Manager (Linux, UNIX)” on page 239.

You do not have to restart the node agents and application servers. They are automatically synchronized with the Deployment Manager after it is running. The synchronization process takes a few seconds. After the synchronization is complete, you can safely stop or start node agents or application servers when necessary.

8. If one of the node agents was not running when you changed the password in step 2 on page 113, the user cannot start that node agent because the passwords no longer match at the Deployment manager and node level. To fix this problem, run the WebSphere Application Server `syncNode` command to synchronize the node with the Deployment manager. To run the `syncNode` command:

a. Log into the node.

b. Run the `syncNode` command.

```
Linux
/opt/IBM/WebSphere/AppServer/profiles/custom_profile/bin/syncNode.sh
 dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password

Windows
C:\IBM\WebSphere\AppServer\profiles\custom_profile\bin\syncNode
 dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password
```

In the command:

- `dmgr_hostname` is the host name of the computer where the Deployment Manager is running.
- `dmgr_port` is the port number of the Deployment Manager (default is 8879).
was_admin_username is the user name of the WebSphere Application Server administrator.

was_admin_password is the administrator password.

c. Restart the node agent. See "Starting IBM WebSphere Application Server (Windows)" on page 235 and "Starting IBM WebSphere Application Server (Linux, UNIX)" on page 238.

9. When restarting WebSphere Application Server, regardless of the method that you use, the startup method returns before the application server is fully started. To verify that WebSphere Application Server has started, monitor the log files. See "Checking the status of IBM WebSphere Application Server startup (clustered installation)" on page 243.

Metadata repository database owner password changing

The procedure for changing the metadata repository database owner password differs depending upon whether IBM WebSphere Application Server clustering is implemented within your installation.

Changing the metadata repository database owner password in a stand-alone IBM WebSphere Application Server installation

You can change the metadata repository database owner account password after installation. Follow this procedure if your implementation includes a stand-alone installation of WebSphere Application Server.

About this task

Follow this procedure to change the metadata repository database owner password. The metadata repository database owner user name cannot be changed.

Procedure

1. Stop WebSphere Application Server. See "Stopping IBM WebSphere Application Server (Windows)" on page 231 or "Stopping IBM WebSphere Application Server (Linux, UNIX)" on page 233.

2. Change the metadata repository database owner account password on the computer:
   - If your database is implemented within IBM DB2, change the password by using standard operating system utilities.
   - If your database is implemented within another database management system, refer to the database management system documentation for information about changing the password.

3. Log in to the services tier computer. Use an account with administrator credentials.

   Linux  UNIX

   The account must have execution permission for the tools in the ASBServer/bin directory within the InfoSphere Information Server installation directory.

4. Run the AppServerAdmin command with the -db option to update the password across your configuration.

   For example, to update your configuration with password mypassword, run the following command:

   Linux  UNIX

   /opt/IBM/InformationServer/ASBServer/bin/AppServerAdmin.sh -db -user xmeta1 -password mypassword

   Windows
C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -db -user xmeta1 -password mypassword

Tip: The -password parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command. This command updates the WebSphere Application Server user registry configuration. You do not have to use the WebSphere Application Server administrative console.

5. Restart WebSphere Application Server. See "Starting IBM WebSphere Application Server (Linux, UNIX)" on page 238 or "Starting IBM WebSphere Application Server (Windows)" on page 235.

6. When restarting WebSphere Application Server, regardless of the method that you use, the startup method returns before the application server is fully started. To verify that WebSphere Application Server has started, monitor the log files. See "Checking the status of IBM WebSphere Application Server startup (stand-alone installation)" on page 242.

Changing the metadata repository database owner password in a clustered installation
You can change the metadata repository database owner password after installation. Follow this procedure if IBM WebSphere Application Server clustering is implemented within your installation.

About this task
Follow this procedure to change the metadata repository database owner password. The metadata repository database owner user name cannot be changed.

Procedure
1. Stop all WebSphere Application Server processes, including the Deployment Manager, node agents and cluster members.
2. Change the metadata repository database owner account password on the computer:
   - If your database is implemented within IBM DB2, change the password by using standard operating system utilities.
   - If your database is implemented within another database management system, refer to the database management system documentation for information about changing the password.
3. Log in to the computer that hosts the WebSphere Application Server Deployment Manager.
   - Linux | UNIX Log in as root.
   - Windows Use an account with administrator privileges.
4. Run the AppServerAdmin command with the -db option to update the credentials across your configuration.
   For example, to update your configuration with password mypassword, run the following command:
   - Linux | UNIX

   /opt/IBM/InformationServer/ASBServer/bin/AppServerAdmin.sh -db -user xmeta1 -password mypassword

   To run this command, use an account that has execution permission for the tools in the ASBServer/bin directory.
Windows
C:\IBM\InformationServer\ASBServer\bin\AppServerAdmin.bat -db -user xmeta1 -password mypassword

Tip: The -password parameter is optional. If not provided, you will be prompted for a password. If you do provide a password, it can be either plain text or an encrypted string that has been created with the encrypt command. This command updates the WebSphere Application Server user registry configuration. You do not have to use the WebSphere Application Server administrative console.

5. Restart the Deployment Manager. See “Starting the IBM WebSphere Application Server Deployment Manager (Windows)” on page 236 or “Starting the IBM WebSphere Application Server Deployment Manager (Linux, UNIX)” on page 239.

Do not restart the node agents and cluster members yet.

6. On each managed node, run the WebSphere Application Server syncNode command to resynchronize the nodes with the Deployment Manager:

   • Linux
     opt/IBM/WebSphere/AppServer/profiles/custom_profile/bin/syncNode.sh
dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password

   • Windows
     C:\IBM\WebSphere\AppServer\profiles\custom_profile\bin\syncNode
dmgr_hostname dmgr_port -user was_admin_username -password was_admin_password

   In the command:
   • dmgr_hostname is the host name of the computer where the Deployment Manager is running.
   • dmgr_port is the port number of the Deployment Manager (default is 8879).
   • was_admin_username is the user name of the WebSphere Application Server administrator.
   • was_admin_password is the administrator password.

7. Restart the node agents and cluster members. See “Starting IBM WebSphere Application Server (Windows)” on page 235 or “Starting IBM WebSphere Application Server (Linux, UNIX)” on page 238.

8. When restarting WebSphere Application Server, regardless of the method that you use, the startup method returns before the application server is fully started. To verify that WebSphere Application Server has started, monitor the log files. See “Checking the status of IBM WebSphere Application Server startup (clustered installation)” on page 243.

Changing the analysis database owner account credentials

You can change your IBM InfoSphere Information Analyzer analysis database owner account credentials after installation.

Before you begin

You must have InfoSphere Information Analyzer administrator authority.
About this task

The analysis database owner account has ownership authority over the analysis database. By default, the user name of this account is `iauser`.

Follow this procedure to change the analysis database owner account credentials.

Procedure

1. Change the analysis database owner credentials on the computer. If your database is implemented within IBM DB2, change the credentials by using standard operating system utilities. If your database is implemented within another database management system, refer to the database management system documentation for information about changing the credentials.

2. Log in to the IBM InfoSphere Information Server console. Specify a user name and password of an account with InfoSphere Information Analyzer administrator authority.

3. From the Home navigator menu in the console, select Configuration > Analysis Settings. If these items do not appear in the Home menu, log out of the console and log in with an account with InfoSphere Information Analyzer administrator authority.

4. Click the Analysis Database tab.

5. Change the information in the fields.

6. Click Save All.

Changing IBM DB2 passwords

You can change the DB2 administrator account or other DB2 account passwords after installation.

About this task

The DB2 administrator account owns the DB2 database management system for IBM InfoSphere Information Server. DB2 runs under this account.

An InfoSphere Information Server installation also requires a non-fenced instance user and a fenced user.

Procedure

To change a DB2 password, see the IBM DB2 documentation:


Administration commands and tools

Use the IBM InfoSphere Information Server administration commands and tools to complete security administration tasks, such as updating new credentials across your configuration and searching for users in a configured user registry, and to troubleshoot your security configuration.
**AppServerAdmin command**

If you change the default IBM WebSphere Application Server administration credentials or the repository credentials, use the AppServerAdmin command to update the new credentials across your configuration.

**Location**

Issue the command from the `root_directory/InformationServer/ASBServer/bin` directory.

The **AppServerAdmin** command has the following options:

- **-was option**
  If you change the default IBM WebSphere Application Server administrator user name and password, this command updates the user name and password throughout the WebSphere Application Server configuration.

  You can change the WebSphere Application Server default administrator user name and password in the following cases:
  
  - If you change the WebSphere Application Server user registry configuration in the WebSphere Application Server Administrative Console and the server ID and password for the current user registry is changed or a new user registry is configured.
  
  - If the WebSphere Application Server default administrator is deleted from the configured user registry or if that user's password is changed or expired.

  You must run the -was option each time the WebSphere Application Server default administrator credentials are changed.

- **-db option**
  The repository user credentials are used by WebSphere Application Server to connect to the IBM InfoSphere Information Server metadata repository. The user account for the metadata repository is typically called "xmeta." If you change the repository user password, this command updates the password throughout WebSphere Application Server and the InfoSphere Information Server configuration.

  You must run this command each time the repository user password is changed.

  You cannot specify a new user name for the metadata repository with this command. The user name must match the schema of the database.

- **-dbs option**
  The staging repository user credentials are used by WebSphere Application Server to connect to the IBM InfoSphere Information Server metadata staging repository. The user account for the metadata staging repository is typically called "xmetasr." If you change the staging repository user password, this command updates the password throughout WebSphere Application Server and the InfoSphere Information Server configuration.

  You must run this command each time the staging repository user password is changed.

  You cannot specify a new user name for the staging repository with this command. The user name must match the schema of the database.
Password prompting

To avoid the display of passwords, you can either provide an encrypted password with the -password option, or you can run the command without the -password option. Without this option, you are prompted to provide a password (which is not displayed). You will be asked to provide the password again for verification. To provide an encrypted password, use the string generated from the encrypt command.

Syntax

The command syntax for the -was option:

Windows

AppServerAdmin.bat -was -user username [-password password]

Linux | UNIX

AppServerAdmin.sh -was -user username [-password password]

The command syntax for the -db option:

Windows

AppServerAdmin.bat -db -user repository_userid [-password repository_password]

Linux | UNIX

AppServerAdmin.sh -db -user repository_userid [-password repository_password]

The command syntax for the -dbs option:

Windows

AppServerAdmin.bat -dbs -user staging_repository_userid [-password staging_repository_password]

Linux | UNIX

AppServerAdmin.sh -dbs -user staging_repository_userid [-password staging_repository_password]

Parameters

-was

Updates the new user credentials throughout the WebSphere Application Server configuration. WebSphere Application Server does not need to be up and running to run this command. If WebSphere Application Server is running, it must be restarted after this command is run.

-user The new WebSphere Application Server user name.

-password

Optional. The new password of the WebSphere Application Server user. You can provide the password as plain text or as a string that has been encrypted with the encrypt command. You will be prompted for a password if one is not provided.

-db

Updates the new user password throughout the WebSphere Application Server configuration and the InfoSphere Information Server configuration. WebSphere
Application Server does not need to be up and running to run this command. If WebSphere Application Server is running, it must be restarted after you run this command.

-**user**  The metadata repository user name, which matches the schema name.
  You cannot change the user name with this command.

-**password**  Optional. The new password of the repository user. You can provide the password as plain text or as a string that has been encrypted with the encrypt command. You will be prompted for a password if one is not provided.

-**dbs**  Updates the new user password throughout the WebSphere Application Server configuration and the InfoSphere Information Server configuration. WebSphere Application Server does not need to be up and running to run this command. If WebSphere Application Server is running, it must be restarted after you run this command.

-**user**  The staging repository user name, which matches the schema name.
  You cannot change the user name with this command.

-**password**  Optional. The new password of the staging repository user. You can provide the password as plain text or as a string that has been encrypted with the encrypt command. You will be prompted for a password if one is not provided.

### Changing the RunAs user of the ASB_managers.ear application

An administrative role other than the default primary IBM WebSphere Application Server administrator role can be used to deploy and undeploy applications in IBM InfoSphere Information Services Director. You can use this option if you have security concerns about propagating the primary WebSphere Application Server administrator credentials.

#### About this task

As part of the procedure to switch to a Lightweight Directory Access Protocol (LDAP) registry, you must run the AppServerAdmin -was command to propagate the primary WebSphere Application Server administrator user credentials to a few places in WebSphere Application Server (for example, the RunAs user within ASB_managers.ear).

For more information about WebSphere Application Server administrative roles, go to the following documentation:

- Administrative roles in 8.5
- Administrative roles in 8.0

If you have concerns about IBM InfoSphere Information Server propagating the primary WebSphere Application Server Administrator credentials, you can use other roles, such as the Deployer role, which has fewer permissions than the WebSphere Application Server Administrator role, to accomplish tasks as the RunAs user within ASB_managers.ear.
**Procedure**

To update the RunAs role of the ASB_managers.ear application with a user that has Deployer administrative privileges:

1. In the WebSphere administrative console, click **Users and Groups > Administrative user roles > Add...**
2. Assign an existing user the WebSphere deployer role:
   - Select **Deployer** and search for the user to be assigned this role. Select and add that user to the **Mapped to role** list.
   - Click **OK** and **Save**.
3. Go to the User RunAs roles page in the administrative console:
   - Click **Applications > Application Type > WebSphere enterprise applications > ASB_managers.ear > User RunAs roles**.
4. Update the RunAs role of the ASB_managers.ear application:
   a. Remove the current RunAs user.
   b. Add the user that was configured in step 2 as the new RunAs user.
5. Restart WebSphere Application Server.

**Results**

You can use this configuration to deploy and undeploy applications in IBM InfoSphere Information Services Director.

**DirectoryAdmin tool**

The DirectoryAdmin tool provides a command-line interface that you can use to interact with the metadata repository and complete a variety of IBM InfoSphere Information Server user registry tasks. You should only use this tool and these commands for advanced configuration, such as configuring the InfoSphere Information Server internal user registry or cleaning up the repository if you are changing a registry configuration on a system that has been in production, or for troubleshooting or recovery tasks.

The tool is available in the ASBServer\bin directory of your InfoSphere Information Server directory, for example C:\IBM\InformationServer\ASBServer\bin.

**Creating a user in the IBM InfoSphere Information Server user registry**

Use the following command to create a user in the IBM InfoSphere Information Server internal user registry. This command should only be used for troubleshooting or recovery, or if it is specified in other procedures in the documentation.

IBM WebSphere Application Server does not need to be running to run this command.

**Syntax**

**Windows**

```
DirectoryAdmin.bat -user -userid username -password password
```

**Linux**

```
DirectoryAdmin.bat -user -userid username -password password
```
DirectoryAdmin.sh -user -userid username -password password

Parameters

The following parameters are available for the DirectoryAdmin command.

-user
   The command line option that specifies that this task is to work with users.

-userid username
   Specifies the name of the user that you want to create.

-password password
   Specifies the password of the user that you want to create. You can provide the
   password as plain text or as a string that has been encrypted with the encrypt
   command.

Resetting the password of a user

If you use the IBM InfoSphere Information Server internal user registry, you can
use this command to set or reset the credentials of a user. This command should
only be used for troubleshooting or recovery, or if it is specified in other
procedures in the documentation.

IBM WebSphere Application Server does not need to be running to run this
command.

Syntax

Windows

DirectoryAdmin.bat -user -userid username -password password

Linux

DirectoryAdmin.sh -user -userid username -password password

Parameters

The following options are available for the DirectoryAdmin command.

-user
   The command line option that specifies that this task is to work with users.

-userid username
   Specifies the name of the user whose password needs to be reset.

-password password
   Specifies the user password that you want to set. You can provide the
   password as plain text or as a string that has been encrypted with the encrypt
   command.

Assigning the IBM InfoSphere Information Server administrator role to a user

Use the following command to add the IBM InfoSphere Information Server Suite
Administrator role to a user. Only use this command if you are fixing your user
registry configuration, or if it is specified in other procedures in the
documentation.

IBM WebSphere Application Server does not have to be running to run this
command unless the -checkid option is also used.
Syntax

**Windows**

DirectoryAdmin.bat -user -userid username -admin [-checkid]

**Linux**

DirectoryAdmin.sh -user -userid username -admin [-checkid]

Parameters

The following parameters are available for the DirectoryAdmin command.

- **-user**
  The command line option that specifies that this task is to work with users.

- **-userid username**
  Specifies the name of the user that you want to make a Suite Administrator.
  Note that the user ID syntax differs depending on the user registry that is configured in IBM WebSphere Application Server (local, operating system, LDAP, or custom).

  **Local OS on UNIX**
  Provide the UNIX user ID, such as "isadmin."

  **Local OS on Windows**
  COMPUTER_NAME\userid, such as MYSERVER\isadmin where MYSERVER is the name of the Microsoft Windows computer. If the Microsoft Windows computer is registered in a domain, the syntax might also be DOMAIN_NAME\userid. The name must be uppercase.

  **LDAP**
  The full distinguished name (DN) must be provided in the proper case.
  For more information on retrieving the DN, refer to "LDAP distinguished name (DN) determination" on page 49.

  **Note:** To add users with long and composed user IDs, like LDAP fully qualified names, surround the user IDs with double quotation marks when using the command.

- **-admin**
  Assigns the InfoSphere Information Server Suite Administrator role to the user.

- **-checkid**
  (Optional) Ensures that the given user ID exists before applying the Suite Administrator role to that user.

**Checking to see if a user exists in the configured user registry**

Use this command to see if a user name exists in the configured user registry. Use this command only for troubleshooting or recovery, or if it is specified in other procedures in the documentation.

- IBM WebSphere Application Server must be running to run this command.

Syntax

**Windows**

DirectoryAdmin.bat -user -userid username -checkid [-admin]

**Linux**

DirectoryAdmin.sh -user -userid username -checkid [-admin]
Parameters

The following options are available for the DirectoryAdmin command.

-user
   The command line option that specifies that this task is to work with users.

-userid username
   Specifies the name of the user to search for. Note that the user ID syntax
differs depending on the user registry that is configured in IBM WebSphere
Application Server (local, OS, LDAP , or custom).

Local OS on UNIX
   Provide the UNIX user ID, such as "isadmin."

Local OS on Windows
   COMPUTER_NAME\userid, such as MYSERVER\isadmin where
   MYSERVER is the name of the Microsoft Windows computer. If the
   Microsoft Windows computer is registered in a domain, the syntax
   might also be DOMAIN_NAMEuserid. The name must be uppercase.

LDAP
   The full distinguished name (DN) must be provided in the proper case.
   For more information on retrieving the DN, refer to "LDAP
distinguished name (DN) determination" on page 49.

Note: To include users with long and composed user IDs, like LDAP fully
qualified names, surround the user IDs with double quotation marks when
using the command.

-checkid
   Ensures that the given user ID already exists in the configured directory before
   creating or updating the user in the security directory.

-admin
   (Optional) Assigns the IBM InfoSphere Information Server Suite Administrator
   role to the user, if the user exists.

Configuring the IBM InfoSphere Information Server user registry
to use the internal user registry

Use this command to point the IBM InfoSphere Information Server user registry to
the internal user registry.

IBM WebSphere Application Server does not need to be running to run this
command. If IBM WebSphere Application Server is up and running, it must be
restarted for these changes to take effect.

Use this command only for troubleshooting. If there are some errors in the
auto-configuration mechanism during IBM WebSphere Application Server startup,
you can use the DirectoryAdmin command to force the provider change. This
command can be used as a recovery or resolution mechanism.

Syntax

Windows
DirectoryAdmin.bat -set_provider ISF

Linux UNIVERSITY
DirectoryAdmin.sh -set_provider ISF
Parameters

The following options are available for the DirectoryAdmin command.

- **set_provider**
  The command line option that sets a provider to active.

**ISF**
Indicates that the tool should configure the InfoSphere Information Server user registry to use the internal user registry.

**Configuring the IBM InfoSphere Information Server user registry to use the application server registry**
Use this command to point the IBM InfoSphere Information Server user registry to the application server registry.

The application server does not need to be running to run this command. If it is running, it must be restarted for these changes to take effect.

Use this command only for troubleshooting. If there are errors in the auto-configuration mechanism during application server startup, you can use the DirectoryAdmin command to force the provider change. This command can be used as a recovery or resolution mechanism.

**Syntax**

**Windows**
DirectoryAdmin.bat -set_provider J2EE

**Linux**
DirectoryAdmin.sh -set_provider J2EE

**Parameters**

The following options are available for the DirectoryAdmin command.

- **set_provider**
  The command line option that sets a provider to active.

**J2EE**
Indicates that the tool should configure the InfoSphere Information Server user registry to use the IBM WebSphere Application Server user registry.

**Deleting users from the IBM InfoSphere Information Server user registry**
Use this command to delete users from the IBM InfoSphere Information Server user registry. This command deletes all the users in the InfoSphere Information Server user registry. If you are using an external user registry, such as LDAP or a local operating system user registry, this command deletes only the proxies of the users that were created in the internal repository and their role assignments.

IBM WebSphere Application Server does not need to be running to run this command. This command should only be used for troubleshooting or recovery.

You can use this command when changing the user registry configuration after the system has been in production. This command removes all security settings for all users. You can then safely switch to a different user registry.
Attention: This command deletes all the users in the InfoSphere Information Server user registry. From the IBM InfoSphere Information Server Web console, you can delete users selectively.

Use this command only for troubleshooting.

Syntax

**Windows**

```batch
DirectoryAdmin.bat -delete_users
```

**Linux**

```bash
DirectoryAdmin.sh -delete_users
```

**Parameters**

The following options are available for the `DirectoryAdmin` command.

- `delete_users`
  
  Deletes all the users in the IBM InfoSphere Information Server user registry.

**Deleting groups from the IBM InfoSphere Information Server user registry**

Use this command to delete groups from the IBM InfoSphere Information Server user registry. This command deletes all the groups in the InfoSphere Information Server user registry. If you are using an external registry, such as LDAP or a local operating system user registry, this command deletes only the proxies of the groups that were created in the internal repository and their role assignments.

IBM WebSphere Application Server does not need to be running to run this command. This command should only be used for troubleshooting or recovery.

You can use this command when changing the user registry configuration after the system has been in production. This command removes all security settings for all groups which allows for a safe switch to a different registry.

Attention: This command deletes all the groups in the InfoSphere Information Server user registry. From the IBM InfoSphere Information Server Web console, you can delete groups selectively.

Use this command only for troubleshooting.

Syntax

**Windows**

```batch
DirectoryAdmin.bat -delete_groups
```

**Linux**

```bash
DirectoryAdmin.sh -delete_groups
```

**Parameters**

The following options are available for the `DirectoryAdmin` command.
-delete_groups
   Deletes all the groups in the InfoSphere Information Server user registry.

Searching for users in the configured user registry
Use this command to specify a user name criterion and return a list of users that
meet that criterion in the configured user registry. This command should only be
used for troubleshooting or recovery.

IBM WebSphere Application Server must be running to run this command.

Syntax

Windows
DirectoryAdmin.bat -user -search -idp userid_pattern -max_count maxcount

Parameters

The following options are available for the DirectoryAdmin command.

-user
   The command line option that specifies that this task is to work with users.

-search
   Specifies that the DirectoryAdmin command should perform a search.

-idp
   Specifies the user name pattern to search for. The pattern must contain either
   the full user name or, if the full user name is not used, a part of the user name
   with a prepended or appended asterisk (*). For example, you might want to
   use DirectoryAdmin -user -search -idp a* -max_count 4 to search for all
   users whose user names start with "a".

-max_count
   Limits the number of users that are returned as part of the search.

Searching for groups in the configured user registry
Use this command to specify a group name criterion and return a list of groups
that meet that criterion in the configured user registry. This command should only
be used for troubleshooting or recovery.

IBM WebSphere Application Server must be running to run this command.

Syntax

Windows
DirectoryAdmin.bat -group -search -idp userid_pattern -max_count maxcount

Parameters

The following options are available for the DirectoryAdmin command.
The command line option that specifies that this task is to work with groups.

-search
Specifies that the DirectoryAdmin command should perform a search.

-idp
Specifies the group ID pattern to search for. The pattern must contain either the full group name or, if the full group name is not used, a part of the group name with a prepended or appended asterisk (*). For example, you might want to set -idp group* to return all groups that start with group, such as "groupname" or "grouplogin".

-max_count
Limits the number of groups that are returned as part of the search.

Displaying user details
Use this command to query for detailed information about a user, such as the security roles that are assigned to the user name or the groups that the user belongs to. This command should only be used for troubleshooting or recovery.

IBM WebSphere Application Server must be running to run this command.

Syntax

Windows
DirectoryAdmin.bat -user -userid username -display

Linux
DirectoryAdmin.sh -user -userid username -display

Parameters

The following options are available for the DirectoryAdmin command.

-user
The command line option that specifies that this task is to work with users.

-userid username
Specifies the name of the user to look up the details for. Note that the user ID syntax differs depending on the user registry that is configured in IBM WebSphere Application Server (local, OS, LDAP, or custom).

Local OS on UNIX
Provide the UNIX user ID, such as "isadmin."

Local OS on Windows
COMPUTER_NAME\userid, such as MYSERVER\isadmin where MYSERVER is the name of the Microsoft Windows computer. If the Microsoft Windows computer is registered in a domain, the syntax might also be DOMAIN_NAME\userid. The name must be uppercase.

LDAP
The full distinguished name (DN) must be provided in the proper case. For more information on retrieving the DN, refer to "LDAP distinguished name (DN) determination" on page 49.

Note: To add users with long and composed user ids, like LDAP fully qualified names, surround the user IDs with double quotation marks when using the tool.
Accessing LDAP attributes
When the IBM WebSphere Application Server user registry is configured as a federated repository, you can use the DirectoryAdmin tool to map the attributes. When this is done, the directory service is able to access the user and group attributes stored in the LDAP user registry. For example, when you search for user and group attributes, the mapped attributes are also retrieved. The IBM InfoSphere Information Server user and group information includes the mapped attribute values from the federated repositories.

Procedure
1. To use the DirectoryAdmin tool to set and display LDAP attribute mappings, refer to the IBM WebSphere Application Server documentation to first configure the user registry as a federated repository, using the WebSphere Application Server Virtual Member Manager (VMM) interface:
2. Once configured, use the DirectoryAdmin tool with the -set_attribute_map parameter to map attribute names in the federated repository configuration to the InfoSphere Information Server attribute names. The mapping configuration settings are stored in the repository.
3. Restart WebSphere Application Server.
4. After the mappings are set and the application server is restarted, you can use the DirectoryAdmin tool with the -display_attribute_map parameter to display them for verification.

After the mappings are made, searches on the mapped attribute values are done in the VMM, that is, on the external user registries for the mapped attributes. Attributes that are not mapped will continue to be used to search the internal user registry. The results of the external and internal user registry searches are merged into a single result set.

Syntax

```
Syntax
```

```
Linux | UNIX
DirectoryAdmin.sh
[{-set_attribute_map|sam}]
[{-user_map|um} user_mapping]
[{-group_map|gm} group_mapping]
[{-display_attribute_map|dam}]

Windows
DirectoryAdmin.bat
[{-set_attribute_map|sam}]
[{-user_map|um} user_mapping]
[{-group_map|gm} group_mapping]
[{-display_attribute_map|dam}]
```
Parameters

The following options are available for the DirectoryAdmin command.

- `{set_attribute_map|sam}`
  The command parameter used to create mappings between VMM attributes and IBM InfoSphere Information Server attributes. Use this parameter in conjunction with the -user_map parameter, the -group_map, or both.

- `{user_map|um} user_mapping`
  The mapping to use to associate VMM user attributes with IBM InfoSphere Information Server user attributes. The user_mapping value is specified as `ldapAttr=isfAttr[,ldapAttr=isfAttr]+`, where `ldapAttr` is the name of the attribute in the VMM-configured registry, and `isfAttr` is the corresponding attribute in the IBM InfoSphere Information Server internal user registry. For a reference of the available VMM attributes see [http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.wim.doc/dataobjectperson.html](http://pic.dhe.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.wim.doc/dataobjectperson.html) In WebSphere Application Server, it is also possible to configure different VMM attributes.

<table>
<thead>
<tr>
<th>isfAttr</th>
<th>Description (and a typical ldapAttr to use in the mapping, if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail</td>
<td>email address (mail)</td>
</tr>
<tr>
<td>firstName</td>
<td>first name (givenName)</td>
</tr>
<tr>
<td>lastName</td>
<td>last name (sn)</td>
</tr>
<tr>
<td>title</td>
<td>title (title)</td>
</tr>
<tr>
<td>jobTitle</td>
<td>job title</td>
</tr>
<tr>
<td>homePhone</td>
<td>home phone</td>
</tr>
<tr>
<td>imName</td>
<td>instant messaging name</td>
</tr>
<tr>
<td>location</td>
<td>location</td>
</tr>
<tr>
<td>officePhone</td>
<td>office phone number (telephoneNumber)</td>
</tr>
<tr>
<td>cellPhone</td>
<td>mobile phone number (mobile)</td>
</tr>
<tr>
<td>pagerNumber</td>
<td>pager phone number (pager)</td>
</tr>
<tr>
<td>faxNumber</td>
<td>FAX phone number (facsimileTelephoneNumber)</td>
</tr>
<tr>
<td>businessAddr</td>
<td>business address (businessAddress)</td>
</tr>
<tr>
<td>organization</td>
<td>organization name</td>
</tr>
</tbody>
</table>

If the -user_map argument is specified with no data, then the configuration setting will be cleared.

- `{group_map|gm} group_mapping`
  The LDAP group mapping to map to the LDAP user. The group_mapping value is specified as `ldapAttr=isfAttr[,ldapAttr=isfAttr]+`, where `ldapAttr` is the name of the attribute in the VMM-configured registry, and `isfAttr` is the corresponding attribute in the IBM InfoSphere Information Server internal user registry.

<table>
<thead>
<tr>
<th>isfAttr</th>
<th>Description (and a typical ldapAttr to use in the mapping, if any)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>group name (cn)</td>
</tr>
<tr>
<td>type</td>
<td>group type</td>
</tr>
</tbody>
</table>
If the -group_map argument is specified with no data, then the configuration setting will be cleared.

-\{display_attribute_map|dam\}
   Displays the current attribute mapping information.

Example

After configuring the IBM WebSphere Application Server user registry as a federated repository, run the DirectoryAdmin tool to set the mapping.

```
DirectoryAdmin.bat -sam -um "mail=mail,sn=lastName,givenName=firstName" -gm "cn=name"
```

Display the mapping to verify its settings.

```
DirectoryAdmin.bat -dam
```

Example output:

User attribute mappings:
  mail = mail
  sn = lastName
  givenName = firstName

Group attribute mappings:
  cn = name

Now, you can access the mapping in the user registry, for example to search for and retrieve LDAP user and group attributes.

The following example illustrates how to delete the user attribute mapping:

```
DirectoryAdmin.bat -sam -um
```

Troubleshooting examples that use the DirectoryAdmin tool

If you run into the following problems while administering IBM InfoSphere Information Server, you can use the DirectoryAdmin tool to help you determine and address the problem.

Lost user password

This example is only applicable to internal user registry configuration. From the command line, enter the following command:

```
DirectoryAdmin.bat -user -userid admin_user_id -password new_password
```

You can provide the password as plain text or as a string that has been encrypted with the encrypt command.

Note: If you have multiple InfoSphere Information Server Suite Administrators, you could instead ask one of these administrators to log in to the IBM InfoSphere Information Server Web console and reset the lost user password in the IBM InfoSphere Information Server Web console.
User registry configuration is not working and you cannot log in to the IBM InfoSphere Information Server Web console

To reset the user registry configuration to use the IBM InfoSphere Information Server internal user registry:

1. From the command line, set the InfoSphere Information Server to use the InfoSphere Information Server internal user registry by entering the following command:
   ```batch
   DirectoryAdmin.bat -set_provider ISF
   ```
2. Create the default InfoSphere Information Server Suite administrator user by using the following command:
   ```batch
   DirectoryAdmin.bat -user -userid default_isadmin_userid -password password -admin
   ```
   You can provide the password as plain text or as a string that has been encrypted with the `encrypt` command.
3. Log in to the IBM WebSphere Application Server Administrator console and set the IBM WebSphere Application Server user registry to the InfoSphere Information Server internal user registry.

To reset the user registry configuration to use the IBM WebSphere Application Server user registry:

1. Ensure that the IBM WebSphere Application Server user registry is configured to use the local operating system user registry or LDAP user registry of your choice.
2. From the command line, set InfoSphere Information Server to use the IBM WebSphere Application Server user registry by entering the following command:
   ```batch
   DirectoryAdmin.bat -set_provider J2EE
   ```
3. Assign a user the necessary security roles to make that user the default InfoSphere Information Server Suite Administrator by entering the following command:
   ```batch
   DirectoryAdmin.bat -user -userid default_isadmin -admin
   ```
The default InfoSphere Information Server administrator user syntax differs depending on the user registry that is configured in IBM WebSphere Application Server.

**Local OS on UNIX**
Provide the UNIX user ID, such as "isadmin."

**Local OS on Windows**
COMPUTER_NAME\userid, such as MYSERVER\isadmin where MYSERVER is the name of the Microsoft Windows computer. If the Microsoft Windows computer is registered in a domain, the syntax might also be DOMAIN_NAME\userid. The name must be uppercase.

**LDAP**
The full distinguished name (DN) must be provided in the proper case. For more information on retrieving the DN, refer to "LDAP distinguished name (DN) determination" on page 49.

**DirectoryCommand tool**
You can use the DirectoryCommand tool to run some of the same operations that can be from the Web Console. With the tool, you can add users, add groups, add users to groups, add roles to users, add roles to groups, and so on.
Usage

On the services tier, the command is installed in the following location:

- **Linux**
  
  `IS_install_path/ASBServer/bin/DirectoryCommand.sh`

- **Windows**
  
  `IS_install_path\ASBServer\bin\DirectoryCommand.bat`

On the client, the command is installed in the following location:

- **Linux**
  
  `IS_install_path/ASBNode/bin/DirectoryCommand.sh`

- **Windows**
  
  `IS_install_path\ASBNode\bin\DirectoryCommand.bat`

The command has many options that control a separate operation. The tool supports multiple operations to be specified at the same time. For example, you could specify both the `-add_user` and the `-add_group` options in the same run of the tool. The operations can be run in batch by using the `-file` option, or they can be run in a script. See the examples at the bottom of this topic.

Syntax

```
DirectoryCommand
  [-{add_ds_credentials | ds_cred} value]
  [-{add_group | a_grp} value]*
  [-{add_user | a_usr} value]*
  [-{add_users_group | a_usr_grp} value]*
  [-{assign_group_roles | grp_roles} value]*
  [-{assign_user_roles | usr_roles} value]*
  [-{assign_project_group_roles | proj_grp_roles} value]
  [-{assign_project_user_roles | proj_usr_roles} value]
  [-authfile value]
  [-{datastage_server | ds_svr} value]
  [-{delete_group | del_grp} value]
  [-{delete_user | del_usr} value]
  [-{details | det}] [-{file | f} value]
  [-{force}]
  [-{get_default_ds_credentials | get_dflt_ds_cred}]
  [-{host | ?}]
  [-{list | l} value]
  [-{log | l} value]
  [-{logerror | error} value]
  [-{loginfo | info} value]
  [-{loglevel | level} value]
  [-{password | pwd} value]
  [-{port | p} value]
  [-{primary}]
  [-{remove_group_roles | rm_grp_roles} value]
  [-{remove_project_group_roles | rm_proj_grp_roles} value]
  [-{remove_project_user_roles | rm_proj_usr_roles} value]
  [-{remove_user_roles | rm_usr_roles} value]
  [-{remove_users_group | rm_usr_grp} value]
  [-{results | res} value]
  [-{separator | sep} value]
  [-{set_default_ds_credentials | set_dflt_ds_cred} value]
  [-{set_shared_registry | shr_reg} value]
  [-{sub_list_separator | sub_list_sep} value]
  [-{update_group | upd_grp} value]
  [-{update_user | upd_usr} value]
  [-{user | usr} value]
  [-{verbose | v}]
```
Parameters

Command parameter syntax
The \{x | y\} syntax of the parameters indicates that you can enter either the long form of the parameter (x) or the shortcut parameter name (y). The value indicates that a value must be specified. Each parameter description that follows indicates the syntax of the parameters and associated values. The asterisk (*) on the specification means that the command parameter can be repeated multiple times in the same command line.

Value lists and sublists
Most of the operational parameters have values that consist of lists and sublists.

- In the value list syntax, \["value"]* means that you can optionally specify a list of the indicated values separated by the separator character, a tilde (~) by default.
- A list is a set of values separated by a character, a tilde (~) by default. In some lists, the actual value assigned is determined by the position of the value in the list, such as in the -add_group and -add_user options. For each value in the list, if not all values are assigned between values, at least the separator character must be specified so that the position can be determined. Any trailing separators, however, should be omitted.
  \n  ListValue1~ListValue2~~~ListValue5
  
  For example, the following list is used to add a new user and assign the user ID, password, first name, last name, job title, and business phone number:
  -add_user "jsmith~pa55word~John~Smith~DS Admin~408-555-0122"
- A sublist is a set of values also separated by a character. Sublists differ from lists in that they are accompanied by another sublist, separated by a different character, a dollar sign ($) by default. For sublists, the values are not positional. The values of each sublist are assigned to the values of the accompanying sublists.
  Sublist1Value1$Sublist1Value2$Sublist2Value1$Sublist2Value2$Sublist3Value1$Sublist3Value2
  
  For example, the following sublists are used to assign the roles in the right sublist to the user in the left sublist:
  -assign_user_roles adminUser$SuiteUser$DataStageAdmin

[-{add_ds_credentials | ds_cred} value]
Maps one or more user credentials to the specified operating system user credentials for the engine, which is specified with the -datastage_server parameter, which must be included with this one. Specify the value as one string with the following syntax:

userID["userID"]+credUserID=credPassword

The value must contain at least one sublist separator character ($). If multiple user IDs are specified, they are all assigned the specified credentials. The password value can be specified as plain text or as text encrypted with the encrypt command.

To clear the credentials, pass a quoted exclamation mark (!) as either the credUserID or credPassword values.

[-{add_group | a_grp} value]*
Create a group. Multiple instances of this option can be specified. Specify the value as one string with the following syntax:
Each entry in the value must contain at least one separator character (~).

[-{add_user | a_usr} value]*
Create a user. Multiple instances of this option can be specified. Specify the value as one string with the following syntax:

```
userId~password~firstName~lastName
```

Each entry in the value must contain at least one separator character (~). The password value can be specified as plain text or as text encrypted with the encrypt command.

[-{add_users_group | a_usrgrp} value]*
Add users to groups. Multiple instances of this option can be specified. Specify the value as one string with the following syntax:

```
userId~userId*$groupId~groupId*
```

The value must contain at least one sublist separator character ($). For sublists that contain multiple entries, each entry of one sublist is assigned to each entry of the other sublist.

[-{assign_group_roles | grp_roles} value]*
Assign roles to groups. Multiple instances of this option can be specified. Specify the value as one string with the following syntax:

```
groupId~groupId*$roleId~roleId*
```

The value must contain at least one sublist separator character ($). For sublists that contain multiple entries, each entry of one sublist is assigned to each entry of the other sublist.

[-{assign_user_roles | usr_roles} value]*
Assign roles to users. Multiple instances of this option can be specified. Specify the value as one string with the following syntax:

```
userId~userId*$roleId~roleId*
```

The value must contain at least one sublist separator character ($). For sublists that contain multiple entries, each entry of one sublist is assigned to each entry of the other sublist.

[-{assign_project_group_roles | proj_grp_roles} value]
Assign project group roles. Multiple instances of this option can be specified. Specify the value as one string with the following syntax:

```
projectName~projectName*$groupId~groupId*$roleId
```

The value must contain 2 sublist separator characters ($). For sublists that contain multiple entries, each entry of each sublist is assigned to each entry of the other sublists. The projectName values are case sensitive and must be in the format of DSServer/projectID, where DSServer must match the registered engine name. The name could be registered as the short host name or as the fully qualified host name with a domain. Whichever way it is registered, this is
how it must be specified here. You can see a list of project names by using the
-list DSPROJECTS option. The roleID must be an InfoSphere DataStage project
role.

[-{assign_project_user_roles | proj_usr_roles} value]
Assign project user roles. Multiple instances of this option can be specified.
Specify the value as one string with the following syntax:

\[\text{projectName}[^\text{projectName}]\ast\text{userId}[^\text{userId}]\ast\text{roleID}\]

The value must contain 2 sublist separator characters ($). For sublists that
contain multiple entries, each entry of each sublist is assigned to each entry of
the other sublists. The projectName values are case sensitive and must be in
the format of DSServer/projectID, where DSServer must match the registered
engine name. The name could be registered as the short host name or as the
fully qualified host name with a domain. Whichever way it is registered, this is
how it must be specified here. You can see a list of project names by using the
-list DSPROJECTS option. The roleID must be an InfoSphere DataStage project
role.

[-authfile value]
Use the specified credentials file for the credentials of the administrator user
ID running this command. Either the -authfile option or the -user and
-password options are required.

[-{datastage_server | ds_svr} value]
Specifies the host name or configured alias name of the InfoSphere Information
Server engine to use when setting the shared registry and when setting and
getting the engine credentials. The value cannot contain a forward slash
character (/). The value is validated against the engines that are registered
with IBM InfoSphere Information Server.

You must specify this -datastage_server parameter when you use following
parameters:
• -add_ds_credentials
• -get_default_ds_credentials
• -set_default_ds_credentials
• -set_shared_registry

[-{delete_group | del_grp} value]
Delete existing groups. Specify the value as one string with the following
syntax:

\[\text{groupId}[^\text{groupId}]\ast\]

You will be prompted to confirm the delete unless the -force option is
specified. If a specified group does not exist, it will be ignored.

[-{delete_user | del_usr} value]
Delete existing users. Specify the value as one string with the following syntax:

\[\text{userId}[^\text{userId}]\ast\]

You will be prompted to confirm the delete unless the -force option is
specified. If a specified user does not exist, it will be ignored.

[-{details | det}]
Provides additional information in the output when used with the -list option
for USERS and GROUPS.

For users, the following information is provided:
• detailed user information
• groups that the user is a member of
• suite and product roles that are assigned to the user
• mapped engine credentials for this user

For groups, the following information is provided:
• detailed group information
• suite and product roles that are assigned to the group

[-{file | f} value]
Read the commands from a file. When you specify the -file option, other specified command options are ignored. See the end of this topic for an example of how to use the -file option. If you intend to load a large number of users with the file option, break them up so that each file contains about 100 users to avoid server time outs.

In a file, each command must be specified on a separate line and must end with a semicolon (;). This is true even for command options that have additional required options, such as -separator, -sublist_separator, -datastage_server, -details, and -force. The commands with these options must also each be on a separate line, and the line must be terminated with a semicolon. The value specified for these applies to all commands included in the file.

[-force]
Suppress the confirmation prompt for the -delete_user and -delete_group options.

[-{get_default_ds_credentials | get_dflt_ds_cred}]
Retrieve the default credentials for the InfoSphere Information Server engine that is specified with the -datastage_server option.

[-{help | ?}]
Display usage information.

[-host value]
The host name of the services tier computer. The default value is localhost.

[-list value]
List the existing users, groups, InfoSphere DataStage projects, or system-defined roles. Specify the value as one string with the following syntax:

```
type[^"type]*
```

The type values can be USERS, GROUPS, ROLES, DSPROJECTS, or ALL.

[-{log | l} value]
Print all runtime output to the specified file.

[-{logerror | error} value]
Print all ERROR and FATAL runtime logging messages to the specified file.

[-{loginfo | info} value]
Print all INFO, WARN, DEBUG, and TRACE runtime logging messages to the specified file.

[-{loglevel | level} value]
The level at which runtime logging messages are enabled. The value can be FATAL, ERROR, INFO, WARN, DEBUG, TRACE, or ALL.

[-{password | pwd} value]
The password for the suite administrator user ID running this command.
[-port value]
The HTTP port of the services tier computer. The default value is 9080.

[-primary]
Log in to the primary services host if one is available. If this option is used, the
-host and -port options are ignored.

[-{remove_group_roles | rm_grp_roles} value]
Removes roles from groups. Multiple instances of this option can be specified.
Specify the value as one string with the following syntax:

\[groupId[^groupId]*$roleId[^roleId]*\]

The value must contain at least one sublist separator character ($). For sublists
that contain multiple entries, each entry of the role sublist is removed from
each entry of the group sublist.

[-{remove_project_group_roles | rm_proj_grp_roles} value]
Removes project user roles. Multiple instances of this option can be specified.
Specify the value as one string with the following syntax:

\[projectName[^projectName]*$groupId[^groupId]*$roleId[^roleId]*\]

For sublists that contain multiple entries, each entry of the group and role
sublists are removed from each entry of the project sublist. The projectName
values are case sensitive and must be in the format of \texttt{DSServer/projectID},
where \texttt{DSServer} must match the registered engine name. The name could be
registered as the short host name or as the fully qualified host name with a
domain. Whichever way it is registered, this is how it must be specified here.
You can see the list of project names by using the -list DSPROJECTS option.

[-{remove_project_user_roles | rm_proj_usr_roles} value]
Removes project user roles. Multiple instances of this option can be specified.
Specify the value as one string with the following syntax:

\[projectName[^projectName]*$userId[^userId]*$roleId[^roleId]*\]

For sublists that contain multiple entries, each entry of the user and role
sublists are removed from each entry of the project sublist. The projectName
values are case sensitive and must be in the format of \texttt{DSServer/projectID},
where \texttt{DSServer} must match the registered engine name. The name could be
registered as the short host name or as the fully qualified host name with a
domain. Whichever way it is registered, this is how it must be specified here.
You can see the list of project names by using the -list DSPROJECTS option.

[-{remove_user_roles | rm_usr_roles} value]
Removes roles from users. Multiple instances of this option can be specified.
Specify the value as one string with the following syntax:

\[userId[^userId]*$roleId[^roleId]*\]

The value must contain at least one sublist separator character ($). For sublists
that contain multiple entries, each entry of the role sublist is removed from
each entry of the user sublist.

[-{remove_users_group | rm_usr_grp} value]
Removes users from groups. Multiple instances of this option can be specified.
Specify the value as one string with the following syntax:

\[groupId[^groupId]*$userId[^userId]*\]
The value must contain at least one sublist separator character ($). For sublists that contain multiple entries, each entry of the user sublist is removed from each entry of the group sublist.

```
[-{results | res} value]
```

Print all the runtime output to the specified file.

```
[-{seperator | sep} value]
```

Overides the default list separator (-). The value can be any single character other than those listed:

- ^ (caret)
- & (ampersand)
- * (asterisk)
- - (dash or hyphen)
- | (pipe)
- " (quotation mark)
- < (less than)
- > (greater than)

If you want to specify a character value that has special meaning to the command shell (for example, # or !), specify the character in single quotes, such as: -seperator '#'.

```
[-{set_default_ds_credentials | set_dflt_ds_cred} value]
```

Sets the default InfoSphere Information Server engine credentials. Specify the value as one string with the following syntax:

```
credUserId~credPassword
```

The value must contain at least one separator character (~). The credentials are set for the server specified by the -datastage_server option. The specified engine must be registered with InfoSphere Information Server. The password value can be specified as plain text or as text encrypted with the encrypt command.

To clear the default credentials, pass a quoted exclamation mark ('!'') as either the credUserId or credPassword values.

```
[-{set_shared_registry | shr_reg} {ON|OFF}]
```

Sets the flag that indicates whether InfoSphere Information Server and InfoSphere DataStage share the same user registry. The valid values are ON or OFF.

```
[-{sub_list_separator | sub_list_sep} value]
```

Overides the default list separator ($). The value can be any single character other than those listed:

- ^ (caret)
- & (ampersand)
- * (asterisk)
- - (dash or hyphen)
- | (pipe)
- " (quotation mark)
- < (less than)
- > (greater than)
If you want to specify a character value that has special meaning to the command shell (for example, # or !), specify the character in single quotes, such as: -separator '#'.

[-{update_group | upd_grp} value]*
Update an existing group. Multiple instances of this option can be specified. The group being updated must exist. Specify the value as one string with the following syntax:

```
groupId~name~groupType~webAddress
"location"~officePhoneNumber~cellPhoneNumber
"pagerNumber"~faxNumber~emailAddress
"businessAddress"~organization
```

Each entry in the value must contain at least one separator character (~). A value of '!' specified for a group setting will clear the setting.

[-{update_user | upd_usr} value]
Update an existing user. Multiple instances of this option can be specified. The user being updated must exist. Specify the value as one string with the following syntax:

```
userId~password~firstName~lastName
"title"~jobTitle~homePhoneNumber~imName
"location"~officePhoneNumber~cellPhoneNumber
"pagerNumber"~faxNumber~emailAddress
"businessAddress"~organization
```

Each entry in the value must contain at least one separator character (~). A value of '!' specified for a user setting other than password will clear the setting. The password value can be specified as plain text or as text encrypted with the encrypt command.

[-{user | usr} value]
The suite administrator user ID running this command. Either the -authfile option or the -user and -password options are required.

[-{verbose | v}] Display detailed runtime output other than logging messages.

**Example: Writing a script to quickly add users to a typically used project**

Suppose you regularly add new InfoSphere DataStage users to multiple projects with various group assignments. You could create a script for these operations:

```sh
#!/bin/sh
echo Adding a typical DataStage user with the default password.

npass={iisenc}HEf6s6cG+Ee6NdGDQppQNg=
nrole=DataStageUser
prole=DataStageOperator
cmd=/opt/IBM/InformationServer/ASBNode/bin/DirectoryCommand.sh
af=/opt/IBM/InformationServer/ASBNode/conf/isadmin.credentials

echo New user ID to create:
read nuser
echo First name for the user:
read fname
echo Last name for the user:
read lname

$cmd -authfile $af -a_usr $nuser~$npass~$fname~$lname
```

Chapter 6. Managing security 141
Windows

@echo off
setlocal

echo Adding a typical DataStage user with the default password.

set npass={iisenc}HEf6s6cG+Ee6NdGDQppQNg==
set nrole=DataStageUser
set prole=DataStageOperator
set cmd=C:\IBM\InformationServer\ASBNode\bin\DirectoryCommand.bat
set af=C:\IBM\InformationServer\ASBNode\conf\isadmin.credentials

echo New user ID to create
set /p nuser="--> "

echo First name for the new user
set /p fname="--> "

echo Lastname for the new user
set /p lname="--> "

call %cmd% -authfile %af% -a_usr %nuser%~%npass%~%fname%~%lname%
call %cmd% -authfile %af% -usr_roles %nuser%$%nrole%
call %cmd% -authfile %af% -a_usr_grp %nuser%~dsusr~qsusr
call %cmd% -authfile %af% ^
    -proj_usr_roles HOSTNAME/DSProd~HOSTNAME/DSDev$%nuser%$%prole%

In this example, the following values would need to be replaced with actual values. The groups and projects must be created before running the command.

- dsusr and qsusr: groups that the user is being added to
- HOSTNAME: the registered engine host name or configured DSAlias for the engine.
- DSProd and DSDev: project names that the user is being added to as an InfoSphere DataStage operator.

This script would create the specified user ID and assign the default password, which has been encrypted with the encrypt command and pasted into the script. (You could send e-mail with the plain text password to the user with a request to change it upon first login.) The DirectoryCommand then assigns the user to the DataStageUser role. It then assigns the user to the dsusr and qsusr groups. It then assigns the user to the DSProd and DSDev projects on the InfoSphere Information Server engine, indicated here as HOSTNAME. And, in the same command, assigns the user to the DataStageOperator project role.

Example: Using the -file option to migrate users

1. Create the list of users:
   DirectoryCommand -authfile admin.creds
   -host original_services_tier_host
   -port original_services_tier_port
   -list ALL -details -results userlist.txt

2. Edit the list of users into a format that the -file option can use:
   -add_user TestOper"TempP4ss"TestOperFirst"TestOperLast;
   -add_user TestSuOper"TempP4ss"TestSuOperFirst"TestSuOperLast;
   -add_user TestProMan"TempP4ss"TestProManFirst"TestProManLast;
   -add_user adminUser"TempP4ss"adminUserFirst"adminUserLast;
   -assign_user_roles TestOper$SuiteUser"DataStageUser"FastTrackUser"GlossaryUser;
   -assign_user_roles TestSuOper$SuiteUser"DataStageUser"
-assign_user_roles TestProMan$SuiteUser~DataStageUser;
-assign_user_roles adminUser$SuiteUser~DataStageAdmin;
-assign_user_roles wasUser$SuiteAdmin~DataStageAdmin;
-add_group TestGroup~TestGroup~TestGroup;
-proj_usr_roles dshost/dstage1~dshost/dstage2$TesProMan$DataStageProductionManager;

3. Run the directory command to migrate the users to the new server:
   DirectoryCommand -authfile admin.creds -host new_server
   -port new_port -file userlist.txt

Encrypt command

The encrypt command provides a method to encrypt user credentials. The encrypted strings can be stored in a credentials file or used on the command line with many IBM InfoSphere Information Server tools.

The command uses Advanced Encryption Standard (AES) 128-bit encryption as the default provider, which meets US export regulation requirements. You might also choose to provide your own password encryption algorithm.

Running the encrypt command

You run the encrypt command in a command window to encrypt text strings. The encrypted and encoded strings can then be used for user credentials in a credentials file for later use. You can also use the command to encrypt any data that you want to encrypt. You can use the provided default encryption provider, or you can set up your own custom encryption provider.

About this task

You run the encrypt command with no parameters or with the text to encrypt as the first and only parameter. The second option is less secure, especially if your shell command history is enabled. When you run the encrypt command with no parameter, you are prompted for a text string, which is hidden from the terminal.

The string that you provide is encrypted with the configured encryption provider, and the encrypted output is displayed in base64-encoded format, prefixed with an alias. You then copy and paste the encoded string—including the alias prefix—to your desired location. The location could be a credentials file or a value for the password parameter in some commands. When the string is decrypted, the alias name is used to determine the type of encryption provider that was used.

When you run the encrypt command, use the full path name. The encrypt command is located in the following locations, depending on which tiers are installed on your computer:

- **Linux**
  - install_root/InformationServer/ASBNode/bin/encrypt.sh
  - install_root/InformationServer/ASBServer/bin/encrypt.sh

- **Windows**
  - install_root\InformationServer\ASBNode\bin\encrypt.bat
  - install_root\InformationServer\ASBServer\bin\encrypt.bat
Procedure

1. Optional: If you have configured your own custom encryption provider, ensure that you have specified the provider in the appropriate `iis.crypto.site.properties` file. You must create the properties file in the `conf` directory, under the same parent directory as the encrypt command that you will run.

   Command location:
   `install_root\InformationServer\ASBNode\bin\encrypt.bat`
   Its properties file location:
   `install_root\InformationServer\ASBNode\conf\iis.crypto.site.properties`

   Command location:
   `install_root\InformationServer\ASBServer\bin\encrypt.bat`
   Its properties file location:
   `install_root\InformationServer\ASBServer\conf\iis.crypto.site.properties`

   The contents of the `iis.crypto.site.properties` file is one entry:
   `iis.crypto.default.provider=class_of_custom_provider`

2. Using the full path name, run the encrypt command, with or without the text to be encrypted as a parameter. If the text contains spaces, enclose it in quotation marks.

   • Running the encrypt command with the text provided on the command line:
     `bash$: /opt/IBM/InformationServer/ASBNode/bin/encrypt.sh myPa$$w0rd`
     `bash$: {iisenc}PvqKLr7z3QOLJCQ4QhbrrA==`

   • Running the encrypt command with a prompt to hide the text:
     `bash$: /opt/IBM/InformationServer/ASBNode/bin/encrypt.sh`
     `bash$: Enter the text to encrypt:
     bash$: Enter the text again to confirm:
     bash$: {iisenc}PvqKLr7z3QOLJCQ4QhbrrA==`

3. Copy the encrypted string to a credentials file or as a value to the password parameter for any of the commands that support it. For example:

   • Used in a credentials file:
     ```
     user=dsadm
     password={iisenc}PvqKLr7z3QOLJCQ4QhbrrA==
     ```

   • Used on the command line:
     ```
     AppServerAdmin -username isadmin -password {iisenc}YJD9OKOxT2otQvTQFca1qg==
     ```

The credentials file

The credentials file contains user credentials that can be used by many IBM InfoSphere Information Server commands that support the `-authfile` option, such as dsjob, DirectoryCommand, and others.

Attention: Because the credentials file is used to run commands that require a password, it is essential to store the credentials file in a secure location and hide its contents. The file must not be readable, writeable, or executable by anyone other than a user or group with administrator access. Also, users that run commands that use the credentials file must have the same access as the file.

The credentials file has the following format:

• It must be encoded with your platform default character set or ASCII characters only.
• Each entry must occupy a whole line without leading and trailing white space.
• The file must contain a user and password entry, although some tools, such as **dsjob** support additional name-value pairs, such as domain and server.

• The name and value pairs are separated by an equals sign (=). For example:

  name=value

• When a value is specified in encrypted text, it must have been encrypted with the encrypt command. The encrypted string is prefixed with '{alias}', where alias is the alias of the encryption provider.

• When a value is specified in plain, non-encrypted text, the value must not start with an opening brace ({{) nor contain a closing brace (}}) in the plain text string.

• You can add comment lines, which must start with the number sign (#).

• If the same key name exists multiple times in the file, the first name-value pair is used.

A sample credentials file:

```java
# dsadm credentials
user=dsadm
password={iisenc}HEf6s6cG+Ee6NdG0ppQNg==
server=RemoteServer
```

**Adding a custom encryption provider**

You can create and configure your own encryption provider. If you want to provide your own encryption, you can do so by creating an implementation of the EncryptionProvider interface.

**Procedure**

1. In the JAR file containing your custom class, create a file named `META-INF\services\com.ibm.iis.spi.security.crypto.EncryptionProvider`, which must list the class name of your encryption provider implementation. The encryption provider is loaded as a service provider. See the Java documentation for information about service providers.

2. Deploy your class files in the class path of the Java runtime environment.
   a. Copy your JAR file to the following directories, depending on the tiers installed on the computer.
      • `install_root/InformationServer/ASBNode/lib/java`
      • `install_root/InformationServer/ASBServer/lib/java`
   b. Add the full paths to these JAR files to the ISF_UTIL_EXT_CP environment variable. The value of this environment variable is added to the class path when the encrypt command is run from either of these directories:
      • `install_root/InformationServer/ASBNode/bin`
      • `install_root/InformationServer/ASBServer/bin`

3. To use your new custom encryption provider when you run the encrypt command, create a file named `iis.crypto.site.properties` in the following directories, depending on the tiers installed on the computer.

   ```text
   install_root/InformationServer/ASBNode/conf
   install_root/InformationServer/ASBServer/conf
   ```

   Include the following one-line entry in the file:

   ```
   iis.crypto.default.provider=class_name_of_your_custom_provider
   ```
Results

With these changes, when you run the encrypt command, your custom encryption provider is used to encrypt the text.

Note: If you have previously created a different custom encryption provider, then it can still be used to decrypt text that has been encrypted with it. To continue to use a previous provider along with the new one, you must keep both sets of JAR files in the class path. You must also ensure that the providers use unique aliases.

EncryptionProvider interface:

Reference for the interface implemented by encryption providers.

```
public interface com.ibm.iis.spi.security.crypto.EncryptionProvider
```

The encrypt and decrypt methods are the encryption and decryption methods for the provider.

The getAlias method must return a short name (usually an acronym) that uniquely identifies the encryption provider. This alias can be used by callers to mark the encrypted data with a prefix in braces ({} ) to determine which provider was used to encrypt the data. IBM InfoSphere Information Server uses the standard Java service provider mechanism to load the encryption provider from the class path. Therefore, the `META-INF/services/com.ibm.iis.spi.security.crypto.EncryptionProvider` configuration file must be created and bundled. The location of the JAR file to use for compilation is `installation_directory/InformationServer/ASBNode/eclipse/plugins/com.ibm.isf.client/iis_util.jar`. See the Java documentation for information about service providers.

Method summary

<table>
<thead>
<tr>
<th>Returns</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>byte[]</code></td>
<td><code>decrypt(byte[] encryptedBytes)</code></td>
</tr>
<tr>
<td></td>
<td>The decrypt method takes an encrypted array of bytes and returns a decrypted array of bytes.</td>
</tr>
<tr>
<td><code>byte[]</code></td>
<td><code>encrypt(byte[] clearBytes)</code></td>
</tr>
<tr>
<td></td>
<td>The encrypt method takes an array of bytes and returns an encrypted array of bytes.</td>
</tr>
<tr>
<td><code>java.lang.String</code></td>
<td><code>getAlias()</code></td>
</tr>
<tr>
<td></td>
<td>Returns the encryption provider alias.</td>
</tr>
<tr>
<td><code>void</code></td>
<td><code>initialize(java.util.HashMap initData)</code></td>
</tr>
<tr>
<td></td>
<td>Reserved for future use.</td>
</tr>
</tbody>
</table>

Method detail

```
getAlias
getAlias()
```
Returns the encryption provider alias. The encryption provider alias is alphanumeric ASCII characters, which can contain only [0-9][a-z][A-Z]. It must uniquely identify the encryption provider. The return value of this method is used by callers to prefix the encrypted data with `{alias_value}`. The alias itself cannot contain opening brace (`) or closing brace (`) characters.

**Returns:**

`String`

**initialize**

```java
initialize(java.util.HashMap initData) throws InitializationException
```

Reserved for future use.

**Parameters:**

`java.util.HashMap - initData`

**Throws:**

`InitializationException`

**encrypt**

```java
encrypt(byte[] clearBytes)
```

The encrypt method takes an array of bytes and returns an encrypted array of bytes.

**Parameters:**

`byte[] - clearBytes`

**Returns:**

`byte[]`

**decrypt**

```java
decrypt(byte[] encryptedBytes)
```

The decrypt method takes an encrypted array of bytes and returns a decrypted array of bytes.

**Parameters:**

`byte[] - encryptedBytes`

**Returns:**

`byte[]`

**Enabling stronger encryption:**

IBM provides Java Cryptography Extension (JCE) unlimited jurisdiction policy files that allow the use of stronger (longer) key sizes for Java encryption. If you want to create a custom encryption provider using these stronger key sizes, download and install the IBM unlimited jurisdiction policy files using the following steps.

**About this task**

These Java JCE unlimited jurisdiction policy files contain keys that are longer than 128 bits. You can find more information about the encryption algorithms and key sizes of the IBM JRE and these policy files in Appendixes A, B, and E of the JCE API Specification & Reference at developerWorks® [http://www.ibm.com/developerworks/java/jdk/security/60/secguides/JceDocs/api_users_guide.html#AppA](http://www.ibm.com/developerworks/java/jdk/security/60/secguides/JceDocs/api_users_guide.html#AppA).
Procedure
2. Click the IBM SDK Policy files link.
3. Log in with your IBM user ID and password.
4. Select Unrestricted JCE Policy files for SDK 1.4.2 and click Continue.
5. Select Unrestricted JCE Policy files for SDK for all newer versions and click Continue.
6. If you accept the license, download unrestrict142.zip and extract the local_policy.jar and US_export_policy.jar files.
7. Save these two files to the root_directory/InformationServer/ASBNode/apps/jre/lib/security directory and root_directory/InformationServer/ASBServer/apps/jdk/jre/lib/security directories, and replace the existing files of the same names.
8. Restart the JRE for the new policy to be effective.

What to do next

Create and add a custom implementation of the EncryptionProvider interface that uses these policy files.
Chapter 7. Activating entitled IBM InfoSphere DataStage editions and feature packs

If your entitlement to IBM InfoSphere DataStage editions, trade-up, or feature packs changes after you have installed IBM InfoSphere Information Server, you must activate any newly entitled items before you can use them. If you no longer have entitlements for items, you must deactivate them.

When you install IBM InfoSphere DataStage by using the InfoSphere Information Server installation program, the program prompts you to select the InfoSphere DataStage editions and feature packs to install and activate. Each item in the selection list enables associated InfoSphere DataStage canvases and job features. Select the items for which you have a valid Proof of Entitlement from IBM. The installation program activates the features that are associated with the items that you select. Any other editions or feature packs are deactivated and cannot be used.

If you later acquire entitlements for an additional InfoSphere DataStage edition or feature pack, to use the features that are included in the item you must activate the item within InfoSphere Information Server. If you no longer have entitlement for an item, you must deactivate it. When you deactivate the edition or feature pack, the features within the item are no longer available for use.

To activate or deactivate an edition or feature pack, run the LicensingServiceAdmin command-line tool.

If you installed InfoSphere DataStage, the full product with all optional features was installed. However, the installation program activated only the features that are associated with the edition and features that you selected at install time. If you acquire entitlements for additional InfoSphere DataStage features, enable them by using the LicensingServiceAdmin tool. Also use the tool if you are entitled to an additional edition or trade up to a different edition.

For example, a company is entitled to IBM InfoSphere DataStage Server, and enables this item. At a later time, they become entitled to the IBM InfoSphere DataStage from DataStage Server Trade Up. They use the LicensingServiceAdmin tool to enable the full functionality of the InfoSphere DataStage product.

As another example, a company is entitled to InfoSphere DataStage, and enables this item. At a later time, they become entitled to the IBM InfoSphere DataStage Balanced Optimization feature pack and add the IBM InfoSphere DataStage MVS Edition. They enable these editions and features by using the LicensingServiceAdmin tool.

The following table lists the InfoSphere DataStage editions and feature packs that the InfoSphere Information Server installation program can install. The table also lists the features that are included within each item.
### Table 9. InfoSphere DataStage editions and feature packs

<table>
<thead>
<tr>
<th>Installable item</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM InfoSphere DataStage</td>
<td>• InfoSphere DataStage job features</td>
</tr>
<tr>
<td></td>
<td>• Parallel canvas</td>
</tr>
<tr>
<td></td>
<td>• Server canvas</td>
</tr>
<tr>
<td>IBM InfoSphere DataStage Server Edition</td>
<td>• InfoSphere DataStage job features</td>
</tr>
<tr>
<td></td>
<td>• Server canvas</td>
</tr>
<tr>
<td>IBM InfoSphere DataStage MVS Edition</td>
<td>• InfoSphere DataStage job features</td>
</tr>
<tr>
<td></td>
<td>• MVS (mainframe) canvas</td>
</tr>
<tr>
<td>IBM InfoSphere DataStage Pack for SAS</td>
<td>• SAS features</td>
</tr>
<tr>
<td>IBM InfoSphere DataStage Balanced Optimization</td>
<td>• InfoSphere DataStage balanced optimization features</td>
</tr>
</tbody>
</table>

If jobs are created that depend upon certain editions or feature packs, and those editions or feature packs are deactivated, the jobs remain in the repository. However, they cannot be opened, or cause an error message when opened.

### Viewing a list of activated IBM InfoSphere DataStage editions and feature packs

Run the `LicensingServiceAdmin` command line tool to list the activated IBM InfoSphere DataStage editions and feature packs within your suite.

#### Before you begin

You must have at least Suite User authority.

#### Procedure

1. Log in to the computer on which the `LicensingServiceAdmin` tool is installed:
   - If you have implemented IBM WebSphere Application Server clustering within your installation, log in to the computer that hosts the WebSphere Application Server Deployment Manager.
   - If you have not implement clustering, log in to the services tier computer.
   In either case, use an account that has execution permission for the tools in the `ASBServer/bin` directory, as described in the next step.
2. Change to the `ASBServer/bin` directory within the directory in which IBM InfoSphere Information Server is installed. For example:
   - Linux/UNIX: `cd /opt/IBM/InformationServer/ASBServer/bin`
   - Windows: `cd C:\IBM\InformationServer\ASBServer\bin`
3. Run the `LicensingServiceAdmin` command with the `-list_features` option. Instead of the `-user` and `-password` options, you can provide a credentials file with the `-authfile` option. If you do not provide a user, password, or credentials file, you are prompted for a user ID and password.
   - Linux/UNIX: `./LicensingServiceAdmin.sh -user iauser -password iapswd -list_features`
   - Windows: `LicensingServiceAdmin -user iauser -password iapswd -list_features`
In the command,

- **iuser** is the name of a user that has suite user authority.
- **iapswd** is the user password.

The command lists the features that are activated. Deactivated features are not listed. For example:

```
DS,DS$Server,DSMVS,BalOpt,SAS,QS
```

**Enabled components:**
- IBM InfoSphere DataStage
- IBM InfoSphere DataStage Server
- IBM InfoSphere DataStage MVS Edition
- IBM InfoSphere DataStage Balanced Optimization
- IBM InfoSphere DataStage Pack for SAS
- IBM InfoSphere QualityStage
- DataStage and QualityStage Administrator
- DataStage and QualityStage Director
- DataStage and QualityStage Designer

**Enabled features:**
- `job-type = DataStage`
- `job-type = QualityStage`
- `licensed-feature = BAL_OPT`
- `licensed-feature = SAS_PACK`
- `canvas = Parallel`
- `canvas = Server`
- `canvas = MVS`

Since IBM InfoSphere QualityStage shares the InfoSphere DataStage components and client applications, it is also listed as one of the activated features if InfoSphere QualityStage is installed. Even though it is listed as one of the features, InfoSphere QualityStage cannot be activated or deactivated with the **LicensingServiceAdmin** tool. To activate InfoSphere QualityStage, install InfoSphere QualityStage by using the installation program. To deactivate InfoSphere QualityStage, uninstall InfoSphere QualityStage by using the software removal program.

The list of enabled InfoSphere DataStage and InfoSphere QualityStage client applications is also shown. All three applications are enabled when InfoSphere QualityStage or any version of InfoSphere DataStage is installed. If IBM InfoSphere Information Analyzer is installed without InfoSphere DataStage or InfoSphere QualityStage, then only the InfoSphere DataStage and QualityStage client is enabled.

### Activating and deactivating IBM InfoSphere DataStage editions and feature packs

Run the **LicensingServiceAdmin** command-line tool to change the InfoSphere DataStage features that were activated when the services tier was installed. The tool can activate or deactivate InfoSphere DataStage editions and feature packs within your suite if InfoSphere DataStage is installed.

**Before you begin**

You must have suite administrator authority.

**About this task**

To activate or deactivate InfoSphere DataStage editions and feature packs in the suite, run the **LicensingServiceAdmin** command. Each time you run the command, specify all items that you want to activate. Any editions or feature packs that you do not specify are deactivated by the command. The actual features enabled
depend on the combination of editions and features that you specify. For this reason, they must all be provided in a single command.

The tool cannot be used to activate InfoSphere DataStage features if InfoSphere DataStage is not installed. Also the tool cannot be used to deactivate all InfoSphere DataStage features. To remove all InfoSphere DataStage features, remove InfoSphere DataStage by using the IBM InfoSphere Information Server software removal program.

Procedure
1. Log in to the computer on which the LicensingServiceAdmin tool is installed:
   - If you have implemented IBM WebSphere Application Server clustering within your installation, log in to the computer that hosts the WebSphere Application Server Deployment Manager.
   - If you have not implemented clustering, log in to the services tier computer.
   In either case, use an account that has execution permission for the tools in the ASBServer/bin directory, as described in the next step.
2. Change to the ASBServer/bin directory within the directory in which InfoSphere Information Server is installed. For example:
   - Linux/UNIX cd /opt/IBM/InformationServer/ASBServer/bin
   - Windows cd C:\IBM\InformationServer\ASBServer\bin
3. Run the LicensingServiceAdmin command with the -set_features option.
   Instead of the -user and -password options, you can provide a credentials file with the -authfile option. If you do not provide a user, password, or credentials file, you are prompted for a user ID and password.

   ./LicensingServiceAdmin.sh -user isadmin -password ispswd -set_features codes

   LicensingServiceAdmin -user isadmin -password ispwd -set_features codes

   In the command,
   - isadmin is the name of a user that has suite administrator authority.
   - ispwd is the user password.
   - codes is a comma-separated list of codes that specify the editions and feature packs to activate. The following table describes valid feature codes:

<table>
<thead>
<tr>
<th>Feature code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS</td>
<td>Activates IBM InfoSphere DataStage</td>
</tr>
<tr>
<td>DSServer</td>
<td>Activates IBM InfoSphere DataStage Server</td>
</tr>
<tr>
<td>DSMVS</td>
<td>Activates IBM InfoSphere DataStage MVS Edition</td>
</tr>
<tr>
<td>SAS</td>
<td>Activates IBM InfoSphere DataStage Pack for SAS</td>
</tr>
<tr>
<td>BalOpt</td>
<td>Activates IBM InfoSphere DataStage Balanced Optimization</td>
</tr>
</tbody>
</table>

Table 10. Feature codes for LicensingServiceAdmin

Each time you run the command, specify the feature codes for all editions and feature packs to activate. Include any editions and feature packs that are already activated, that you want to remain activated. Any editions and feature packs that you do not list in the command are deactivated.
If you are entitled to both IBM InfoSphere DataStage Server and IBM InfoSphere DataStage from DataStage Server Trade Up, specify the DS feature code only. Do not specify the DSServer feature code.

Feature codes are not case sensitive. To include white space within the feature code list, enclose the list in quotation marks.

For example, to activate InfoSphere DataStage, InfoSphere DataStage Balanced Optimization, and the InfoSphere DataStage Pack for SAS, run the following command.

```
LicensingServiceAdmin -user isadmin -password ispwd -set_features DS,SAS,BalOpt
```

The command activates the features. In this example, the Mainframe canvas is not enabled within the InfoSphere DataStage client applications. The command then lists the results:

```
DS,SAS,BalOpt,QS
```

**Enabled components:**
- IBM InfoSphere DataStage
- IBM InfoSphere DataStage Pack for SAS
- IBM InfoSphere DataStage Balanced Optimization
- IBM InfoSphere QualityStage
- DataStage and QualityStage Administrator
- DataStage and QualityStage Director
- DataStage and QualityStage Designer

**Enabled features:**
- job-type = DataStage
- job-type = QualityStage
- licensed-feature = BAL_OPT
- licensed-feature = SAS_PACK
- canvas = Parallel
- canvas = Server

Since IBM InfoSphere QualityStage shares the InfoSphere DataStage components and client applications, it is also listed as one of the activated features if InfoSphere QualityStage is installed. Even though it is listed as one of the features, InfoSphere QualityStage cannot be activated or deactivated with the `LicensingServiceAdmin` tool. To activate InfoSphere QualityStage, install InfoSphere QualityStage by using the installation program. To deactivate InfoSphere QualityStage, uninstall InfoSphere QualityStage by using the software removal program.

The list of enabled InfoSphere DataStage and InfoSphere QualityStage client applications is also shown. All three applications are enabled when InfoSphere QualityStage or any version of InfoSphere DataStage is installed. If IBM InfoSphere Information Analyzer is installed without InfoSphere DataStage or InfoSphere QualityStage, then only the InfoSphere DataStage and QualityStage client is enabled.

---

**LicensingServiceAdmin command reference**

Run the `LicensingServiceAdmin` command to manage activation and deactivation of IBM InfoSphere DataStage editions and feature packs after InfoSphere DataStage is installed.

**Purpose**

If you are entitled to certain InfoSphere DataStage editions or feature packs after you run the IBM InfoSphere Information Server installation program, run this command to activate the newly entitled items. If you no longer have entitlements for the items, run this command to deactivate them.
If you no longer have entitlement to any InfoSphere DataStage edition or feature, you must remove InfoSphere DataStage by using the InfoSphere Information Server software removal program. You cannot use the tool to deactivate all InfoSphere DataStage editions and features.

If you have implemented IBM WebSphere Application Server clustering within your installation, the command is located on the computer that hosts the WebSphere Application Server Deployment Manager. If you have not implemented clustering, the command is located on the services tier computer.

The command can be found on the services tier computer, in the ASBServer/bin subdirectory of the directory in which InfoSphere Information Server is installed. For example:

- Linux
  /opt/IBM/InformationServer/ASBServer/bin
- Windows
  C:\IBM\InformationServer\ASBServer\bin

To use the tool, log in by using an account that has execution permission for the tools in this directory.

**Command syntax**

For **Linux** or **UNIX**:

```
```

For **Windows**:

```
```

**Parameters**

- **help**
  Displays usage information for the tool.

- **authfile credentials_filename**
  The name of the credentials file that contains the user ID and password of a user that has suite administrator authority. You can use this option in place of the user and password options.

- **user user**
  The name of a user that has suite administrator authority. You can use the -user option or its short form: -u.

- **password password**
  The password for the user. You can use the -password option or its short form: -p.

- **set_features featurecodes**
  Specifies a list of InfoSphere DataStage editions and feature packs to activate. The items are specified as a comma-separated list of codes. The following table describes valid feature codes. Feature codes are not case sensitive.

**Table 11. Feature codes for LicensingServiceAdmin**

<table>
<thead>
<tr>
<th>Feature code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS</td>
<td>Activates IBM InfoSphere DataStage</td>
</tr>
<tr>
<td>DSServer</td>
<td>Activates IBM InfoSphere DataStage Server</td>
</tr>
<tr>
<td>Feature code</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DSMVS</td>
<td>Activates IBM InfoSphere DataStage MVS Edition</td>
</tr>
<tr>
<td>SAS</td>
<td>Activates IBM InfoSphere DataStage Pack for SAS</td>
</tr>
<tr>
<td>BalOpt</td>
<td>Activates IBM InfoSphere DataStage Balanced Optimization</td>
</tr>
</tbody>
</table>

Each time you run the command, specify the feature codes for all editions and feature packs to activate. Include any editions and feature packs that are already activated, that you want to remain activated. Any editions and feature packs that you do not listed in the command are deactivated.

If you are entitled to both IBM InfoSphere DataStage Server and IBM InfoSphere DataStage from DataStage Server Trade Up, specify the DS feature code but not the DSServer feature code.

You can use the `-set_features` option or its short form: `-sf`.

**list_features**

Causes `LicensingServiceAdmin` to output a list of activated editions and feature packs. If the `-set_features` option is also specified, the `LicensingServiceAdmin` command activates the specified editions and feature packs and then outputs the list. The list is output to stdout.

You can use the `-list_features` option or its short form: `-lf`.

The following command activates all editions and feature packs, and lists the activated items on a Linux or UNIX computer:

```
/opt/IBM/InformationServer/ASBServer/bin/LicensingServiceAdmin.sh
-u myadmin -p myadminpwd -lf -sf DS,DSMVS,BalOpt,SAS,DSServer
```
Chapter 8. Managing active sessions

In the IBM InfoSphere Information Server Web console, you can view a list of all the users that are currently connected to the server that you logged in to.

About this task

You can view the starting time of each session and the timestamp of the most recent action that each user performed. You can force active sessions to end immediately, which is useful when preparing to stop the system.

Viewing all active sessions

In the IBM InfoSphere Information Server Web console, you can view and manage the active user sessions.

Before you begin

You must have suite administrator authority.

About this task

A user session is an instance of a user with a connection to the IBM InfoSphere Information Server. You might want to view all of the active sessions to determine if you need to set thresholds for the maximum amount of user sessions to allow, to disconnect one or more users, or to view details about the user who is connecting.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Session Management > Active Sessions. The Active Sessions pane shows the users who are currently connected to the server.

Setting session limits

You can set the maximum number of active sessions on the server. You can also specify how long a session can remain inactive before it is automatically disconnected and how often the sessions are polled for inactivity.

Before you begin

You must have suite administrator authority.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Session Management > Active Sessions.
3. In the Active Sessions pane, click Global Session Properties.
4. Optional: Specify settings for inactive sessions and maximum number of sessions.
5. Click **Save and Close**.

---

### Opening user details

To view information about a current session that includes the user record, the duration of the session, and the security roles that are assigned to the user, you can open the details of a user session.

**Before you begin**

You must have suite administrator authority.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Session Management > Active Sessions**.
3. In the Active Sessions pane, select a user session.
4. Click **Open**. The Open User Details pane shows detailed information about the user session.

---

### Disconnecting all sessions

To force all of the active sessions to end immediately, you can disconnect all of the user sessions. You might want to disconnect all users to prepare for a system shutdown.

**Before you begin**

You must have suite administrator authority.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Session Management > Active Sessions**.
3. In the Active Sessions pane, click **Disconnect All**.
4. In the Disconnect All window, click **Yes** to immediately end all sessions.

---

### Disconnecting a session

You can disconnect an individual user session.

**Before you begin**

You must have suite administrator authority.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Session Management > Active Sessions**.
3. In the Active Sessions pane, select a session. If multiple users signed in with the same user account, only the selected session is disconnected.
4. Click **Disconnect**.
5. Click **Yes** to immediately end the session.
Chapter 9. Managing repositories

You can centrally manage the installed repositories that are used by various tools and product modules in IBM InfoSphere Information Server.

When you install InfoSphere Information Server, you create and register the repositories needed for the various product modules. The product modules’ repositories are located within one or more databases on one or more database servers. Regardless of the location of a repository, its name must be unique across all database servers in InfoSphere Information Server. Likewise, database names must also be unique.

Although you register repositories during installation, there might be cases where you want to change and manage the repositories, for example, if you are moving from test into production or if you want to add another operational database for an additional engine. There are various tasks for managing repositories and various reasons for doing each.

RepositoryAdmin tool reference

Metadata about the repositories that are used in IBM InfoSphere Information Server is stored in the metadata repository. The RepositoryAdmin tool is provided for you to define and manage this metadata for some of the repositories.

Purpose

You can use the installation program to create the repositories used by InfoSphere Information Server. You can also choose to create some of the repositories as a post-installation step, for example if you are not using the DB2 database system. If you do not use the installation program to create a particular repository, you can use the RepositoryAdmin tool to create the SQL scripts necessary to create and configure the repository. You also use the tool to register the repository (and its hosting database, database platform, and database server) with the metadata repository.

Even after installation, there might be times when you need to manage the repository registration, such as when you relocate a repository to another server or if you need to change the connection properties.

You cannot manage the following repositories with the RepositoryAdmin tool:

- Metadata repository
- IBM InfoSphere Metadata Asset Manager staging area
- IBM InfoSphere Information Analyzer analysis databases

Syntax

RepositoryAdmin[.bat|.sh]

[-connectionManagedDSN | cm] <value>
[-connectionName | cn] <value>
[-connectionPassword | cw] <value>
[-connectionProperties | cp] <value>
[-connectionURL | cr] <value>
[-connectionUser | cu] <value>
[-databaseType | dt] <value>
Usage

Some of the commonly-used parameters are listed in the topics that follow. The `RepositoryAdmin` tool must be run from the services tier. In each of the following topics, the `RepositoryAdmin` tool is displayed with just the name of the command with the Microsoft Windows .bat extension. However, when you run the command, provide the correct extension for the operating system and the full path to the command (or include the directory that contains the command in your PATH environment variable). The full path and extension of the command is as follows:

- **Windows**
  ```bash
  is_install_dir\ASBServer\bin\RepositoryAdmin.bat
  ```
- **Linux**
  ```bash
  is_install_dir/ASBServer/bin/RepositoryAdmin.sh
  ```
List and display options

Use the following options to list and display information about your registered repositories, databases, database platforms, database servers, and SQL scripts.

The list options list the entities that are registered with the metadata repository. The display options display information about a particular entity. The display options can be used to create the properties files that are required for the registration options.

- listDatabasePlatforms
  Shorthand: -lp
  Lists the database platforms supported by the current version of IBM InfoSphere Information Server.
  Example command string:
  RepositoryAdmin.bat -listDatabasePlatforms

  Example output:
  DB2 9.5
  DB2 9.7
  DB2 10.1
  ORACLE 10g
  ORACLE 11g
  SQLSERVER 2005
  SQLSERVER 2008
  SQLSERVER 2012

  Restriction: In InfoSphere Information Server Version 9.1, DB2 9.5 and Oracle 10g are supported only if you have upgraded from an earlier version of InfoSphere Information Server.

- listDatabaseServers -databaseType type -databaseVersion version
  Shorthand: -ls -dt type -dv version
  Lists each of the database servers that are registered with a given database platform. You can obtain the available database platforms with the listDatabasePlatforms option.
  Example command string:
  RepositoryAdmin.bat -listDatabaseServers -dt DB2 -dv 10.1

  Example output:
  DB2 10.1 on localhost:50000
  SQLSERVER 2012 on host25:1433
  SQLSERVER 2012 on host37:1433

- listDatabases
  Shorthand: -ld
  Lists the registered databases.
  Example command:
  RepositoryAdmin.bat -listDatabases

  Example output:
-listRepositories

Shorthand: -lr

Lists the registered repositories. A repository is implemented as a separate schema in a given database and has its own set of tablespaces and associated user connections. In that sense multiple repositories can be collocated in the same database or be created in separate databases. If the repository context information was provided when the repository was registered or updated, it will be displayed next to the repository, as in the first line of the following example output.

Example command:
RepositoryAdmin.bat -listRepositories

Example output:
odb (production)
srd

-listSQLScripts -databaseType type -databaseVersion version -scriptTool tool

Shorthand: -lt -dt type -dv version -sto tool

Lists each of the SQL scripts that are registered with a given tool for a given database platform. You can obtain the available database platforms with the `listDatabasePlatforms` option. The following tools are available:

- DataQualityConsole
- DataStage
- StandardizationRulesDesigner

Example command string:
RepositoryAdmin.bat -listSQLScripts -dt DB2 -dv 10.1 -sto DataStage

Example output:
dsodb_db_creation
dsodb_drop_tables
dsodb_grant_permissions_newdb
dsodb_grant_permissions_newschema
dsodb_remove_db
dsodb_remove_functions
dsodb_remove_schema
dsodb_remove_user
dsodb_table_creation
dsodb_tablespace_creation
dsodb_upgrade_87to91
dsodb_user_config

-displayDatabasePlatform -databaseType type -databaseVersion version [-results filename]

Shorthand: -dp -dt type -dv version [-res filename]

Displays details about a particular database platform. The values that you provide for the type and version must match exactly that which is displayed with the `listDatabasePlatforms` option. The `results` option can be used for all command options to redirect the results to a file; however, it is most useful for the `display*` options to create files to use when registering objects.
Example command:
RepositoryAdmin -displayDatabasePlatform -dt DB2 -dv 10.1

Example output:
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabasePlatform.jdbcDriverClass=com.ibm.db2.jcc.DB2Driver
DatabasePlatform.jdbcJarFiles=db2jcc.jar,db2jcc_license_cu.jar

-displayDatabaseServer -databaseType type -databaseVersion version
-serverHost hostname [-results filename]

Shorthand: -ds -dt type -dv version -sh hostname [-res filename]

Displays details about a particular database server. The values that you provide for the type, version, and host name must match exactly that which is displayed with the [listDatabaseServers] option. The -results option can be used for all command options to redirect the results to a file; however, it is most useful for the -display* options to create files to use when registering objects.

Example command:
RepositoryAdmin -displayDatabaseServer -dt DB2 -dv 10.1 -sh localhost

Example output:
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=localhost
DatabaseServer.port=50000
DatabaseServer.binPath=C:\IBM\SQLLIB\BIN
DatabaseServer.adminUser=db2admin
DatabaseServer.adminPassword={iisenc}fwGPejos3/I1QmTGHExwGc==

-displayDatabase -dbName name [-results filename]

Shorthand: -dd -dn name [-res filename]

Displays details about a particular database. The value that you provide for the name must match exactly that which is displayed with the [listDatabases] option. The -results option can be used for all command options to redirect the results to a file; however, it is most useful for the -display* options to create files to use when registering objects.

Example command:
RepositoryAdmin -displayDatabase -dn odb

Example output:
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=localhost
DatabaseServer.port=50000
Database.name=odb
Database.alias=odb
Database.location=C:\

-displayRepository -reposName name [-results filename]

Shorthand: -dr -rn name [-res filename]

Displays details about a particular repository. The name that you provide for the repository must match exactly the name that is displayed with the [listRepositories] option. The -results option can be used for all command
options to redirect the results to a file; however, it is most useful for the `display*` options to create files to use when registering objects.

Example command:
```
RepositoryAdmin -displayRepository -rn odb
```

Example output:
```
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=localhost
DatabaseServer.port=50000
Database.name=odb
Database.alias=odb
Database.location=C:\
Repository.name=odb
Repository.description=Production engine ODB.
Repository.tool=DataStage
Repository.context=production
Repository.schema=odb
RepositoryConnection.name=odb
RepositoryConnection.userName=odb
RepositoryConnection.password={iisenc}gwFQseoj24I/SnCFEH+cWg==
RepositoryConnection.connectionURL=jdbc:db2://localhost:50000/odb
RepositoryConnection.managedDataSourceName=odb
Tablespace.name=DSODBSPACE
```

**Tip:** You can capture the output produced by the `-displayRepository` option to create a properties file that you can use as a starting point to register another repository. To capture the output, either redirect to a file or provide a filename with the `-results` option.

Example:
```
RepositoryAdmin.bat -displayRepository -rn odb -res odb.properties
```

Make edits, such as changing the server from 'localhost' to 'testserver' and the database from 'odb' to 'odb1', then register the new repository.
```
RepositoryAdmin.bat -registerRepository -propertyFile odb.properties
```

**-displayRepositoryConnection -connectionName name -reposName name [-results filename]**

Shorthand: `-dc -cn name -rn name [-res filename]`

Displays details about the connection for a repository. The `-results` option can be used for all command options to redirect the results to a file; however, it is most useful for the `display*` options to create files to use when registering objects.

Example command:
```
RepositoryAdmin.bat -displayRepositoryConnection -cn odb -rn odb
```

Example output:
```
RepositoryConnection.name=odb
RepositoryConnection.userName=odb
RepositoryConnection.password={iisenc}gwFQseoj24I/SnCFEH+cWg==
RepositoryConnection.connectionURL=jdbc:db2://localhost:50000/odb
RepositoryConnection.managedDataSourceName=odb
```

**Note:** Currently, RepositoryConnection.managedDataSourceName is not used and is optional.
The option to save SQL scripts

Use the following option to save SQL scripts.

*saveSQLScripts [-databaseType type] [-databaseVersion version] [-reposTool name] [ -reposName name] [-scriptLocation path]*

Shorthand: *-sss [-dt type] [-dv version] [-to name] [-rn name] [-sl path]*

Retrieves the SQL scripts associated with a specified tool for a given database platform. You can provide the tool and database platform as parameters or you can provide a repository name. If you provide the tool and database platform, the original scripts will be saved as registered. If you provide a repository name, the formal script parameters will be replaced with the respective repository registration properties before the scripts are saved. If you provide a script location, the files will be saved there.

Example command, using the tool and database platform as parameters:

```
RepositoryAdmin -saveSQLScripts -dt DB2 -dv 10.1 -to DataStage
```

This command saves the SQL scripts as they were originally registered without performing any parameter substitution.

Example command, using the repository and optional script location as parameters:

```
RepositoryAdmin -saveSQLScripts -rn odb -sl C:\tmp
```

This command saves the SQL scripts after first substituting the formal parameters with the respective repository registration properties. The scripts are saved in C:\tmp.

Registration options

Use the following options to register repositories, databases, and servers with the metadata repository.

Each of the registration options requires the use of the *propertyFile* option and a properties file. Some product modules provide property file templates that you can edit, such as one for an IBM InfoSphere DataStage operations database. Or, if a repository similar to the one that you want to register has already been registered, then you can use a display option with the *results* parameter to redirect the output to a file and edit the resulting file. You can also, of course, create the properties file from scratch. Each of the following options shows an example properties file with the entries that are required for the particular entity to be registered.

*registerRepository -propertyFile filename*

Shorthand: *-rr -pf filename*

Registers a repository with the metadata repository. A repository is typically registered by the installation program during its corresponding tool installation, or manually as part of an upgrade. New repositories can also be registered for any given tool after installation, for tools that support multiple repositories, or as part of the process of relocating an existing repository to a different database.

The properties file that you provide with the command must contain at least the properties identifying the database with which the repository is to be registered, in addition to the full set of required repository properties.

Example command:
RepositoryAdmin.bat -registerRepository -pf odb.properties

Example of a properties file with the properties needed for repository registration:

```
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=localhost
DatabaseServer.port=50000
Database.name=odb
Database.alias=odb
Database.location=C:\
Repository.name=odb
Repository.description=Production engine ODB.
Repository.tool=DataStage
Repository.context=production
Repository.schema=odb
RepositoryConnection.name=odb
RepositoryConnection.userName=odb
RepositoryConnection.password={iisenc}gwFQseoj24I/SnCFEH+cWg==
```

Tip: It is best to provide the password as an encrypted string by using the `encrypt` command, or you can provide a plain text password. The password is stored in encrypted form, however, and will always be shown as an encrypted string when you display the repository.

If you have not yet registered a server or database, these will also be registered when you register the repository. In such a case, however, your properties file must contain the necessary information associated with the database and server to be registered.

In this example, a new repository named odb is registered with a database named odb. If the database is not already registered, then the database is first registered with the database server on the host localhost for the DB2 10.1 platform. If the database server is not already registered, the database server is registered so that the new database and repository can be registered with it. The repository connection is also registered.

If you are registering a new repository, you can provide the `-saveSQLScripts` parameter at the same time that you register a repository. By specifying this parameter, the SQL scripts necessary to create and set up the repository, with replaced parameters, are saved to disk. For example:

```
RepositoryAdmin.bat -rr -pf odb.properties -saveSQLScripts
```

Saving the SQL scripts here is a shortcut to avoid the need to run the RepositoryAdmin tool again with the `-saveSQLScripts` parameter.

**-registerDatabase -propertyFile filename**

Shorthand: `-rd -pf filename`

Registers a database with the metadata repository. The database is typically registered by the installation program as part of the repository registration during the installation process. You can register a database on its own, independently of any tool after installation, and then register new repositories with the database later.

The properties file that you provide with the command must contain at least the properties identifying the database server with which the database is to be registered, in addition to the full set of required database properties.

Example command:

```
RepositoryAdmin.bat -registerDatabase -propertyFile dbsrv.properties
```
Example properties file:
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=localhost
DatabaseServer.port=50000
Database.name=odb
Database.alias=odb
Database.location=C:\

-registerDatabaseServer -propertyFile filename

Shorthand: -rs -pf filename

Registers a database server with the metadata repository. The database server is typically registered by the installation program as part of the repository registration during the installation process. You can register a server on its own, independently of any tool after installation, and then register new databases with the server later.

The properties file that you provide with the command must contain at least the properties identifying the database platform with which the database server is to be registered, in addition to the full set of required database server properties.

Example command:
RepositoryAdmin.bat -registerDatabaseServer -propertyFile dbsrv.properties

Example properties file:
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=localhost
DatabaseServer.port=50000
DatabaseServer.binPath=C:\IBM\SQLLIB\BIN
DatabaseServer.adminUser=db2admin
DatabaseServer.adminPassword={iisenc}fwGPejos3/I1QmTGHExwGc==

Tip: It is best to provide the password as an encrypted string by using the encrypt command, or you can provide a plain text password. The password is stored in encrypted form, however, and will always be shown as an encrypted string when you display the database server.

Update options
Use the following options to update registrations of the database repositories, database servers, and repository connections.

-updateRepository -reposName name -reposContext name -description "description"

Shorthand: -ur -rn name -ct name -de "description"

Updates a repository registration with the information provided. The repository context and description can be any string that is useful to you. For example, if you have multiple operations databases, you might want to add keywords to indicate the context in which each is used and more fully describe each repository in the description.

Example command:
RepositoryAdmin.bat -updateRepository -rn odb -ct QA -de "QA engine ODB"

-updateRepositoryConnection -connectionName name -reposName name [-connectionPassword "password"] [-connectionURL URL] [-connectionProperties {property=value}...]

Chapter 9. Managing repositories 169
Shorthand: `-uc -cn name -rn name [-cw "password"] [-cr URL] [-cp {property=value}...]

Updates the repository connection registration with the information provided. If you are updating a password, you can provide the plain text password or a string encrypted by the `encrypt` command. You can add or modify other connection properties as well by providing the properties and values. The properties can be specific to a database or JDBC driver and are intended to be used to handle special cases, as needed. If you provide more than one property and value combination, separate them by a semi-colon (;). It’s good practice to always test the connection after updating the connection properties.

Example command that updates a password and sets some additional properties:
```
RepositoryAdmin.bat -updateRepositoryConnection -cn odb -rn odb -cw "{iisenc}gwFQseojZ4I/SnCFEH+cWg==" -cp traceFileSize=2621440;traceOption=1
```

If you want to remove a property, provide the property name without a value as in the following example.

Example command that removes a property:
```
RepositoryAdmin.bat -updateRepositoryConnection -cn odb -rn odb -cp traceOption=
```

The connection URL is normally derived from other registration properties at runtime, such as when an application attempts to retrieve it to connect to the repository or when the repository properties are displayed. But you can choose to explicitly specify the connection URL yourself.

Example command that updates a connection URL:
```
RepositoryAdmin.bat -updateRepositoryConnection -cn odb -cr jdbc:db2://localhost:50000/odb
```

You can also remove the explicitly set connection URL by providing a blank space as a value. When you do this, the connection URL is again derived from other properties.

Example command that removes an explicit connection URL:
```
RepositoryAdmin.bat -updateRepositoryConnection -cn odb -rn odb -cr ""
```

Shorthand: `-us -dt type -dv version -sh hostname [-su username] [-sw "password"]

Updates a database server registration with the information provided. You can update the administrator credentials with this command. Note that the administrator credentials are not required for registration or by the tool’s runtime operations to access the repositories. However, the credentials might be needed by other processes, such as migration, and can be set or updated at any time after registration.

Example command:
```
RepositoryAdmin.bat -updateDatabaseServer -dt DB2 -dv 10.1 -sh localhost -sw "{iisenc}fwGpejos3/I1qMTGHExW6c=="
```

Tip: It is best to provide the password as an encrypted string by using the `encrypt` command, or you can provide a plain text password.
Unregistration options

Repositories, connections, and database servers will be unregistered from the metadata repository during a normal uninstallation process. However, there are situations where you can unregister these entities using the `RegistrationAdmin` tool, for example, if you relocate a repository.

`-unregisterRepository -reposName name`

Shorthand: `-urr -rn name`

Unregisters a repository from the metadata repository. A repository must be unregistered when its corresponding tool is uninstalled or as part of the relocation of a registered repository to another database.

Example command:
`RepositoryAdmin.bat -unregisterRepository -rn odb`

`-unregisterDatabase -dbName name`

Shorthand: `-urd -dn name`

Un registers a database from the metadata repository. A database can be unregistered only if it does not have any repositories registered with it. To unregister a database, you must first unregister each of its repositories. You might want to manually unregister a database when you are relocating all of its repositories to another database server.

Example command:
`RepositoryAdmin.bat -unregisterDatabase -dn odb`

`-unregisterDatabaseServer -databaseType type -databaseVersion version -serverHost hostname`

Shorthand: `-urs -dt type -dv version -sh hostname`

Unregisters a database server from the metadata repository. A database server can be unregistered only if it does not have any databases registered with it. To unregister a database server, you must first unregister each of its databases. You might want to manually unregister a database server when you are relocating all of its databases to another server.

Example command:
`RepositoryAdmin.bat -unregisterDatabaseServer -dt DB2 -dv 10.1 -host localhost`

The option to test a repository connection

Use the following option to test a repository connection. It's good practice to always test the connection after updating the connection properties.

`-testRepositoryConnection -reposName name -connectionName name`

Shorthand: `-tc -rn name -cn name`

Tests a repository connection. Provide the name of the repository and repository connection.

Example command:
`RepositoryAdmin.bat -testRepositoryConnection -rn odb -cn odb`

Example: Changing connection properties

In this scenario, you want to update the password for the database user that is used in the connection.
Before you begin

This procedure only changes the password used in the connection. For the connection to succeed, first change the password in the database itself.

Procedure

1. If you do not know the name of the repository to change, first list the repositories:
   
   ```
   cd \IBM\InformationServer\ASBServer
   RepositoryAdmin.bat -listRepositories
   ```

2. Create a new password by using the `encrypt` command and copy the returned string to the clipboard.
   
   ```
   ..\ASBNode\encrypt.bat
   Enter the text to encrypt:
Enter the text again to confirm:
   {iisenc}PsqKlr7z3JOLJCQ4QhbrrA==
   ```

3. Update the connection providing the repository name and password that you paste from the clipboard.
   
   ```
   RepositoryAdmin.bat -updateRepositoryConnection
   -cn odb -rn odb -cw "{iisenc}PsqKlr7z3JOLJCQ4QhbrrA=="
   ```

---

Example: Manually registering a repository

In this scenario, you want to manually register a new repository. For example, the upgrade of an application might require that its repository be manually registered and created. Using the `RepositoryAdmin` tool, you register the repository and generate SQL scripts to use to create and set up the repository.

About this task

This example assumes that you have done an upgrade and that the upgrade process requires that you create and register a new repository. This example uses the Standardization Rules Designer database as an example.

Procedure

1. Create and edit a new repository properties file with the complete information needed for the new repository. For the Standardization Rules Designer database, specify the following properties and values in the file.

<table>
<thead>
<tr>
<th>Property name</th>
<th>Value description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DatabasePlatform.databaseType</td>
<td>Specify the type of database platform to use. The value must match one of the supported database platforms, as displayed in the first value on a row of output from the <code>RepositoryAdmin -ls</code> command.</td>
</tr>
<tr>
<td>DatabasePlatform.version</td>
<td>Specify the type of database platform to use. The value must match one of the supported database platform versions, as displayed in the second value on a row of output from the <code>RepositoryAdmin -ls</code> command.</td>
</tr>
<tr>
<td>DatabaseServer.host</td>
<td>Specify the hostname of the database server where the Standardization Rules Designer repository is to be located.</td>
</tr>
<tr>
<td>Property name</td>
<td>Value description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DatabaseServer.port</td>
<td>Specify the port number of the database server where the Standardization Rules Designer repository is to be located.</td>
</tr>
<tr>
<td>Database.name</td>
<td>Specify the name of the database where the Standardization Rules Designer repository is to be located.</td>
</tr>
<tr>
<td>Database.alias</td>
<td>Specify the alias of the database where the Standardization Rules Designer repository is to be located. This must match the database name.</td>
</tr>
<tr>
<td>Database.location</td>
<td>Specify the filesystem path location where the Standardization Rules Designer repository is to be located.</td>
</tr>
<tr>
<td>Repository.name</td>
<td>Specify the name to give the Standardization Rules Designer repository.</td>
</tr>
<tr>
<td>Repository.tool</td>
<td>Specify StandardizationRulesDesigner</td>
</tr>
<tr>
<td>Repository.schema</td>
<td>Set this value to match the Repository.userName value.</td>
</tr>
<tr>
<td>RepositoryConnection.name</td>
<td>Set this value to match the Repository.name</td>
</tr>
<tr>
<td>RepositoryConnection.userName</td>
<td>Specify the owner user name for the Standardization Rules Designer repository. Do not use the metadata repository owner user name (typically xmeta).</td>
</tr>
<tr>
<td>RepositoryConnection.password</td>
<td>Specify the password for the repository connection user name.</td>
</tr>
<tr>
<td></td>
<td>Tip: The connection password can be provided as plain text or as a string encrypted with the encrypt command.</td>
</tr>
<tr>
<td>RepositoryConnection.properties</td>
<td>For Oracle, specify:</td>
</tr>
<tr>
<td></td>
<td>SID=Oracle_SID;batchPerformanceWorkaround=true</td>
</tr>
<tr>
<td></td>
<td>The Oracle_SID is the unique name of the Oracle database instance.</td>
</tr>
<tr>
<td></td>
<td>You can leave this value blank for other database systems.</td>
</tr>
<tr>
<td>Tablespace.name</td>
<td>Specify QSSRDSPACE.</td>
</tr>
</tbody>
</table>

Example contents of a properties file, which is here called srd.properties:

```properties
DatabasePlatform.databaseType=DB2
DatabasePlatform.version=10.1
DatabaseServer.host=prod1
DatabaseServer.port=50000
Database.name=srd
Database.alias=srd
Database.location=C:\
Repository.name=QSSRDDB
Repository.description=Production Standardization Rules Designer db.
Repository.tool=StandardizationRulesDesigner
Repository.schema=srduser
RepositoryConnection.name=QSSRDDB
RepositoryConnection.userName=srduser
RepositoryConnection.password={iisenc}gwFQseoj24I/SnCFEH+cWg==
Tablespace.name=QSSRDSPACE
```

2. On the services tier computer, register the new repository and save the SQL scripts that are required to create and set up the new repository.

   ```bash
   RepositoryAdmin.bat -registerRepository -pf srd.properties
   ```
3. Generate the SQL scripts that you will use to create the repository and edit and provide password values in the scripts that contain them.

   RepositoryAdmin.bat -saveSQLScripts -rn QSSRDDB

   The scripts are saved for the respective registered database platform. Relevant parameters in the scripts are replaced with appropriate values as specified in the registration, with the exception of password values.

4. If the computer to host the repository is different than the services tier computer, copy the SQL scripts to the computer to contain the new repository.

5. Run the scripts. For the Standardization Rules Designer database, run the scripts as indicated in the following steps:

   **IBM DB2**
   
   As the DB2 instance owner, complete the following steps:
   
   a. If you want to create the Standardization Rules Designer repository in a database that is separate from the metadata repository, run the following script:

      ```
      db2 -tf qssrd_db_creation.sql
      ```

   b. Run the following scripts to create the table space, schema, and tables that are required for the repository, connecting to the database as indicated:

      ```
      db2 -tf qssrd_tablespace_creation.sql
      db2 -tf qssrd_permissions_schema_creation.sql
      db2 connect to SRD_db_name user SRD_db_user_name
      using SRD_db_user_password
      db2 -tf qssrd_table_creation.sql
      ```

   **Oracle**
   
   Run the following scripts to create the table space, schema, and tables that are required for the repository:

   ```
   sqlplus -L system/password@SID @qssrd_tablespace_creation.sql
   sqlplus -L system/password@SID @qssrd_user_config.sql @RD_user_password
   sqlplus -L system/password@SID @qssrd_table_creation.sql
   ```

   **Microsoft SQL Server**
   
   a. If the server to host the Standardization Rules Designer repository does not host the metadata repository and is not set up for XA transactions, enable XA transactions by completing steps 1 - 3 in the topic for your SQL Server version:

      - [Steps for SQL Server 2008](#)
      - [Steps for SQL Server 2012](#)

   b. If you want to create the Standardization Rules Designer repository in a database that is separate from the metadata repository, run the following script:

      ```
      sqlcmd -b -i qssrdb_db_creation.sql
      ```

   c. Run the following scripts to set up the repository:

      ```
      sqlcmd -b -i qssrd_user_config.sql -vPASSWORD=SRD_db_user_password
      sqlcmd -b -i qssrdb_db_creation.sql
      ```

6. From the services tier, test the connection to the new repository.

   RepositoryAdmin.bat -testRepositoryConnection -cn QSSRDDB -rn QSSRDDB

---

**Example: Relocating a repository**

In this scenario, you want to relocate a repository to a different computer. Perhaps you have just acquired one with more resources or you are moving from a test environment into production.
About this task

This scenario assumes that you are relocating from a test environment into production. In this example, the names of the computers are different, but the credentials and database properties remain the same.

Procedure

1. If you do not know the name of the existing repository, first list the repositories:
   
   ```
   cd \IBM\InformationServer\ASBServer
   RepositoryAdmin.bat -listRepositories
   ```

   odb
   srd
esdb

2. Create a repository properties file to use as a template by displaying the properties and redirecting the output to a file. You need a properties file in subsequent steps to register the new repository.
   
   ```
   RepositoryAdmin.bat -displayRepository -rn odb -res odb.properties
   ```

   Contents of the odb.properties file:

   ```
   DatabasePlatform.databaseType=DB2
   DatabasePlatform.version=10.1
   DatabaseServer.host=test1
   DatabaseServer.port=50000
   Database.name=odb
   Database.alias=odb
   Database.location=C:\
   Repository.name=odb
   Repository.description=Test engine ODB.
   Repository.tool=DataStage
   Repository.context=test
   Repository.schema=odb
   RepositoryConnection.userName=odb
   RepositoryConnection.password={iisenc}gwFQseoj24I/SnCFEH+cWg==
   ```

3. Edit the odb.properties file with the values to use for the production computer. Note that the connection URL is removed. The tool can derive the URL from other properties in the file.

   ```
   DatabasePlatform.databaseType=DB2
   DatabasePlatform.version=10.1
   DatabaseServer.host=prod1
   DatabaseServer.port=50000
   Database.name=odb
   Database.alias=odb
   Database.location=C:\
   Repository.name=odb
   Repository.description=Production engine ODB.
   Repository.tool=DataStage
   Repository.context=production
   Repository.schema=odb
   RepositoryConnection.userName=odb
   RepositoryConnection.password={iisenc}gwFQseoj24I/SnCFEH+cWg==
   ```

4. Unregister the existing repository. Because your new production repository will have the same name as the existing test repository, you must first unregister the test repository. Repository names must be unique. Also, provide the -saveSQLScripts parameter to create the scripts that must be manually run to complete the uninstallation of the unregistered repository in the corresponding repository tier.

   ```
   RepositoryAdmin.bat -unregisterRepository -rn odb -saveSQLScripts
   ```
5. Run the scripts in step 4 on page 175 to clean out the old repository.

6. Optional: If you are moving everything from test into production and this is the last repository in the database, you can unregister the database if you no longer need to use it.
   
   RepositoryAdmin.bat -unregisterDatabase -dn odb

7. Optional: If you are moving everything from test into production, and this is the last database on the server, you can unregister the server host if you no longer need to use it.
   
   RepositoryAdmin.bat -unregisterServer -dt DB2 -dv 10.1 -sh localhost

8. Register the new server, database, and repository. For this step, you need only register the repository. When you register a repository with the RepositoryAdmin tool, if the server and database have not yet been registered, they will be registered during the same operation. Also, in the same operation, you can provide the -saveSQLScripts parameter to save the SQL scripts at the same time. These scripts are required to set up the new production repository.
   
   RepositoryAdmin.bat -registerRepository -pf odb.properties -saveSQLScripts

9. Copy the SQL scripts to the computer to contain the new production repository, and run them to create, configure, and set up the new repository.

10. In this example, the production database that is used is an IBM InfoSphere DataStage operations database, and it is on a separate computer. When connecting from a remote engine computer, a connection configuration file is required for the connection to succeed. On the new engine tier, update the connection configuration file with the new repository, by using the RegistrationCommand tool.
   
   install_dir\ASBNode\bin\RegistrationCommand.bat -get_config -authfile isadmin.credentials -rn odb -cf DSODBConnect.template -res DSODBConnect.cfg

   With the -cf option, the formal parameters in the configuration file are replaced with the corresponding connection properties in the resulting output file DSODBConnect.cfg. The following parameters will be replaced if found in the specified file: @DBTYPE@, @DRIVER_CLASS@, @DRIVER_JARFILES@, @CONNECTION_URL@, @DATABASE_USER@, @PASSWORD@.

11. From the services tier, test the connection to the new repository.
   
   RepositoryAdmin.bat -testRepositoryConnection odb

12. Repeat the procedure for each repository that you want to relocate.

---

**Example: Upgrading the schema of an existing repository**

If you are upgrading IBM InfoSphere Information Server, the schema of some of the databases might require an upgrade. For example, in version 9.1, the IBM InfoSphere DataStage operations database schema has changed and requires an upgrade.

**About this task**

This scenario assumes that you are upgrading the schema for an existing operations database. You have already run the installation tool to upgrade the product. You have also manually registered the repository with the metadata repository. To complete the upgrade, you create and run the SQL scripts to update the repository with new tables and new columns.
**Procedure**

1. From the services tier computer, save the SQL scripts related to the operations database.
   
   `RepositoryAdmin.bat -saveSQLScripts -rn odb`

2. If the computer that hosts the operations database is different than the services tier computer, copy the SQL scripts to the computer that contains the database. To upgrade the schema of the operations database, run the scripts that pertain to an upgrade operation.
Chapter 10. Managing clusters and high availability configurations

If you have implemented clustering or other high availability configurations within your IBM InfoSphere Information Server installation, administer them by using administration tools.

Active-passive configuration administration

If your engine tier (or all tiers) is set up in an active-passive configuration, administer the cluster by using the administration tools that are provided with your high availability software.

For more information about active-passive configurations, see "Creating a two-server active-passive high availability topology" in the IBM InfoSphere Information Server Planning, Installation, and Configuration Guide.

Administering an active-passive configuration based on Tivoli System Automation for Multiplatforms

For information about managing an active-passive configuration that is based on Tivoli® System Automation for Multiplatforms, refer to the Tivoli documentation.


WebSphere Application Server cluster administration

Administer and maintain your IBM WebSphere Application Server clusters after you have installed or updated IBM InfoSphere Information Server in a clustered environment. This documentation assumes that you understand WebSphere Application Server clustering.

Important: The IBM InfoSphere Information Server documentation assumes that you are already familiar with distributed computing, particularly with WebSphere Application Server clustering. You must familiarize yourself with the IBM WebSphere Application Server Network Deployment documentation.

WebSphere Application Server cluster administration tools

You use the following tools to install, configure, and administer IBM WebSphere Application Server clusters.

This information assumes that you have completed the required procedures for installing a highly available clustered configuration. For more information, refer to the IBM InfoSphere Information Server Planning, Installation, and Configuration Guide.

WebSphere Application Server administrative console

The WebSphere Application Server administrative console is a Web interface that provides configuration, operation, and administration...
capabilities. You can use the administrative console to start and stop an application, deploy an application, configure resources, and implement security configurations.

Use this tool to create a cluster and configure its members, nodes, and processes. If you are interested in using scripts to accomplish these tasks, see the IBM WebSphere Application Server Network Deployment documentation:


**WebSphere Application Server Launchpad**

The WebSphere Application Server Launchpad identifies components on the WebSphere Application Server product media (disk or download) that you can install. It is the single point of reference for installing the WebSphere Application Server environment, an integrated platform that contains an application server, a Web server, a set of Web development tools, and additional supporting software and documentation.

Use this tool to install WebSphere Application Server and a front-end Web server if you are creating a clustered WebSphere Application Server configuration.

**WebSphere Edge Components Launchpad**

The WebSphere Application Server Edge Components Launchpad contains a software load balancer. You can use this tool to front an IBM WebSphere Application Server Network Deployment cluster instead of using the IBM HTTP Server.


For information about WebSphere Edge Components, Version 8.0, refer to: http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/topic/com.ibm.websphere.edge.doc/lb/info/ae/welcome_edge.html

**Profile Management tool**

The Profile Management tool performs the initial setup of WebSphere Application Server cells and nodes. The Profile Management tool creates batch jobs, scripts, and data files that you can use to do WebSphere Application Server customization tasks.

Use this tool to create a deployment manager profile and a custom profile.

**InfoSphere Information Server installation program**

The InfoSphere Information Server installation program detects the deployment manager process that is installed as a prerequisite on your computer and prompts you for the information that it needs to run a cluster installation.

Use this tool during the installation process to specify the WebSphere Application Server directory location, deployment manager profile, and the host name and port number of the front-end Web server or load balancer.
For more information about WebSphere Application Server, see the WebSphere Application Server documentation:


### Propagating the plugin-cfg.xml file to the front-end Web server

The plugin-cfg.xml file is used by the front-end Web server at runtime to perform workload management across the cluster. You must update and propagate this file to the Web server when a new member is added to the cluster or when a new J2EE application is deployed in the cluster.

#### Before you begin

If you are unfamiliar with HTTP servers in an IBM WebSphere Application Server Network Deployment environment, read the following IBM WebSphere Application Server Network Deployment information center topics and subsections for the version that applies to you:


#### About this task

The plugin-cfg.xml file is a configuration file that is generated by IBM WebSphere Application Server Network Deployment. It is in the `<webserver_plugin_install_path>/config/<webserver_definition>` path, for example, `C:/IBM/HTTPServer/Plugins/config/webserver1`.

It is used at run time by the front-end Web server to perform workload management across the cluster. The file is on the computer where the Web server is installed. This file must be kept up-to-date at all times in order for Workload Management to be correctly implemented at the Web level. Regenerate and propagate the plugin-cfg.xml file when the following events occur:

- The domain tier of the suite is newly installed (installed for the time).
- A product of the suite is newly installed as an add-on.
- A product of the suite is removed after an uninstallation.
- A new member is added to the cluster.
- A new IBM InfoSphere Information Services Director application is generated and deployed in the cluster.
- The front-end Web server is replaced by another Web server.

To facilitate the management of this configuration file, IBM WebSphere Application Server Network Deployment can automatically propagate the plugin-cfg.xml file to the Web server. Depending on your Web server topology, this automation might not always be possible. You might have to regenerate and propagate this file to the Web server computer manually. There are three possible scenarios:
Scenario 1: The Web server is installed in a managed node.
In this case, the plugin-cfg.xml file is automatically regenerated and propagated by the IBM WebSphere Application Server Network Deployment to the managed node hosting the Web server. It might take a few minutes for WebSphere Application Server to regenerate and propagate the plugin file to the Web server. You do not need to propagate the plugin-cfg.xml file because this step is completed for you.

Scenario 2: The Web server is installed in an unmanaged node (in other words, there is no node agent to manage the Web server definition).
In this case, IBM WebSphere Application Server Network Deployment can not automatically propagate the plugin-cfg.xml file to the Web server, so you need to manually propagate it.

Scenario 3: The Web server is installed in an unmanaged node and is the IBM HTTP Server (IHS).
In this special case, the plugin-cfg.xml file also is automatically propagated by IBM WebSphere Application Server Network Deployment to the unmanaged node that hosts IHS. This functionality is achieved because of the IHS administration process that runs on the Web server computer, which can act as a node agent for the Web server.

Procedure

To manually propagate the plugin-cfg.xml file:

For the appropriate topology (either a remote distributed installation scenario or a local distributed installation scenario), refer to the sections about regenerating the plugin-cfg.xml file and propagating the plugin-cfg.xml file in the following topics:

- IBM WebSphere Application Server Network Deployment 8.5:

- IBM WebSphere Application Server Network Deployment 8.0:

For more information about managed and unmanaged nodes in IBM WebSphere Application Server Network Deployment, see the following resources:


- Information about Managed and unmanaged nodes in the IBM WebSphere Application Server Network Deployment 8.0 information center:

Adding a new cluster member

You can create additional cluster members from the IBM WebSphere Application Server administrative console. Additional cluster members are essentially copies of the existing cluster members. This procedure is referred to as vertical clustering or scaling up.

Before you begin

You must have an existing node agent and at least one cluster member running on the machine where you want to create a new cluster member. If you want to create a new cluster member on a machine that does not already host a node agent, then refer to the Adding a new managed node section.

Procedure

1. Follow these instructions to create a new cluster member on an existing managed node, directly from the IBM WebSphere Application Server administrative console. You will be asked to specify the node on which to create the new cluster member. Optionally, you can also specify a server weight that will be used for load balancing at run time and whether to generate unique HTTP ports.

2. If you are using an HTTP server as the front-end dispatcher for your cluster, regenerate and propagate the `plugin-cfg.xml` file.
   You need this in order for the front-end web server workload management plugin to take into account the new cluster member. Regenerate and propagate the `plugin-cfg.xml` file to the front-end Web server as described in Propagating the `plugin-cfg.xml` file to the front-end web server.

Adding a new managed node

You create a new managed node to expand the scope of a cluster. This procedure is horizontal clustering or scaling out.

Before you begin

- Ensure that the Deployment Manager is running. If it is not running, start it as described in “Starting the IBM WebSphere Application Server Deployment Manager (Windows)” on page 236 or “Starting the IBM WebSphere Application Server Deployment Manager (Linux, UNIX)” on page 239.

Important: Ensure that the clock of the system where you want to create a new managed node is synchronized with the Deployment Manager system clock and the other node systems. When the clocks of the various node computers are not synchronized, multiple problems can arise at run time. Verify that the clocks on all systems are synchronized by using the universal date and time.
About this task

This procedure is the same procedure on IBM WebSphere Application Server Network Deployment 8.5 and 8.0.

Procedure

1. **Linux** Configure file descriptor resources on the node as described in “Configuring file descriptor resources for IBM WebSphere Application Server (Linux)” on page 240.

2. **AIX** Unset the LDR_CNTRL variable on the node as described in “Configuring memory allocation for IBM WebSphere Application Server (AIX)” on page 241.

3. Create a custom profile on the node agent computer by using the Profile Management Tool. Follow the steps in the IBM InfoSphere Information Server Planning, Installation, and Configuration Guide.

   **Remember:** When you create a custom profile, on the Federation page, specify a WebSphere Application Server administrator user name and password to connect to the Deployment Manager.

   **Note:** Do not select the **Federate this node later** check box.

4. Create a cluster member (for example, “server3”) on the node agent machine. Follow the steps in the IBM InfoSphere Information Server Planning, Installation, and Configuration Guide.

   **Note:** When selecting the node to create the cluster member, on the Create additional cluster members page, make sure to select the new managed node that you created in the previous step.

5. Synchronize the new managed node. Run the **syncNode** WebSphere Application Server command from the computer that hosts the managed node. You must specify the host name and port of the Deployment Manager and the WebSphere Application Server administrator user name and password as input arguments.

   **Note:** Do not start the node agents yet. The syncNode operation takes a couple of minutes to complete.

Refer to the IBM WebSphere Application Server Network Deployment documentation for complete reference information about the **syncNode** command.


The following shows the syntax for the **syncNode** command, followed by an example of the **syncNode** command log file found under the custom profile directory.

```
syncNode dmgr_hostname dmgr_port -username was_admin_username
   -password was_admin_password

C:\IBM\WebSphereND70\AppServer\profiles\Custom01\bin>syncNode myDmgr01 8879
   -username wasadmin -password *******

ADMU0116I: Tool information is being logged in file
   C:\IBM\WebSphereND70\AppServer\profiles\Custom01\logs\syncNode.log
```
ADMU0128I: Starting tool with the Custom01 profile
ADMU0401I: Begin syncNode operation for node myNode01 with Deployment Manager localhost: 8879
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0402I: The configuration for node myNode01 has been synchronized with Deployment Manager myDmgr01: 8879

When the synchronization is complete, verify that the custom profile contains both newly created directories: the classes directory and the informationServer directory. These two directories and the files they contain are the result of the synchronization operation.

**Note:** If the synchronization fails, you can review the `syncNode` command log file (`syncNode.log`) in the custom profile directory.

6. Start the new node agent on the node agent computer by using the `startNode` WebSphere Application Server command.

Refer to the IBM WebSphere Application Server Network Deployment documentation for information about the `startNode` command.


7. Start the newly created cluster member from the WebSphere Application Server administrative console.

8. Enable last participant support (LPS). LPS must be enabled on the new node for IBM InfoSphere Metadata Asset Manager to function properly. To enable LPS:
   a. In the WebSphere Application Server administrative console, select **Servers** > **Server Types** > **WebSphere application servers** and select the server associated with the new node.
   b. Under Container Setting on the right side, expand Container Services and click **Transaction service**. A page opens with the configuration for the Transaction service of the new node you just added.
   c. Select the **Accept heuristic hazard** option under General Properties and click **OK**
   d. Save your changes.
   e. Propagate the changes to other nodes by selecting **System Administration** > **Save changes to master repository**, checking **Synchronize changes with Nodes**, and clicking **Save**.
   f. Restart the node for the changes to take effect by selecting **Servers** > **Server Types** > **WebSphere application servers**, checking the server name for your new node, and clicking **Restart**.

9. Propagate the `plugin-cfg.xml` to the front-end Web server WLM plug-in to take into account the new cluster member. See “Propagating the `plugin-cfg.xml` file to the front-end Web server” on page 181.

**Synchronizing nodes after changing the master repository configuration**

When you change the master repository configuration, synchronize the nodes to ensure that changes are propagated to all nodes in the cell. This procedure is the same for IBM WebSphere Application Server Network Deployment Versions 8.5 and 8.0.
About this task

WebSphere Application Server synchronizes nodes internally on a regular and automatic basis. However, you can also synchronize the nodes whenever you need to, instead of waiting for WebSphere Application Server. For example, change the master repository configuration when you add a new cluster member or change a security setting.

Important: Nodes need to be synchronized whenever there is a change to the master repository configuration, including updates to the topology or cell configurations.

Procedure

1. Log in to the WebSphere Application Server administrative console.
2. Expand the System administration section and then click Nodes.
3. Select the nodes that you want to synchronize (most likely all of them).
4. Click Synchronize or Full Synchronize.

For information about the difference between Synchronize and Full Synchronize, refer to the IBM WebSphere Application Server Network Deployment section about synchronizing the node configuration:


Restarting application server processes

When you change a configuration at the cell-level, you must restart all IBM WebSphere Application Server Network Deployment processes to make the changes effective. You should restart the application servers, node agents, and deployment manager on each machine in a specific order.

About this task

You must restart all IBM WebSphere Application Server Network Deployment processes when you modify anything at the cell-level (deployment manager-level). For example, restart application server processes after you do any of the following tasks:

- Change security at the cell-level (for example, when you enable SSL, replace SSL certificates, or switch user registry)
- Modify configurations for a data source
- Change other cell-level settings

For information about how to do the tasks involved in each of these steps in this topic, refer to the following tables.

Note: The simplest way to restart node agents and application servers (clusters) is through the WebSphere Application Server administrative console. If you use the command line tools instead, make sure to specify a WebSphere Application Server administrator user name and password.
**Procedure**

1. Stop all WebSphere Application Server processes in the following order:
   a. Stop all application servers on every computer.
   b. Stop all node agents on every computer.
   c. Stop the deployment manager.

   To stop application servers, node agents, and deployment managers for IBM WebSphere Application Server Network Deployment, Versions 8.5 and 8.0, refer to the following table.

<table>
<thead>
<tr>
<th>WebSphere Application Server Process</th>
<th>Stopping the process in Version 8.5</th>
<th>Stopping the process in Version 8.0</th>
</tr>
</thead>
</table>

2. After you have stopped all WebSphere Application Server processes, you can proceed to restart them. Start all WebSphere Application Server processes in the following order:
   a. Start the deployment manager.
   b. Start all node agents on every machine.
   c. Start all application servers on every machine.

   **Note:** When you restart the application server, you restart the cluster.

   To start application servers, node agents, and deployment managers for IBM WebSphere Application Server Network Deployment, Versions 8.5 and 8.0, refer to the following table.

<table>
<thead>
<tr>
<th>WebSphere Application Server Process</th>
<th>Starting the process in Version 8.5</th>
<th>Starting the process in Version 8.0</th>
</tr>
</thead>
</table>

**Note:** For more information about node agents:

Setting up HTTP session database persistence

When you install IBM InfoSphere Information Server in a cluster environment, HTTP session management is configured to use memory-to-memory replication.

If you want to use a database persistence approach, configure IBM WebSphere Application Server Network Deployment as described in Section 6.8.5 of the IBM Redbooks publication, *WebSphere Application Server V6 Scalability and Performance Handbook*: [http://www.redbooks.ibm.com/abstracts/sg246392.html]. Refer to section 6.8 for more information about the advantages and drawbacks of the two mechanisms.

To configure for database session persistence, use the instructions in the IBM WebSphere Application Server information center:


IBM DB2 high availability configuration administration

These tasks outline how to administer an IBM InfoSphere Information Server database in an IBM DB2 cluster or high availability disaster recovery (HADR) configuration.

Use these procedures if your metadata repository or IBM InfoSphere Information Analyzer analysis database is set up in one of these configurations.

For detailed information about DB2 cluster or HADR administration, see the following resources:


Failover in an IBM DB2 HADR configuration

If the primary database fails in a DB2 HADR configuration, IBM InfoSphere Information Server can continue functioning by using the standby database.

To start using the standby database, the following things must occur:

- The services tier (IBM WebSphere Application Server) must reconnect to the standby server. The DB2 automatic client reroute (ACR) feature automatically reconnects the services tier to the standby server.
- The database administrator must run the TAKEOVER HADR command on the standby database.
Attention: A failure might cause a loss of data.

If a user writes data to a database and a failure occurs during the data replication to the backup server, the updates might be lost. In most cases, the user can redo the edit or import operation to restore the data after the switchover to the standby database is complete.

The likelihood and extent of transaction loss depends on the synchronization mode in which HADR is configured. The following table lists synchronization modes and data loss scenarios.

<table>
<thead>
<tr>
<th>HADR synchronization mode</th>
<th>Data loss scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYNC</td>
<td>Least risk of data loss.</td>
</tr>
<tr>
<td>NEARSYNC</td>
<td>The standby database can lose transactions if both the primary and standby databases fail at the same time.</td>
</tr>
</tbody>
</table>
| ASYNC                    | The standby database can lose transactions in cases like these:  
  - The standby database does not receive all the log records for the transactions before the takeover operation is performed.  
  - Both the primary and standby databases fail at the same time. |

If the primary database fails while in remote catchup pending state, transactions that the standby database has not processed are lost.

Note: Any log gap shown in the database snapshot represents the gap at the last time the primary and standby databases communicated. The primary database might have processed many transactions since that time.

Recovering from failover in a DB2 HADR scenario

If your installation includes an IBM DB2 database that is configured with high availability disaster recovery (HADR), the database administrator must complete the failover process manually.

About this task

If the primary HADR database fails, follow this procedure to restore service.

Attention: A failure might cause a loss of data.

Procedure

1. If the DB2 fault monitor feature (db2fm) is enabled on the primary database server, the database might automatically restart on the primary server. Direct the user to try the transaction again to see if the database is operational. If the database is operational, no further action is required.
2. Deactivate the primary database or stop its instance, if possible. If the primary database is still running, but cannot communicate with the standby database, running the takeover operation could result in two primary databases (a “split-brain” scenario).
3. Start the takeover operation by using one of the following administration interfaces:  
   - The DB2 command-line processor (CLP).
• The Manage High Availability Disaster Recovery window in the DB2 Control Center.
• The db2HADRTakeover application programming interface (API).

Recovering from a failover in a DB2 clustered configuration

If your IBM InfoSphere Information Server databases are set up in an IBM DB2 clustered configuration, failover is automatic.

If the primary node fails in such a configuration, the passive node connects to the database file system, and continues. If you have automatic client reroute (ACR) configured, the services tier (IBM WebSphere Application Server) reconnects to the passive node. No database administrator intervention is required.

Any transactions other than read-only transactions are stopped and rolled back. Users must resubmit the transactions.

Refer to the DB2 documentation for more detailed information.

Engine tier failover recovery

If the engine tier (and possibly other tier software as well) is set up in an active-passive configuration, hardware or network errors cause a failover to the passive server. You can also force a failover to occur to free the active server for maintenance or upgrade tasks.

The high availability (HA) software that is installed on the servers manages the fault detection and failover process.

During a failover, the sequence of events differs depending on whether the failover is due to a failure or is forced.

Failover due to a failure

When the active server hardware or network fails, the heartbeat mechanism between the nodes signals the passive server that the active server has failed. The HA software restores service on the passive server by doing the following actions:

• Ensures that the primary server is no longer running.
• Assigns the IP address that is associated with the resource group to the new server.
• Mounts the floating mount point for the software on the new server.
• Starts the engine tier software on the new server by calling the InfoSvrEngine script with the start option.
• If other tier software is installed on the server, the HA software starts it by calling the InfoSvrServices script with the start option. This script starts the services tier. It also starts the metadata repository tier if the tier is installed with the engine tier.

Forced failover

When you force a failover, the HA software shuts down the software before starting it up on the other node. The HA software does the following steps:
If software is installed for tiers other than the engine tier, the HA software stops it by calling the `InfoSvrServices` script with the `stop` option. This script stops the services tier. It also stops the metadata repository tier if the tier is installed with the engine tier.

- Stops the engine tier software on the server by calling the `InfoSvrEngine` script with the `stop` option.
- Unmounts the floating mount point for the software.
- Unmounts the data files mount point.
- Unassigns the IP address associated with the resource group from the old server.
- Reassigns the resource group IP address and mounts the floating mount point.
- Starts the engine tier software on the new server by calling the `InfoSvrEngine` script with the `start` option.
- If other tier software is installed on the server, the HA software starts it by calling the `InfoSvrServices` script with the `start` option. This script starts the services tier. It also starts the metadata repository tier if the tier is installed with the engine tier.

### Recovery process

In a production system, if server engine services did not shut down normally, the `DSHARestart` tool starts automatically on the passive server. The tool checks and repairs dynamic files that are associated with any jobs that were running on the primary server when the failover occurred. The state of these jobs is set to `crashed` for easy identification.

In a development system where users were creating, editing, or compiling projects when a failover occurred, the restart might leave projects in an inconsistent state. You can use the `SyncProject` tool to resolve any inconsistencies in these projects.

### Recovering from an engine tier failover

When an engine tier failover occurs, follow this procedure to recover projects and restart any interrupted jobs.

If IBM InfoSphere Information Server engine services did not shut down normally (for example, if a failover occurred due to a failure), the `DSHARestart` tool starts automatically on the passive server. The tool checks and repairs dynamic files that are associated with any jobs that were running on the primary server when the failover occurred. The state of these jobs is set to `crashed` for easy identification.

The tool is intended to handle unattended failover events on a production system. No user interaction is required to ensure that running jobs can be restarted.

InfoSphere Information Server engine services do not start up fully until the `DSHARestart` tool has completed its tasks. While the tool is running, users cannot connect and use the InfoSphere Information Server engine. This design ensures that jobs are not further corrupted during the recovery process.

While the `DSHARestart` tool runs, it records its actions in the `HAReStart.log` file. If an issue arises during the recovery process, refer to this file for more information. This file is located in the following directory:

- **Linux** /opt/IBM/InformationServer/Server/DSEngine
- **Windows** C:\IBM\InformationServer\Server\DSEngine
After the **DSHARestart** tool has finished, recover projects by using the **SyncProject** tool. Then restart any interrupted jobs. Replace the server and bring the new server online.

### Recovering projects by using the SyncProject tool

After a failover, you can run the **SyncProject** tool to repair inconsistencies in your projects.

#### About this task

After a failure, the repository that holds design-time assets for a project can be left out of step with the repository that holds the runtime assets. This situation can cause the project, or assets contained with the project, to become unusable. You can run the **SyncProject** tool to check for inconsistencies, and repair inconsistencies if any are detected.

#### Procedure

Run the **SyncProject** tool to analyze and recover projects.

#### Example

The following example command displays a consistency report for all projects. The **SyncProject** tool also writes the report to the `/tmp/myprojrep.txt` file.

```shell
SyncProject -ISHost R101:9080 -IAUser admin -IAPassword pword -project -report /tmp/myprojrep.txt
```

In this case, the **SyncProject** tool returns results for four projects. It finds two inconsistencies in the project named dstage9, as shown in the following example.

```
DSEngine Restorer Report
Feb 05, 2009 9:39:00 AM
IS Host = R101
IS Port = 9080
IS User = admin
DS Host = R101
DS Port = 31538
DataStage Project: dstage3
--------------------------
0 Issues Found.
DataStage Project: dstage4
--------------------------
0 Issues Found.
DataStage Project: dstage5
--------------------------
0 Issues Found.
DataStage Project = dstage9
---------------------------
2 Issues Found.
DS Engine Job 'testJob' is missing.
DS Engine Job 'testJob2' category 'incorrectCategory' should be 'correctCategory'
```

The following command causes the **SyncProject** tool to try to fix the dstage9 project.

```shell
SyncProject -ISFile islogin -project dstage9 -Fix
```

The command makes the necessary repairs and outputs the following report:

```
DSEngine Restorer Fix Results
Feb 05, 2009 9:39:00 AM
IS Host = R101
IS Port = 9080
IS User = admin
```

---

**192 Administration Guide**
Identifying and restarting crashed jobs

After the **DSHARestart** tool finishes, restart jobs by using the **dsjob** tool.

**About this task**

After the **DSHARestart** tool finishes, recovered job sequences are left in one of two states:

- **Crashed/Restartable.** You can run these job sequences from where they stopped, or reset and run them.
- **Crashed.** You must reset these jobs before you can run them.

**Procedure**

Use any of the following tools to identify jobs that are in a **crashed/restartable** or **crashed** state.

**The dsjob tool**

To use the **dsjob** tool:

1. Log in to the computer that hosts the engine tier. Use an account with administrator or IBM InfoSphere DataStage user privileges.
2. Change to the directory that contains the **dsenv** file. This directory is specified in the **$DSHOME** environment variable. By default, the directory is `/opt/IBM/InformationServer/Server/DSEngine`.
3. Source the **dsenv** file:
   
   . dsenv

4. Run the **dsjob** tool. Specify the **-status** option with a value of **96**.
   
   ```
   dsjob -ljobs -status 96
   ```

5. To restart checkpointed job sequences that are in the **crashed/restartable** state, specify the **-mode** option with a value of **RESTART**, and specify the job sequence.

   ```
   dsjob -run -mode RESTART project jobsequence
   ```

**The IBM InfoSphere DataStage and QualityStage Director client**

To use the InfoSphere DataStage and QualityStage Director client, start the client and view jobs. Look for jobs where the Status column reads **Crashed** or **Crashed/Restartable**.

**The C or DSBasic Job Control API DSRunJob function.**

For information about the C or DSBasic Job Control API **DSRunJob** function, see the IBM InfoSphere DataStage documentation.

**What to do next**

After you identify and restart crashed jobs, investigate and resolve the cause of the primary server failure.
Chapter 11. Managing logs

You can access logged events from a view, which filters the events based on criteria that you set. You can also create multiple views, each of which shows a different set of events.

You can manage logs across all of the IBM InfoSphere Information Server suite components. The console and the Web console provide a central place to view logs and resolve problems. Logs are stored in the metadata repository, and each InfoSphere Information Server suite component defines relevant logging categories.

Logging

You can configure log views to manage the log messages that are generated when activities run in the suite.

You create log views to query log messages. Log messages show details about the activities that run in the suite. After you create a log view, you use filters to restrict the information in the log view. Only a suite administrator can delete log messages. If you want to delete log messages, you select the log view that contains the information that you want to remove.

You can restrict access to a log view by making the log view private. Private log views are available only to the user who created the log view. If you want a log view to be available to all users, you can share the log view. Shared log views can be edited only by the user who created the shared log view or by a suite administrator.

Logging components

A logging component is a named entity that represents a suite component in IBM InfoSphere Information Server or a shared service, such as reporting, that uses the logging service.

A logging component defines one or more logging categories. Each logging category is a group of logged messages that represent one functional aspect of the component.

For example, the category ISF-REPORTING-ENGINE has one set of logged messages for the reporting engine, which is a functional aspect of the logging component called the Reporting Services.

Logging configurations

You can use a logging configuration to set the criteria for logging events for a suite component.

Both the configuration and the individual categories that belong to a configuration set severity level filters for saving events in the metadata repository. At runtime, the severity level for the configuration overrides the filters of the categories.

Each logging component can have multiple logging configurations. The active configuration determines which events are saved in the metadata repository.
Severity levels

Severity levels specify the threshold for saving events in the metadata repository.

In a configuration, you set the lowest threshold for inclusion, which also captures all of the higher levels. For example, if you select the **Warning** level, warning, error, and fatal events are logged. The levels are ordered from the highest level (fatal) to the lowest level (trace):

- Fatal
- Error
- Warn
- Info (information only)
- Debug
- Trace

You can use the debug level and trace level to troubleshoot problems at runtime that involve specific logging categories. But, unless you want to troubleshoot a specific issue, leave the logging threshold at its default value. At the default value, only critical errors are logged and disk space usage does not grow unnecessarily.

Each logging component can have multiple logging configurations. The active configuration determines which events are saved in the metadata repository.

Views of logged events

You access logged events from a view. The view filters the events based on criteria that you select.

You can create multiple views, each of which shows a different set of events.

You can filter messages by the following criteria:

**Message strings**

You can filter messages by full or partial message text. Two wildcard characters are supported:

- An asterisk (*) finds one or more characters.
- A question mark (?) finds any single character at the current position.

**Categories**

You can filter messages by category name.

**Severity level**

You can filter messages by severity level.

**Time frame**

A view can capture activity in a date range or show the latest events. You can specify the number of events to include in the initial view and the refresh rate. The logging service automatically refreshes the view.

Shared and private views

A view can be private or shared. A suite administrator or suite user who creates a private view has exclusive access to the view.

The following table describes the levels of access, based on the creator and type of view.
Table 15. Access to views

<table>
<thead>
<tr>
<th>Type of view</th>
<th>Created by</th>
<th>Who can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>Suite administrator</td>
<td>Creator can edit, view, and delete.</td>
</tr>
<tr>
<td>Shared</td>
<td>Suite administrator</td>
<td>Creator and other suite administrators can edit, view, and delete. Suite users can view.</td>
</tr>
<tr>
<td>Private</td>
<td>Suite user</td>
<td>Creator can edit, view, and delete.</td>
</tr>
<tr>
<td>Shared</td>
<td>Suite user</td>
<td>Creator can edit, view, and delete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suite administrators can view and delete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other suite users can view.</td>
</tr>
</tbody>
</table>

Managing logging views in the console

In the console, you can create logging views, access logged events from a view, edit a log view, and purge log events.

Creating a view of logged events in the console

You can create views of events that suite component users and shared services initiate. These events are stored in the metadata repository.

Before you begin

You must have suite administrator or suite user authority.

Procedure

1. On the Operate navigator menu in the console, select Log View.
2. In the Tasks pane, click New Log View.
3. Specify a name and a description for the log view.
4. In the Access menu, select the access level.
5. Specify the parameters of the log view.
   a. In the Message field, type a pattern for filtering message text. Two wildcard characters are supported:
      • An asterisk (*) finds one or more characters.
      • A question mark (?) finds any single character at the current position.
   b. In the Severity Levels pane, select one or more severity levels to filter the messages.
   c. Select one or more categories to filter on.
   d. In the Timestamp pane, specify a date range, event count, or the elapsed time.
   e. In the Context pane, select from the available list to include only the logging events that are generated by the selected components. Each component defines its own logging message fields.
6. Optional: Click View Log to view the results of the log view before saving.
7. Click Save > Save and Close to save the view.

Viewing logged events

You can open a log view to inspect the events that the view captured.
Procedure
1. On the Operate navigator menu in the console, select Log View.
2. In the Log View workspace, select the log view that you want to open.
3. In the Tasks pane, click View Log.
4. In the View Log pane, select an event to view the detailed log events. You can view the details of the logging view by clicking Open Properties.

Editing a log view
You can edit a view of logged events to modify which events are included in the log view.

Procedure
1. On the Operate navigator menu, select Log View.
2. In the Log View workspace, select the log view that you want to edit.
3. In the Tasks pane, click Open.
4. In the Open pane, modify the criteria for the view.
5. Optional: Click View Log to view the results of the modified log view before saving.
6. Click Save > Save and Close to save the view.

Copying a log view
To create a new log view that is based on the configuration details of a previous log view, you can create a copy of a log view.

Procedure
1. On the Operate navigator menu, select Log View.
2. In the Log View workspace, select the log view that you want to copy.
3. In the Tasks pane, click Copy.
4. Type a new name and a new description for the log view.
5. Optional: Modify the filters of the view.
6. Click Save > Save and Close to save the view.

Purging logged messages
The logged messages that are in the metadata repository have no expiration. You can delete the logged messages for the events that a logging view captures. This action is useful for managing large volumes of events.

Before you begin
You must have suite administrator authority.

Procedure
1. On the Operate navigator menu, select Log View.
2. In the Log View workspace, select one or more log views.
3. In the Tasks pane, click Purge Log.
4. In the confirmation window, click OK to confirm that you want to purge the log events. The logged messages for the selected views are deleted from the metadata repository.
Results

Logged messages are deleted in the background to allow you to continue to work on other tasks. When you delete a large number of logged messages, the events for logged messages that have yet to be deleted might still be displayed after the screen is refreshed. These events are no longer displayed after all the logged messages are deleted from the metadata repository.

Managing logging views in the IBM InfoSphere Information Server Web console

In the Administration tab of the IBM InfoSphere Information Server Web console, you can create logging views, access logged events from a view, edit a log view, purge log events, and delete logging views. You can also manage log views by logging component.

Creating a view of logged events in the IBM InfoSphere Information Server Web console

You can create views of events that suite component users and shared services initiate. These events are stored in the metadata repository.

Before you begin

You must have suite administrator or suite user authority.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Log Management > Log Views.
3. In the Log Views pane, click New.
4. Specify a name and a description for the log view.
5. In the Log View Access list, select the access level.
6. Optional: In the Message field, type a pattern for filtering message text. Two wildcard characters are supported:
   * An asterisk (*) finds one or more characters.
   * A question mark (?) finds any single character at the current position.
7. Optional: In the Severity Level group, select one or more severity levels to filter the messages.
   a. In the Categories pane, click Browse.
   b. In the Browse Categories window, select one or more categories.
   c. Click OK to close the window.
9. Optional: In the Timestamp pane, specify a date range, event count, or the elapsed time.
<table>
<thead>
<tr>
<th>Option Description</th>
</tr>
</thead>
</table>
| To specify a date range: | 1. Select **Range**.  
2. Type a start date and time and an end date and time or use the calendar to specify a starting date and optionally an ending date. |
| To schedule real-time update: | 1. Select **Real-Time Logging**.  
2. Specify the number of events to include and the refresh rate, in seconds. |
| To specify elapsed time: | 1. Select **Interval**.  
2. Specify an interval number and select the type of interval, such as 5 days. |

10. Optional: In the Context pane, select from the available list to include only the logging events that are generated by the selected components. Each component defines its own logging message fields.

11. Optional: Specify the table columns that will show in the log view.

12. Click **Save and Close** to save the view.

### Viewing log events in the IBM InfoSphere Information Server Web console

You can open a log view to inspect the events that the view captured.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Log Management > Log Views**.
3. In the Log Views pane, select the log view that you want to open.
4. Click **View Log**. The View Logs pane shows a list of the logged events.
5. Select an event to view the detailed log events.
6. Optional: Click **Export Log** to save a copy of the log view on your computer.
7. Optional: Click **Purge Log** to purge the log events that are currently shown.

### Editing a log view in the IBM InfoSphere Information Server Web console

You can edit a view of logged events to modify which events are included in the log view.

**Procedure**

1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Log Management > Log Views**.
3. In the Log Views pane, select the log view that you want to edit.
4. Click **Open**.
5. In the Open pane, change the criteria for the view.
6. Click **Save and Close** to save the view.
Copying a log view in the IBM InfoSphere Information Server Web console

To create a log view that is based on the configuration details of a previous log view, you can create a copy of a log view.

**Procedure**
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Log Management > Log Views.
3. In the Log Views pane, select the view that you want to copy.
4. Click Copy.
5. Type a new name and a new description for the log view.
6. Optional: Modify the filters of the view.
7. Click Save and Close to save the view.

Purging logged messages in the IBM InfoSphere Information Server Web console

The logged messages that are in the metadata repository have no expiration. You can delete the logged messages for the events that a logging view captures. This action is useful for managing large volumes of events.

**Before you begin**

You must have suite administrator authority.

**Procedure**
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Log Management > Log Views.
3. In the Log Views pane, select one or more views.
4. Click Purge Log.
5. In the confirmation window, click Yes to confirm that you want to purge the log events. The logged messages for the selected views are deleted from the metadata repository.

**Results**

Logged messages are deleted in the background to allow you to continue to work on other tasks. When you delete a large number of logged messages, the events for logged messages that have yet to be deleted might still display after the screen is refreshed. These events are no longer displayed after all the logged messages are deleted from the metadata repository.

Managing logging by component

For each logging component in IBM InfoSphere Information Server, you can manage logging by modifying the thresholds at which events are logged in the metadata repository, specifying that a logging configuration is active, specifying that a logging configuration is the default, or deleting a logging configuration.
About this task

A logging component is a named entity that represents a suite component in InfoSphere Information Server or a shared service, such as the session or monitoring service, that uses the logging service.

Creating a logging configuration

You can create a logging configuration to set the criteria for logging events in a suite component.

Before you begin

You must have suite administrator authority.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Log Management > Logging Components.
3. In the Logging Components pane, select one of the logging components.
4. Click Manage Configurations.
5. Click New Logging Configuration.
6. In the New pane, type a name for the configuration.
7. In the Threshold menu, select a threshold level for writing logging events to the metadata repository. The threshold value has precedence over individual category severity levels (below) and will limit what is logged. If the threshold is set to Off, nothing will be logged for this configuration. To troubleshoot a specific issue, set the threshold value to All and use the category severity levels to specify what is logged.
8. Add logging categories to the configuration.
   a. Click Browse.
   b. In the Browse Categories window, select the categories that you want to include in the configuration.
   c. Click OK to close the window.
9. Optional: Modify the severity levels for the included categories. Leave the setting to Warn unless you want to debug a specific issue.
10. Click Save and Close to save the configuration in the metadata repository.

Results

The logging configuration displays the names of the logging categories specified in the preceding task and the root logging category for the component that you are working with. Always specify the root logging category in the logging configuration.

Editing a logging configuration

If you want to change the logging categories and the filtering of the views, you can edit a logging configuration.

Before you begin

You must have suite administrator authority.
Procedure
1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Log Management > Logging Components**.
3. In the Logging Components pane, select one of the logging components.
4. Click **Manage Configurations**.
5. Select a configuration.
6. Click **Open**.
7. Modify the details of the configuration.
8. Click **Save and Close** to save the configuration.

**Copying a logging configuration**
To create a new logging configuration that is based on the configuration details of another logging configuration, you can create a copy of a logging configuration.

**Before you begin**
You must have suite administrator authority.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Log Management > Logging Components**.
3. In the Logging Components pane, select one of the logging components.
4. Click **Manage Configurations**.
5. Select a configuration.
6. Click **Copy**.
7. Optional: In the Copy pane, type a new name for the logging configuration.
8. Modify the configuration details.
9. Click **Save and Close** to save the configuration.

**Setting a default logging configuration**
You can set a default logging configuration. A default configuration is the active configuration if no other configuration is activated.

**Before you begin**
You must have suite administrator authority.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the **Administration** tab.
2. In the Navigation pane, select **Log Management > Logging Components**.
3. In the Logging Components pane, select one of the logging components.
4. Click **Manage Configurations**.
5. Select a configuration.
6. Click **Set as Default**.
Activating a logging configuration
You activate a logging configuration to log events in the metadata repository that uses that configuration.

Before you begin
You must have suite administrator authority.

About this task
You can create multiple logging configurations for each suite component. Only active logging configurations log events in the metadata repository.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Log Management > Logging Components.
3. In the Logging Components pane, select one of the logging components.
4. Click Manage Configurations.
5. Select a configuration.
6. Click Set as Active.
Chapter 12. Managing schedules

In the IBM InfoSphere Information Server Web console, you can query all of the schedules that are defined across all of the suite components, check their status, history, and forecast, perform maintenance tasks such as purging the schedule execution history, and stop or start existing schedules to prevent system overload.

Many of the suite components use scheduling capabilities. For example, a report run and an analysis job in IBM InfoSphere Information Analyzer are scheduled tasks. Typically, you create, update, and manage these schedules in the suite component. For example, you create a schedule for a column analysis job to run weekly in an InfoSphere Information Analyzer project in the IBM InfoSphere Information Server console.

As a suite administrator, you might also want to have a global view of all of the scheduled activities that are created by each of the suite components to ensure that enough resources are available to process these schedules and to monitor who is scheduling tasks and with what frequency.

Criteria for schedule views

You access schedules from a view, which filters the events based on criteria that you set.

To create views, you can filter messages by the following criteria:

Name  You can filter tasks of a schedule by their names. Two wild cards are supported:
• An asterisk (*) finds one or more characters.
• A question mark (?) finds any single character at the current position.

Description  You can filter tasks of a schedule by their descriptions.

Schedule status  A schedule has three statuses: Complete, Started, and Paused.

Task Run status  Each task instance can have one of four statuses: Abnormally Ended, Finished, Canceled by User, or Running.

Creators  You can filter schedules by users.

Dates  You can filter schedules by three sets of dates:
• The dates on which schedules are created.
• The dates on which any task executions of the schedule were started.
• The updates, such as run start or completion, of any task executions for the schedule.

Origin  You can filter tasks based on the application components that originated the tasks.
Shared and private views

A view can be private or shared. A suite administrator or suite user who creates a private view has exclusive access to the view.

The following table describes the levels of access, based on the creator and type of view.

Table 16. Access to views

<table>
<thead>
<tr>
<th>Type of view</th>
<th>Created by</th>
<th>Who can access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private</td>
<td>Suite administrator</td>
<td>Creator can edit, view, and delete.</td>
</tr>
<tr>
<td>Shared</td>
<td>Suite administrator</td>
<td>Creator and other suite administrators can edit, view, and delete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suite users can view.</td>
</tr>
<tr>
<td>Private</td>
<td>Suite user</td>
<td>Creator can edit, view, and delete.</td>
</tr>
<tr>
<td>Shared</td>
<td>Suite user</td>
<td>Creator can edit, view, and delete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suite administrators can view and delete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other suite users can view.</td>
</tr>
</tbody>
</table>

Creating a schedule view

You create a schedule view to access and manage a list of schedules and scheduled tasks.

Before you begin

You must have suite administrator or suite user authority.

Procedure

1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, click New Scheduling View.
4. Specify the name, description, and access level of the view.
5. Optional: In the Filters pane, specify criteria for filtering schedules.
6. Click Save and Close to save the schedule view.

What to do next

You can now view all of the schedules that are captured by this schedule view.

Creating a schedule view from a copy

To create a schedule view that is based on the configuration details of another schedule, you can create a copy of a schedule view.

Before you begin

You must have suite administrator or suite user authority.
Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, select a view.
4. Click Copy.
5. In the Copy pane, type a new name and description for the schedule view.
6. Optional: Change the criteria of the view.
7. Click Save and Close.

Viewing the schedules that are captured by a schedule view

You can view the schedules that are captured by a schedule view. From this view, you can then manage the schedules and scheduled tasks.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, select a view.
4. Click View Schedules. A list of schedules that fit the criteria of the view opens.

Pausing all the schedules in a view

To pause a set of schedules, you can pause all of the schedules that are captured by a schedule view.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, select a view.
4. Click Pause. The schedules that are captured by the view are paused. All tasks in them will not run until the schedules are resumed.

Resuming all the schedules in a view

After you pause all of the schedules in a schedule view, you can resume all of the schedules that are captured by the scheduled view.

Procedure
To reuse all of the schedules in a schedule view:
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, select a view.
4. Click Resume. The schedules that are captured by the view are resumed.
Purging the history for all the schedules in a view

To quickly purge the run history of a number of schedules, you can purge the history of a schedule view. The run history for all of the schedules that are captured by the schedule view are purged from the metadata repository.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, select a view.
4. Click Purge Run History.
5. In the Purge window, specify an action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge all run history</td>
<td>Select All.</td>
</tr>
<tr>
<td>Purge run history in a date range</td>
<td>1. Select Range. 2. Type dates and times or use the calendar to specify a start date and an end date.</td>
</tr>
</tbody>
</table>

6. Click Yes. The run history is deleted from the metadata repository.

Working with the scheduled tasks in a view

After you create a schedule view, you can access the individual schedules and scheduled tasks that are captured by the view. You can stop and start the individual tasks. You can also view a summary of the completed tasks, the running tasks, or the future tasks that are captured by that view.

Stopping a scheduled task

While you are viewing the schedules that are captured by a schedule view, you can stop a scheduled task.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules tab, select a view.
4. Click View Schedules.
5. In the View Schedules pane, select a scheduled task.
6. Click Stop. The task is stopped.

Purging the history of a scheduled task

You can remove the run history of a scheduled task from the metadata repository. The task and its schedule remain in the metadata repository.

Procedure
1. In the IBM InfoSphere Information Server Web console, click the Administration tab.
2. In the Navigation pane, select Schedule Monitoring > Views of Schedules.
3. In the Views of Schedules pane, select a view.
4. Click View Schedules.
5. In the View Schedules pane, select a task.
6. Click Purge. The run history of the scheduled task is deleted from the metadata repository.

**Viewing a list of completed schedules**
If you are viewing an ongoing scheduled task, you can view a summary of all instances of this scheduled task that have completed.

**Procedure**
1. In the View Schedules pane, select a schedule.
2. Click View Complete.

**Viewing a list of running schedules**
For a scheduled task, you can view which instances of the schedule are currently running.

**Procedure**
1. In the View Schedules pane, select a schedule.
2. Click View Running.

**Viewing a list of upcoming scheduled tasks**
If you are viewing an ongoing scheduled task, you can view the tasks that will run in the future.

**Procedure**
1. In the View Schedules pane, select a schedule.
2. Click View Forecast.
Chapter 13. Backing up and restoring IBM InfoSphere Information Server

To prevent the loss of data and to prepare for disaster recovery, you can back up and restore the databases, profiles, and directories that are associated with IBM InfoSphere Information Server.

About this task

The services tier, engine tier, and metadata repository tier consist of various elements that require back up. The procedures documented here do not cover backing up and restoring InfoSphere Information Server clients that are running on Microsoft Windows computers. Back up and restore is typically not required for client-only installations as only local, user-specific customizations are stored on client computers. To recover a client-only installation, you can reinstall the clients.

The InfoSphere Information Server recovery assistant back up and restore wizards walk you through interviews that collect information about your system. The wizards automatically create a response file, which is used to back up and restore the services, engine, and metadata repository tiers. When you run a back up or recovery, all tiers installed on the computer are backed up. If your system is dispersed across computers, back them all up individually.

The engine tier installation contains files and configuration data that are linked to elements stored in the metadata repository. IBM InfoSphere DataStage and IBM InfoSphere QualityStage projects are stored in the engine tier installation directory or elsewhere on the same computer. They are linked to elements stored in the metadata repository. There is also information stored in files in the IBM WebSphere Application Server directory that is linked to elements stored in the metadata repository. Finally, while the IBM InfoSphere Information Analyzer analysis database and InfoSphere QualityStage Match Designer database are separate from the metadata repository database, there are cross-database references between them.

Because of these interdependencies, to guarantee a successful back up, the metadata repository, the InfoSphere QualityStage Match Designer database, the InfoSphere Information Analyzer analysis database, the IBM InfoSphere DataStage and InfoSphere QualityStage projects, and all of the file system-based elements that change after installation must be backed up, and the back up must occur while all services and IBM WebSphere Application Server are shut down. If you do not shut them down manually, the recovery tool shuts them down.

When you restore an installation, all of the same elements that were backed up need to be restored during the same restore session. Restore all elements before you start IBM WebSphere Application Server or InfoSphere Information Server.

Verifying system and disk space requirements

The InfoSphere Information Server recovery tool verifies that your computers meet the system requirements for the version to which you are performing back up or restore operations, and ensures that the systems have enough disk space for the back up and restore directories and data.
About this task

The InfoSphere Information Server, Version 9.1 recovery tool backs up and recovers only Version 9.1 of InfoSphere Information Server. System requirements, such as the version of the operating system or database, might change between releases of the software. Before you begin the back up or restore operation, verify that your computers meet all of the system requirements for the version of InfoSphere Information Server to which you are performing back up or restore operations.

The InfoSphere Information Server recovery tool requires two directories, the work directory and the archive directory. The tool checks to ensure that each computer has enough disk space for these directories.

Procedure

1. See this topic for complete information about the system requirements for InfoSphere Information Server, Version 9.1: [http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html](http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html)

2. Verify the following disk space requirements on the systems that you are backing up:
   - The work directory for the Services tier is the database size plus 15%.
   - The work directory for the Engine tier is the combined size of all project directories plus 15%.
   - The archive directory is 25% of the size of the work directory.

3. Verify the following disk space requirements on the systems that you are restoring data to:
   - The work directory for the Services tier is the size of the source work directory plus 10%. In addition, the Services tier must have enough disk space for the migrated database.
   - The work directory for the Engine tier is the size of the target work directory plus 10%. In addition, the Engine tier must have enough disk space for the migrated projects.

Credential information

Collect these user names and passwords before starting back up or restore operations. The passwords must be valid and unexpired.

You will need to enter the credentials below when you are using the back up and restore wizards.

<table>
<thead>
<tr>
<th>User</th>
<th>Default user name</th>
<th>User name (if you did not use the default)</th>
<th>Password or encrypted password</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoSphere Information Server administrator</td>
<td>isadmin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM WebSphere Application Server administrator</td>
<td>wasadmin</td>
<td></td>
<td></td>
</tr>
<tr>
<td>InfoSphere DataStage administrator</td>
<td>dsadm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 17. User credentials (continued)

<table>
<thead>
<tr>
<th>User</th>
<th>Default user name</th>
<th>User name (if you did not use the default)</th>
<th>Password or encrypted password</th>
</tr>
</thead>
</table>
| Metadata repository IBM DB2 database owner | - Linux  
db2inst1  
- UNIX  
- Windows  
db2admin | | |
| Metadata repository database Oracle system administrator | system | | |
| Metadata repository database Microsoft SQL Server administrator | system | | |
| InfoSphere Information Analyzer analysis database owner | iauser | | |
| InfoSphere DataStage Operations Database owner | dsodbuser | | |
| IBM InfoSphere QualityStage Standardization Rules Designer database owner | srduser | | |

Back up IBM InfoSphere Information Server components

To back up IBM InfoSphere Information Server components, you use the InfoSphere Information Server recovery assistant back up wizard to create a response file. The response file is then used by the recovery tool for the back up operation. Some components must be backed up manually.

Before you begin

Refer to the following technote for any additional information that might be required to run a back up operation [http://www.ibm.com/support/docview.wss?uid=swg21516582](http://www.ibm.com/support/docview.wss?uid=swg21516582).

Before running a back up operation, ensure that there are no active client connections and [place the server in maintenance mode](#). The back up operation shuts down all active services, which might cause unexpected errors if clients are connected.

You can determine if there are active connections and optionally terminate the connections in the IBM InfoSphere Information Server Web console. For more information, see [Managing active sessions](#).

Although clients might not be connected, the server might still be in use if jobs are running or might start running before all server components can be stopped. The jobs might belong to IBM InfoSphere DataStage, IBM InfoSphere QualityStage, or IBM InfoSphere Information Analyzer. You can use the IBM InfoSphere Information
Server Web console to determine if any jobs are running or are scheduled to run soon. For more information, see Managing schedules.

Requirements

- The recovery tool backs up data and metadata, not the product installation. Before a restore operation, InfoSphere Information Server must be reinstalled at the exact version, with the same products as the backed up system. For example, if you have installed InfoSphere DataStage, InfoSphere Information Analyzer, and not IBM InfoSphere FastTrack, then the restored computer must also contain InfoSphere DataStage, InfoSphere Information Analyzer, and not InfoSphere FastTrack. Also, the installation topology and operating systems must be the same as the original. For example, you cannot back up two engines on Microsoft Windows computers and restore them to a single Linux computer. To determine the version and patch level of the software installed on the computer to be backed up, you can run the IBM Support Assistant Lite for InfoSphere Information Server tool and generate the Migration reference report. To generate the report, select All Collectors > Migration reference report. The System Summary report, included with the Migration reference report, contains additional information about the installation.

- Disconnect all user sessions.

- The services tier, engine tier, and metadata repository tier must all be backed up for a successful restore. If all tier archives from a back up session are not available during a restore session, the restore results in a system that is in an inconsistent state.

Procedure

Complete the following steps on each computer where the services tier, engine tier, or metadata repository tier are installed for back up.

1. Navigate to the directory where you installed InfoSphere Information Server and open the recovery folder.
   - install_dir/recovery/bin
   - install_dir\recovery\bin

2. At the command line, log in as an administrator.

3. Enter this command:
   - install_dir/recovery/bin/isrecovery.sh
   - install_dir\recovery\bin\isrecovery.bat

   Several messages are displayed. The program then displays a message about how to access the InfoSphere Information Server recovery assistant back up wizard. For example:
   ======> Use a browser to connect to the web server at https://localhost:8443/ibm/iis/mbr/console

4. Open a web browser, and navigate to the address that is listed in the messages issued in the command line interface. A message might appear in the browser that reads “The publisher cannot be verified...” You can safely ignore the message and continue. This message does not indicate a security risk when it appears during InfoSphere Information Server back up.

5. Click Get Started under the Back up section.

6. Continue to follow the prompts in the InfoSphere Information Server recovery assistant back up wizard.
7. Click **Finish** after the wizard has finished creating the response file that it will use to complete the backup operation. Click **Print** to print out the next steps that you need to do to complete the backup operation.

8. Switch to back to the command line to start the backup operation. Log into the command line as an administrator.

9. Issue the following command:
   - `isrecovery.sh -resp <path/to/ResponseFilePath/ResponseFileName.xml>`.
   - `isrecovery.bat -resp <C:\ResponseFilePath\ResponseFileName.xml>`.

   You must provide the path to the response file, as well as the name of the response file that you specified during the interview you completed while running the wizard. The default response file directory is `/opt/IBM/InformationServer/Recovery` or `C:\IBM\InformationServer\Recovery` on a Windows computer. The default name for the response file name is `recovery_backup.xml`.

10. Optional: Disconnect all user sessions and place InfoSphere Information Server into maintenance mode. For more information, see “Maintenance mode” on page 228.

**What to do next**
- Complete the backup interview by using the InfoSphere Information Server recovery assistant on each of the remote systems that you want to back up, and then complete the backup operation by running the `isrecovery.sh` or `isrecovery.bat` script on the command line.
- Review the to-do file that was generated during backup and perform all actions described in the file. The `recovery.todo.txt` file is located in the `/opt/IBM/InformationServer/Recovery` folder.
- Manually back up any components that you chose to manually back up during the interview you completed while using the wizard. You manually back up the components by using scripts that were generated by the recovery tool. The scripts are stored in the folder that you specified in the **Directory for generated scripts** field in the wizard. The default directory is:
  - `/opt/IBM/InformationServer/Recovery/DatabaseSupport`
  - `C:\IBM\InformationServer\Recovery\DatabaseSupport`

Scripts to manually back up each database are stored in folders such as `C:\IBM\InformationServer\Recovery\DatabaseSupport\Metadata` or `/opt/IBM/InformationServer/Recovery/DatabaseSupport/Metadata` for the metadata repository database and `C:\IBM\InformationServer\Recovery\DatabaseSupport\ia` or `/opt/IBM/InformationServer/Recovery/DatabaseSupport/ia` for the InfoSphere Information Analyzer analysis database.
- After all tiers are backed up, you can:
  - Restart the InfoSphere Information Server services and WebSphere Application Server services. For more information, see Chapter 14, “Administering IBM InfoSphere Information Server and IBM WebSphere Application Server services,” on page 227.
  - Disable maintenance mode if it is enabled, disable it. For more information, see “Maintenance mode” on page 228.
Restoring IBM InfoSphere Information Server components

To restore IBM InfoSphere Information Server components, you use the InfoSphere Information Server recovery assistant wizard to create a response file. The response file is then used by the recovery tool for the restore operation. Some components must be restored manually.

Before you begin

Refer to the following technote for any additional information that might be required to run a restore operation [http://www.ibm.com/support/docview.wss?uid=swg21516582](http://www.ibm.com/support/docview.wss?uid=swg21516582)

Before running a restore operation, ensure that there are no active client connections. This task assumes that your backup topology has been out of operation. Or, if you are restoring to the same computers, uninstall the previous installation and reinstall a clean installation with no projects except the default (dstage1). Ensure that users are restricted from logging in during the entire restore session by placing the server in maintenance mode. Otherwise, the restore operation might fail or users might lose data in that it would be overwritten when the metadata repository is restored.

Requirements

- The recovery tool restores data and metadata, not the product installation. If you are restoring InfoSphere Information Server to different computers, the components must first be installed at the exact version, with the same product selection as the backed up system. For example, if you have installed IBM InfoSphere DataStage, IBM InfoSphere Information Analyzer, and not IBM InfoSphere FastTrack, then the restored computer must also contain InfoSphere DataStage, InfoSphere Information Analyzer, and not InfoSphere FastTrack. Also, the installation topology and operating systems must be the same as the original. For example, you cannot back up two engines on Microsoft Windows computers and restore them to a single Linux computer.
- The services, engine, and metadata repository tiers must have all been backed up for a successful restore. If all tier archives from a backup session are not available during a restore session, the restore operation would result in a system in an inconsistent state.
- It is possible to restore to computers with different host names. Additional configuration steps are required and are described.

Procedure

Complete the following steps on each computer where the services tier, engine tier, or metadata repository tier are installed for restore.

1. Navigate to the directory where you installed InfoSphere Information Server and open the recovery folder. For example:
   - `install_dir\InformationServer\recovery\bin`
   - `install_dir\InformationServer\recovery\bin`
2. At the command line, log in as an administrator.
3. Enter this command:
   - `install_dir\InformationServer\recovery\bin\isrecovery.sh`
   - `install_dir\InformationServer\recovery\bin\isrecovery.bat`
Several messages are displayed. The program then displays a message about how to access the InfoSphere Information Server recovery assistant restore wizard. For example:

======> Use a browser to connect to the web server at https://localhost:8443/ibm/iis/mbr/console

4. Open a web browser, and navigate to the address that is listed in the messages issued in the command line interface. A message might appear in the browser that reads “The publisher cannot be verified...” You can safely ignore the message and continue. This message does not indicate a security risk when it appears during InfoSphere Information Server restore operation.

5. Click Get Started under the Restore section.

6. Continue to follow the prompts in the InfoSphere Information Server recovery assistant restore wizard.

7. Click Finish after the wizard has finished creating the response file that it will use to complete the restore operation. Click Print to print out the next steps that you need to do to complete the restore operation.

8. Switch back to the command line to start the restore operation. Log into the command line as an administrator.

9. Issue the following command:
   • isrecovery.sh -resp /opt/ResponseFilePath/RecoveryResponseFileName.xml
   • isrecovery.bat -resp C:\ResponseFilePath\RecoveryResponseFileName.xml

You must provide the path to the response file, as well as the name of the response file that you specified during the interview you completed while running the wizard. The default response file directory is:
   • /opt/IBM/InformationServer/Recovery
   • C:\IBM\InformationServer\Recovery

The default name for the response file name is recovery_restore.xml.

10. Optional: Disconnect all user sessions and place InfoSphere Information Server into maintenance mode. For more information, see “Maintenance mode” on page 228.

What to do next
   • If you manually backed up the metadata repository database, the recovery tool prompts you to run the restore script in the folder you specified in the Directory for generated scripts field. The default folder is:
     – /opt/IBM/InformationServer/Recovery/DatabaseSupport/Metadata
     – C:\IBM\InformationServer\Recovery\DatabaseSupport\Metadata

After you run the script to manually restore the metadata repository database, issue the following command:
   – isrecovery.sh -restart
   – isrecovery.bat -restart

• Complete the restore interview by using the InfoSphere Information Server recovery assistant on each of the remote systems that you want to restore, and then complete the restore operation by running the isrecovery.sh or isrecovery.bat file on the command line.

• Review the to-do file that was generated during the restore operation and perform all actions described in the file. The recovery.todo.txt file is located in the following folder if you used the default directory:
- /opt/IBM/InformationServer/Recovery
- C:\IBM\InformationServer\Recovery

• Manually restore any components that you chose to manually restore during
  the interview you completed while using the wizard. You manually restore the
  components by using scripts that were generated by the recovery tool. The
  scripts are stored in the folder that you specified in the **Directory for generated
  scripts** field in the wizard. The default directory is /opt/IBM/InformationServer/
  Recovery/DatabaseSupport. Scripts to manually restore each database are stored
  in folders such as C:\IBM\InformationServer\Recovery\DatabaseSupport\IA or
  /opt/IBM/InformationServer/Recovery/DatabaseSupport/IA for the InfoSphere
  Information Analyzer analysis database.

• When all tiers are restored, you can:
  – Start the InfoSphere Information Server services and WebSphere Application
    Server services. For more information, see Chapter 14, “Administering IBM
    InfoSphere Information Server and IBM WebSphere Application Server
    services,” on page 227.
  – Disable maintenance mode if it is enabled. For more information, see
    “Maintenance mode” on page 228.

---

**Back up and restore scenarios**

Consider these typical scenarios when you are deciding how to back up or restore
using the InfoSphere Information Server recovery assistant back up and restore
wizards.

### Back up and restore scenarios for the metadata repository

The back up and restore wizards offer two ways to back up and restore the
metadata repository. If the metadata repository and the services tier are co-located,
you can automatically or manually back up and restore the metadata repository. If
the metadata repository is on a separate machine from the services tier, then you
must back up and restore the metadata repository manually.

The back up and restore wizards walk you through an interview. During the
interview, the wizards collect information about the metadata repository. The
collected information is used to automatically create a response file. The response
file is then used to back up or restore the metadata repository.

During the interview you will have the choice to automatically or manually back
up or restore the metadata repository. If you chose to back up or restore the
metadata repository manually, then scripts are generated, which you later run to
manually back up or restore the metadata repository. The following list describes
the options you have to manually or automatically back up or restore the metadata
repository:

• If the source metadata repository tier that you back up is co-located with the
  services tier and will be co-located with the services tier in the target topology
  that you want to restore to, then you can automatically or manually restore.

• If the source metadata repository tier that you back up is co-located with the
  services tier, but you want to move the metadata repository to a separate
  computer in the target topology that you are restoring to, then you must
  manually back up and restore the metadata repository.

• If the source services tier and the source metadata repository tier are on separate
  computers when you perform back up operations, then manually back up and
  restore the metadata repository.
If your site requires that a database administrator perform the metadata repository back up and restore operations, then manually back up and restore the metadata repository.

Table 18. Questions about how to back and restore up the metadata repository

<table>
<thead>
<tr>
<th>Question</th>
<th>If Yes, perform these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you want to manually back up or restore the metadata repository?</td>
<td>Select <strong>Manual</strong> on the <strong>Metadata Repository Database Options</strong> screen. Specify the directory where you want to store the generated scripts that you will use to manually back up or restore the database.</td>
</tr>
<tr>
<td>Is the metadata repository tier co-located with the services tier?</td>
<td>You can manually or automatically back up or restore the metadata repository database. Select <strong>Automatic</strong> or <strong>Manual</strong> on the <strong>Metadata Repository Database Options</strong> screen.</td>
</tr>
<tr>
<td>Is the metadata repository tier currently on a separate computer?</td>
<td>You must manually back up and restore the metadata repository database. If the metadata repository is installed on a separate computer, the scripts to back up the metadata repository are generated when you run the recovery tool on the services tier computer and select <strong>Manual</strong> on the <strong>Metadata Repository Database Options</strong> screen. Then you move the scripts directory to the computer that hosts the metadata repository and follow the instructions in the generated <strong>readme.txt</strong> file to run the scripts that back up and restore the metadata repository.</td>
</tr>
<tr>
<td>If the metadata repository tier is co-located with the services tier when you perform a back up operation, do you want to move the metadata repository tier to a separate computer in the installation that you are restoring to?</td>
<td>You must manually back up and restore the metadata repository database. Follow the instructions in the generated <strong>readme.txt</strong> file to run the scripts that back up and restore the metadata repository.</td>
</tr>
</tbody>
</table>
Table 18. Questions about how to back and restore up the metadata repository (continued)

<table>
<thead>
<tr>
<th>Question</th>
<th>If Yes, perform these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which user name do I enter?</td>
<td>DB2 User name of the DB2 database user who has SYSADM, SYSCtrl, or SYSMaint privileges and who can run back up and restore operations on the metadata repository database. The db2instance user typically has SYSADM authority. On Microsoft Windows, this user is the operating system user. The operating system user must have authority either directly as a DB2 user or indirectly as part of the operating system administrators group. Oracle User name of a user that has system administrator authority (SYSDBA). SQL Server User name of a user that has Microsoft SQL Server system administrator privileges.</td>
</tr>
</tbody>
</table>

Back up and restore scenarios for the engine tier and InfoSphere DataStage

Multiple engine tiers require additional configuration for back up and restore. You also need to consider how you want to back up and restore InfoSphere DataStage projects.

Table 19. Questions about how to back up and restore the engine tier and InfoSphere DataStage

<table>
<thead>
<tr>
<th>Question</th>
<th>If Yes, perform these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system you are backing up or recovering include multiple engine tiers?</td>
<td>You must run the back up and recovery wizards on each of the engine tier computers.</td>
</tr>
<tr>
<td>If the system you are backing up or restoring runs multiple versions of InfoSphere Information Server, which version do you want to back up or restore to Version 9.1?</td>
<td>You can only back up Version 9.1 using the 9.1 back up wizard. To back up or restore Version 8.5 or earlier, you must perform a manual back up or restore. To back up or restore Version 8.7, use Version 8.7 of the isrecovery tool.</td>
</tr>
<tr>
<td>All projects are restored to install_dir/Server/Projects by default. Do you want to restore one or more projects to a different directory?</td>
<td>Select Specify a new default project directory on the InfoSphere DataStage Engine Properties screen, and browse to the default directory that you want to use.</td>
</tr>
<tr>
<td>Is the physical host name on the computer that you backed up different from the physical host name on the computer that you are restoring?</td>
<td>On the Physical Host Name Configuration screen in the restore wizard, map the physical host name on the computer that you backed up to the physical host name that it maps to on the computer that you are restoring to. Drag physical host names in the target computer column so they correspond to the appropriate physical host names in the source computer column. This is only relevant if there is more than one engine in the InfoSphere Information Server installation.</td>
</tr>
</tbody>
</table>

Back up and restore scenarios for the InfoSphere Information Analyzer analysis database

The back up and restore wizards offer two ways to back up and restore the InfoSphere Information Analyzer analysis database. Which approach you use depends on where the analysis database is located. You also have the options of backing up and restoring or not backing or not restoring the analysis database.
Table 20. Questions about how to back up and restore the InfoSphere Information Analyzer analysis database

<table>
<thead>
<tr>
<th>Question</th>
<th>If yes, perform these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the analysis database is local to the services tier, do you want to back up or restore the analysis database?</td>
<td>Select <strong>Back up the InfoSphere Information Analyzer analysis database</strong> or <strong>Restore the InfoSphere Information Analyzer analysis database</strong> on the <strong>InfoSphere Information Analyzer Analysis Database Options</strong> screen in the back up or restore wizard. You can manually or automatically back up or restore the analysis database. Select <strong>Automatic</strong> or <strong>Manual</strong> on the <strong>InfoSphere Information Analyzer Database Options</strong> screen.</td>
</tr>
<tr>
<td>If the analysis database is local to the services tier, do you NOT want to back up or restore the analysis database?</td>
<td>Deselect <strong>Back up the InfoSphere Information Analyzer analysis database</strong> or <strong>Restore the InfoSphere Information Analyzer analysis database</strong> on the <strong>InfoSphere Information Analyzer Analysis Database Options</strong> screen in the back up or restore wizard.</td>
</tr>
<tr>
<td>Is the analysis database on a separate computer? Do you want to back up or restore the analysis database?</td>
<td>Select <strong>Back up the InfoSphere Information Analyzer analysis database</strong> or <strong>Restore the InfoSphere Information Analyzer analysis database</strong> on the <strong>InfoSphere Information Analyzer Analysis Database Options</strong> screen in the back up or restore wizard. You must manually back up or restore the analysis database and specify the directory where you want to store the generated script. Note: After you finish walking through the back up wizard, you copy the scripts from the services tier computer to the computer that hosts the analysis database. Then you run the scripts to manually back up the database. When you need to perform a restore operation, you copy the database backup to the computer that hosts the analysis database where you are restoring your computer. After you complete restore operations, use the generated scripts from the restore operation to the computer that hosts the target analysis database and restore the database backup.</td>
</tr>
</tbody>
</table>

**Back up and restore scenarios for the user registry**

Identify the type of user registry that is used by the installation that you are backing up.

The back up wizard automatically backs up the local operating system or LDAP user registry from the source computer. The user registry can be restored by the recovery tool. If credential mapping is used, the recovery tool creates credential mappings on the computer that is being restored.

Table 21. Questions about the user registry

<table>
<thead>
<tr>
<th>Question</th>
<th>More information</th>
</tr>
</thead>
<tbody>
<tr>
<td>What type of user registry (internal, local operating system, or LDAP) is IBM InfoSphere Information Server configured for?</td>
<td>If the source uses credential mapping, you must ensure that the local operating system IDs that are used for credential mapping are created on the engine tier computer that you are restoring. For example, if user val on the computer that was backed up is mapped to local operating system user vpech and the target computer that you are restoring to does not have a local operating system user named vpech, when user val tries to use the target, the follow message displays: “User name and/or password incorrect. If credential mapping is used, check that the credential mapped user name and password are correctly configured.” The recovery tool backs up the source user registry unless it is a federated or LDAP user registry, and is using an SSL configuration. Internal, local operating system, and LDAP (non-SSL), will be backed up and restored. For more information about credential mapping, see the following topic: <a href="http://publib.boulder.ibm.com/infocenter/iisinfsv/v9r1/topic/com.ibm.swg.im.iis.found.moz.wc_admin.doc/topics/wsisinst_config_user_mappings.html">http://publib.boulder.ibm.com/infocenter/iisinfsv/v9r1/topic/com.ibm.swg.im.iis.found.moz.wc_admin.doc/topics/wsisinst_config_user_mappings.html</a></td>
</tr>
<tr>
<td>Do you want to change the type of user registry?</td>
<td>Configure the new user registry before you use the recovery tool to perform a back up operation. Then when you back up the source, the recovery tool detects that the user registry is not the internal registry and does not back up the source system configuration. Note: If the new registry uses a different InfoSphere Information Server administrator ID and password, when you use the recovery tool to start the recovery operation, you must specify the new administrator ID and password on the <strong>Engine Tier Credentials</strong> screen.</td>
</tr>
</tbody>
</table>

**InfoSphere DataStage project folder options**

The recovery tool helps you configure InfoSphere DataStage project locations and updates in order to restore them.

Using the restore wizard, you specify the project directory into which projects are restored. On the **InfoSphere DataStage project options** screen, you have three options for specifying the project directory:
• You can automatically restore all projects to the default directory that the restore wizard provides:
  – IBM/InformationServer/Server/Projects
  – IBM\InformationServer\Server\Projects
To restore projects to this default project directory, select **Use the default project directory on the target system.**

• You can restore all projects to a user-specified default project directory. To restore all projects to a user-specified default project directory, select **Use a user-specified default project directory** in the restore wizard, and specify the directory. This user-specified directory overrides the default directory setting.

• You can restore some projects to a user-specified default project directory and restore one or more other projects to other user-specified directories. You select **Use a user-specified default project directory** and specify the user-specified default project directory. Then you specify the directory for each project that you want to restore in the **Location** field in the **InfoSphere DataStage Projects** section of the screen.

For example, if the **InfoSphere DataStage project options** screen contains the following entry in the **Use the default project directory on the target system** field:

/dastage/team1_projects

and the **InfoSphere DataStage Projects** area specifies that project ProjectA has the following location:

/dastage/team2_projects

all projects will be restored to /dastage/team1_projects, except for projectA, which will be restored to /dastage/team2_projects/. You will have a directory structure that looks like this:

datastage
team1_projects
  project1
  project2
team_2_projects
  projectA

**Additional files to back up**
The recovery tool does not automatically back up all data on your computer. The back up wizard allows you to specify additional files to back up in a text file.

To back up additional files, create a text file that contains a list of the files that you want to back up. You must specify each file name, along with a full path, on a single line. Do not specify a delimiter after each file name.

The following table shows the data that is not automatically backed up by the back up wizard.
Table 22. Data that is not automatically backed up by the back up wizard

<table>
<thead>
<tr>
<th>Product</th>
<th>Data that is not automatically backed up</th>
</tr>
</thead>
</table>
| InfoSphere DataStage and QualityStage | • Data sets  
• For Version 8.0.1 and Version 8.1, job run time  
• Run-time log files  
• Operational metadata  
• Job schedules or job invocations  
• InfoSphere DataStage hash files that are not saved in a project directory  
• Data files that are accessed by InfoSphere DataStage and QualityStage with the sequential file method  
• Data files used by InfoSphere DataStage that contain user-defined SQL statements for writing data to databases |
| InfoSphere QualityStage modules | • Postal validation reference files  
• Geocoding reference files  
• Match Designer database |
| InfoSphere Information Server Enterprise Packs | • Reference files |

**Back up and restore commands for the recovery tool**

You run the recovery tool from the command line by specifying the recovery script, followed by a command, and optional parameters.

The recovery tool script is located in this default directory:

- **Windows**
  
  `install_dir\InformationServer\Recovery\bin\isrecovery.bat`

- **Linux**  
  
  `install_dir/InformationServer/Recovery/bin/isrecovery.sh`

The recovery tool command syntax is as follows:

```
isrecovery  
isrecovery -resp ResponseFileName [-force] [-validateonly]  
isrecovery --restart  
isrecovery -version  
isrecovery -help
```

**Response command**

The recovery tool uses a response file to perform back up and restore operations. The response file is automatically created when you use the back up and restore wizards. You must run the `-resp` command to start the actual back up or restore process. Run the response command on the services tier first, then the engine tier.

**The response command**

You use the `-resp` command to start the back up or restore operations.
The `-resp` command requires the path to the response file, as well as the response file name.

The `-resp` command:

```
install_dir/recovery/bin/isrecovery.sh -resp response_file_name
install_dir\recovery\bin\isrecovery.bat -resp response_file_name [-force] [-validateonly]
```

Optional parameters

When you run the recovery tool, you can include additional, optional parameters.

**-force**  Use this parameter after you run the `-resp` command, and receive a message that says only the `-restart` command can be used. The force parameter can be specified to remove the previous back up or restore operation’s checkpoint and work files. The force command starts the recovery tool from the beginning.

**-validateonly**  Use this parameter to verify that the environment meets the requirements for the back up or restore operation. The command also verifies that the values in the response file are appropriate for the environment and the command that you specify.

Response command example for a restore operation

Starting a restore operation:

```
/IBM/InformationServer/recovery/bin/isrecovery.sh
-rep /opt/IBM/InformationServer/Recovery/recovery_restore.xml
```

Response command example for a back up operation

Starting a back up operation:

```
/IBM/InformationServer/recovery/bin/isrecovery.sh
-rep /opt/IBM/InformationServer/Recovery/recovery_backup.xml
```

Response command example for a back up operation with the force option

Starting a back up operation with the force option:

```
/IBM/InformationServer/recovery/bin/isrecovery.sh
-rep /opt/IBM/InformationServer/Recovery/recovery_backup.xml -force
```

Response command example for a back up operation with the validate only option

Starting a back up operation with the validate only option:

```
/IBM/InformationServer/recovery/bin/isrecovery.sh
-rep /opt/IBM/InformationServer/Recovery/recovery_backup.xml -validateonly
```

Restart command

The recovery tool automatically creates checkpoint files throughout the back up and restore operations. The `-restart` command restarts the back up process or the restore process from the last saved checkpoint.
The restart command

You use the **-restart** command after a **-backup** or **-restore** command fails and you resolve the errors. You also use the command after you back up or restore the metadata repository or the analysis database manually and after you generate and review the scripts that configure IBM WebSphere Application Server.

Because the checkpoint file provides details about the **-backup** or **-restore** command, when you use the **-restart** command, you do not specify the additional parameters that you specified as part of those commands.

The **-restart** command:
```
install_dir/recovery/bin/isrecovery.sh -restart
install_dir\recovery\bin\isrecovery.bat -restart
```

**Important:** If a back up or restore process fails, view the console log and the error logs in the logs directory to determine whether you can resolve the errors. The log files are in this directory:
- `install_dir/Recovery/logs`
- `install_dir\Recovery\logs`

### Restart command example

You might see the following error:
```
Back up side validation failed. DB2 user db2inst1 doesn't have authority to backup database.
[ibm][db2][jcc][t4][2012][11248] Connection authorization failure occurred.
  Reason: Password expired.
```

After you see this error and fix the problem, run the **-restart** command to resume the back up or restore process from the last saved checkpoint:
```
install_dir/Recovery/bin/isrecovery.sh -restart
```

### Restart command example

The back up or restore resumes the back up process or the restore process from the last saved checkpoint.
```
install_dir\recovery\bin\isrecovery.bat -restart
```

### Version command

The recovery tool **-version** command shows the current version of the recovery tool.

**The version command**

The **-version** command:
```
install_dir/recovery/bin/isrecovery.sh -version
install_dir\recovery\bin\isrecovery.bat -version
```

**Version command usage example**

The version number of the recovery tool is displayed.
```
/recovery/bin/recovery.sh -version
C:\IBM\InformationServer\recovery\bin\isrecovery.bat -version
```
The version number is displayed. For example, information similar to the following is displayed for version number 9.1.0.0.0.125:

Information Server Recovery Tool version 9.1.0.0.0.125 2012-11-30
Chapter 14. Administering IBM InfoSphere Information Server and IBM WebSphere Application Server services

Follow these procedures to administer IBM InfoSphere Information Server services and IBM WebSphere Application Server services. For example, check the status of services and stop and restart them when you back up or restore your system, or to do other maintenance tasks.

For further information about the WebSphere Application Server tools and processes mentioned in these procedures, see the WebSphere Application Server Information Center:

- IBM WebSphere Application Server Network Deployment 8.5:
- IBM WebSphere Application Server Network Deployment 8.0:
  [http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp](http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp)

For further information about various tools to use to manage a WebSphere Application Server, see the following topics in the WebSphere Application Server documentation:

**WebSphere Application Server 8.5**

Starting the Deployment Manager by using the `startManager` tool:

Stopping the Deployment Manager by using the `stopManager` tool:

Starting a node agent by using the `startNode` tool:

Stopping a node agent by using the `stopNode` tool:

Starting cluster members:

Stopping cluster members:

Starting stand-alone application servers and cluster members by using the `startServer` tool:

**WebSphere Application Server 8.0**

Starting the Deployment Manager by using the `startManager` tool:
Stopping the Deployment Manager by using the `stopManager` tool:

Starting a node agent by using the `startNode` tool: http://

Stopping a node agent by using the `stopNode` tool: http://


### Maintenance mode

To prevent users from authenticating to IBM InfoSphere Information Server during maintenance, you can place it into maintenance mode with the `SessionAdmin` command. Use the same command to take InfoSphere Information Server out of maintenance mode and to determine the current maintenance mode.

Placing InfoSphere Information Server in maintenance mode is useful when you do routine maintenance such as applying a fix pack or backing up the system. When in maintenance mode, only users with the suite administrator role and system users can authenticate. Note also that in the Web admin console, **Maximum Sessions** is not editable while InfoSphere Information Server is in maintenance mode.

### Usage

Use the `SessionAdmin` command to set the maintenance mode for InfoSphere Information Server. You must have suite administrator authority to run this command. The command is in the following locations:

- **UNIX**
  - `IS_install_dir/ASBServer/bin/SessionAdmin.sh`
  - `IS_install_dir/ASBNode/bin/SessionAdmin.sh`

- **Windows**
  - `IS_install_dir\ASBServer\bin\SessionAdmin.bat`
  - `IS_install_dir\ASBNode\bin\SessionAdmin.bat`

**Tip:** In the following usage examples, you can choose to use the `-authfile` option instead of `-user` and `-password.
Placing InfoSphere Information Server in maintenance mode
SessionAdmin -user username -password plaintext_password -kill-user-sessions
SessionAdmin -user username -password plaintext_password -set-maint-mode ON

Taking InfoSphere Information Server out of maintenance mode
SessionAdmin -user username -password plaintext_password -set-maint-mode OFF

Determining the current maintenance mode
SessionAdmin -user username -password plaintext_password -get-maint-mode

Syntax
SessionAdmin
[-{verbose | v}]
[-{results | res} value ]
[-{log | l} value ]
[-{logerror | error} value ]
[-{loginfo | info} value ]
[-{loglevel | level} value ]
[-{help | ?} ]
[-{host | h} value ]
[-{port | p} value ]
[-{user | ur} value ]
[-{password | pw} value ]
[-{authfile | af} value ]
[-{kill-user-sessions | kus} ]
[-{get-maint-mode | gmm}]
[-{set-maint-mode | smm} value ]

Parameters
[-{verbose | v}]
Display detailed runtime output, except for the runtime logging messages.

[-{results | res} value ]
Print all the enabled runtime output to the specified file.

[-{log | l} value ]
Print the runtime logging messages to the specified file. This option is used with loglevel.

[-{logerror | error} value ]
Print all ERROR and FATAL runtime logging messages to the specified file.

[-{loginfo | info} value ]
Print all INFO, WARN, DEBUG, and TRACE runtime logging messages to the specified file.

[-{loglevel | level} value] The level at which runtime logging messages are enabled.

[-{help | ?} ]
Displays the usage message.

[-{host | h} value]
Host machine name. The default value is localhost.

[-{port | p} value]
Host machine HTTP port. The default value is 9080.

[-{user | ur} value ]
The administrator user ID to run this command. If not specified and if the -authfile parameter is not specified, you are prompted for a user ID.
The password of the administrator user ID specified in the -user parameter. This parameter cannot be specified without the -user parameter. If the -user parameter is specified without the -password parameter, you are prompted for a password.

The path for the credentials file that contains the administrator user ID and password to run this command. If the -user parameter is also specified, the credentials file is ignored and you are prompted for a password.

Stop all user sessions.

Display the current maintenance mode setting.

Set the maintenance mode. Acceptable values are ON or OFF.

## Shutting down services (Windows)

Follow this procedure to shut down the IBM InfoSphere Information Server services and IBM WebSphere Application Server services in a Microsoft Windows installation. Shut down services before you back up or restore your system, or do other maintenance tasks.

### Before you begin

If your metadata repository tier is set up in a clustered configuration, make sure that the databases are shut down last, if you shut them down at all.

Note: To perform a cold backup, you must shut down the databases.

### About this task

The paths shown in this task assume that WebSphere Application Server and InfoSphere Information Server are installed in the default locations. Your paths and profile names are different if you installed these products in different locations.

### Procedure

1. Stop the following services: InfoSphere DataStage Engine Resource Service, IBM InfoSphere DataStage Telnet Service, DSRPC Service, ASB Agent, and Logging Agent. To stop the services:
   a. On each computer that hosts an engine tier, log in as a user that has local administrator privileges.
   b. Use the Services Administrative Tool or the sc command-line tool to stop the services. Stop the services in the order in which they appear in the table.

<table>
<thead>
<tr>
<th>Service full name</th>
<th>Service short name</th>
<th>Process name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataStage Engine Resource Service</td>
<td>DSEngine</td>
<td>dsservice.exe</td>
</tr>
<tr>
<td>DataStage Telnet Service</td>
<td>dstelnet</td>
<td>tl_dsservice.exe</td>
</tr>
<tr>
<td>DSRPC Service</td>
<td>dsrpc</td>
<td>dsrpcd.exe</td>
</tr>
<tr>
<td>ASB Agent</td>
<td>ASBAgent</td>
<td>ASBAgent.exe</td>
</tr>
</tbody>
</table>


Table 23. Services to stop, in the order in which they must be stopped (continued)

<table>
<thead>
<tr>
<th>Service full name</th>
<th>Service short name</th>
<th>Process name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Agent</td>
<td>LoggingAgent</td>
<td>LoggingAgent.exe</td>
</tr>
</tbody>
</table>

2. Stop WebSphere Application Server.

**Stopping IBM WebSphere Application Server (Windows)**

Follow this procedure to shut down WebSphere Application Server services in a Microsoft Windows installation.

**Procedure**

Do either of the following tasks, depending on whether you have a stand-alone or clustered configuration:

**Stopping a stand-alone WebSphere Application Server configuration:**

1. On the computer that hosts the services tier, log in as a user that has local administrator privileges.

2. On the Windows desktop, click **All Programs > IBM WebSphere > Application Server > Profiles > InfoSphere > Stop the server.**
   
   *InfoSphere* is the profile name where InfoSphere Information Server is installed.

3. When prompted, enter a user name and password for an account that has WebSphere Application Server administrator privileges.

4. Verify that WebSphere Application Server processes have stopped. See "Checking the status of IBM WebSphere Application Server (stand-alone installation)" on page 241.

**Stopping a clustered WebSphere Application Server configuration:**

1. Start the WebSphere Application Server administrative console.

2. In the console navigation tree, click **Servers > Clusters.** The Server Cluster page appears.

   **Note:** Depending on the WebSphere Application Server version, you might have to click **Servers > Clusters > WebSphere Application Server clusters** to access the Server Cluster page.

3. Select the cluster.

4. Click **Stop.** This command allows each application server to finish existing requests and allows failover to another member of the cluster. When the stop operation begins, the cluster status changes to *partially stopped.* After all application servers stop, the cluster status becomes *Stopped.*

5. On each node, log in as a user with local administrator privileges.

6. On the node, run the **stopNode** command to stop the node agent:

   ```
   C:\IBM\WebSphere\AppServer\profiles\Custom01\bin\stopNode -user wasadmin -password password
   ```

   In the command, *Custom01* is the WebSphere Application Server custom profile that hosts a node of the IBM InfoSphere Information Server cluster. *wasadmin* and *password* are the WebSphere Application Server administrator user name and password.

   Control returns to the command line after the node agent shuts down.
Note: If the node agent runs as a Windows service, the `stopNode` command stops the associated Windows service and the node agent.

7. Verify that all cluster members and node agents are stopped. See "Checking the status of IBM WebSphere Application Server cluster members" on page 244 and "Checking the status of IBM WebSphere Application Server node agents" on page 244.

8. Stop the Network Deployment manager process. See "Stopping the IBM WebSphere Application Server Deployment Manager (Windows)."

Stopping the IBM WebSphere Application Server Deployment Manager (Windows)

Follow this procedure to stop the IBM WebSphere Application Server Network Deployment Deployment Manager in a Microsoft Windows installation with WebSphere Application Server clustering.

Procedure

1. On the node that hosts the Deployment Manager, log in as a user with local administrator privileges.

2. On the node, run the `stopManager` command to stop the Network Deployment manager process:

```
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\stopManager
-user wasadmin -password password
```

`Dmgr01` is the WebSphere Application Server Deployment Manager profile. `wasadmin` and `password` are the WebSphere Application Server administrator user name and password.

Note: If the Deployment Manager is running as a Windows service, the `stopManager` command stops the associated Windows service and also stops the Deployment Manager.

3. Verify that the Deployment Manager has stopped by using the WebSphere Application Server `serverStatus` command-line tool.

For more information, see the `serverStatus` documentation:


Shutting down services (Linux, UNIX)

Follow this procedure to shut down the IBM InfoSphere Information Server services and IBM WebSphere Application Server services in a Linux or UNIX installation. Shut down services before you back up or restore your system, or do other maintenance tasks.

Before you begin

If your metadata repository tier is set up in a clustered configuration, make sure that the databases are shut down last, if you shut them down at all.

Note: To perform a cold backup, you must shut down the databases.
**About this task**

The paths shown in this task assume that WebSphere Application Server and InfoSphere Information Server are installed in the default locations. Your paths and profile names are different if you installed these products in different locations.

**Procedure**

1. Stop the following services: Metadata Server services, ASB Agent, Logging Agent, and DSRPC Server.
   a. Log in to each computer that hosts an engine tier. Use the following credentials:
      - If you have configured the InfoSphere Information Server agents for non-root administration, and the services were started and are currently running under this non-root user, use the credentials for the administrator user that you previously configured.
      - If you have not configured the agents in this manner, log in as root.
   b. Run the following command to source the dsenv file:
      `. /opt/IBM/InformationServer/Server/DSEngine/dsenv`
   c. Make sure that the `.dshome` file contains the current engine location. UNIX systems support multiple instances of InfoSphere DataStage.
   d. Run the following commands to stop the InfoSphere DataStage services. The `bin/uv -admin -stop` command stops the instance of InfoSphere DataStage that is in the `.dshome` file.
      `cd /opt/IBM/InformationServer/Server/DSEngine
      bin/uv -admin -stop`
   e. Run the following commands to stop the agents:
      `cd /opt/IBM/InformationServer/ASBNode/bin
      ./NodeAgents.sh stop`
   f. Run the `top` command to verify that the processes have stopped.

2. Stop WebSphere Application Server.

**Stopping IBM WebSphere Application Server (Linux, UNIX)**

Follow this procedure to shut down WebSphere Application Server services in a Linux or UNIX installation.

**Procedure**

Do either of the following tasks, depending on whether you have a stand-alone or clustered configuration:

**Stopping a stand-alone WebSphere Application Server configuration:**

1. Log in to the computer that hosts the services tier. Use the following credentials:
   - If you have configured WebSphere Application Server for non-root administration, use the credentials for the non-root user that is configured to administer WebSphere Application Server.
   - If you have not configured WebSphere Application Server in this manner, log in as root.
2. Run the following commands:
   `cd /opt/IBM/InformationServer/ASBServer/bin
   ./MetadataServer.sh stop`
3. Verify that WebSphere Application Server processes have stopped. See “Checking the status of IBM WebSphere Application Server (stand-alone installation)” on page 241.

Stopping a clustered WebSphere Application Server configuration:

1. Log in to the node that hosts the Deployment Manager. Use the WebSphere Application Server administrator credentials.
2. In the console navigation tree, click Servers > Clusters to access the Server Cluster page.

   **Note:** Depending on your WebSphere Application Server version, you might have to click Servers > Clusters > WebSphere Application Server clusters to access the Server Cluster page.
3. Select the cluster.
4. Click Stop. This command allows each application server to finish existing requests and allows failover to another member of the cluster. When the stop operation begins, the cluster status changes to **partially stopped**. After all application servers stop, the cluster status becomes **Stopped**.
5. On each node, log in by using WebSphere Application Server administrator credentials.
6. On the node, run the **stopNode** command to stop the node agent. Specify the correct profile:

   ```
   /opt/IBM/WebSphere/AppServer/profiles/Custom01/bin/stopNode.sh
   -user wasadmin -password mypassword
   ```

   *Custom01* is the WebSphere Application Server custom profile that hosts a node of the IBM InfoSphere Information Server cluster. *wasadmin* is the user name of the WebSphere Application Server administrator. *password* is the password.
7. Verify that all cluster members and node agents are stopped. See “Checking the status of IBM WebSphere Application Server cluster members” on page 244 and “Checking the status of IBM WebSphere Application Server node agents” on page 244.
8. Stop the Deployment Manager. See “Stopping the IBM WebSphere Application Server Deployment Manager (Linux, UNIX).”

### Stopping the IBM WebSphere Application Server Deployment Manager (Linux, UNIX)

Follow this procedure to stop the WebSphere Application Server Deployment Manager in a Linux or UNIX installation with WebSphere Application Server clustering.

**Procedure**

1. Log in to the node that hosts the Deployment Manager by using WebSphere Application Server administrator credentials.
2. On the node, run the **stopManager** command to stop the Deployment Manager process:

   ```
   /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin/stopManager.sh -user wasadmin -password password
   ```

   In the command, *Dmgr01* is the WebSphere Application Server Deployment Manager profile. *wasadmin* is the user name of the WebSphere Application Server administrator. *password* is the password.
Control returns to the command line after the Deployment Manager process shuts down.

3. Verify that the Deployment Manager has stopped.

To verify that the processes have stopped, run the WebSphere Application Server `serverStatus.sh` command. For more information, see the `serverStatus.sh` documentation:


### Starting services (Windows)

Follow this procedure to start the IBM InfoSphere Information Server services and IBM WebSphere Application Server services in a Microsoft Windows installation.

**Before you begin**

Make sure that the database is operational before you do this procedure.

**About this task**

The paths in this task assume that WebSphere Application Server and InfoSphere Information Server are installed in the default location. Your paths and profile names are different if you installed these products in a different location.

**Procedure**

1. Start WebSphere Application Server. See "Starting IBM WebSphere Application Server (Windows)."

2. When WebSphere Application Server is fully started, log in to each computer that hosts an engine tier.

3. On each computer, start the following services: Logging Agent, ASB Agent, DSRPC Service, IBM InfoSphere DataStage Telnet Service, and InfoSphere DataStage Engine Resource Service. You can use the Services Administrative Tool or the `sc` command-line tool to start the services.

Start these services in the order shown in the following table.

<table>
<thead>
<tr>
<th>Service full name</th>
<th>Service short name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Agent</td>
<td>LoggingAgent</td>
</tr>
<tr>
<td>ASB Agent</td>
<td>ASBAgent</td>
</tr>
<tr>
<td>DSRPC Service</td>
<td>dsrpc</td>
</tr>
<tr>
<td>IBM InfoSphere DataStage Telnet Service</td>
<td>dstelnet</td>
</tr>
<tr>
<td>InfoSphere DataStage Engine Resource Service</td>
<td>DSEngine</td>
</tr>
</tbody>
</table>

### Starting IBM WebSphere Application Server (Windows)

Follow this procedure to start the IBM WebSphere Application Server services in a Microsoft Windows installation.
Procedure

Do either of the following tasks, depending on whether you have a stand-alone or clustered configuration:

Starting a stand-alone WebSphere Application Server configuration:

1. On the computer that hosts the services tier, log in as a user with local administrator privileges.
2. On the Windows desktop, click All Programs > IBM WebSphere > Application Server > Profiles > InfoSphere > Start the server. *InfoSphere* is the profile name where InfoSphere Information Server is installed.
3. Even though the status might show as Started within the IBM InfoSphere Information Server Web console, it might still not be available for use by InfoSphere Information Server until the InfoSphere Information Server applications are fully initialized. To verify that WebSphere Application Server has started, monitor the log files. See “Checking the status of IBM WebSphere Application Server startup (stand-alone installation)” on page 242.

Starting a clustered WebSphere Application Server configuration:

1. Start the Deployment Manager. See “Starting the IBM WebSphere Application Server Deployment Manager (Windows).”
2. On each node, run the startNode command to start the node agent:
   ```
   C:\IBM\WebSphere\AppServer\profiles\Custom01\bin\startNode
   ```
   where Custom01 is the WebSphere Application Server custom profile that hosts a node of the IBM InfoSphere Information Server cluster.
3. Start the WebSphere Application Server administrative console.
4. In the console navigation tree, click Servers > Clusters to access the Server Cluster page.
   
   **Note:** Depending on the WebSphere Application Server version, you might have to click Servers > Clusters > WebSphere Application Server clusters to access the Server Cluster page.
5. Select the cluster.
6. Click Start. This command starts the server process of each member of the cluster by calling the node agent for each server to start the application servers. After all application servers are running, the state of the cluster changes to running. If the call to a node agent for an application server fails, the application server does not start.
7. Even though the status returned by the serverStatus command indicates STARTED, it might still not be available for use by InfoSphere Information Server until the InfoSphere Information Server applications are fully initialized. To verify that WebSphere Application Server has started, monitor the log files. See "Checking the status of IBM WebSphere Application Server startup (clustered installation)" on page 243.

Starting the IBM WebSphere Application Server Deployment Manager (Windows)

Follow this procedure to start the IBM WebSphere Application Server Deployment Manager in a Microsoft Windows installation with WebSphere Application Server clustering.
Procedure

1. On the node that hosts the Deployment Manager, log in as a user with local administrator privileges.

2. On the node that hosts the Deployment Manager, run the `startManager` command to start the Network Deployment manager process:
   
   ```
   C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\startManager
   ```

   where `Dmgr01` is the WebSphere Application Server Deployment Manager profile.

   If the Deployment Manager runs as a Windows service, the `startManager` command starts the associated Windows service and the Deployment Manager.

---

Starting services (Linux, UNIX)

Follow this procedure to start the IBM InfoSphere Information Server services and IBM WebSphere Application Server services in a Linux or UNIX installation.

**Before you begin**

Make sure that the database is operational before you do this procedure.

The paths in this task assume that WebSphere Application Server and InfoSphere Information Server are installed in the default location. Your paths are different if you installed these products in a different location.

**Procedure**

1. **Start WebSphere Application Server.** See "Starting IBM WebSphere Application Server (Linux, UNIX)" on page 238.

2. On each computer, start the following services: ASB Agent, Logging Agent, and DataStage Service.
   
   a. Wait until WebSphere Application Server is fully started.
   
   b. Log in to each computer that hosts an engine tier. Use the following credentials:
      
      • If you configured the InfoSphere Information Server agents for non-root administration, use the credentials for the administrator user that you selected.
      
      • If you did not configure the agents in this manner, log in as root.
   
   c. Run the following command as the InfoSphere DataStage administrator (dsadm by default) to source the dsenv file:
      
      ```
      su - dsadm
      . /opt/IBM/InformationServer/Server/DSEngine/dsenv
      ```
   
   d. Make sure that the `.dshome` file contains the current engine location. UNIX systems support multiple instances of InfoSphere DataStage. The `bin/uv -admin -start` command starts the instance of InfoSphere DataStage that is in the `.dshome` file.
   
   e. As the InfoSphere DataStage administrator user, run the following commands to start the InfoSphere DataStage services. Then, exit the su session for the InfoSphere DataStage administrator:
      
      ```
      cd /opt/IBM/InformationServer/Server/DSEngine
      ./bin/uv -admin -start
      ```
   
   f. Run the following commands to start the ASB Agent and the Logging Agent:
Starting IBM WebSphere Application Server (Linux, UNIX)

Follow this procedure to start the IBM WebSphere Application Server services in a Linux or UNIX installation.

Before you begin

For cluster environments:

- **Linux** If you did not configure file descriptor resources for WebSphere Application Server before you installed IBM InfoSphere Information Server, make sure that WebSphere Application Server is stopped and configure your managed nodes as described in "Configuring file descriptor resources for IBM WebSphere Application Server (Linux)" on page 240.

- **AIX** If you did not unset the LDR_CNTRL variable before you installed IBM InfoSphere Information Server, make sure that WebSphere Application Server is stopped and configure your cluster computers as described in "Configuring memory allocation for IBM WebSphere Application Server (AIX)" on page 241.

For stand-alone environments, these settings are automatically configured by the MetadataServer script.

Procedure

Do either of the following tasks, depending upon whether you have a stand-alone or clustered configuration:

**Starting a stand-alone WebSphere Application Server configuration:**

1. Log in to the computer that hosts the services tier. Use the following credentials:
   - If you configured WebSphere Application Server for non-root administration, use the credentials for the non-root user that is configured to administer WebSphere Application Server.
   - If you did not configure WebSphere Application Server in this manner, log in as root.

2. Run the following commands:
   ```
   cd /opt/IBM/InformationServer/ASBServer/bin
   ./MetadataServer.sh run
   ```

   **Note:** The `run` argument echoes all output to the console.

Alternatively, if you want to embed this script in another script, use the `MetadataServer.sh start` command to launch the start process in the background:

```
cd /opt/IBM/InformationServer/ASBServer/bin
./MetadataServer.sh start
```
where wasadmin is the non-root user that is configured to administer WebSphere Application Server.

3. Even though the WebSphere Application Server status might show as Started within the IBM InfoSphere Information Server Web console, it might still not be available for use by InfoSphere Information Server until the InfoSphere Information Server applications are fully initialized. To verify that WebSphere Application Server has started, monitor the log files. See “Checking the status of IBM WebSphere Application Server startup (stand-alone installation)” on page 242.

Starting a cluster WebSphere Application Server configuration:

1. Start the Deployment Manager. See “Starting the IBM WebSphere Application Server Deployment Manager (Linux, UNIX).”

2. Log in to each node. Use the same credentials that you used to log in to the Deployment Manager node.

3. On each node, run the startNode command to start the node agent:
   
   /opt/IBM/WebSphere/AppServer/profiles/Custom01/bin/startNode.sh
   
   where Custom01 is the WebSphere Application Server custom profile that hosts a node of the IBM InfoSphere Information Server cluster. Control returns to the command line when the node agent startup is complete.

4. Log in to the WebSphere Application Server administrative console.

5. In the console navigation tree, click Servers > Clusters. The Server Cluster page appears.

   Note: Depending upon your WebSphere Application Server version, you might need to click Servers > Clusters > WebSphere Application Server clusters to access the Server Cluster page.

6. Select the cluster.

7. Click Start. This command starts the server process of each member of the cluster. To do so, it calls the node agent for each server to start the application servers. After all application servers are running, the state of the cluster changes to running. If the call to a node agent for an application server fails, the application server does not start.

8. Even though the status returned by the serverStatus command indicates STARTED, it might still not be available for use by InfoSphere Information Server until the InfoSphere Information Server applications are fully initialized. To verify that WebSphere Application Server has started, monitor the log files. See “Checking the status of IBM WebSphere Application Server startup (clustered installation)” on page 243.

Starting the IBM WebSphere Application Server Deployment Manager (Linux, UNIX)

Follow this procedure to start the IBM WebSphere Application Server Deployment Manager in a Linux or UNIX installation with WebSphere Application Server clustering.

Procedure

1. Log in to the node that hosts the Deployment Manager. Use the following credentials:
- If you have configured WebSphere Application Server for non-root administration, use the credentials for the non-root user that is configured to administer WebSphere Application Server.
- If you have not configured WebSphere Application Server in this manner, log in as root.

2. On the node, run the `startManager` command to start the Network Deployment manager process:

```
/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin/startManager.sh
```

where `Dmgr01` is the WebSphere Application Server Deployment Manager profile.

### Configuring file descriptor resources for IBM WebSphere Application Server (Linux)

On Linux, the default setting for the maximum number of file descriptors allowed is not sufficient to run WebSphere Application Server. You must configure the file descriptor resources for WebSphere Application Server to run correctly.

**About this task**

If your installation includes a stand-alone instance of WebSphere Application Server, configure the file descriptor resources on the computer on which WebSphere Application Server is installed. For cluster environments, you must configure the file descriptor resources on each computer where WebSphere Application Server is installed (Deployment Manager and managed nodes). The resources can be permanently configured if appropriate for your environment.

**Procedure**

1. Make sure all WebSphere Application Server processes are stopped. See "Stopping IBM WebSphere Application Server (Linux, UNIX)" on page 233.
2. Configure the computer to support a large number of file descriptors. Refer to your system administrator if you are unsure about this process.
   The following example shows how to set the number of file descriptors to 10240 if your login shell is `/bin/bash`. WebSphere Application Server requires a value over 10000 to run properly.
   - To apply the settings to the entire system, add the following to the `/etc/profile` file:
     ```
     ulimit -n 10240
     ```
   - To set the soft and hard limits for all users, add the following to the `/etc/security/limits.conf` file:
     ```
     * soft nofile 10240
     * hard nofile 10240
     ```

   If you do not want to permanently configure these values as shown in the example, you can instead run the `ulimit -n` command just before you start a WebSphere Application Server process. All WebSphere Application Server processes must be stopped before you run these commands.

3. Start all WebSphere Application Server processes. See "Starting IBM WebSphere Application Server (Linux, UNIX)" on page 238.

4. In a cluster environment, repeat this procedure on all systems where WebSphere Application Server is installed.
Configuring memory allocation for IBM WebSphere Application Server (AIX)

On AIX, the LDR_CNTRL environment variable controls the way AIX handles the memory space available to programs and the page sizes used in each segment. To provide sufficient memory allocation for WebSphere Application Server, you must unset this environment variable for WebSphere Application Server to run correctly.

About this task

If your installation includes a stand-alone instance of WebSphere Application Server, unset the LDR_CNTRL environment variable on the computer on which WebSphere Application Server is installed. For cluster environments, you must unset the LDR_CNTRL environment variable on each computer where WebSphere Application Server is installed (Deployment Manager and managed nodes). The change can be permanently configured if appropriate for your environment.

Procedure

To unset the LDR_CNTRL environment variable:

1. Make sure all WebSphere Application Server processes are stopped. See “Stopping IBM WebSphere Application Server (Linux, UNIX)” on page 233.
2. Configure the LDR_CNTRL environment variable. Refer to your system administrator if you are unsure about this process.
   The following example shows how to unset the LDR_CNTRL environment variable if your login shell is /bin/bash.
   • To apply the setting to all users on the system, add the following line to the /etc/profile file:
     unset LDR_CNTRL
   • To apply the setting to a specific user, add the line to the ~/.profile file for the user. The user to configure is typically root unless you reconfigured WebSphere Application Server for non-root administration.
     If you do not want to permanently configure the environment variable as shown in the example, you can run the unset LDR_CNTRL command just before you start a WebSphere Application Server process. All WebSphere Application Server processes must be stopped before you run these commands.
3. Start the WebSphere Application Server processes. See “Starting IBM WebSphere Application Server (Linux, UNIX)” on page 238.
4. In a clustered environment, repeat this procedure on all computers where WebSphere Application Server is installed.

IBM WebSphere Application Server process status checking

Follow these procedures to check the status of a WebSphere Application Server stand-alone installation, or of cluster members, node agents, and the Deployment Manager in a clustered installation.

Checking the status of IBM WebSphere Application Server (stand-alone installation)

In a WebSphere Application Server stand-alone installation, use the serverStatus command to check the status of the application server startup.
Procedure

For more information about the `serverStatus` command, see the WebSphere Application Server documentation.


What to do next

When an application server is starting up, even when the status returned by the `serverStatus` command indicates that the application server is STARTED, it is not ready for use by IBM InfoSphere Information Server until all InfoSphere Information Server applications have completed initialization. See “Checking the status of IBM WebSphere Application Server startup (stand-alone installation)” for more information.

Checking the status of IBM WebSphere Application Server startup (stand-alone installation)

Whenever you restart WebSphere Application Server, make sure that the application server is fully started before you take any further action. This procedure applies to a stand-alone installation of WebSphere Application Server.

About this task

Even though the status of an application server might show as STARTED, it might still not be available for use by IBM InfoSphere Information Server because the InfoSphere Information Server applications not yet fully initialized. The InfoSphere Information Server applications typically complete initialization within two to four minutes after the application server status first changes to STARTED.

If you started WebSphere Application Server by running `startServer` or `MetadataServer.sh run`, control returns when WebSphere Application Server has completed starting all applications but before InfoSphere Information Server has completed application initialization. Running `serverStatus` at this point shows a status of STARTED. However, initialization is not yet complete.

If you started WebSphere Application Server by running `MetadataServer.sh start`, control returns immediately before WebSphere Application Server starts any applications. After a delay, running `serverStatus` will show a status of STARTING. After a few minutes, running `serverStatus` will show a status of STARTED. This status indicates that WebSphere Application Server has completed starting all applications. However, it does not indicate that InfoSphere Information Server has completed application initialization.

Procedure

Follow this procedure to determine if the InfoSphere Information Server applications have completed initialization.

1. Log in to the services tier computer.
2. Locate the `SystemOut.log` file. The file is located in the following directory:
   
   `{WAS_install_path}/profiles/profile/logs/serverx`

   In the directory path:
Checking the status of IBM WebSphere Application Server startup (clustered installation)

Whenever you start a cluster member, make sure the application server associated with that cluster member is fully started before you take any further action. This procedure applies to a clustered installation of WebSphere Application Server.

About this task

Even though the status of a cluster member might show as Started within the IBM InfoSphere Information Server Web console, or the status returned by the `serverStatus` command indicates that the application server is STARTED, it might still not be available for use by InfoSphere Information Server until the InfoSphere Information Server applications are fully initialized. The InfoSphere Information Server applications typically complete initialization within two to four minutes after the application server status first changes to Started.

Procedure

Follow this procedure to determine if the InfoSphere Information Server applications have completed initialization.

1. Log in to each computer that hosts a cluster member.
2. On the computer, locate the `SystemOut.log` file. The file can be found in the following directory:
   
   ```
   WAS_install_path/profiles/profile/logs/serverx
   ```

   In the directory path:

   - `WAS_install_path` is the location where WebSphere Application Server is installed. The default installation path is:
     
     ```
     - UNIX/Linux /opt/IBM/WebSphere/AppServer
     - Windows C:\IBM\WebSphere\AppServer
     ```

   - `profile` is the profile name of the managed node in which InfoSphere Information Server is running. The default profile name is `Custom01`.

   The `SystemOut.log` file might contain log entries that span multiple application server restarts. For this reason, the file might contain multiple lines that read `EJB Initializations complete`. Use the timestamps of the log entries to determine if this message is associated with the application server startup that you want.
serverx is the name of the application server instance. The default value is serverx, where x is the number of one of the application server instances.

3. Check the SystemOut.log file in each server instance:
   a. In the SystemOut.log file, in the timeframe in which the application server is being started, look for the following line. This line indicates that InfoSphere Information Server is fully initialized and ready for operation:
      Initialization: EJB Initializations complete
      The SystemOut.log file might contain log entries that span multiple application server restarts. For this reason, the file might contain multiple lines that read EJB Initializations complete. Use the timestamps of the log entries to determine if this message is associated with the application server startup that you want.

4. Repeat this procedure for each computer that hosts a cluster member.

What to do next

InfoSphere Information Server can be used as soon as one cluster member is fully initialized. However, for best performance, wait until all members of the cluster are fully initialized. Allowing all the members of the cluster to initialize fully also maximizes the number of members that can take over in case of a failover.

Checking the status of IBM WebSphere Application Server cluster members

In a WebSphere Application Server cluster installation, use the WebSphere Application Server administrative console to check the status of cluster members.

Procedure
1. Log in to the WebSphere Application Server administrative console.
2. Access the cluster list in the console. In the navigation pane, expand Servers, expand Clusters, and click WebSphere application server clusters.
3. In the workspace, click the cluster name. The cluster page appears.
4. Click Cluster members. The Cluster members page appears. Each cluster member is listed on the page. The Status column indicates the status of each cluster member.

What to do next

When an application server is starting up, even when the status of the cluster member in the WebSphere Application Server administrative console shows as Started or when the status returned by the serverStatus command indicates that the application server is STARTED, it is not ready for use by IBM InfoSphere Information Server until all InfoSphere Information Server applications have completed initialization. See Checking the status of IBM WebSphere Application Server startup (clustered installation) for details on how to tell when InfoSphere Information Server applications have completed initialization.

Checking the status of IBM WebSphere Application Server node agents

In a WebSphere Application Server cluster installation, use the WebSphere Application Server administrative console to check the status of node agents.
Procedure
1. Log in to the WebSphere Application Server administrative console.
2. In the navigation pane, expand System administration and click Node agents.
The Node agents page appears. Each node agent is listed on the page. The Status column indicates the status of each node agent.

Checking the status of the IBM WebSphere Application Server Deployment Manager
In a WebSphere Application Server cluster installation, use the serverStatus command to check the status of the deployment manager.

Procedure
Run the serverStatus command. The command is located on the computer on which the Deployment Manager runs, in the following directory:

\WAS_install_path\profiles\profile\bin

In the directory path:
- WAS_install_path is the location where WebSphere Application Server is installed. The default installation path is:
  - UNIX /opt/IBM/WebSphere/AppServer
  - Windows C:\IBM\WebSphere\AppServer
- profile is the name of the Deployment Manager profile.

For more information about the serverStatus command, see the WebSphere Application Server documentation.

IBM WebSphere Application Server system log files
The WebSphere Application Server log files contain information that allows you to monitor WebSphere Application Server startup and diagnose errors.

The log files that are most useful for diagnosing IBM InfoSphere Information Server-related issues are:

SystemOut.log
WebSphere Application Server messages to STDOUT are redirected to this file.

SystemErr.log
WebSphere Application Server messages to STDERR are redirected to this file.

These files are located in the following directories on each node in your WebSphere Application Server installation:

- Linux
  \path\profiles\profile\logs\server1
- Windows
  \path\profiles\profile\logs\server1
In the directory path:

- **path** is the WebSphere Application Server installation path. By default, path is one of the following paths:
  - **Linux**
    ```
    /opt/IBM/WebSphere/AppServer
    ```
  - **Windows**
    ```
    C:\IBM\WebSphere\AppServer
    ```
- **profile** is the profile name where IBM InfoSphere Information Server is installed. For a stand-alone installation, the default value is *InfoSphere*. For a clustered installation, the default value for a custom profile is *Custom\&x\#. For a Deployment Manager profile, the default value is *dmgr*. For a node agent under the custom profile, the default value is *nodeagent*.

- **server1** is the name of the application server. For a stand-alone installation, the default value is *server1*. For cluster installations, there might be multiple application server directories under the custom profile. The typical value is *server\&x\#, where \( x \) is the number of the application server instance. For a Deployment Manager profile, the default value is *dmgr*. For a node agent under the custom profile, the default value is *nodeagent*.

For more information about WebSphere Application Server log files, see the WebSphere Application Server documentation:

- IBM WebSphere Application Server Network Deployment 8.5:
  ```
  ```
- IBM WebSphere Application Server Network Deployment 8.0:
  ```
  ```
Chapter 15. Managing assets by using the command line

You can use the command line to move assets between different metadata repositories for environments such as development, test, and production. You can also query and delete common metadata assets and generate glossary assets from BI assets and logical data models.

Using the istool command line

You can use the command line to import and export assets and to perform other tasks.

Location of the istool command line

The istool command line is available on the client and engine tiers.

For Windows, the istool command framework is located in: 
`installation_directory\Clients\istools\cli`, where `installation_directory` is the directory where you installed IBM InfoSphere Information Server. For example, `c:\IBM\InformationServer`.

For UNIX or Linux, the istool command framework is located in: 
`installation_directory/Clients/istools/cli`, where `installation_directory` is the directory where you installed InfoSphere Information Server. For example, `/opt/IBM/InformationServer`.

The istool framework is installed on all client and engine tier computers. The framework installation provides the ability to run commands and options for the following tools and components:

- IBM InfoSphere DataStage and QualityStage
- Common metadata assets
- Reporting assets
- Security assets

Command options for each of the following tools are installed with the framework only when the tool is installed:

- IBM InfoSphere Data Quality Console – client and engine
- IBM InfoSphere Information Analyzer – client and engine
- IBM InfoSphere Metadata Workbench – client and engine
- IBM InfoSphere Business Glossary – client only
- IBM InfoSphere FastTrack – client only
- IBM InfoSphere Streams – client only

This means, for example, that to move InfoSphere DataStage and QualityStage assets, you can run the build package, deploy package, and send package commands, and the -datastage options from any computer on the client or engine tier. To move InfoSphere FastTrack assets, you must run the istool command line from the client computer where InfoSphere FastTrack is installed.
Commands and common parameters for istool

You can use the istool commands to manage assets that are stored in the metadata repository of IBM InfoSphere Information Server.

For Windows, the istool command framework is located in:
installation_directory\Clients\istools\cli, where installation_directory is the directory where you installed InfoSphere Information Server. For example, c:\IBM\InformationServer.

For UNIX or Linux, the istool command framework is located in:
installation_directory/Clients/istools/cli, where installation_directory is the directory where you installed InfoSphere Information Server. For example, /opt/IBM/InformationServer.

The basic syntax of the istool command is:
istool command authentication_parameters [generic_parameters] [command_parameters]

When you run an istool command, details are written to a log file:
- On Windows computers, the log file is located in C:\Documents and Settings\user_name\istool_workspace\.metadata\.log.
- On UNIX or Linux computers the log file is located in user_home/user_name/istool_workspace/.metadata/.log.

The commands are given in the following table.

Table 25. istool commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>istool export</td>
<td>Export assets to a file.</td>
</tr>
<tr>
<td>istool import</td>
<td>Import assets from a file.</td>
</tr>
<tr>
<td>istool glossary export</td>
<td>Export assets from IBM InfoSphere Business Glossary to a file.</td>
</tr>
<tr>
<td>istool glossary import</td>
<td>Import glossary assets from a file.</td>
</tr>
<tr>
<td>istool build package</td>
<td>Build a package of IBM InfoSphere DataStage and QualityStage assets to be deployed.</td>
</tr>
<tr>
<td>istool deploy package</td>
<td>Deploy a package.</td>
</tr>
<tr>
<td>istool send package</td>
<td>Send a package to the local client computer.</td>
</tr>
<tr>
<td>istool query</td>
<td>Query common metadata (implemented data resources, logical and physical data models, and business intelligence assets) and write the results to a file.</td>
</tr>
<tr>
<td>istool deletecm</td>
<td>Delete common metadata.</td>
</tr>
<tr>
<td>istool delete</td>
<td>Delete InfoSphere DataStage and QualityStage assets.</td>
</tr>
</tbody>
</table>

Use the authentication parameters to specify the InfoSphere Information Server services tier to connect to. The authentication parameters are mandatory for all istool commands, and are in the following table.
Table 26. Authentication parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| -domain or -dom | String[:Number]  | <domain[:port]> | Depends on the configuration of IBM WebSphere Application Server:  
  - If clustering is set up, the name or IP address and the port of the front-end dispatcher (either the web server or the load balancer). Do not use the host name and port of a particular cluster member.  
  - If clustering is not set up, the host name or IP address of the computer where WebSphere Application Server is installed and the port number that is assigned to the IBM InfoSphere Information Server Web console, by default 9080.  
  If you use an IPV6 address, you must enclose it in square brackets ([ ]). For example, istool export -domain [2002:920::2002:217:9:32:217:32]:9080 -username user1 -password pass1 -archive "c:\arc.isx" -datastage "serv2/Proj/Jobs/Mine/ajobj.pjb" |
| -username or -u | String            | <user name>     | Name of the user account on the services tier |
| -password or -p | String            | <password>      | Password for the account that is specified in the -username option. (Optional after the first login). |
| -authfile or -af | String            | <path to credentials file> | The path to a file that contains encrypted credentials for logging on to InfoSphere Information Server. If you use -authfile you do not need to specify -username or -password on the command line. If you specify both the -authfile option and the explicit user name and password options, the explicit options take precedence. For more information see the topic Encrypt command. |

The generic parameters in the following table are optional parameters that can be used with all istool commands.

Table 27. Generic parameters

<table>
<thead>
<tr>
<th>Option long name</th>
<th>Option short name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-help</td>
<td>-h</td>
<td>Prints the list of command options. To view help for a specific command, enter istool command -help.</td>
</tr>
<tr>
<td>-verbose</td>
<td>-v</td>
<td>Prints detailed information throughout the operation.</td>
</tr>
<tr>
<td>-silent</td>
<td>-s</td>
<td>Silences non-error command output.</td>
</tr>
</tbody>
</table>
The following table lists parameters that are common to the istool import or export commands for most tools and asset types.

**Table 28. Common parameters for the istool import and istool export commands**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Argument</th>
<th>Description</th>
<th>Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>-preview or -pre</td>
<td>Boolean</td>
<td>N/A</td>
<td>Optional. Used with istool import and istool export.</td>
<td>Not supported with glossary export or glossary import commands.</td>
</tr>
<tr>
<td>-replace</td>
<td>N/A</td>
<td>N/A</td>
<td>Required only for security and reporting imports, otherwise optional.</td>
<td>Not supported for glossary import command. Use -mergemethod for glossary imports. Some tools have additional options for replacing assets. The -replace option for the istool send package command has different functionality.</td>
</tr>
<tr>
<td>-archive or -ar</td>
<td>string</td>
<td>&lt;archive name&gt;</td>
<td>Require. Used with istool import and istool export.</td>
<td>Not supported for glossary import and export commands.</td>
</tr>
</tbody>
</table>
Table 28. Common parameters for the istool import and istool export commands (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Argument</th>
<th>Description</th>
<th>Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>-updatearchive or -up</td>
<td>Boolean</td>
<td>N/A</td>
<td>Optional. Used with istool export. Updates the specified archive file by adding new assets or overwriting changed assets. No assets in the archive file are deleted.</td>
<td>Not supported for glossary export command.</td>
</tr>
<tr>
<td>-abortIferror or -abort</td>
<td>Integer/number</td>
<td>&lt;number of errors&gt;</td>
<td>Optional. Used with istool export. Terminate the export after the specified number of errors.</td>
<td>Not supported for glossary export command.</td>
</tr>
<tr>
<td>-abortAfter or -abort</td>
<td>Integer/number</td>
<td>&lt;number of errors&gt;</td>
<td>Optional. Used with istool import. Terminate the import after the specified number of errors.</td>
<td>Not supported for glossary import command.</td>
</tr>
</tbody>
</table>

Command modes for istool

You can use the istool commands in different modes: command line, console, or script.

The istool commands can be invoked in any of the following modes:

Command mode (in a command prompt)

In the command mode, enter commands one at a time on a command line. Start each command with istool followed by a command, then the parameters. You must surround parameter values that contain embedded spaces with double quotation mark characters (").

Console mode (in a command prompt)

Enter istool on a command line with no parameters to enter console mode.

In console mode, istool prints a command prompt and waits for a command. Each command is processed without exiting istool. You must enter authentication details for every command. You can exit the console mode by entering a period character (.), exit, or quit at the prompt.

The istool command framework in console mode also has a history feature, which recalls the last 30 commands entered. You can recall and execute each command. To view the most recent commands, enter history. To repeat a command, enter !command_number, for example, !2.

Script mode

The istool command can be used to execute commands read directly from a text file. The file is read and executed as a series of command lines.
In script mode, each line in the input file must be formatted the same as a command line entered manually, except for the following stipulations.

- You do not need to include the `istool` string on each command line.
- Multiple commands are separated by a semicolon character (`;`) at the end of an input line.
- Command lines can cross line boundaries.

Command syntax:

```
istool -script filename
```

---

**Asset interchange**

You can use the command line to move assets between the metadata repositories of different installations of InfoSphere Information Server. For example, you can move assets from a development environment to a test, production, or source control environment.

InfoSphere Information Server is a suite of components that together provide a single unified platform that enables companies to understand, cleanse, transform, and deliver information.

Each of the components has a set of assets that are stored in the shared metadata repository. A single asset might be used by more than one of the suite components. For example, security assets are the users defined in the suite and given access to suite components. Asset interchange provides command-line interface commands that you can use to write these assets to an archive. You can then back up the archive to preserve your InfoSphere Information Server assets, or you can move the archive to a different system and import the assets from the archive. You can also submit the archive file to a source code control system to provide version controlling of your assets.

You can use the asset interchange `istool` command-line interface to move individual assets, or large groups of assets. You can build the asset interchange commands into scripts to facilitate the routine back-up or movement of large groups of assets. The speed of the import or export process depends on the size of the project.

The following table lists the asset categories, and the individual assets they contain.

**Table 29. Assets that can be moved by using asset interchange**

<table>
<thead>
<tr>
<th>Asset category</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM InfoSphere Business Glossary</td>
<td>• Categories</td>
</tr>
<tr>
<td></td>
<td>• Terms</td>
</tr>
<tr>
<td>IBM InfoSphere FastTrack</td>
<td>• Mapping components</td>
</tr>
<tr>
<td></td>
<td>• Mapping compositions</td>
</tr>
<tr>
<td></td>
<td>• Mapping specifications</td>
</tr>
<tr>
<td></td>
<td>• Project templates</td>
</tr>
<tr>
<td></td>
<td>• Projects</td>
</tr>
<tr>
<td></td>
<td>• Role assignments, reports, common metadata, glossary assets, and IBM Information Server DataStage and QualityStage assets that are associated with a project</td>
</tr>
</tbody>
</table>
Table 29. Assets that can be moved by using asset interchange (continued)

<table>
<thead>
<tr>
<th>Asset category</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM InfoSphere Information Analyzer</td>
<td>• Projects, including the assets that are associated with them, such as analysis results, data rules, and data classes</td>
</tr>
<tr>
<td></td>
<td>• All data classes, regardless of which project they are associated with</td>
</tr>
<tr>
<td></td>
<td>• Reports and common metadata that are associated with a project</td>
</tr>
<tr>
<td>IBM InfoSphere DataStage and QualityStage</td>
<td>• Custom folders (external files in the project directory)</td>
</tr>
<tr>
<td></td>
<td>• Data connections</td>
</tr>
<tr>
<td></td>
<td>• Data elements</td>
</tr>
<tr>
<td></td>
<td>• Data quality specifications (lookup tables, rule sets, and match specifications)</td>
</tr>
<tr>
<td></td>
<td>• IMS databases</td>
</tr>
<tr>
<td></td>
<td>• IMS viewsets</td>
</tr>
<tr>
<td></td>
<td>• Jobs (mainframe, parallel, sequence, and server)</td>
</tr>
<tr>
<td></td>
<td>• Job executables</td>
</tr>
<tr>
<td></td>
<td>• Machine profiles</td>
</tr>
<tr>
<td></td>
<td>• Parameter sets</td>
</tr>
<tr>
<td></td>
<td>• Routines (mainframe, parallel, and server)</td>
</tr>
<tr>
<td></td>
<td>• Shared containers (parallel and server)</td>
</tr>
<tr>
<td></td>
<td>• Stage types</td>
</tr>
<tr>
<td></td>
<td>• Table definitions</td>
</tr>
<tr>
<td></td>
<td>• Transforms</td>
</tr>
<tr>
<td></td>
<td>• Shared tables and related common metadata assets that are associated with table definitions</td>
</tr>
<tr>
<td>IBM InfoSphere Data Quality Console</td>
<td>• Activity log settings</td>
</tr>
<tr>
<td></td>
<td>• Custom labels for the status and priority settings</td>
</tr>
<tr>
<td></td>
<td>• Exception descriptors, including associated exceptions and changes to the owner, priority, and status</td>
</tr>
<tr>
<td></td>
<td>• Project connections</td>
</tr>
<tr>
<td></td>
<td>• Saved sets of search criteria</td>
</tr>
<tr>
<td>Asset category</td>
<td>Assets</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Common metadata assets</td>
<td>Business intelligence (BI) assets:</td>
</tr>
<tr>
<td></td>
<td>• BI models</td>
</tr>
<tr>
<td></td>
<td>• BI collections</td>
</tr>
<tr>
<td></td>
<td>• Cubes</td>
</tr>
<tr>
<td></td>
<td>• BI reports</td>
</tr>
<tr>
<td></td>
<td>• BI report queries</td>
</tr>
<tr>
<td></td>
<td>• BI Report Section</td>
</tr>
<tr>
<td></td>
<td>• BI Folder</td>
</tr>
<tr>
<td></td>
<td>• BI Server</td>
</tr>
<tr>
<td></td>
<td>Implemented data resources:</td>
</tr>
<tr>
<td></td>
<td>• Host computers</td>
</tr>
<tr>
<td></td>
<td>• Databases</td>
</tr>
<tr>
<td></td>
<td>• Database schemas</td>
</tr>
<tr>
<td></td>
<td>• Database domain</td>
</tr>
<tr>
<td></td>
<td>• Database tables</td>
</tr>
<tr>
<td></td>
<td>• Stored procedures</td>
</tr>
<tr>
<td></td>
<td>• Data files</td>
</tr>
<tr>
<td></td>
<td>• Data file structures</td>
</tr>
<tr>
<td></td>
<td>• Data connections</td>
</tr>
<tr>
<td></td>
<td>• Data item definitions</td>
</tr>
<tr>
<td></td>
<td>Logical data model assets:</td>
</tr>
<tr>
<td></td>
<td>• Logical data models</td>
</tr>
<tr>
<td></td>
<td>• Logical entities</td>
</tr>
<tr>
<td></td>
<td>• Logical relationships</td>
</tr>
<tr>
<td></td>
<td>• Entity generalization hierarchies</td>
</tr>
<tr>
<td></td>
<td>• Logical domains</td>
</tr>
<tr>
<td></td>
<td>• Subject areas</td>
</tr>
<tr>
<td></td>
<td>• Diagrams</td>
</tr>
<tr>
<td></td>
<td>Physical data model assets:</td>
</tr>
<tr>
<td></td>
<td>• Physical data models</td>
</tr>
<tr>
<td></td>
<td>• Design tables</td>
</tr>
<tr>
<td></td>
<td>• Design stored procedures</td>
</tr>
<tr>
<td></td>
<td>• Physical domains</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous assets</td>
</tr>
<tr>
<td></td>
<td>• Custom attributes</td>
</tr>
<tr>
<td></td>
<td>• Contact libraries</td>
</tr>
<tr>
<td>Reporting assets</td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td>• Report results</td>
</tr>
<tr>
<td>Security assets</td>
<td>• Users, with or without roles, credentials, and credential mapping</td>
</tr>
<tr>
<td></td>
<td>• Groups, with or without roles</td>
</tr>
</tbody>
</table>
- You can use InfoSphere Information Server Manager to build deployment packages of assets and move these packages between InfoSphere Information Server systems, or submit the packages to a source code control system.
- You can use the InfoSphere Information Server Manager and the asset interchange commands in conjunction with one another by browsing a tree of InfoSphere DataStage and QualityStage assets in InfoSphere Information Server Manager, and selecting which assets to include in a package. You can then define a script of asset interchange commands that regularly rebuilds the specified package and deploys the package to a target system or project, ensuring that the target has an up-to-date version of those assets.

**Common asset-interchange scenarios**

You can use asset interchange to address scenarios that occur commonly with IBM InfoSphere Information Server.

**Moving projects from development to test**

In a typical InfoSphere Information Server environment, there is a dedicated development system. This system is used to prototype and perform rudimentary testing on your enterprise data solutions.

When initial development is complete, and your project is ready to test, you can use asset interchange to deploy the entire system to the test system by using the asset interchange commands in a script. It is likely that there will be some iteration between the test and development machines:

1. Faults are discovered on the test system.
2. Fixes made on the development system.
3. Results moved once more to the test system

You could define a script with the following commands:

- One command to export the required assets from the development system
- A second command to import the exported assets to the test system.

You can rerun this script each time fixes are made on the development system.

**Moving a subset of items**

While you iterate between development and test systems, you might find that you want to move just a subset of assets, rather than your entire project. In this case, you can use asset interchange commands directly on the command line and explicitly specify one or more assets to move. For example, if one InfoSphere DataStage job needs changing, you can change the job on the development system. You can then re-export the job and reimport the job on the test system.

**Moving projects from test to production**

After the test cycles are complete, the assets can be deployed to the production system, where the system processes real data. You can once again use the asset interchange commands to export the assets to an archive, and to import them to the production system.
InfoSphere Business Glossary assets

Use the business glossary command-line interface (CLI) to move business glossary assets between different IBM InfoSphere Information Server metadata repositories or to back up the assets. You can also use the command-line interface to convert business intelligence (BI) model elements, glossary model elements, or logical data model elements to business glossary terms and categories.

You must have the Business Glossary Administrator role.

You must run the istool glossary commands on a Microsoft Windows computer on the client tier where IBM InfoSphere Business Glossary is installed.

You can use the istool glossary export command to export assets to one of the following types of file:
- XML file
- XMI file (business glossary archive)
- CSV file

When you export to XML, XMI, or CSV, you can export all categories, or you can export specified top-level categories. If you are exporting to an XML or XMI file, you can export links to assets that are assigned to exported terms. If you are exporting to an XML or XMI file, you can optionally include stewardship links of exported categories and terms. (Stewardship links are always included in CSV files.)

You can use the istool glossary import command to import assets from one of the following types of file:
- XML file
- XMI file (business glossary archive)
- CSV file
- NDM file (glossary model) created by IBM InfoSphere Data Architect

You can use the istool glossary bi2bg command to convert BI model elements to business glossary terms and categories.

You can use the istool glossary ldm2bg command to convert logical model elements to business glossary terms and categories.

When the bi2bg or ldm2bg commands are used, the BI assets or logical data model assets must exist in the metadata repository. You can use IBM InfoSphere Metadata Asset Manager to import logical data models and BI models into the metadata repository.

Export command for business glossary assets

Use the istool glossary export command to export business glossary assets to a file.

Command syntax
istool glossary export
authentication parameters
[generic parameters]
[-format XML | XMI | CSV]
Command options

The following table shows the options that are specific to the istool glossary export command. For authentication parameters and generic parameters, see Commands and common parameters for istool.

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Value, if any</th>
<th>Description</th>
</tr>
</thead>
</table>
| -filename                  | -f         | pathname            | Specifies the file to export business glossary assets to. If the pathname contains space characters, you must enclose the pathname in double quote characters (").
| -format                    | -fm        | XML | XMI | CSV | Specifies the format of the exported file. By default the format is XML. |
| -allcategories             | -all       |                   | Specifies that all categories in the source business glossary are exported to the specified file. |
| -topcategories             | -top       | cat1, cat2, ... catN | Use this parameter to specify a comma-separated list of top-level categories that are exported. Category names can contain spaces. |
| -categories                | -cat       | cat1::cat2::cat3..., catN::...::catNN | Use this parameter to specify a comma-separated list of specific categories and subcategories. Specify the full path of the category you want to export, using :: as a separator between the parent category and subcategories. For example, Cat1::Cat2::Cat3, Cat7::Cat8, Cat10 exports all of the content in the categories Cat3, Cat8, and the root category Cat10. |
| -includeassignedassets     | -incasst   |                   | Specifies that links to assets assigned to exported terms are exported. By default this option is false. |
### Long name

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Value, if any</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-includestewardship</td>
<td>-incstwd</td>
<td></td>
<td>Specifies that stewardship links of exported categories and terms are included in the export. By default this option is false. (Export files in CSV format always contain stewardship links.)</td>
</tr>
<tr>
<td>-includepoliciesrules</td>
<td>-incpolrul</td>
<td></td>
<td>Specifies that policies and rules are exported. By default this option is false.</td>
</tr>
</tbody>
</table>

### Examples

The following command exports all the categories in the source business glossary to the file named exp_all.xml. Because no format is explicitly specified, the categories are exported in XML format:

```
istool glossary export –dom ABC:9080 –u xmetauser –p xmetapwd -filename "c:\exp_all.xml" -allcategories
```

The following command exports the named categories in the source business glossary to the CSV file named exp_sel.csv.

```
istool glossary export –dom ABC:9080 –u xmetauser –p xmetapwd -filename "c:\exp_sel.csv" -format CSV -topcategories "dept AB, dept XM, dept HR"
```

The following command exports the categories Account ID and Regions to the file exp_sel2.xml.

```
istool glossary export –dom ABC:9080 –u xmetauser –p xmetapwd -filename "c:\exp_sel2.xml" -categories "Customer::Accounts::Account ID, Customer::Regions"
```

### Import command for business glossary assets

Use the `istool glossary import` command to import your business glossary assets from a file of previously archived assets, or to import a glossary model (*.ndm) file from IBM InfoSphere Data Architect.

### Command syntax

You must have the Business Glossary Administrator role to import business glossary assets.

You must run the command from a computer on the client tier where IBM InfoSphere Business Glossary is installed.

```
istool glossary import authentication parameters [generic parameters] -filename PNAME [-format XML | XMI | CSV | NDM] [-mergemethod overwrite | ignore | mergeignore | mergeoverwrite] [-mappingfile PNAME]
```

### Command options

`authentication parameters`

Specifies connection details for a specific IBM InfoSphere Information Server.
generic parameters
Use the generic parameters to request help on command syntax, or specify silent or verbose operation.

-filename pathname or -f pathname
Specifies the file to import business glossary assets from. If the path name contains space characters, you must enclose the path name in double quotation marks (").

-format XML | XMI | CSV | NDM or -fm XML | XMI | CSV | NDM
Specifies the format of the import file. By default the format is XML.

XML, XML, and CSV files must contain business glossary content that adheres to the format required by InfoSphere Business Glossary. For more information about format, download the sample files available from the InfoSphere Business Glossary import and export wizard or see Importing and exporting glossary content.

Files imported with the NDM option must be glossary model files (*.ndm) that were created with or imported into IBM InfoSphere Data Architect. The glossaries and words in the glossary model file are converted into InfoSphere Business Glossary categories and terms according to the mapping described in "Generating business glossary content from InfoSphere Data Architect glossary models" on page 260.

-mergemethod overwrite | ignore | mergeignore | mergeoverwrite or -mrg overwrite | ignore | mergeignore | mergeoverwrite
Only applies when assets are imported from XML or XMI files. Specifies one of the following merge methods:

overwrite
Specify this option to overwrite assets that exist in the target repository with imported assets.

ignore This is the default option. Assets that exist in the target repository are not overwritten.

mergeignore
Specify this option to merge the asset and ignore imported attributes that cannot be merged.

mergeoverwrite
Specify this option to merge the asset and overwrite existing attributes that cannot be merged.

-mapping pathname or -map pathname
Applies only when assets are imported from XMI files. Specifies a mapping file to use to modify the imported assets. If the path name contains space characters, you must enclose the pathname in double quotation marks ("). A mapping file enables you to change attributes of exported business glossary content before you import it.

Examples
The following command imports all the business glossary assets contained in the CSV format file named bgexp.csv:

```bash
istool glossary import -dom ABC:9080 -u xmetauser -p xmetapwd
-filename c:\bgexp.csv -format CSV
```
The following command imports all the business glossary assets contained in the XML format file named bg.ximp.xml. If assets with the same name are encountered in the target repository, they are overwritten with the imported assets:

istool glossary import -dom ABC:9080 -u xmetauser -p xmetapwd -filename "c:\bg.ximp.xml" -format XML -mergemethod overwrite

The following command imports a glossary model created with InfoSphere Data Architect. It converts the glossary model elements in the file named NDMTest.ndm to InfoSphere Business Glossary categories and terms.

istool glossary import -dom ABC:9080 -u xmetauser -p xmetapwd -format ndm -f "C:\tmp\NDMTest.ndm"

### Generating business glossary content from other sources

You can generate business glossary content from other sources, such as logical data models, glossary models, and BI (business intelligence) models, by using variants of the istool glossary command.

### Generating business glossary content from InfoSphere Data Architect glossary models

By using the NDM option with the glossary import command, you can convert IBM InfoSphere Data Architect glossary models to IBM InfoSphere Business Glossary terms and categories.

The glossary model must be created or imported into one of the following versions of InfoSphere Data Architect: 7.5.2.1, 7.5.3.1, 7.6, or 8.1.

When you convert InfoSphere Data Architect glossaries or subglossaries to InfoSphere Business Glossary categories and terms, each glossary or subglossary becomes an InfoSphere Business Glossary category, and each contained word in an InfoSphere Data Architect glossary becomes a separate InfoSphere Business Glossary term.

The following table describes how each property is converted.

### Mappings to categories

<table>
<thead>
<tr>
<th>This property of an InfoSphere Data Architect glossary model glossary...</th>
<th>...becomes this property of an InfoSphere Business Glossary category</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>category name</td>
</tr>
<tr>
<td>parent</td>
<td>parent category</td>
</tr>
<tr>
<td>abstract</td>
<td>short description</td>
</tr>
<tr>
<td>documentation</td>
<td>long description</td>
</tr>
<tr>
<td>contained words</td>
<td>contained terms</td>
</tr>
<tr>
<td>referenced words</td>
<td>referenced terms</td>
</tr>
<tr>
<td>annotation</td>
<td>no property assigned</td>
</tr>
<tr>
<td>label</td>
<td>no property assigned</td>
</tr>
</tbody>
</table>
Mappings to terms

Table 31. Mappings from InfoSphere Data Architect words to InfoSphere Business Glossary terms

<table>
<thead>
<tr>
<th>This property of an InfoSphere Data Architect glossary model word...</th>
<th>...becomes this property of an InfoSphere Business Glossary term</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>term name</td>
</tr>
<tr>
<td>parent</td>
<td>parent category</td>
</tr>
<tr>
<td>abstract</td>
<td>short description</td>
</tr>
<tr>
<td>abbreviation</td>
<td>abbreviation</td>
</tr>
<tr>
<td>alternate abbreviation</td>
<td>alternate abbreviation</td>
</tr>
<tr>
<td>contained words</td>
<td>contained terms</td>
</tr>
<tr>
<td>modifier</td>
<td>is modifier</td>
</tr>
<tr>
<td>type PRIME</td>
<td>primary</td>
</tr>
<tr>
<td>type CLASS</td>
<td>secondary</td>
</tr>
<tr>
<td>type BUSINESS TERM</td>
<td>no property assigned</td>
</tr>
<tr>
<td>type NONE</td>
<td>no property assigned</td>
</tr>
<tr>
<td>status</td>
<td>status</td>
</tr>
<tr>
<td>related words</td>
<td>related terms</td>
</tr>
<tr>
<td>synonym</td>
<td>synonym</td>
</tr>
<tr>
<td>replaced by</td>
<td>replaced by</td>
</tr>
<tr>
<td>description</td>
<td>long description</td>
</tr>
<tr>
<td>annotation</td>
<td>no property assigned</td>
</tr>
<tr>
<td>documentation</td>
<td>no property assigned</td>
</tr>
<tr>
<td>label</td>
<td>no property assigned</td>
</tr>
</tbody>
</table>

Generating business glossary content from business intelligence models

You can generate categories and terms from business intelligence (BI) models by using the `glossary bi2bg` command. For example, you can generate categories and terms from an IBM Cognos® Framework Manager model or from a BusinessObjects Universe.

To generate categories and terms from a BI model, the model must have been previously imported into the metadata repository of IBM InfoSphere Information Server. You can import BI models into the metadata repository by using a bridge.

The `glossary bi2bg` command parses a BI model to create a hierarchy of categories and terms and then creates these categories and terms in InfoSphere Business Glossary. You can specify multiple BI models in a single `glossary bi2bg` command.

Note:

The business glossary content is created in the following way:

- For each model that is specified, a business glossary category is created for each token that is separated by a forward slash (/) in the namespace of the model. The top-level category that is created has the same name as the BI model.
For each BI collection contained in the BI model, a subcategory is created. Each such subcategory has the same name as the name of the BI collection.

For each BI collection member in the BI collection, a term is created. Each such term has the same name as the BI collection member, and is contained by the category that is created for the BI collection. Other properties of the term (all those properties besides its name and place in the business glossary hierarchy) are obtained from a configuration file. The BI collection member that corresponds to the created term can be assigned to the term by a specification in the configuration file.

For example, suppose you have the following BI model:

Namespace: /content/package[@name='SimpleReports'] contains the model MyModel. MyModel contains the BI collection Car and the collection contains the collection member Wheels. The following figure illustrates the results of using the bi2bg command:

![Diagram showing the relationship between BI model and glossary content]

Before you create terms and categories, you can also use the glossary bi2bg command to create a preview of the results. You specify the preview option in the configuration file. This preview is written to a file in CSV (comma-separated values) format or to the log file. The preview shows you what content will be created when you run the command a second time but without the preview option. After you have inspected the preview and are satisfied, run the command again to create categories and terms.

bi2bg command:

Use the istool glossary bi2bg command to generate categories and terms from business intelligence (BI) models.

Command syntax

```
istool glossary bi2bg
```

authentication parameters

```
[generic parameters]
-config-file | -cfg <pathname>
-log <pathname>
```
Command options

The following table shows the options that are specific to the `istool glossary bi2bg` command. For authentication parameters and generic parameters, see `Commands and common parameters for istool`.

Table 32. Command options for `istool glossary bi2bg`

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-config-file</td>
<td>-cfg</td>
<td>Specifies the directory path to the configuration file that defines how business glossary content is generated from a BI model. If the path contains space characters, enclose the path in double quotation marks (').</td>
</tr>
<tr>
<td>-log</td>
<td>none</td>
<td>Specifies the directory path where you want the log file to be placed. If the path contains space characters, enclose the path in double quotation marks (').</td>
</tr>
</tbody>
</table>

Configuration file

A configuration file defines additional command parameters. The file is a text file with the extension `.ini` that you create. It can contain the parameters shown in the following table. Each parameter name is a single string with no spaces.

Table 33. Configuration file command parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
<th>Valid values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ModelsToProcess</td>
<td>Specifies the names of the models to be processed. To process all models set to *</td>
<td>Comma-separated names of models.</td>
<td>*</td>
</tr>
<tr>
<td>MemberTypeRegular</td>
<td>When a term is created from BI collection members, a string that indicates the member type is listed in the Example attribute of the term. For BI collection members whose type is &quot;Regular,&quot; specifies the string to be displayed.</td>
<td>User-specified string.</td>
<td>Regular</td>
</tr>
<tr>
<td>MemberTypeMeasure</td>
<td>For BI collection members whose type is &quot;Measure,&quot; specifies the string to be displayed in the Example attribute of the corresponding term.</td>
<td>User-specified string.</td>
<td>Measure</td>
</tr>
<tr>
<td>ClassifyMemberTargetSource</td>
<td>If TRUE, BI collection members are assigned to the terms that are created from them.</td>
<td>TRUE/FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
<td>Valid values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>CategoriesToExclude</td>
<td>Specifies the categories to be excluded. You can choose not to create some of the parent categories that are generated from the namespace. If a category is excluded, its subcategories and terms are also excluded. The configuration file must include this parameter even if you do not specify a value for it.</td>
<td>Comma-separated names of categories. Use the full path of the category, starting from the top-level category. You can obtain the full path of the categories from the preview file.</td>
<td></td>
</tr>
<tr>
<td>MergeOption</td>
<td>Specifies the merge option to use when the categories and terms are imported.</td>
<td>MERGE_SOURCE_BIAS/ MERGE_TARGET_BIAS/ MERGE_SOURCE_BIAS/ MERGE_TARGET_BIAS</td>
<td>MERGE_TARGET_BIAS</td>
</tr>
<tr>
<td></td>
<td><strong>MERGE_TARGET_BIAS</strong></td>
<td>Merge the asset and ignore imported attributes that cannot be merged.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MERGE_SOURCE_BIAS</strong></td>
<td>Merge the asset and overwrite existing attributes that cannot be merged.</td>
<td></td>
</tr>
<tr>
<td>IsModifier</td>
<td>If TRUE, sets the value of the IsModifier attribute of all imported terms to &quot;Yes&quot;.</td>
<td>TRUE/FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the status attribute of all imported terms.</td>
<td>CANDIDATE/ ACCEPTED/ DEPRECATED/ STANDARD</td>
<td>CANDIDATE</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type attribute of all imported terms.</td>
<td>PRIMARY/SECONDARY/ NONE</td>
<td>NONE</td>
</tr>
<tr>
<td>CreateBusinessGlossaryPreview</td>
<td>If TRUE, creates a preview of the business glossary content in a CSV file or in the log file instead of importing the categories and terms.</td>
<td>TRUE/FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>BusinessGlossaryPreview Format</td>
<td>Specifies whether to write the preview to a CSV file or to the log file (SYSTEMOUT).</td>
<td>CSV / SYSTEMOUT</td>
<td>SYSTEMOUT</td>
</tr>
</tbody>
</table>
### Table 33. Configuration file command parameters (continued)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
<th>Valid values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>BusinessGlossaryPreview</td>
<td>Specifies full path to the preview CSV file to be created. The CSV file cannot be imported. To import the content, run the command again with CreateBusinessGlossary Preview set to FALSE in the configuration file.</td>
<td>c:\Default.csv</td>
<td></td>
</tr>
<tr>
<td>CSVFilePath</td>
<td>Specifies full path to the preview CSV file to be created. The CSV file cannot be imported. To import the content, run the command again with CreateBusinessGlossary Preview set to FALSE in the configuration file.</td>
<td></td>
<td>c:\Default.csv</td>
</tr>
<tr>
<td>FirstRowColumnNames</td>
<td>If TRUE, the first field on the preview file contains the column names.</td>
<td>TRUE/FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>ImportToTopCategory</td>
<td>If TRUE, imports the business glossary content under a top category that is specified by the TopCategoryName parameter. Use this setting if you want to use an existing top category to contain the imported content, or to avoid merge issues by creating a new top category.</td>
<td>TRUE/FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>TopCategoryName</td>
<td>If you set ImportToTopCategory to TRUE specifies the name of a top-level category to contain the generated business glossary content. You can use an existing category name or specify a new category to be created.</td>
<td>TRUE/FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>CheckForDuplicateTerms</td>
<td>If TRUE, if terms with duplicate names are created, output the list of duplicates to a text file.</td>
<td>TRUE/FALSE</td>
<td>TRUE</td>
</tr>
<tr>
<td>DuplicateTermsFileName</td>
<td>Specifies the path of the output file for a list of duplicate terms, if CheckForDuplicateTerms is TRUE,</td>
<td>c:\Duplicates.txt</td>
<td></td>
</tr>
</tbody>
</table>

### Example

The following command creates categories and terms from a BI model that has been imported into the metadata repository that resides on localhost. The command and uses configuration file BGlossaryBuilder.ini. No preview file is created. The categories and terms are contained by the top category BI.

```bash
istool glossary bi2bg --domain localhost:9080 --u isadmin --p isadminpwd -cfg c:\temp\BGlossaryBuilder.ini -log c:\temp\bi.log
```

The configuration file BGlossaryBuilder.ini contains the following text:
ModelsToProcess = *
MemberTypeRegular = Dimension
MemberTypeMeasure = Measure
CategoriesToExclude = test
ClassifyMemberTargetSource = FALSE
MergeOption = MERGE_SOURCE_BIAS
IsModifier = FALSE
Status = CANDIDATE
Type = NONE
CreateBusinessGlossaryPreview = FALSE
BusinessGlossaryPreviewCSVFilePath = c:\tmp\preview.csv
FirstRowColumnNames = TRUE

TopCategoryName = BI
ImportToTopCategory = TRUE
DuplicateTermsFileName = c:\tmp\dup.txt
CheckForDuplicateTerms = TRUE

Status reporting

The log file shows the following status messages.

On success:
b2bg completed successfully!
n categories created
n terms created
n categories updated
n terms updated
n categories deleted
n terms deleted

On success, creation of preview file:
Glossary preview file is generated!

On failure:
Building glossary from BI failed, Error Occurred: error_message

where error_message is a more specific message.

Generating business glossary content from logical data models
You can generate categories and terms from existing logical data models by using the glossary ldm2bg command.

You run the glossary ldm2bg command from the IBM InfoSphere Information Server istool command line interface. To generate categories and terms from a logical data model, the model must have been previously imported into the metadata repository. You can use IBM InfoSphere Metadata Asset Manager to import logical data models from design tools such as IBM InfoSphere Data Architect or CA ERwin.

The glossary ldm2bg command parses a logical data model to create a hierarchy of categories and terms and then creates these categories and terms in InfoSphere Business Glossary. You can specify multiple logical models in a single glossary ldm2bg command.
During the `dm2bg` conversion process, two custom attributes are created. Both custom attributes are called Logical Model Src Info. One Logical Model Src Info custom attribute applies to categories, and the other Logical Model Src Info custom attribute applies to terms. These two Logical Model Src Info custom attributes are associated with the categories and terms that are created by the conversion process. The value of the Logical Model Src Info custom attribute is a text string composed of the values of the properties of the logical data model assets from which the term or category is derived. The value is displayed in the form of a string of property: value pairs separated by semicolons (,).

The following table shows the correspondence between elements of the logical data model and generated terms and categories.

<table>
<thead>
<tr>
<th>Names of these parts of a logical data model...</th>
<th>...become these items in the business glossary</th>
<th>Description</th>
<th>Value of custom attribute Logical Model Src Info contains these properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>model category</td>
<td>Description</td>
<td>Name Space, Author, Version, Design Tool, Model Paradigm, Physical Name, Data Schema</td>
<td></td>
</tr>
<tr>
<td>submodel category</td>
<td>Description</td>
<td>Name Space, Author, Version, Design Tool, Model Paradigm, Physical Name, Data Schema</td>
<td></td>
</tr>
<tr>
<td>subject area category</td>
<td>Description</td>
<td>Author</td>
<td></td>
</tr>
<tr>
<td>logical entity term</td>
<td>Description</td>
<td>Entity Type</td>
<td></td>
</tr>
<tr>
<td>logical entity attribute term</td>
<td>Description</td>
<td>Data Type, Is Required</td>
<td></td>
</tr>
</tbody>
</table>
In addition to the logical data model attributes that are represented in the Logical Model Src Info custom attribute, the logical data model attributes Business Name, Physical Name, and Abbreviation are also reflected in the generated categories and terms. The following table shows which term and category properties are created from which logical data model attributes.

<table>
<thead>
<tr>
<th>Attributes of the logical data model</th>
<th>Business glossary asset type</th>
<th>Term or category property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Name, Physical Name, Abbreviation</td>
<td>Category</td>
<td>Note</td>
</tr>
<tr>
<td>Business Name, Physical Name</td>
<td>Term (created from logical entity)</td>
<td>Note</td>
</tr>
<tr>
<td>Business Name, Physical Name</td>
<td>Term (created from entity attribute)</td>
<td>Note</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Term (created from logical entity)</td>
<td>Abbreviation</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Term (created from entity attribute)</td>
<td>Abbreviation</td>
</tr>
</tbody>
</table>

Other properties of the generated category and terms are obtained from a configuration file, including the optional assignment of the logical data model to resulting terms.

Before you create terms and categories, you can also use the `glossary ldm2bg` command to create a preview of the results. You specify the preview option in the configuration file. This preview is written to a file in CSV (comma-separated values) format, standard output, or to the log file. The preview of the results shows you what business glossary content will be created when you run the command a second time but without the preview option.

**Example**

Suppose that you have the MyLogicalModel logical data model, which contains the submodel MySubLogicalModel and the subject area MySubjectArea. The submodel MySubLogicalModel contains the entity MyLogicalEntity, which contains attributes MyAttribute1 and MyAttribute2.

Each category and term that is created has a Logical Model Src Info custom attribute. For each term and category, the value of Logical Model Src Info will be a string of the properties and values of the logical model element that corresponds to the particular term or category. For example, the value of Logical Model Src Info for the term MyAttribute1 might be the following string:

Data Type: Boolean; Is Required: no

The following figure illustrates the results of using the `ldm2bg` command on MyLogicalModel:
In the business glossary, the parent category is MyLogicalModel. Category MyLogicalModel contains the subcategories MySubLogicalModel and MySubjectArea. Category MySubLogicalModel is the parent category of the terms MyLogicalEntity, MyAttribute1, and MyAttribute2. The terms MyLogicalEntity, MyAttribute1, and MyAttribute2 are related terms.

If more than one element of a logical model has the same name, the terms and categories created after the first instance are appended with the name of the containing element. This convention avoids the creation of duplicate names in a parent category. For example, suppose that the previous example also included another entity called MyLogicalEntity2 in the submodel MySubLogicalModel, and MyLogicalEntity2 had attributes MyAttribute1 and MyAttribute2. Because attributes MyAttribute1 and MyAttribute2 are also the names of attributes of the entity MyLogicalEntity, the terms created from MyAttribute1 and MyAttribute2 of MyLogicalEntity2 are called MyAttribute1_MyLogicalEntity2 and MyAttribute2_MyLogicalEntity2.

**ldm2bg command:**

Use the `istool glossary ldm2bg` command to generate categories and terms from logical data models.

**Command syntax**

```
istool glossary ldm2bg
-config-file-sample <pathname> | -config-file <pathname>
```

**Authentication parameters**

```
[authentication parameters]
[-log-file <pathname>]
```

**Command options**

The following table shows the options that are specific to the `istool glossary ldm2bg` command. For authentication parameters and generic parameters, see [Commands and common parameters for istool](#).

Chapter 15. Managing assets by using the command line  269
Table 36. Command options for istool glossary ldm2bg

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Description</th>
</tr>
</thead>
</table>
| -config-file-sample | -cfg-sample        | Specifies the path in which to place a generated sample configuration file. This command generates a sample configuration file but does not generate any terms or categories corresponding to the logical data model. You can edit the sample configuration file to specify the options that you want to use, and then run the command with the -config-file option to create categories and terms. If the path contains space characters, enclose the path in double quotation marks ("). The config-file-sample and -config-file options are mutually exclusive. **Note:**  
  • When it is used, the config-file-sample option must be the first option specified.  
  • Either config-file-sample or -config-file is required. |
| -config-file      | -cfg               | Specifies the path to the configuration file that defines how business glossary content is generated from a logical data model. If the path contains space characters, enclose the path in double quotation marks ("). The -config-file and -config-file-sample options are mutually exclusive. Either -config-file or -config-file-sample is required. |
| -log-file         | none               | Specifies the path where you want the log file to be placed. If the path contains space characters, enclose the path in double quotation marks (").                                                                                                                                                                                                         |

Configuration file

A configuration file defines additional command parameters. The file is a text file with the extension .ini that you create. It can contain the parameters shown in the following table. Each parameter name is a single string with no spaces.

Table 37. Configuration file command parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
<th>Valid values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ModelsToProcess</td>
<td>Specifies the names of the models to be processed. To process all models, specify an asterisk (*).</td>
<td>Comma-separated names of models.</td>
<td>*</td>
</tr>
<tr>
<td>ClassifyMemberTarget</td>
<td>Specifies whether logical data model assets are assigned to the terms that are created from them.</td>
<td>TRUE, FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>TopCategoryName</td>
<td>Specifies the name of a top-level category that you want to contain the generated business glossary content. You can use an existing category name or specify a new category, which will be created. If multiple models are specified, multiple top-level categories are created that each correspond to a model.</td>
<td>Any string</td>
<td>Name of parent logical data model or models.</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Description</td>
<td>Valid values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>MergeOption</td>
<td>Specifies the merge option to use when the categories and terms are imported.</td>
<td>MERGE_SOURCE_BIAS, MERGE_TARGET_BIAS</td>
<td>MERGE_TARGET_BIAS</td>
</tr>
<tr>
<td></td>
<td><strong>MERGE_TARGET_BIAS</strong></td>
<td>Merge the asset and ignore imported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attributes that cannot be merged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MERGE_SOURCE_BIAS</strong></td>
<td>Merge the asset and overwrite existing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attributes that cannot be merged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CreateBusinessGlossaryPreview</td>
<td>Specifies whether a preview of the business glossary content is created</td>
<td>TRUE, FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>instead of importing the categories and terms. Use the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BusinessGlossaryPreviewFormat parameter and, optionally, the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BusinessGlossaryPreview parameter with this option to specify the location</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and format of the preview file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BusinessGlossaryPreviewFormat</td>
<td>Specifies whether to write the preview to a CSV file or to the log file</td>
<td>CSV, SYSTEMOUT</td>
<td>SYSTEMOUT</td>
</tr>
<tr>
<td></td>
<td>(SYSTEMOUT).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BusinessGlossaryPreviewCSVFilePath</td>
<td>Specifies the full path for the preview CSV file. The CSV file</td>
<td>c:\Default.csv</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cannot be imported. To import the content, run the command again with</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CreateBusinessGlossaryPreview set to FALSE in the configuration file.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FirstRowColumnNames</td>
<td>Specifies whether the preview file contains column headings corresponding</td>
<td>TRUE, FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>to InfoSphere Business Glossary properties.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Sets the given value as the default status for all the terms created.</td>
<td>CANDIDATE, ACCEPTED, STANDARD,</td>
<td>CANDIDATE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DEPRECATED</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

The following command creates categories and terms from a logical data model that has been imported into the metadata repository that resides on localhost. The command uses configuration file LDMGlossaryBuilder.ini. The categories and terms are contained by the top category LDMTestTopCat. The terms and categories have candidate status. No preview file is created. If the CreateBusinessGlossaryPreview option was later set to true, a CSV preview file would be created in the file preview.csv.
On Windows operating systems, you issue this command:

```plaintext
istool glossary ldms2bg -cfg c:\temp\LDMGlossaryBuilder.ini -domain localhost:9080 -username isadmin -password isadminpwd -log c:\temp\bi.log
```

On UNIX-based operating systems, you issue this command:

```plaintext
istoolglossary ldms2bg -cfg /temp/LDMGlossaryBuilder.ini -domain localhost:9080 -username isadmin -password isadminpwd -log /temp/ldm.log
```

The configuration file LDMGlossaryBuilder.ini contains the following text:

```plaintext
ModelsToProcess = *
ClassifyMemberTargetSource = TRUE
MergeOption = MERGE_SOURCE_BIAS
Status = CANDIDATE
CreateBusinessGlossaryPreview= FALSE
BusinessGlossaryPreviewCSVFilepath = c:\\tmp\\preview.csv
FirstRowColumnNames = TRUE
TopCategoryName = LDMTestTopCat
```

**Status reporting**

When the `ldm2bg` command completes successfully, the following status messages are included in the log file:

`ldm2bg` completed successfully!

- `n` categories created
- `n` terms created
- `n` categories updated
- `n` terms updated
- `n` categories deleted
- `n` terms deleted

When the `ldm2bg` command with the CreateBusinessGlossaryPreview option completes successfully, the following status messages are included:

Glossary preview file is generated!

When the `ldm2bg` command completes with errors, the following status messages are included:

Building glossary from LDM failed, Error Occurred: `error_message`

where `error_message` is a more specific message.

---

**InfoSphere FastTrack assets**

You can use the command line to move assets from one IBM InfoSphere Information Server metadata repository to another.

You can specify the mapping specifications, mapping components, project templates, or projects to be moved by using the `-fasttrack` option of the `istool import` and `istool export` commands. This is useful in a case where you need to transfer data from a development environment to a test or production environment.

When you export project assets you can also include the related jobs, database tables, and reports.
Asset IDs

Identify assets that you want to move using asset IDs.

An asset ID describes a project, folder, or a specific asset. An asset ID is a fully qualified path that can be specified in one of the following formats:

```
asset-id ::= 
  <project-name>.ftp | 
  <project-template-name>.ftt | 
  <project-name>/<mapping-specification-name>.spc 
  <project-name>/<mapping-component-name>.cmp 
  <project-name>/<mapping-composition-name>.cps
```

where

- `<project-name>` is the name of a project.
- `<project-template-name>` is the name of a FastTrack project template.
- `<mapping-specification-name>` is the name of a mapping specification.
- `<mapping-component-name>` is the name of a mapping component.

If there is a space in a name, the entire name must be surrounded with double quotation marks (").

**Using wildcard characters in the asset identifier**

You can use the wildcard character in element names to specify multiple assets.

The asterisk wildcard character (*) represents 0 or more characters. The question mark wildcard character (?) represents exactly 1 character. You cannot use the wildcard to specify the asset type.

For multipart names (such as mapping specification, mapping component, and mapping composition names), the separator character (/) is required, even if one or more wildcard characters is used. For example, the following names are valid uses of the wildcard:

- Project*.ftp
  All FastTrack projects whose name begins with the prefix "Project".
- Project1/*Cust.spc
  All mapping specifications that are contained in the project "Project1" where the name of the specification ends with the suffix "Cust".
- Project*/Cust.cmp
  All mapping components that are contained in any project where the name the project begins with the prefix "Project" and where the name of the component ends with the suffix "Cust".
- */*.cps
  All mapping compositions that are contained in all projects.

The following names are invalid uses of the wildcard:

- Project.*
  The asset type cannot be a wildcard.
- *.*spc
  The mapping specification must have a two-part name.
Export command for InfoSphere FastTrack assets

Use the istool export command to create an archive file that can be used to transfer some or all of your IBM InfoSphere FastTrack assets from one environment to another.

You must have the FastTrack Administrator role.

You must run the command on a computer on the client tier where InfoSphere FastTrack is installed.

The result of the export command is an archive file, which contains all the assets that are being transferred.

istool export -domain <domain>[:<port>]
-username <username>
-password <password>
-archive <filename>
[-preview]
-fasttrack '[[fasttrack-export-options]]'

where

<fasttrack-export-options>::=
[-includeGenerationHistory | -includeReports | -includeCommonMetadata | -includeDataStageAssets | -includeDependent -includeProjectRoleAssignments]*
<asset-id-list>

Note: The two single quotation marks (') are required after the -fasttrack or -ft option even if no export options are specified.

The <asset-id-list> is a list of asset identifiers that are specified in the format defined in the section “Asset IDs”. The asset identifiers in this list are separated by blanks.

If you select a project, all of the contained mapping specifications, mapping components, and mapping compositions are also selected and written to the archive. If the project is defined based on a project template, the template is automatically included.

For example:

export -u admin -p admin100 -dom KILIMANJARO -ar ft_archive1.isx
-fasttrack 'FTPProject1.ftp -incCM'

Command options

The following list shows the export command options. These options are not required.

Table 38. Export command options

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-includeGenerationHistory</td>
<td>-incGen</td>
<td>Includes generation history.</td>
</tr>
<tr>
<td>-includeReports</td>
<td>-incRep</td>
<td>Includes related reports in the exported archive.</td>
</tr>
</tbody>
</table>
Table 38. Export command options (continued)

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-includeCommonMetadata</td>
<td>-incCM</td>
<td>Includes related common metadata in the exported archive.</td>
</tr>
<tr>
<td>-includeDataStageAssets</td>
<td>-incDS</td>
<td>Includes related IBM InfoSphere DataStage and QualityStage assets in the exported archive.</td>
</tr>
<tr>
<td>-includeProjectRoleAssignments</td>
<td>-incRole</td>
<td>Includes InfoSphere FastTrack role assignments in the exported archive.</td>
</tr>
<tr>
<td>-includeDependent</td>
<td>-incDep</td>
<td>Includes all types of referenced assets in the exported archive.</td>
</tr>
</tbody>
</table>

**Note:** If you include related reports, common metadata, or InfoSphere DataStage and QualityStage assets in the archive file, you must specify each type of included metadata on the command line when you import the archive file, otherwise only InfoSphere FastTrack assets are imported.

**Exit status**

When exporting assets, if at least one item is successfully exported, an archive file is created.

**Exit status = 0**

The package was built successfully.

**Values greater than 0**

An error occurred.

**Import command for InfoSphere FastTrack assets**

Use the `istool import` command to import an archive file that contains IBM InfoSphere FastTrack assets. This command is used when transferring assets metadata repository to another.

You must have the FastTrack Administrator role.

You must run the command on a computer on the client tier where InfoSphere FastTrack is installed.

If the archive contains related IBM InfoSphere DataStage and QualityStage assets you must have privileges to edit those assets. If the archive contains related common metadata, you must have the Common Metadata Administrator role. If the archive contains related reports, you must be the owner of the reports or have the Suite Administrator role.

```
istool import -domain <domain>[:<port>]
-username <username>
-password <password>
-archive <filename>
[-preview|-replace]
-fasttrack '[:<fasttrack-import-options>]' 
```

where
<fasttrack-import-options>::=
  [
    [-onNameConflict [ ignore | replace | rename ] ] |
    [-renameSuffix <suffix>] |
    [-dsNamespace <server[/project]>]
  ]

Note: Two single quotation marks (') are required after the -fasttrack or -ft option even if no import options are specified.

Command options

The following list shows the import command options.

Table 39. Import command options

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-onNameConflict</td>
<td>-nameconf</td>
<td>ignore</td>
<td>replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ignore</td>
<td>replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>replace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>rename</td>
<td></td>
</tr>
<tr>
<td>-renameSuffix</td>
<td>-rensuf</td>
<td>&lt;suffix&gt;</td>
<td>A string that is appended to the end of each imported project (except for projects that match a name in the rename list). The default is _New.</td>
</tr>
<tr>
<td>-dsNamespace</td>
<td>-dsns</td>
<td>server [/project]</td>
<td>The name of the InfoSphere DataStage and QualityStage server and optionally the project into which to import mapping components. This option is required when mapping components are present in the archive file to be imported.</td>
</tr>
</tbody>
</table>

If the -fasttrack parameter is specified on the istool import command, the parameter must be followed by a string to indicate the options. For example:

```
import -u admin -p admin100 -dom EVEREST -ar ft_archive1.isx
-fasttrack '-dsNamespace=EVEREST/DSProject'
```

If no options are required, then an empty string must be specified. For example:
Importing multiple types of assets

If the archive file includes multiple types of assets, you must specify each type of included metadata on the command line when you import the archive file, otherwise only InfoSphere FastTrack assets are imported. For example, if the archive was exported with the -includeDependent option, it could include related reports, common metadata, and InfoSphere DataStage and QualityStage assets.

For best import performance, run separate commands to import each type of metadata that was exported to the archive file. Run the commands in the following order:
1. Import common metadata with the -cm option.
2. Import InfoSphere DataStage and QualityStage assets with the -ds option.
3. Import reports with the -rep and -replace options.
4. Import InfoSphere FastTrack assets with the -fasttrack option.

Note: You must use the -replace option when you import report assets from an archive. If you do not want to use the -replace option for other types of assets in the archive, you must use a separate command to import the reports. If you import InfoSphere FastTrack assets without the -replace option and import their related reports with the -replace option, some of the reports might not be accurate for the unreplaced assets in the target environment. Check the reports and run them again in the new environment if necessary.

In the following example, the exported assets from the file ft_archive1.isx are imported in the correct order for best performance. The common metadata assets, InfoSphere DataStage and QualityStage assets, and InfoSphere FastTrack assets are imported without using the -replace option. The reporting assets are imported with the required -replace option.

import -u admin -p admin100 -dom EVEREST -ar ft_archive1.isx
-cm ''
import -u admin -p admin100 -dom EVEREST -ar ft_archive1.isx
-ds '<import-options>'
import -u admin -p admin100 -dom EVEREST -ar ft_archive1.isx
-replace -rep
import -u admin -p admin100 -dom EVEREST -ar ft_archive1.isx
-fasttrack '<import options>'

The import options for the InfoSphere FastTrack assets must include the -dsNamespace option, which specifies the server and project that the InfoSphere DataStage and QualityStage assets were imported to.

Exit status

The command returns the following exit values:

Exit status = 0
The package was built successfully.

Values greater than 0
An error occurred.

A summary report is printed upon completion.
InfoSphere Information Analyzer assets

You can import and export IBM InfoSphere Information Analyzer project and analysis assets and move them between metadata repositories by using the command line. For example, you can move them from a development to a test environment.

Export command for InfoSphere Information Analyzer assets

Use the istool export command to export some or all of your IBM InfoSphere Information Analyzer assets to an archive file. You can use the archive file to import the assets into a different installation of IBM InfoSphere Information Server.

You must have project administrator authority.

You must run the command on a computer on the client or engine tier where InfoSphere Information Analyzer is installed.

```
istool export -domain <domain>[:<port>]
-username <username>
-password <password>
-archive <filename>
[-preview]
-ia '[-ia-export-options]'
```

where

```
<ia-export-options>::=
-ia '{
[:-includeAllDataClasses]*
[:-projects]+
[:-includeReports]*
[:-includeCommonMetadata]*
[:-includeProjectRoleAssignments]*
[:-includeResultHistory]*
}';
```

Examples

The following example shows the export of the project1 project as ia_archive1.isx and includes the common metadata for that project:

```
istool export -u admin -p admin100 -dom KILIMANJARO -ar ia_archive1.isx
-ia '-projects="project1" -includeCommonMetadata'
```

The following example shows the export of the project 2 project as ia_archive2.isx:

```
istool export -dom localhost:9080 -u admin -p admin -ar ia_archive2.isx
-ia '-projects="\project 2\''
```

The following example shows the export of the project 3 project and the project4 project as ia_archive3.isx. The example also shows the export of the common metadata assets and reports for those projects:

```
istool export -dom localhost:9080 -u admin -p admin -ar ia_archive3.isx
-ia '-projects="\project 3\ "\project4\'' -inccm -incrpt'
```

Export command options

The following list shows the export command options. These options are not required.
Table 40. Export command options

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-projects</code></td>
<td><code>-projects</code></td>
<td>Includes project names that you specify in the exported archive. You delimit multiple project names with a blank space between each name, unless one of the project names contains spaces. If one of the project names contains spaces, instead of using blank spaces as delimiters, use two backslashes (\). To specify all project names, use an asterisk (-projects=&quot;*&quot;).</td>
</tr>
<tr>
<td><code>-includeAllDataClasses</code></td>
<td><code>-dataclass</code></td>
<td>Includes all data classes for the project names specified in the exported archive.</td>
</tr>
<tr>
<td><code>-includeCommonMetadata</code></td>
<td><code>-incmm</code></td>
<td>Includes all common metadata for the project names specified in the exported archive.</td>
</tr>
<tr>
<td><code>-includeProjectRoleAssignments</code></td>
<td><code>-incroles</code></td>
<td>Includes all project role assignments for the project names specified in the exported archive.</td>
</tr>
<tr>
<td><code>-includeReports</code></td>
<td><code>-incrpt</code></td>
<td>Includes reports for the project names specified in the exported archive.</td>
</tr>
<tr>
<td><code>-includeResultHistory</code></td>
<td><code>-incresult</code></td>
<td>Includes history for the data quality results.</td>
</tr>
<tr>
<td><code>-username</code></td>
<td><code>-u</code></td>
<td>Specifies the user name</td>
</tr>
<tr>
<td><code>-password</code></td>
<td><code>-p</code></td>
<td>Specifies the password</td>
</tr>
<tr>
<td><code>-archive</code></td>
<td><code>-ar</code></td>
<td>Specifies the name of the archive</td>
</tr>
<tr>
<td><code>-domain</code></td>
<td><code>-dom</code></td>
<td>Specifies the domain name</td>
</tr>
</tbody>
</table>

**Note:** If you include reports or common metadata assets in the archive file, you must specify each type of included metadata on the command line when you import the archive file, otherwise only InfoSphere Information Analyzer assets are imported.

**Exit status**

When exporting assets, if at least one item is successfully exported, an archive file is created.

**Exit status = 0**

The package was built successfully.

**Values greater than 0**

An error occurred.

**Note:** Archive files of assets that are exported by using the istool command can be imported only by using the istool command line.
Import command for InfoSphere Information Analyzer assets

Use the istool import command to import an archive file of assets that was created by the istool export function.

You must have project administrator authority to import IBM InfoSphere Information Analyzer assets. To import related common metadata, you must have the Common Metadata Administrator role.

You must run the command on a computer on the client or engine tier where InfoSphere Information Analyzer is installed.

```
istool import -domain <domain>[[:<port>]
-username <username>
-password <password>
-archive <archive_name>
[-preview | -replace]
-ia'
[-onNameConflict < ignore | replace | rename >]+
[-renameSuffix <is_New>]
)
```

Command options

The following list shows the command options for imports. These options are not required.

**Table 41. Import command options**

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-onNameConflict</td>
<td>-nameConf</td>
<td>Specifies an action that you want to perform when a name conflict is detected for an InfoSphere Information Analyzer project. The default action is to ignore the conflict.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>ignore</strong> If a project with the same name already exists on the target, then the image is not imported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>replace</strong> If a project with the same name already exists on the target, then replace the target with the imported image.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>rename</strong> If a project with the same name already exists on the target, then rename the new asset that is being imported.</td>
</tr>
<tr>
<td>-renameSuffix</td>
<td>-renSuf</td>
<td>Specifies the suffix that would be used if there was a name conflict. For example, if a project named Customer_Data is being imported, and a project named Customer_Data already exists on the target system, then the new project being imported would be renamed to Customer_Data_New.</td>
</tr>
</tbody>
</table>

280 Administration Guide
If the -ia parameter is specified on the istool import (or istool export) command, the parameter must be followed by a string to indicate the options. If no options are required, then an empty string must be specified. For example:

```
import -u admin -p admin100 -dom EVEREST -ar ia_archive1.isx -ia ''
```

**Importing multiple types of assets**

If the archive file includes multiple types of assets, you must specify each type of included metadata on the command line when you import the archive file, otherwise only InfoSphere Information Analyzer assets are imported. For example, if the archive is exported with the -includeCommonMetadata and -includeReports options, you must specify the -cm and -rep options in addition to the -ia options when you import the archive.

**Note:** You must use the -replace option when you import report assets from an archive. If you do not want to use the -replace option for the other types of assets in the archive, you must use a separate command to import the reports. If you import InfoSphere Information Analyzer assets without the -replace option and import their related reports with the -replace option, some of the reports might not be accurate for the unreplaced assets in the target environment. Check the reports and run them again in the new environment if necessary.

In the following example, the first command imports InfoSphere Information Analyzer assets and common metadata assets from the file ia_archive1.isx without using the -replace option. The second command imports reporting assets from the same archive file while using the required -replace option.

```
import -u admin -p admin100 -dom EVEREST -ar ia_archive1.isx -ia '' -cm ''
import -u admin -p admin100 -dom EVEREST -ar ia_archive1.isx -replace -rep
```

**InfoSphere DataStage and QualityStage assets**

These assets are created in projects. They include jobs, table definitions, rule sets, and other project assets.

You can interchange IBM InfoSphere DataStage and QualityStage assets by using two different methods:

- You can use the graphic interface of IBM InfoSphere Information Server Manager to define a package of assets. You can then build that package and deploy that package to another project or services tier by using the build package and deploy package commands. The package is an object that is held in the InfoSphere Information Server metadata repository, and can be rebuilt or deployed by users who have access to the repository. After you have defined a package, you can rebuild and redeploy the package whenever any of the assets that it contains change. A history is maintained to help you track the package.

- You can export a list of named DataStage assets to an archive file by using the istool export command. You can then import the assets to another project or domain by using the istool import command. If any of the objects contained in the archive change, you can reexport them to a new archive or update the existing archive file. The archive is created by, and belongs to, a particular user, and can be shared only by physically distributing the file.

The package and deploy method is suited to the product lifecycle scenario, where you are repeatedly moving assets between development, test, and production systems. The archive file method is suited to an asset sharing or asset backup scenario.
You can use InfoSphere Information Server Manager to identify the names of the assets that you want to export, and then capture those names for inclusion in istool commands.

**Build package command**

You can use the istool command-line interface (CLI) to build packages of IBM InfoSphere DataStage and QualityStage assets that are defined in the IBM InfoSphere Information Server Manager.

**Purpose**

The istool build package command is used to build a package ready for deployment. You must first define the package in the InfoSphere Information Server Manager, including specifying the assets that it contains and the build and deploy paths. In a clustering environment, set the build and deploy paths to shared directories that are accessible from every cluster node. The package that you specify resides in the metadata repository.

To build a package, you must have an InfoSphere DataStage and QualityStage role that grants you permission to edit the assets in the package.

**Command syntax**

istool build package
authentication options
[generic options]
-package package
[ -label "buildlabel" ]
[ -comment "comment" ]
[ -overwrite ]
[ -preview ]

**Command options**

authentication options
Use authentication options to connect to a specific installation of InfoSphere Information Server.

generic options
Use the generic options to request help on command syntax, or to specify silent or verbose operation.

-package name or -pkg name
Specifies the name of an existing deployment package definition in the metadata repository.

-comment "comment_text" or -c "comment_text"
Adds a comment to the deployment package information.

-preview or -pre
Specify this option to preview the build operation without building a package.

-label "label_text" or -l "label_text"
Specifies a label for the build. You can use the label to version different builds of your deployment package.

-overwrite or -o
Rebuilds an existing deployment package. This option removes all history from the package.
Exit status

A return value of 0 indicates successful completion, any other value indicates failure. The list of exit codes is shown in the command help. Enter istool build package -help to see the list of possible exit codes for the build package command.

Error handling

When building a deployment package, if at least one object is successfully built, a deployment package file is created. If one or more objects fails to build, the command completes with a non-zero exit code.

Example

The following example shows how to build two versions of a package.

1. Define a package named DeployPackage1 by using the InfoSphere Information Server Manager to include tabledef1.tbd.
2. Build the package DeployPackage1, add the comment "my first package" to the build, and label the build "version 1.1":

   ```
   istool build package -domain myhost:9080
   -username user1 -password pass1 -package DeployPackage1
   -label "version 1.1" -comment "my first package"
   ```

3. Modify tabledef1.tbd in the Designer client. For example, add a row.
4. Rebuild the same package, add the label "version 1.2", and add the comment "table def changes":

   ```
   istool build package -domain myhost:9080
   -username user1 -password pass1 -package DeployPackage1
   -label "version 1.2" -comment "table def changes"
   ```

When you open DeployPackage1 in the InfoSphere Information Server Manager, the History tab shows two builds, version 1.1 and version 1.2. You can deploy version 1.1 or version 1.2 of tabledef1.tbd by using the deploy package command and specifying the -label option.

Deploy package command

You can use the istool command-line interface (CLI) to deploy packages of IBM InfoSphere DataStage and QualityStage assets that you have previously built.

Purpose

The istool deploy package command copies the contents of a package to a target metadata repository of IBM InfoSphere Information Server. You must first define the package in the InfoSphere Information Server Manager, including specifying the assets that it contains and the build and deploy paths. In a clustering environment, set the build and deploy paths to shared directories that are accessible from every cluster node. The package is built by using the istool build package command.

To deploy a package, you must have an InfoSphere DataStage and QualityStage role that grants you permission to edit assets in the target project.

Command syntax
istool deploy package
authentication options
[generic options]
[-package package | -file deployfile | -localfile deployfile]
[-label "buildlabel"]
[-preview]

-datastage '[-replace] server/project'

Command options

authentication options
Use authentication options to connect to a specific installation of InfoSphere Information Server.

generic options
Use the generic options to request help on command syntax, or to specify silent or verbose operation.

-package name or -pkg name
Specifies the name of an existing deployment package definition in the metadata repository. The package must already be built. The -package, -file, and -localfile options are mutually exclusive.

-file name or -f name
Specifies a deployment package file name in the target system. The specified file name must be relative to the deploy directory in the target system. Use this option to deploy assets that were packaged on a different computer. You must first transfer the package file from the source system build directory to the target system deploy directory. The -package, -file, and -localfile options are mutually exclusive.

-localfile name or -lf name
Specifies the fully qualified name of a deployment package file on the local file system of the client. The -package, -file, and -localfile options are mutually exclusive.

-label "label_text" or -lab "label_text"
Specifies the label for the build of the package to be deployed.

-preview or -pre
Specify this option to preview the action of the command without changing the repository.

-datastage 'server/project' or -ds 'server/project'
Specifies that InfoSphere DataStage and QualityStage assets are to be deployed to the target server and project.

-replace or -repl
Specifies that assets in the deployment package replace any existing assets in the target project that have the same identity.

Exit status

A return value of 0 indicates successful completion, any other value indicates failure. The list of exit codes is shown in the command help. Enter istool deploy package -help to see the list of possible exit codes for the deploy package command.
**Error handling**

When you deploy a package, the operation continues until the entire deployment package is processed. As many objects are imported as possible. If there is failure in deploying one or more objects to the project, a non-zero exit status is returned.

**Examples**

The following command deploys an existing package named localpackage to the target project named myProject. The target project is on the same computer. If there are any assets with the same name in the target project, they are replaced with assets from the deployment package.

```
istool deploy package -domain myserver:9080
-username user1 -password pass1
-package localpackage
-datastage '-replace sliver/myProject'
```

The following command deploys a package named remotePackage that was created on a different computer. The package file has already been copied to the deploy directory on the target computer. The package is deployed from the file to the project named OtherProject.

```
istool deploy package -domain myserver:9080
-username user1 -password pass1
-file remotePackage.pkg
-datastage 'slice/OtherProject'
```

**Send package command**

You can use the istool command-line interface (CLI) to send package files to a local client computer.

**Purpose**

The istool send package command sends a deployment package from the metadata repository to a file on a local client computer. You can deploy a package from the local client computer by using the deploy package command with the -localfile option.

You must first define the package in the InfoSphere Information Server Manager, including specifying the assets that it contains and the build and deploy paths. In a clustering environment, set the build and deploy paths to shared directories that are accessible from every cluster node. The package is built by using the istool build package command.

**Command syntax**

```
istool send package
authentication options
[generic options]
-package package
-file deployfile
[-replace]
```

**Command options**

authentication options

Use authentication options to connect to a specific installation of InfoSphere Information Server.
generic options

Use the generic options to request help on command syntax, or to specify silent or verbose operation.

**-package name or -pkg name**

Specifies the name of an existing deployment package definition in the metadata repository. The package must already be built.

**-file name or -f name**

Specifies the fully qualified name of a file on the local file system of the client computer to send the deployment package to.

**-replace**

Replaces the file if it exists on the computer.

Exit status

A return value of 0 indicates successful completion, any other value indicates failure. The list of exit codes is shown in the command help. Enter `istool send package -help` to see the list of possible exit codes for the `send package` command.

Example

The following command sends the deployment package, package1, from the system named sliver to a file, package1.pkg in the folder "c:\package dir" in the local file system.

```plaintext
istool send package -domain sliver:9080
-username user1 -password pass1
-package package1
-file "c:\package dir\package1.pkg"
-replace
```

Export command for InfoSphere DataStage and QualityStage assets

You can use the istool command line interface (CLI) to export assets to an archive file. The default extension of the archive file is .isx.

Purpose

Use the DataStage command option with the istool export command to export IBM InfoSphere DataStage and QualityStage assets to an archive file on the local file system. You can then use the istool import command with the DataStage command option to restore the exported assets into a different IBM InfoSphere Information Server metadata repository.

You must have an InfoSphere DataStage and QualityStage role that grants you permission to edit the assets that you are exporting.

Command syntax

```plaintext
istool export
authentication options
[generic options]
-archive "pathname" [-updatearchive]
[-preview ]
[-abortIfError=number_of_errors]
-datastage ' [ -base="server[:port]/project"]
[-includedependent]
```
[-nodesign]
[-includeexecutable]
"dsServer[:port]/project/folder/name.type"

**Command options**

**authentication options**
Use authentication options to connect to a specific installation of InfoSphere Information Server.

**generic options**
Use the generic options to request help on command syntax, or to specify silent or verbose operation.

**-archive "archive_pathname" or -ar "archive_pathname"**
Specifies the path name for the file that the assets are exported to.

**-updatearchive or -up**
Specifies that the archive file is updated if it exists (otherwise it is overwritten)

**-preview or -pre**
Specify this option to preview the export operation without exporting the assets.

**-AbortIfExists number_of_errors or -abort number_of_errors**
Specifies that the export stops if the specified number of errors occur

**-datastage "server/project/folder/name.type" or -ds**
Specifies that InfoSphere DataStage and QualityStage assets are to be exported.

**-nodesign**
Excludes design objects from the export. Use together with the -includeexecutable option to export only runtime executables.

**-includedependent or -incdep**
Includes dependent assets. For example, if you export a job named myjob that uses the table definition named salesdata, then specifying the -includedependent causes the table definition to be automatically included when the job is exported.

**-includeexecutable or -incexe**
Includes runtime executables. Some assets do not have executable components. If you use this option and an asset in the export does not have an executable component, a warning is generated but the export does not fail as a result.

**-base "dsServer[:port]/project/[folder]"**
You can optionally use the -base argument to specify a base path. This path is then prefixed to all the asset path names that you specify. For example, if your base option specifies dsServer/project, then your asset path only specifies folder/name.type.

**Note:** If you specify -includedependent, the archive file can include common metadata assets. When you import the archive file, you must specify the -cm option on the command line. Otherwise, the common metadata assets are not imported.
Exit status

A return value of 0 indicates successful completion, any other value indicates failure. The list of exit codes is shown in the command help. Enter istool export -help to see the list of possible exit codes for the export command.

Error handling

When you are exporting more than one object, a failure does not interrupt the operation. If only one object is successfully exported, an archive file is still created. If no objects are exported, no archive file is created. The exit status reports an error if one or more objects cannot be exported.

Examples

The following command exports the parallel job named ajob from the project named proj on the computer named sliver. The job is located in the Mine subfolder of the Jobs folder. The command also exports all the server jobs in folder2 and its subfolders in the project named anotherProj on the computer named serv2. In this InfoSphere Information Server system, both sliver and serv2 belong to the same domain (sliver:9080). All the assets are written to the archive file C:\arc.isx.

```
istool export -domain sliver:9080 -username user1 -password pass1 -archive "c:\arc.isx" -datastage "sliver:5000/Proj/Jobs/Mine/ajob.pjb"
"serv2/anotherProj/folder2/*/*.sjb"
```

The following command exports all the assets in the folder named tabledefinitions, and all the parallel jobs in the Pivotal subfolder of the Jobs folder. All these folders belong to the project named anotherProj on the computer named serv2. The -updatearchive option is specified, so if the specified archive file, C:\arc.isx, exists, the assets are added to the archive file. The -includedependent option is specified so that any shared tables that are related to the table definitions are also exported.

```
istool export -domain sliver:9080 -username user1 -password pass1 -archive "c:\arc.isx" -updatearchive -datastage '-base="serv2/anotherProj" "tabledefinitions/*.tbd" "Jobs/Pivotal/*.pjb" -includedependent'
```

The following example exports only job executables for the parallel jobs in the Jobs folder. The folder belongs to the project named dstage on the computer named sliver. No design time assets are exported. The job executables are written to the archive file C:\runtime.isx.

```
istool export -domain sliver:9080 -username user1 -password pass1 -archive "c:\runtime.isx" -ds -nodesign -includeexecutable "sliver:5000/dstage/Jobs/*.pjb"
```

Asset paths for InfoSphere DataStage and QualityStage assets

You can export specific assets to an archive file by specifying the paths of the assets on the command line.

Asset path

Assets to export are identified by a path name. An asset path is a fully-qualified path that identify assets to be exported. The path has the following format:

```
engine_host[:portnumber]/project/folder[folder...]//asset.type
```

An asset path consists of the following elements:

- `engine_host`. The name of the computer that hosts the engine tier.
- *port*. Optionally specifies the port used to communicate with the engine tier. The port number is only needed if the engine tier uses a non-default port number. (The default port number is 31538.)

- *project*. The project that contains the asset or assets.
- *folder[/folder...]*. The folder structure that contains the asset or assets.
- *asset.type*. The name of the asset and a suffix that specifies the type of the asset.

### Asset type

Asset types are identified by a type suffix. Type suffixes are not case-sensitive.

**Table 42. Asset type names**

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Type suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data element</td>
<td>det</td>
</tr>
<tr>
<td>IMS database</td>
<td>idb</td>
</tr>
<tr>
<td>IMS viewset</td>
<td>ivs</td>
</tr>
<tr>
<td>Mainframe job</td>
<td>mjb</td>
</tr>
<tr>
<td>Parallel job</td>
<td>pjb</td>
</tr>
<tr>
<td>Sequence job</td>
<td>qjb</td>
</tr>
<tr>
<td>Server job</td>
<td>sb</td>
</tr>
<tr>
<td>Machine profile</td>
<td>mcp</td>
</tr>
<tr>
<td>Mainframe routine</td>
<td>mrt</td>
</tr>
<tr>
<td>Parallel routine</td>
<td>prt</td>
</tr>
<tr>
<td>Server routine</td>
<td>srt</td>
</tr>
<tr>
<td>Parallel shared container</td>
<td>psc</td>
</tr>
<tr>
<td>Server shared container</td>
<td>ssc</td>
</tr>
<tr>
<td>Table definition</td>
<td>tbd</td>
</tr>
<tr>
<td>Transform</td>
<td>tfm</td>
</tr>
<tr>
<td>Data quality specification</td>
<td>dqs</td>
</tr>
<tr>
<td>Stage type</td>
<td>stp</td>
</tr>
<tr>
<td>Data connection</td>
<td>dcn</td>
</tr>
<tr>
<td>Parameter set</td>
<td>pst</td>
</tr>
</tbody>
</table>

### Wildcard character

You can use the wildcard character asterisk (*) in element names. The asterisk wildcard character represents 0 or more characters. You can use the wildcard character to specify multiple assets. The following table shows the ways that the wildcard character can be used.

**Table 43. Use of wildcard character in asset path**

<table>
<thead>
<tr>
<th>Location</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In place of an asset name</td>
<td>server/project/xfolder/*.pjb</td>
<td>All parallel jobs in xfolder</td>
</tr>
</tbody>
</table>
Table 43. Use of wildcard character in asset path (continued)

<table>
<thead>
<tr>
<th>Location</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beginning of an asset name</td>
<td>serve/project/xfolder/job.pjb</td>
<td>All parallel jobs with name ending with 'job' in xfolder</td>
</tr>
<tr>
<td>End of an asset name</td>
<td>server/project/xfolder/job*.pjb</td>
<td>All parallel jobs with name beginning with 'job' in xfolder</td>
</tr>
<tr>
<td>Beginning and end of an asset name</td>
<td>server/project/xfolder/job*.pjb</td>
<td>All parallel jobs with name containing 'job' in xfolder</td>
</tr>
<tr>
<td>In place of an asset type</td>
<td>server/project/xfolder/xjob.*</td>
<td>All assets with name 'xjob' of any type in xfolder</td>
</tr>
<tr>
<td>In place of asset name and asset type</td>
<td>server/project/xfolder/<em>.</em></td>
<td>All exportable assets in xfolder</td>
</tr>
<tr>
<td>In place of a folder for recursive match</td>
<td>server/project/xfolder/<em>/.</em></td>
<td>All exportable assets in xfolder and its subfolders (recursive).</td>
</tr>
<tr>
<td></td>
<td>server/project/<em>/.</em></td>
<td>All exportable assets in the specified project (recursive)</td>
</tr>
<tr>
<td></td>
<td>server/project/xfolder/*/xjob.pjb</td>
<td>All parallel jobs with name=xjob in xfolder and its subfolders (recursive)</td>
</tr>
<tr>
<td></td>
<td>server/project/xfolder/<em>/job</em>.pjb</td>
<td>All parallel jobs with name beginning with 'job' in xfolder and its subfolders (recursive)</td>
</tr>
</tbody>
</table>

Using special characters in an asset path

When the asset path contains characters that conflict with the istool command-line syntax, those characters must be escaped by using special characters. The istool command uses the backslash character (\) as an escape character. Inserting a backslash in front of one of these special characters changes the way istool treats the character.

IBM InfoSphere DataStage and QualityStage does not allow non-alphanumeric characters in asset names, other than underscore (_). The only exception is folder names and machine profiles, where you can use the single quote (‘), double quote ("), or asterisk (*) characters, which must be preceded by backslash (\) if used in an asset string. The following table shows how to enter characters that require special treatment.

You must take special steps when using the istool CLI in command mode on a UNIX computer. When using the command mode in UNIX, the asset path is first processed by the UNIX shell. The single quote character (‘) has a special meaning to UNIX shell, and you cannot escape the single-quote by using the backslash character. To specify an asset path containing a single quote character, you must switch in and out of single-quote mode and use double quotes characters (") to prevent the UNIX shell interpreting the single quote character in the asset path. Switch out of single-quote mode by inserting an additional single quote character.
in the asset path before the existing single quote character in the asset path.
Enclose the single quote character in the asset path within double quote characters ("""). Switch back into single-quote mode for the remaining of the asset path by inserting another single quote character. For example, to specify the following command `istool export ... -ds ""server/project/x'folder/xjob.pjb"", you would actually type the following command at the UNIX command prompt:

```
istool export ... -ds ""server/project/x'folder/xjob.pjb"
```

<table>
<thead>
<tr>
<th>Character</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>double quotes ()</td>
<td>&quot;</td>
<td><code>istool export .... -ds &quot;server/project/x&quot;folder/xjob.pjb&quot;</code></td>
</tr>
<tr>
<td>single quote ()</td>
<td>'</td>
<td><code>Windows</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>istool export .... -ds &quot;server/project/x\folder/xjob.pjb&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>UNIX</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Command mode:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>istool export .... -ds &quot;server/project/x&quot;folder/xjob.pjb&quot;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Console and script mode:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>istool export .... -ds &quot;server/project/x\folder/xjob.pjb&quot;</code></td>
</tr>
<tr>
<td>asterisk (*)</td>
<td>*</td>
<td><code>istool export .... -ds &quot;server/project/x*folder/xjob.pjb&quot;</code></td>
</tr>
</tbody>
</table>

**Retrieving asset names from InfoSphere Information Server Manager**

You can use the IBM InfoSphere Information Server Manager to identify the IBM InfoSphere DataStage and QualityStage assets that you want to add to an archive, and retrieve the names of these assets.

You can retrieve the names of multiple assets in a single operation, or you can retrieve the name of a single asset at a time.

To retrieve the names of multiple assets in a single operation:
1. In the repository view of InfoSphere Information Server Manager, select a number of assets by clicking the assets while holding down CTRL.
2. Right-click and select **Copy** from the pop-up menu.
3. In a text editor program, right-click and select **Paste** from the pop-up menu.

The full text path of the asset is inserted into your document. For example, selecting some job icons in the repository view might result in the following strings being added to your document.

```
SPARK/aTestProject/Jobs/Folder1/Job3.pjb SPARK/aTestProject/Jobs/Job2.sjb
```

To retrieve the name of a single asset at a time:
1. In the repository view of InfoSphere Information Server Manager, select an asset by clicking it.
2. Right-click in the Repository view and select **Show Properties** from the pop-up menu.
3. Select the name of the asset in the properties view.
4. Right-click and select **Copy** from the pop-up menu.
5. In a text editor program, right-click and select **Paste** from the pop-up menu.
After you have assembled the names of the assets that you want to export in a document, you can copy and paste the names from there to a command-line prompt, or to a script that you are building.

**Import command for InfoSphere DataStage and QualityStage assets**

You can use the istool command line interface (CLI) to import assets from a previously exported archive file.

**Purpose**

Use the InfoSphere DataStage command option with the istool `import` command to import IBM InfoSphere DataStage and QualityStage assets from an archive file to the metadata repository of IBM InfoSphere Information Server. This command is the reverse of the `export` command.

To import InfoSphere DataStage and QualityStage assets you must have a role that grants you permission to edit assets in the target project. To include related common metadata assets in the import, you must have the Common Metadata Administrator role.

**Command syntax**

```
istool import
authentication options
[generic options]
-archive pathname
[-preview|-replace]
[-abortAfter=number_of_errors]
-datadstage "[-nodesign]"Server/project"
```

**Command options**

**authentication options**

All asset interchange commands use authentication options to connect to a specific installation of InfoSphere Information Server.

**generic options**

The generic parameters are available by all asset interchange commands. Use the generic options to request help on command syntax, or to specify silent or verbose operation.

- `archive "asset_pathname"` or `-ar "asset_pathname"`
  Specifies the path name for the file that the assets are imported from.

- `replace`
  Specify this option to replace existing assets with imported assets of the same identity.

- `preview` or `-pre`
  Specify this option to preview the action of the command without changing the repository.

- `abortAfter number_of_errors` or `-abort number_of_errors`
  Specifies that the import stops if more than the specified number of errors occur.

- `datadstage "server/project"` or `-ds "server/project"
  Specifies that InfoSphere DataStage and QualityStage assets are to be imported to the target server and project.
-nodesign
   Specifies that job designs are not imported, only job executables

Importing multiple types of assets

If the archive file includes multiple types of assets, you must specify each type of included metadata on the command line when you import the archive file. Otherwise, only InfoSphere DataStage and QualityStage assets are imported. For example, if the archive was exported with the -includedependent option, it could include common metadata assets.

For best import performance, import the common metadata assets first, and then run a command to import the InfoSphere DataStage and QualityStage assets.

The following commands import assets from the archive file arc.isx in the correct order. The common metadata assets are imported first. The InfoSphere DataStage and QualityStage assets are then imported to the project aProj on the server slice.

```
istool import -domain sliver.svl.ibm.com:9080
    -username user1 -password pass1
    -archive "c:\arc.isx" -cm ''
istool import -domain sliver.svl.ibm.com:9080
    -username user1 -password pass1
    -archive "c:\arc.isx" -datastage ' "slice/aProj" '
```

Importing standardization rule sets into multiple projects

If an archive file contains only standardization rule sets from InfoSphere QualityStage, you can import the rule sets into more than one project at the same time.

You can use an asterisk (*) as a wildcard character to indicate the projects that you want to import the rule sets into. For example, the following command imports the rule sets into all projects on the server:

```
istool import -domain test.sample.com:9080
    -username isadmin -password isadmin
    -archive "c:\arc.isx" -datastage ' "test.sample.com/**" '
```

The following command imports the rule sets into the projects on the server that begin with the letter X:

```
istool import -domain test.sample.com:9080
    -username isadmin -password isadmin
    -archive "c:\arc.isx" -datastage ' "test.sample.com/X*" '
```

Exit status

A return value of 0 indicates successful completion, any other value indicates failure. The list of exit codes is shown in the command help. Enter istool import -help to see the list of possible exit codes for the import command.

Error handling

When importing from an archive file that contains more than one object, a single failure does not interrupt the operation. The exit status reports an error if one or more objects cannot be imported.
Examples

The following command previews an import of assets from the file arc.isx. No assets are imported. Job designs are not included.

```
istool import -domain sliver:9080
   -username user1 -password pass1
   -archive "c:\arc.isx" -pre -datastage ' -nodesign "slice/aProj"'
```

After the preview, the command is repeated without the -preview option to import the assets to the project named aProj located on the computer named slice. The InfoSphere Information Server engine on slice is associated with the computer named sliver on the services tier.

```
istool import -domain sliver.svl.ibm.com:9080
   -username user1 -password pass1
   -archive "c:\arc.isx" -datastage ' -nodesign "slice/aProj"'
```

Delete command for InfoSphere DataStage assets

You can use the istool command line interface (CLI) to delete InfoSphere DataStage assets.

Purpose

Use the InfoSphere DataStage command option with the istool delete command to delete InfoSphere DataStage assets from the metadata repository of IBM InfoSphere Information Server.

To delete InfoSphere DataStage assets, you must have a role that grants you permission to edit assets in the target project.

Command syntax

```
istool delete
authentication options
[generic options]
- abort -abortIfError
- np -noprompt
- ds -datastage [-base]
```

Command options

**authentication options**
All asset interchange commands use authentication options to connect to a specific installation of InfoSphere Information Server.

**generic options**
The generic parameters are available by all asset interchange commands. Use the generic options to request help on command syntax, or to specify silent or verbose operation.

**abort | abortIfError**

Stops running the command if errors are encountered.

**np | noprompt**

Suppresses the message confirming that the asset was deleted.

**ds | datastage**
The path name of the InfoSphere DataStage and QualityStage assets that you want to delete. The syntax of the path name is dsserver/project/folder/
When deleting an asset, you must specify the correct suffix for the type of asset that you want to delete. The following table includes asset types and their related suffixes.

Use the base option to specify a base path name. This path will be prefixed to all the asset paths that you specify. For example, if you specify dsserver/project for the base option, then you specify your asset path at folder/name.type_suffix.

Table 45. Include the appropriate suffix for the type of asset that you want to delete.

<table>
<thead>
<tr>
<th>Asset type</th>
<th>Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mainframe job</td>
<td>mjb</td>
</tr>
<tr>
<td>Parallel job</td>
<td>pjb</td>
</tr>
<tr>
<td>Sequence job</td>
<td>sqb</td>
</tr>
<tr>
<td>Server job</td>
<td>sjb</td>
</tr>
<tr>
<td>Parallel shared container</td>
<td>psc</td>
</tr>
<tr>
<td>Server shared container</td>
<td>ssc</td>
</tr>
<tr>
<td>Parameter set</td>
<td>pst</td>
</tr>
<tr>
<td>Transform</td>
<td>tfm</td>
</tr>
<tr>
<td>Data element</td>
<td>det</td>
</tr>
<tr>
<td>Stage type</td>
<td>stp</td>
</tr>
<tr>
<td>IMS database</td>
<td>idb</td>
</tr>
<tr>
<td>IMS viewset</td>
<td>ivs</td>
</tr>
<tr>
<td>Machine profile</td>
<td>mcp</td>
</tr>
<tr>
<td>Mainframe routine</td>
<td>mrt</td>
</tr>
<tr>
<td>Parallel routine</td>
<td>prt</td>
</tr>
<tr>
<td>Server routine</td>
<td>srt</td>
</tr>
<tr>
<td>Table definition</td>
<td>tbd</td>
</tr>
<tr>
<td>Data connection</td>
<td>dcn</td>
</tr>
</tbody>
</table>

Exit status

A return value of 0 indicates successful completion, a value of 1 indicates a warning, and any other value indicates failure. The list of exit codes is shown in the command help. Enter istool delete -help to see the list of possible exit codes for the delete command.

Example: deleting single assets

The following command deletes a single parallel job named ParallelJob1.pjb.

```
istool delete -domain host1 -username xxx -password xxx -datastage 'DSServer/Project1/Jobs/ParallelJob1.pjb'
```

You can run the same command with the -noprompt option to suppress delete confirmation.

```
istool delete -domain host1 -username xxx -password xxx -noprompt -datastage 'DSServer/Project1/Jobs/ParallelJob1.pjb'
```
Example: deleting multiple assets

The following command deletes a parallel job named `ParallelJob1.pjb`, a routine job named `ParallelRoutine.prt`, and a server routine named `ServerRoutine.srt`. By using the `-base` option, you specify the folder names and file names for each asset instead of the full path.

```
istool delete -domain host1 -username xxx -password xxx -noprompt
-datastage
  '-base=DSServer/Project1
    Jobs/ParallelJob1.pjb
    Routines/ParallelRoutine.prt
    Routines/ServerRoutine.srt'
```

The following command deletes multiple assets that have path names containing blank characters.

```
istool delete -domain host1 -username xxx -password xxx -noprompt
-datastage
  '-base=DSServer/Project1
    "Jobs/PX Jobs/Job1.pjb"
    "Jobs/PX Jobs/Job2.pjb"
```

InfoSphere Streams assets

You can use the `istool` command line to manage and move InfoSphere Streams assets, between different InfoSphere Information Server environments.

InfoSphere Streams assets are endpoints that contain tuples and tuple attributes.

You can use endpoints in job designs, assign them to terms in InfoSphere Business Glossary, and view them in data lineage reports in InfoSphere Metadata Workbench.

You can use the `istool export` and `istool import` commands to move assets between development, test, and production environments.

Export command for InfoSphere Streams assets

Use the `istool export` command to export some or all of your InfoSphere Streams assets to an archive file.

You must have the Common Metadata User role.

You must run the command on a computer on the client tier where InfoSphere Streams is installed.

```
istool export
  [authentication parameters]
  [generic parameters]
  -archive <filename>
  [-preview]
  -streamsEndpoint '-endPoints <end-points>'
```

Export command options

All asset interchange commands use authentication parameters to connect to a specific IBM® InfoSphere® Information Server. The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.
The following table shows the export command options.

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-streamsEndpoint</td>
<td>-streams</td>
<td></td>
<td>Enables the export of InfoSphere Streams assets which are endpoints.</td>
</tr>
<tr>
<td>-endPoints</td>
<td>-ep</td>
<td>[*</td>
<td>scope/name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Specify a single * to export all endpoints.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Specify both the specific scope and name of the endpoints. You can use</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>wildcards for both scope and name. Only endpoints that have an application</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>scope are exported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Specify the name of an endpoint to export. You can use wildcards anywhere</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>in the name string. Only endpoints that do not have an application scope are</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>returned.</td>
</tr>
</tbody>
</table>

**Exit status**

A return value of 0 indicates successful completion. Any other value indicates failure.

**Example**

The following example exports all InfoSphere Streams assets that are in the metadata repository to an archive file named ep.isx.

```
istool export -domain ISDOMAIN:9080 -archive c:\temp\ep.isx
-username dsadm -password **** -streams '-ep *'
```

The following command exports all endpoints whose names begin with "Send". The endpoints can have any application scope, but each endpoint must have an application scope.

```
istool export -domain ISDOMAIN:9080 -archive c:\temp\ep.isx
-username dsadm -password **** -streams '-ep */Send*' 
```

The following command exports all endpoints whose names begin with "Send" and whose application scope is null.

```
istool export -domain ISDOMAIN:9080 -archive c:\temp\ep.isx
-username dsadm -password **** -streams '-ep Send*' 
```

**Import command for InfoSphere Streams assets**

Use the `istool import` command to import an archive file that contains endpoints from InfoSphere Streams.

You must have the Common Metadata Importer role to import InfoSphere Streams assets.

You must run the command on a computer on the client tier where InfoSphere Streams is installed.
istool import
  [authentication parameters]
  [generic parameters]
  -streamsEndpoint '-onNameConflict [ ignore | replace ]'

Command options

The following table shows the command options for imports.

Table 47. Import command options

<table>
<thead>
<tr>
<th>Long name</th>
<th>Short name</th>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-streamsEndpoint</td>
<td>-streams</td>
<td></td>
<td>Enables the import of InfoSphere Streams assets which are the endpoints.</td>
</tr>
<tr>
<td>-onNameConflict</td>
<td>-nameconf</td>
<td>[ignore</td>
<td>replace</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ignore</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>replace</td>
</tr>
</tbody>
</table>

Exit status

A return value of 0 indicates successful completion. Any other value indicates failure.

Example

The following example imports endpoints from the archive file ep.isx. When an endpoint of the same name and application scope already exists in the metadata repository, the imported endpoint replaces the existing endpoint.

istool import -domain ISDOMAIN:9080 -archive c:\temp\ep.isx
  -username dsadm -password **** -streams '-nameconf replace'

Common metadata assets

Common metadata assets include implemented data resources, business intelligence assets, custom attribute definitions, contract libraries, logical and physical data model assets, and other assets that are shared by suite tools. These assets are stored in the metadata repository of IBM InfoSphere Information Server.
Common metadata asset types and identity strings for the command line

You specify the identity strings of common metadata assets when you export, query, or delete the assets by using the command line.

The following sections describe common metadata assets and the identity strings that are used on the command line:

- Implemented data resources
- Physical data model assets
- Business intelligence assets
- Logical data model assets
- Custom attribute definitions
- Miscellaneous common metadata assets

Implemented data resources

You can exchange the following implemented data resource assets between IBM InfoSphere Information Server repositories. You can also query and delete the assets by using the command line.

Host
A computer where a database or data file exists.

Database
A relational storage collection that is organized by database schemas and procedures. A database stores data that is represented by tables.

Database schema
A named collection of related database tables and integrity constraints. A schema defines all or a subset of the data that is in a database. A database schema can implement logical data models and physical data models.

Database table
A structure for representing and storing data objects in a database. A database table can implement logical entities or design tables.

Stored procedure
A procedure that is defined and stored within a database to retrieve or manipulate data in that database, or to enforce constraints. Stored procedures can implement design stored procedures.

Data file
An information asset that represents a collection of fields that is stored in a single file. This asset could be a sequential file (a flat file that has no hierarchical structure) or a complex flat file (a file that has hierarchical structure). Examples of complex flat files include COBOL copybooks and XML files. A data file can implement physical data models.

Data file structure
A collection of related fields in a data file. A data file structure is the file equivalent of a database table. A data file structure can implement design tables.

Data item definition
An information asset that represents user-defined types and intermediate elements in the hierarchy of complex data structures. Examples are COBOL structured fields, SAP intermediate segments in IDoc structures, and XML type structures.
**Database domain**

A user-defined datatype that is contained by a database schema. Database domains can implement design domains and logical domains.

The assets beneath the host are hierarchical. Importing or exporting host assets affects only the host asset. Contained objects must be dealt with separately. Importing or exporting other assets automatically includes all the contained assets. Assets contain other assets as described in the following list:

- Databases include all the schemas in the database
- Database schemas include all the sub-schemas, views, tables, stored procedures, and foreign keys that the schema contains
- Database tables include database columns
- Data files include data file structures
- Data file structures include data file fields

The assets are identified by identity strings and are listed in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>/host_name.hst</td>
</tr>
<tr>
<td>Database</td>
<td>/host_name/database_name.db</td>
</tr>
<tr>
<td>Database schema</td>
<td>/host_name/database_name/schema_name/[</td>
</tr>
<tr>
<td>Database table</td>
<td>/host_name/database_name/schema_name/</td>
</tr>
<tr>
<td>Stored procedure</td>
<td>/host_name/database_name/schema_name/[</td>
</tr>
<tr>
<td>Data file</td>
<td>/host_name/datafile_path/datafile_name.fl</td>
</tr>
<tr>
<td>Data file structure</td>
<td>host_name/datafile_path/datafile_name/dfstructure_name.dcl</td>
</tr>
<tr>
<td>Data item definition</td>
<td>/data_item_def_qualifier/data_item_def_name.did</td>
</tr>
<tr>
<td>Database domain</td>
<td>/host_name/database_name/schema_name/[</td>
</tr>
</tbody>
</table>

If any asset names in the identity string contain space characters, the asset string must be enclosed in double quote characters ("'). The asterisk character (*) in the identity strings column indicates that the containment relationship can be recursive.

**Physical data model assets**

A physical data model is a design schema for information assets that defines the physical structures and relationships of data within a subject domain or application. Physical data models are independent of implementation or platform details.

You can exchange the following physical data model assets between IBM InfoSphere Information Server repositories:

**Physical data model**

A design schema for information assets that defines the physical structures and relationships of data within a subject domain or application. A physical data model can implement a logical data model and can be implemented by a database schema or a data file.
Design table
An asset that represents a table structure in the physical data model. The design table defines the design column, the design candidate key, and the design foreign key. A design table can implement a logical entity and can be implemented by a database table or data file structure.

Design stored procedure
An asset that represents the stored procedure structure in the physical data model. The design stored procedure also defines the design stored procedure parameters. A design stored procedure can be implemented by a stored procedure.

Physical domain
A user-defined data type or global attribute that can be reused in multiple design tables. A physical domain can implement a logical domain and can be implemented by a database domain.

The assets are identified by identity strings as listed in the following table.

Table 49. Physical data model assets and identity strings

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical data model</td>
<td>Design table, design stored procedure, and physical domain</td>
<td>/model_namespace/model_name.pm</td>
</tr>
<tr>
<td>Design table</td>
<td>Design column, design candidate key, and design foreign key</td>
<td>/model_namespace/model_name/table_name.dtl</td>
</tr>
<tr>
<td>Design stored procedure</td>
<td>Design stored procedure parameter</td>
<td>/model_namespace/model_name/procedure_name.dp</td>
</tr>
<tr>
<td>Physical domain</td>
<td></td>
<td>/model_namespace/model_name/data_item_def_qualifier/data_item_def_name.pdd</td>
</tr>
</tbody>
</table>

Business intelligence assets

Business intelligence assets comprise the objects that have been imported into the InfoSphere Information Server metadata repository from business intelligence tools.

You can exchange the following business intelligence assets between IBM InfoSphere Information Server repositories. You can also query and delete them by using the command line.

BI model
A grouping of BI data collection views that are relevant to a BI application.

BI collection
A data structure that provides a view of data that is stored in databases and files. In dimensional modeling, these structures are known as dimensions and fact tables. BI collections are the data sources of BI reports.

Cube
A subset of a BI model that consists of a set of related analytic values that share the same dimensionality.

BI report
A business intelligence report that is based on information in a database or a BI model.
BI report section
An asset that defines the presentation of a section of a BI report. A BI report section is a grouping of BI report fields.

BI report query
A query on a database or a BI model whose result set populates a BI report section.

BI server
When a BI tool supports multiple servers on a single host computer, the BI server value is the name of the source tool server. When a BI tool supports a single server per host computer, the BI server value is the name or IP address of the host system.

BI folder
The folder structure that contains BI models, or BI reports, or both in the source tool. BI folders can also contain other BI folders.

The assets are identified by identity strings as listed in the following table. An asterisk (*) indicates the possibility of recursive containment for BI folders.

Note: Identity strings for BI assets were changed at Version 9.1 of InfoSphere Information Server. If you upgraded from a previous version, be sure to rewrite any existing scripts that use identity strings for BI assets.

Table 50. Business intelligence assets and identity strings

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI model</td>
<td>Dimensions, collections, joins, hierarchies, and cubes</td>
<td>/bi_server_name/bi_folder_name[[/bi_folder_name]*]/model_name.omm</td>
</tr>
<tr>
<td>BI collection</td>
<td>Members, levels, and hierarchies</td>
<td>/bi_server_name/bi_folder_name[[/bi_folder_name]*]/model_name/collection_namespace/collection_name.ocl</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This string selects top-level BI collections only. When you export or delete a top-level collection, any subcollections that are contained in the top-level collection are also exported or deleted.</td>
</tr>
<tr>
<td>Cube</td>
<td>Dimensions and measures</td>
<td>/bi_server_name/bi_folder_name[[/bi_folder_name]*]/model_name/cube_namespace/cube_name.ocb</td>
</tr>
<tr>
<td>BI report</td>
<td>Report queries and report sections</td>
<td>/bi_server_name/bi_folder_name[[/bi_folder_name]*]/report_name.rdf</td>
</tr>
<tr>
<td>BI report section</td>
<td>BI report fields</td>
<td>/bi_server_name/bi_folder_name[[/bi_folder_name]*]/report_name/report_section_namespace/report_section_name.rg</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This string selects top-level BI report sections only. When you export or delete a top-level BI report section, any BI report sections that are contained in the top-level BI report section are also exported or deleted.</td>
</tr>
<tr>
<td>BI report query</td>
<td>Query items</td>
<td>/bi_server_name/bi_folder_name[[/bi_folder_name]*]/report_name/report_query_namespace/report_query_name.rds</td>
</tr>
<tr>
<td>BI server</td>
<td>BI folder</td>
<td>/bi_server_name.srv.</td>
</tr>
</tbody>
</table>
Logical data model assets

Logical data model assets comprise the set of related entities and their business associations that have been imported into the InfoSphere Information Server metadata repository.

You can exchange the following logical data model assets between IBM InfoSphere Information Server repositories:

Logical data model
A logical representation of the data objects that are related to a business domain and the rules or constraints that govern their associations in real-world applications. Logical data models consist of a set of entities and relationships. A logical data model can be implemented by physical data models or a database schemas.

Logical entity
An asset that represents the data structure in the logical data model. A logical entity defines entity attributes, entity keys, and entity constraints. A logical entity can be implemented by a design table by physical models or by database tables.

Logical relationship
An asset that represents the set of business rules that define the associations between two logical entities. A logical relationship can be implemented by a design foreign keys and foreign keys for a database table.

Entity generalization hierarchy
An asset that represents the inheritance associations that classify logical entities into subtypes and supertypes. A hierarchy supertype is a logical entity that is the supertype or parent entity in the hierarchy.

Logical domain
A user-defined data type or global attribute that can be reused in multiple logical entities. A logical domain can be implemented by physical domains and database domains.

Subject area
A grouping of related logical entities that focus on a particular business area. A logical entity can be included in more than one subject area to better differentiate it from other logical entities in the logical data model. Subject areas can be represented graphically in subject area diagrams.

Diagram
A graphical representation of a logical data model or a subject area.

The assets are identified by identity strings as listed in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI folder</td>
<td>BI folder, BI model, and BI report</td>
<td>/bi_server_name/bi_folder_name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[[/bi_folder_name]*].fld</td>
</tr>
</tbody>
</table>
Table 51. Logical data model assets and identity strings

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical data model</td>
<td>Diagram, subject area, logical entity, logical relationship, entity generalization hierarchy, logical domain</td>
<td>/model_namespace/model_name/ [nested_model_name]*/lm</td>
</tr>
<tr>
<td></td>
<td>Note: Logical data models can also contain submodels.</td>
<td></td>
</tr>
<tr>
<td>Logical entity</td>
<td>Entity attribute, entity key, entity constraint</td>
<td>/model_namespace/model_name/ [nested_model_name]*/ent</td>
</tr>
<tr>
<td>Logical relationship</td>
<td>Relationship end</td>
<td>/entity_model_namespace/entity_model_name/ [nested_model_name]<em>/entity_name/relationship_model_namespace/relationship_model_name/ [nested_model_name]</em>/relationship_name.rel</td>
</tr>
<tr>
<td>Entity generalization hierarchy</td>
<td>Hierarchy supertype, hierarchy subtype</td>
<td>/entity_model_namespace/entity_model_name/ [nested_model_name]<em>/entity_name/ generalization_model_namespace/generalization_model_name/ [nested_model_name]</em>/generalization_name.gen</td>
</tr>
<tr>
<td>Logical domain</td>
<td></td>
<td>/model_namespace/model_name/ [nested_model_name]*/domain_nameQualifier/doma ndName.dom</td>
</tr>
<tr>
<td>Subject area</td>
<td>A subject area can include but does not contain logical entities, logical relationships, and entity generalization hierarchies. Deleting the subject area does not delete assets of these types. A subject area can contain a diagram.</td>
<td>/model_namespace/model_name/ [nested_model_name]*/subjectArea_name.sa</td>
</tr>
<tr>
<td>Logical model diagram</td>
<td></td>
<td>/model_namespace/model_name/ [nested_model_name]*/diagram_name.ldg</td>
</tr>
<tr>
<td>Subject area diagram</td>
<td></td>
<td>/model_namespace/model_name/ [nested_model_name]*/subject_area_name/diagram_name.sdg</td>
</tr>
</tbody>
</table>

The asterisk character (*) in the identity strings column indicates that the containment relationship can be recursive.

**Custom attributes**

You can use the istool export command with the -ca option to transfer custom attributes that are in the metadata repository to a different metadata repository. The exceptions are custom attributes for categories and terms, which can be transferred only by using the import and export functionality and istool commands of InfoSphere Business Glossary. The custom attribute values are not transferred.
**Custom attributes**

Properties that you create to use with implemented data resources, logical data resources, extended data resources, and mappings. You create custom attributes when the standard properties such as name and description are insufficient or do not meet your business needs. Custom attributes are created in suite tools as properties of various types of assets. When you export common metadata, custom attributes and their values are automatically exported with the metadata.

You cannot export, delete, or query individual custom attribute definitions. All of the custom attribute definitions in the metadata repository are exported, deleted, or queried when you use istool command line. The assets are identified by identity strings as listed in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom attribute definitions</td>
<td>/<em>//</em>.cd</td>
</tr>
</tbody>
</table>

**Miscellaneous common metadata assets**

You can exchange the following miscellaneous assets between IBM InfoSphere Information Server repositories:

**Data connection**

A connection for accessing a database or file. For example, an ODBC or Oracle connection.

**Contract library**

A group of related XML schemas that are imported and used by the InfoSphere DataStage XML stage to transform data.

The assets are identified by identity strings as listed in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Identity string for command line</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data connection</td>
<td>/host_name/database_name/connection_name.dcn</td>
</tr>
<tr>
<td>Data file connection</td>
<td>/host_name/datafile_path/datafile_name/connection_name.fcn</td>
</tr>
<tr>
<td>Contract library</td>
<td>/contractlibrary_name.cl</td>
</tr>
</tbody>
</table>

**Wildcards and special characters in identity strings**

Use wildcards and special characters carefully when you specify identity strings for common metadata assets.

Each common metadata assets that is stored in the metadata repository has a unique identity string that can be used for command-line actions such as exporting and querying. For example, the identity string for a business intelligence (BI) model is /model_namespace/model_name.oml

An identity string for the istool command line consists of multiple *components* that combine to form a unique identity, plus an extension that is unique to the asset type. For example, the command-line identity string for a BI model contains the following elements:
• Namespace component. The namespace of the BI model, which is usually a folder structure separated by backward slashes.

• Name component. The name of the BI model.

• Extension .oml.

Every command-line identity string contains forward slashes at the beginning of each component, but not before the extension.

**Rules for handling wildcards and special characters**

The following rules apply to wildcards and special characters that appear in the identity strings of common metadata assets:

- You can use the wildcard characters asterisk (*) and exclamation point (!) in identity strings. The asterisk wildcard character represents 0 or more characters. The exclamation point wildcard character represents exactly one character. For example, `/Model\Space/Model!.oml` selects the models Model1, Model2, and Model5, but not Model22.

- If a component of the identity string contains asterisks or exclamation points that are not intended as wildcards but are part of the actual name, each asterisk or exclamation point must be preceded by two backward slash characters (\\). For example, if the host name is myhost and the database name is Data\base, then the identity string must be written as `/myhost/Data\\!base.db`

- If a component of the identity string contains a forward slash character (/) as part of the component name, then the forward slash must be preceded by two backward slash characters (\\). For example, if the host name is myhost and the database name is data/base, then the identity string must be written as `/myhost/data\\/base.db`

- If a component of the identity string contains a backward slash character (\) as part of the component name, then add one additional backward slash (\) character. For example, if the host name is myhost and the database name is data\base, then the identity string must be written as `/myhost/data\\\base.db`

- If a component of an identity string ends with a backward slash character (\), then add two backward slash (\) characters at the end of the component in addition to the one additional backward slash character that was indicated in the previous sentence. Alternatively, you can add the asterisk (*) character at the end of the component. The two extra backward slashes are not required for the final component in the identity string.

Examples:
- The identity string of the host system with the name Host\ is written as `/Host\\.hst` because the host name is the final component in the identity string.
- The identity string of the database database, which is contained by the host system with the name Host\, is written as `/Host\\\\/database.db`.

**Example of handling backward slashes**

The BI model the namespace is `192.168.62.131\Public Folders\Executive Insight\Overall\Reports\BI\BI 2011-03-21T21:34:41.692Z\`

The BI model name is P1\`

To construct the command-line identity string, you take the following steps:
1. Add a forward slash at the beginning of each component:
   /192.168.62.131\Public Folders\Executive Insight\Overall\Reports\BI\BI 2011-03-21T21:34:41.692Z\P1\n
2. Add the extension .oml:
   /192.168.62.131\Public Folders\Executive Insight\Overall\Reports\BI\BI 2011-03-21T21:34:41.692Z\P1\.oml

3. Add a backward slash to every backward slash in each component:
   /192.168.62.131]\Public Folders\Executive Insight\Overall\Reports\BI\BI 2011-03-21T21:34:41.692Z\P1\.oml

4. Add two backward slashes to any backward slash that ends a component, except for the last component:
   /192.168.62.131]\Public Folders\Executive Insight\Overall\Reports\BI\BI 2011-03-21T21:34:41.692Z\\P1\.oml

   In the example, two additional backward slashes are added at the end of the namespace component. The two additional backward slashes are not necessary after the name component because it is the final component in the identity string.

The following command exports the BI model to an archive file:

```
istool export -dom is -server.ibm.com:9080 -username <userName> -password <pw> -archive cognosAssets.isx -cm '/192.168.62.131]\Public Folders\Executive Insight\Overall\Reports\BI\BI 2011-03-21T21:34:41.692Z\\P1\.oml'
```

**Importing and exporting common metadata assets by using the command line**

You can import and export common metadata assets such as implemented data resources, business intelligence assets, logical data model assets, physical data model assets, custom attribute definitions, and contract library assets that are stored in the InfoSphere Information Server metadata repository.

**Export command for common metadata assets**

You can export most types of common metadata assets by using the istool export command with the `-cm` parameter.

By using the `-cm` or `-commonmetadata` parameter you can export the following types of assets:

- Implemented data resources
- Business intelligence (BI) assets
- Physical data model assets
- Data connections
- Contract libraries

When you export common metadata assets, any custom attributes and values that are associated with them are also exported. For the full list of assets that you can export by using the -cm parameter, see the topic [Asset types and identity strings](#)

To export logical data model assets, see [Export command for logical data model assets](#)

To export all custom attribute definitions in the repository without their values, see [http://www.ibm.com/support/docview.wss?uid=swg27022191](http://www.ibm.com/support/docview.wss?uid=swg27022191)

The export creates an archive file, which by default has the suffix .isx.

You must have the Suite User role.
Command syntax for implemented data resource assets, business intelligence assets, physical data model assets, and miscellaneous common metadata assets

```
istool export
authentication parameters
[generic parameters]
-archive "pathname" [-updatearchive]
[-AbortIfError number_of_errors]
[-preview]
-commonmetadata ['-base "path"] identity_string...
  [-contactAssignmentOnly]
  [-includeContactAssignment]
  [-includeAnnotation]
  [-includeDataConnection]
  [-creationtoolonly]

Note: The following parameters cannot be used when exporting contract library assets:
  [-contactAssignmentOnly]
  [-includeContactAssignment]
  [-includeAnnotation]
  [-includeDataConnection]
  [-creationtoolonly]

Parameters

authentication
All asset interchange commands use authentication parameters to connect to a specific installation of InfoSphere Information Server.

generic parameters
The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

-arch "path_name" or -ar "path_name"
  Specifies the path name for the file that the assets are exported to.

-updatearchive or -up
  Updates the archive file if it exists (otherwise it is overwritten if it exists).

-AbortIfError number_of_errors or -abort number_of_errors
  Stops the export after the specified number of errors.

-preview or -pre
  Previews the export. The preview lists the assets that will be exported when the export runs.

-commonmetadata identity_string or -cm identity_string
  Specifies that common metadata assets are exported. Specifies the identity string of each asset to export. The format for the identity string is described in Common metadata asset types and identity strings for the command line. If you specify more than one identity string, the identity strings and associated options must be enclosed in single quotation marks ('). To be exported, an asset must have a name and a complete identity string.

-contactAssignment or -incca
  Includes the contact assignments for the exported assets. A contact assignment connects an asset to the person or group who is a contact or steward for the asset. For example, when a database table has a steward, a contact assignment is used to connect the table to the steward.
Stewards are created in InfoSphere Business Glossary. A steward is a user or user group in InfoSphere Information Server. Contacts are created in InfoSphere Information Analyzer. Contacts are people or groups who are not required to have an InfoSphere Information Server login.

When imported to a target system with assets, contact assignments are relinked to the people or groups that they connect, if those people and groups exist in the target repository at the time of import.

-includeAnnotation or -incannot
  Includes the annotations for the exported assets.

-includeDataConnection
  Includes the data connections that are associated with the exported database tables, data files, and stored procedures.

-contactAssignmentOnly or -caonly
  Exports only the contact assignments that are associated with the specified assets, not the assets themselves.
  When imported to a target system, the contact assignments are relinked to the assets, people, or groups that they connect, if those assets, people, or groups exist in the target repository at the time of import.

-base "path"
  Specifies a base path. This path is then prefixed to all the asset identity strings that you specify.

-creationtoolonly or -ctonly
  Exports only the creation tools that are associated with the specified assets, not the assets themselves. A creation tool is the tool, such as a bridge or connector, that is used for importing assets into the metadata repository.

Exit status

A return value of 0 indicates successful completion; any other value indicates failure.

Examples

The following command exports all the tables and associated annotations in the database schema named schema1 to the file myarchive.isx.

    istool export –dom ABC:9080 –username user1 –password pass1
                    –archive "c:\myarchive.isx"
                    –commonmetadata '/host1/db1/schema1/*.tbl
                    -includeAnnotation'

The following command exports all the contact assignments associated to all the tables in the database schema named schema1 to the file myarchive.isx.

    istool export –dom ABC:9080 –u user1 –p pass1
                 -ar "c:\myarchive.isx"
                 -cm '/host1/db1/schema1/*.tbl
                 -contactAssignmentOnly'

The following command exports the specified hosts to the file myarchive.isx.

    istool export –dom ABC:9080 –u user1 –p pass1
                 -ar "c:\myarchive.isx"
                 -cm '/host1.hst /host2.hst'
The following command specifies a base path of /host1/db1/schema1 and uses the base path when specifying tables to export to the file myarchive.isx:

```
istool export –dom ABC:9080 –u user1 –p pass1
-ar "c:\myarchive.isx"
-cm '–base "/host1/db1/schema1" tab1.tbl
    tab2.tbl tab506.tbl'
```

The following command exports all the BI report queries in all BI reports within a specified BI folder and BI server:

```
istool export –dom ABC:9080 –u user1 –p pass1
-ar "c:\myarchive.isx"
-cm '/bi_server_name/bi_folder_name/*/*/*.rds'
```

The following command exports a BI report of a specified name in a specified subfolder of a specified BI folder in a specified BI server:

```
istool export -dom ABC:9080 -u user1 -p pass1
-ar "c:\myarchive.isx"
-cm '/bi_server_name/bi_folder_name/bi_folder_name/report_name.rdf'
```

The following command uses the -base option to specify a base path for the asset identity string that specifies the assets to export:

```
istool export –dom ABC:9080 –u user1 –p pass1
-ar "c:\myarchive.isx"
-cm '-base "/bi_server_name/bi_folder_name/model_name/collection_namespace" collection_name01.ocl collection_name02.ocl'
```

The following command exports all the design tables in the physical data model with name physicalmodel1 and namespace namespace1 to the file myarchive.isx:

```
istool export –dom ABC:9080 –username user1 –password pass1
-archive "c:\myarchive.isx"
-commonmetadata '/namespace1/physicalmodel1/*.dtl'
```

The following command exports all the design tables and design stored procedures in the physical data model with name physicalmodel1 and namespace namespace1 to the file myarchive.isx:

```
istool export –dom ABC:9080 –username user1 –password pass1
-archive "c:\myarchive.isx"
-commonmetadata '-base "/namespace1/physicalmodel1" *.dtl *.dp'
```

**Export command for logical data model assets:**

You can use the istool export command with the -lm parameter to export logical data model assets.

For the full list of logical data model assets that you can export, see the topic "Common metadata asset types and identity strings for the command line" on page 299. When you export logical data model assets, any custom attributes and custom attribute values that have been created for the logical data model assets are also exported.

The export creates an archive file, which by default has the suffix .isx.

You must have the Suite User role.

**Command syntax for logical data model assets**

```
istool export
authentication parameters
[generic parameters]
```
Parameters

/authentication

All asset interchange commands use authentication parameters to connect to a specific installation of InfoSphere Information Server.

generic parameters

The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

/archive "pathname" [-updatearchive]

.specifies the path name for the file that the assets are exported to.

/updatearchive or -up

Updates the archive file if it exists (otherwise it is overwritten if it exists).

/AbortIfError number_of_errors or -abort number_of_errors

Stops the export after the specified number of errors.

/preview or -pre

Previews the export. The preview lists the assets that will be exported when the export runs.

/logicalmetadata identity_string or -lm identity_string

Specifies that logical data model assets are exported. Specifies the identity string of each asset to export. The format for the identity string is described in Common metadata asset types and identity strings for the command line. If you specify more than one identity string, the identity strings and associated options must be enclosed in single quotation marks ('). To be exported, an asset must have a name and a complete identity string.

/includeContactAssignment or -incca

Includes the contact assignments for the exported assets. A contact assignment connects an asset to the person or group who is a contact or steward for the asset. For example, when a database table has a steward, a contact assignment is used to connect the table to the steward.

Stewards are created in InfoSphere Business Glossary. A steward is a user or user group in InfoSphere Information Server. Contacts are created in InfoSphere Information Analyzer. Contacts are people or groups who are not required to have an InfoSphere Information Server login.

When imported to a target system with assets, contact assignments are relinked to the people or groups that they connect, if those people and groups exist in the target repository at the time of import.

/includeAnnotation or -incannot

Includes the annotations for the exported assets.

/contactAssignmentOnly or -caonly

Exports only the contact assignments that are associated with the specified assets, not the assets themselves.
When imported to a target system, the contact assignments are relinked to the
assets, people, or groups that they connect, if those assets, people, or groups
exist in the target repository at the time of import.

-base "path"
Specifies a base path. This path is then prefixed to all the asset identity strings
that you specify.

-creationtoolonly or -ctonly
Exports only the creation tools that are associated with the specified assets, not
the assets themselves. A creation tool is the tool, such as a bridge or broker,
that is used for importing assets into the metadata repository.

Exit status

A return value of 0 indicates successful completion; any other value indicates
failure.

Examples

The following command exports all the entities and associated annotations in the
logical data model named model1 and namespace namespace1 to the file
myarchive.isx:

istool export –dom ABC:9080 –username user1 –password pass1
–archive "c:\myarchive.isx"
–logicalmetadata '/namespace1/model1.lm -includeAnnotation'

The following command exports all the contact assignments associated to all the
entities in the logical data model named model1 to the file myarchive.isx:

istool export –dom ABC:9080 –u user1 –p pass1
–ar "c:\myarchive.isx"
–lm '/*/model1.lm -contactAssignmentOnly'

The following command exports the specified logical data models to the file
myarchive.isx:

istool export –dom ABC:9080 –u user1 –p pass1
–ar "c:\myarchive.isx"
–lm '/namespace1/model1.lm /namespace1/model1/nestedModel2.lm'

The following command specifies a base path of /namespace1/model1/
nestedModel2 and uses the base path when specifying entities and logical domains
to export to the file myarchive.isx:

istool export –dom ABC:9080 –u user1 –p pass1
–ar "c:\myarchive.isx"
–lm '-base '/namespace1/model1/nestedModel2 "entity1.ent
nameQualifier/domain1.dom'

The following command exports the logical relationship identified by the asset
identity string '/namespace1/model1/entity1/namespace1/model1/
relationship1.rel':

istool export –dom ABC:9080 –u user1 –p pass1
–ar "c:\myarchive.isx"
–lm '/namespace1/model1/entity1/namespace1/model1/relationship1.rel '

Export command for custom attributes:

You can use the istool export command with the -ca parameter to export custom
attributes.
For the full list of assets that you can export, see the topic “Common metadata asset types and identity strings for the command line” on page 299.

Custom attributes can be exported two ways:

- The istool export command with the -ca parameter exports all custom attributes in the metadata repository. The only custom attributes that are not exported are custom attributes for InfoSphere Business Glossary categories and terms. The assets that the custom attributes are associated with are not exported.

- The istool export command exports custom attributes that are exported if they are associated with an implemented data resource that is being exported. For example, if you a table has a custom attribute associated with it, then the table and the custom attribute will be exported.

The export creates an archive file, which by default has the suffix .isx.

You must have the Suite User role.

**Command syntax for custom attributes**

```
istool export
authentication parameters
[general parameters]
-archive "pathname" [-updatearchive]
[-AbortIfError number_of_errors]
[-preview]
-customattributes '[-base "path"] identity_string...
```

**Parameters**

**authentication**

All asset interchange commands use authentication parameters to connect to a specific IBM InfoSphere Information Server.

**general parameters**

The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

```
-archive "path_name" or -ar "path_name"
  Specifies the path name for the file that the assets are exported to.

-updatearchive or -up
  Updates the archive file if it exists (otherwise it is overwritten if it exists).

-AbortIfError number_of_errors or -abort number_of_errors
  Stops the export after the specified number of errors.

-preview or -pre
  Previews the export. The preview lists the assets that will be exported when the export runs.

-customattributes identity_string or -ca identity_string
  Specifies that all custom attributes are exported. Specifies the identity string of each asset to export. The format for the identity string is described in Common metadata asset types and identity strings for the command line. If you specify more than one identity string, the identity strings and associated options must be enclosed in single quotation marks ('). To be exported, an asset must have a name and a complete identity string.
```
-base "path"
  Specifies a base path. This path is then prefixed to all the asset identity strings that you specify.

Exit status

A return value of 0 indicates successful completion; any other value indicates failure.

Example

The following command exports all custom attributes in the repository to the file myarchive.isx.

istool export –dom ABC:9080 –username user1 –password pass1
  -archive "c:\myarchive.isx"
  –customattributes ‘/*/*/*.cd’

Import command for common metadata assets

You can import most types of common metadata assets by using the istool import command with the -cm parameter.

By using the -cm or -commonmetadata parameter you can import the following types of assets:

  • Implemented data resources
  • Business intelligence (BI) assets
  • Physical data model assets
  • Data connections
  • Contract libraries

For the full list of assets that you can import by using the -cm parameter, see the topic "Common metadata asset types and identity strings for the command line" on page 299.

To import logical data model assets see "Import command for logical data model assets" on page 315.

To import custom attributes see http://www.ibm.com/support/docview.wss?uid=swg27022191

If you specify the -replace parameter, and a common metadata asset exists in the target metadata repository, then the imported asset is merged with the existing asset.

You import the assets from an archive file that has the .isx extension.

You must have the Common Metadata Administrator role.

Command syntax for implemented data resource assets, business intelligence assets, physical data model assets, and miscellaneous common metadata assets

  istool import
  authentication parameters
  [generic parameters]
Parameters

authentication

All asset interchange commands use authentication parameters to connect to a specific installation of IBM InfoSphere Information Server.

generic parameters

The generic parameters are available to all asset interchange commands. Use the generic parameter to request help on command syntax, or to specify silent or verbose operation.

-AbortAfter number_of_errors or -abort number_of_errors

Specifies that the import stops if more than the specified number of errors occur.

-commonmetadata or -cm

Specifies that common metadata assets are imported. All common metadata assets in the file are imported when you use this parameter, except for logical data model assets, which require the parameter -lm. The parameter must be followed by two single quotation marks ('), for example, -cm ''. 

-archive path_name or -ar path_name

Specifies the path name of the file that the assets were previously exported to.

-preview or -pre

Previews the import. The preview lists the assets that will be imported when the import runs.

-replace

Replaces existing common metadata assets with imported assets.

Exit status

A return value of 0 indicates successful completion, any other value indicates failure.

Example

The following command imports all common metadata assets, except logical data model assets, from the file customer.isx:

```plaintext
istool import –dom ABC:9080 –u user1 –p pass1
-archive "c:\customer.isx" –commonmetadata ''
```

Import command for logical data model assets:

You can use the istool import command with the -lm parameter to import logical data model assets.

For the full list of logical data model assets that you can export, see the topic "Common metadata asset types and identity strings for the command line" on page 299.

You import the assets from an archive file that has the .isx extension.

You must have the Common Metadata Administrator role.
Note: Because of a model change, you cannot import logical data models from archive files that were exported from InfoSphere Information Server, Version 8.7. If you used the migration tool to migrate the contents of the metadata repository from Version 8.7 to InfoSphere Information Server, Version 9.1, all logical models that were in the metadata repository at the time of migration are correctly updated. Alternately, you can use InfoSphere Metadata Asset Manager to import the logical model from the source tool.

Command syntax for logical data model assets

istool import
authentication parameters
[generic parameters]
[-AbortAfter number_of_errors]
-archive "pathname"
[-preview | -replace]
-logicalmetadata ' '  

Parameters

authentication
    All asset interchange commands use authentication parameters to connect to a specific installation of InfoSphere Information Server.

generic parameters
    The generic parameters are available to all asset interchange commands. Use the generic parameter to request help on command syntax, or to specify silent or verbose operation.

-AbortAfter number_of_errors or -abort number_of_errors
    Specifies that the import stops if more than the specified number of errors occur.

-logicalmetadata or -lm
    Specifies that logical data model assets are imported.

-archive path_name or -ar path_name
    Specifies the path name of the file that the assets were previously exported to.

-preview or -pre
    Previews the import. The preview lists the assets that will be imported when the import runs.

-replace
    Replaces existing logical data model assets with the imported assets.

Exit status

A return value of 0 indicates successful completion, any other value indicates failure.

Example

The following command imports all the logical data model assets from the file customer.isx:

```
istool import -dom ABC:9080 -u user1 -p pass1
-archive "c:\customer.isx" -logicalmetadata ''
```

The following command previews the assets in the file customer.isx:

```
istool import -dom ABC:9080 -u user1 -p pass1 -pre
-ar "c:\customer.isx" -lm ''
```
Import command for custom attributes:

You can use the istool import command with the -ca parameter to import custom attributes.

For the full list of custom attributes that you can import, see the topic “Common metadata asset types and identity strings for the command line” on page 299.

Custom attributes can be imported two ways:

- The istool import command with the -ca parameter imports all custom attributes in the metadata repository. The only custom attributes that are not imported are custom attributes for InfoSphere Business Glossary categories and terms. The assets that the custom attributes are associated with are not imported.
- The istool import command imports custom attributes that are imported if they are associated with an implemented data resource that is being imported. For example, if you have a table that has a custom attribute associated with it, then the table and the custom attribute will be imported.

You import the assets from an archive file that has the .isx extension.

You must have the Common Metadata Administrator role.

Command syntax for custom attributes

```
istool import
authentication parameters
[generic parameters]
[-AbortAfter number_of_errors]
-archive "pathname"
[-preview] [-replace]
--customattributes ''
```

Parameters

**authentication**

All asset interchange commands use authentication parameters to connect to a specific InfoSphere Information Server.

**generic parameters**

The generic parameters are available to all asset interchange commands. Use the generic parameter to request help on command syntax, or to specify silent or verbose operation.

- **-AbortAfter number_of_errors or -abort number_of_errors**
  Specifies that the import stops if more than the specified number of errors occur.

- **-customattributes or -ca**
  Specifies that all custom attributes are imported.

- **-archive path_name or -ar path_name**
  Specifies the path name of the file that the assets were previously exported to.

- **-preview or -pre**
  Previews the import. The preview lists the assets that will be imported when the import runs.

- **-replace**
  Replaces existing custom attributes with the imported assets.
Exit status

A return value of 0 indicates successful completion, any other value indicates failure.

Example

The following command imports all the custom attributes from the file custom_attributes.isx:

istool import –dom ABC:9080 –u user1 –p pass1
-archive 'c:custom_attributes.isx' –customattributes ''

Querying and deleting assets by using the command line

You can query implemented data resources, business intelligence assets, physical data model assets, and data connections and delete them from the metadata repository by using the command line. You can also query and delete all types of common metadata assets by using the Repository Management tab in InfoSphere Metadata Asset Manager.

In order to delete an asset, you must specify the identity string of the asset. The identity string includes the following elements:

- Hierarchy of names of the assets that contain the asset to be deleted, separated by forward slashes (/)
- Name of the asset
- File extension for the asset, such as .tbl

For example, the identity string of a database table is /host_computer/database/schema/table.tbl. Therefore, the identity string of the Customer table in the Sales schema of the Production database on a computer named A341K is /A341K/Production/Sales/Customer.tbl.

When you want to delete multiple assets by using the command line, the most efficient way is to run the query command and write the results to a file. You can then specify the file as input to the deletecm command. The query results file includes the identity string and the repository ID (RID) of each asset that is listed. Both the identity string and the RID are required when you specify a file of assets that are to be deleted. Because you must run a query to obtain the RID, you must use a query to create the file.

If the query result contains an asset that does not have required attributes in the identity string, such as database name, “Invalid Identity” is written to the output in place of the identity string.

You can delete assets from the query results file, and add assets to it from other queries, as long as you include both the RID and the identity string of each asset.

When you have many implemented data resources in the repository, it might be more efficient to do successive queries. For example, you could first run a query to find all the schemas in the repository, and then run a second query on only those schemas that have database tables that you want to delete.

If you are deleting a small number of assets, you might want to specify the identity string of each asset on the command line instead of specifying a file. You do not specify the RID of the asset on the command line.
You can determine the identity string of an asset in the following ways:

- Run a command-line query to find the asset.
- In InfoSphere Metadata Asset Manager on the Repository Management tab, browse or search for assets and review properties in the **Properties** section.
- In IBM InfoSphere Metadata Workbench, browse the hosts on the **Browse** tab to find databases and data files. Search or query to find BI assets. When your cursor hovers over the name of an asset in a list, the names of the containing assets are displayed.
- In InfoSphere Business Glossary, search for a type of implemented data resource or BI asset. In the resulting list of assets, the **Context** column displays the elements of the identity string.

If the delete operation fails to delete one of the assets identified, then the entire delete operation is rolled back.

**Implemented data resources**

Implemented data resources comprise the database and data file metadata that is stored in the InfoSphere Information Server metadata repository.

You can delete the following implemented data resources from the IBM InfoSphere Information Server metadata repository:

- Host
- Database
- Database schema
- Database table
- Stored procedure
- Data file
- Data file structure
- Data connection
- Data item definition

Assets that are deleted when you delete implemented data resources are listed in the following table.

*Table 54. Implemented data resources and their contained assets*

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Data connections, databases and data files. Some hosts can also contain projects and jobs from InfoSphere DataStage and QualityStage. You can delete hosts only if they contain no database, data file, connector, or job assets.</td>
</tr>
<tr>
<td>Databases</td>
<td>Database schemas</td>
</tr>
<tr>
<td>Database schemas</td>
<td>Subschemas, views, tables, stored procedures, and foreign keys that the schema contains</td>
</tr>
<tr>
<td>Database tables</td>
<td>Database columns and primary keys</td>
</tr>
<tr>
<td>Stored procedures</td>
<td>Stored procedure parameters</td>
</tr>
<tr>
<td>Data files</td>
<td>Data file structures</td>
</tr>
<tr>
<td>Data file structures</td>
<td>Data file fields</td>
</tr>
<tr>
<td>Data connections</td>
<td>None</td>
</tr>
<tr>
<td>Data item definitions</td>
<td>Data file fields</td>
</tr>
</tbody>
</table>

Chapter 15. Managing assets by using the command line  319
Physical data model assets
A physical data model is a design schema for information assets that defines the physical structures and relationships of data within a subject domain or application. Physical data models are independent of implementation or platform details. Physical data model assets comprise the objects that have been imported into the InfoSphere Information Server metadata repository from data modeling tools.

You can delete the following physical data model assets from the metadata repository:
- Physical data model
- Design table
- Design stored procedure
- Physical domain

Assets that are deleted when you delete a physical data model asset are listed in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical data model</td>
<td>Design tables, design stored procedures, and physical domains</td>
</tr>
<tr>
<td>Design table</td>
<td>Design columns, design candidate keys, and design foreign keys</td>
</tr>
<tr>
<td>Design stored procedure</td>
<td>Design stored procedure parameters</td>
</tr>
<tr>
<td>Physical domain</td>
<td>None</td>
</tr>
</tbody>
</table>

Business intelligence assets
Business intelligence assets comprise the objects that have been imported into the InfoSphere Information Server metadata repository from business intelligence tools.

You can delete the following business intelligence (BI) assets from the metadata repository:
- BI model
- BI collection
- Cube
- BI report
- BI report section
- BI report query
- BI server
- BI folder

Assets that are deleted when you delete a business intelligence assets are listed in the following table.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI model</td>
<td>Dimensions, collections, joins, hierarchies, and cubes</td>
</tr>
<tr>
<td>BI collection</td>
<td>Members, levels, and hierarchies</td>
</tr>
<tr>
<td>Cube</td>
<td>Dimensions and measures</td>
</tr>
</tbody>
</table>
Table 56. Business intelligence assets and their contained assets (continued)

<table>
<thead>
<tr>
<th>Asset</th>
<th>Contained assets that are deleted with the asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI report</td>
<td>Report queries and report layout</td>
</tr>
<tr>
<td>BI report section</td>
<td>BI report fields</td>
</tr>
<tr>
<td>BI report query</td>
<td>Query items</td>
</tr>
<tr>
<td>BI server</td>
<td>BI folders</td>
</tr>
<tr>
<td>BI folder</td>
<td>BI folders, BI models, and BI reports</td>
</tr>
</tbody>
</table>

Query command for common metadata assets

Use the query command to get a list of implemented data resources, physical data model assets, business intelligence assets, and data connections that are stored in the metadata repository.

You can use the query command to get a list of assets. You can write this list to a file that you can then use to specify which assets to delete.

The query command has the following syntax:

```
istool query
authentication parameters
[...]
[-outputfile ["filename"]]
--commonmetadata ['-base "path"'] [identity_string...]+'
```

Parameters

authentication parameters

Use authentication parameters to connect to a specific installation of InfoSphere Information Server.

generic parameters

Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

-`-outputfile ["filename"]` or `-of ["filename"]`
  Specifies that the query results be written to a file. Filenames are automatically appended with the string `_commonmetadata`, for example, if you specify the filename `to_delete.txt`, the results are written to the file `to_delete_commonmetadata.txt`. If you do not specify a file name, the results are written to a file named `query_output_commonmetadata.txt` in the current directory. The results include the repository ID (RID) of each asset and the identity string of each asset. You can edit this file to remove assets from it before you delete.

  Note: The output file is not created if the file path has a period (.) in it in addition to the period before the file extension.

--`-commonmetadata` or `-cm`
  Specifies that common metadata assets are to be queried.

identity_string

Specifies individual assets to query. If you specify more than one identity string, then the identity strings and associated options must be enclosed in single quote characters ('). If you specify only one identity string, then the single quote characters are optional. The query command fails if you specify more than four tilde (~) characters in an identity string.
Note: If you specify both implemented data resources and business intelligence assets in a single query, you cannot use the resulting output file to delete the assets.

-base path
You can optionally use the -base argument to specify a base path. This path is then prefixed to all the asset identity strings that you specify.

Example

The following command writes a list of implemented data resources in the database db1 to the file c:\to_delete_commonmetadata.txt:

```
istool query –dom ABC:9080 –u xmetauser –p xmetapwd
-outputfile "c:\to_delete.txt"
–commonmetadata '/host1/db1.db'
```

The following command writes a list of BI reports whose names begin with “rep” to the file c:\to_delete_businessintelligence.txt:

```
istool query –dom ABC:9080 –u xmetauser –p xmetapwd
-outputfile "c:\to_delete.txt"
–cm '/bi_server1/bi_folder1/rep*.rdf'
```

The following command selects the tables that begin with “table” in schema schema1 and writes them to the file c:\to_delete_commonmetadata.txt:

```
istool query –dom ABC:9080 –u xmetauser –p xmetapwd
-outputfile "c:\to_delete.txt"
–commonmetadata '/host1/db/schema1/table*.tbl'
```

The following command queries what hosts, databases, and schemas the specified repository contains and writes the result to the file query_results_commonmetadata.txt:

```
istool query –dom ABC:9080 –u xmetauser –p xmetapwd
- cm '/*.hst /*/*.db /*/*/*.sch' -outputFile "C:\query_results.txt"
```

The following command writes the details of all the tables belonging to the database db1 to the file query_results2_commonmetadata.txt.

```
is tool query –dom ABC:9080 –u xmetauser –p xmetapwd
-cm '/hostname/db1/schema1/x.tbl' -outputFile "C:\query_results2.txt"
```

Delete command for common metadata assets

Use the istool deletecm command to delete implemented data resources, physical data model assets, business intelligence assets, and data connections from the metadata repository.

You must have the Common Metadata Administrator role to delete common metadata assets.

Before you delete the assets, you can use the query command to write a list of assets to a file. You can use the file as an input to the deletecm command to specify which assets to delete. Alternatively you can specify identity strings on the command line that identify individual assets to delete.

If you use a file as the input to the deletecm command, the file must include both the repository identifier (RID) of each asset and the identity string of each asset. The input file cannot include only the identity string. For this reason, you must use the query command with the -outputfile option to obtain a properly formatted file
that includes both the RID and the identity string. You can edit this file to remove
assets before you specify it as input to the `deletecm` command.

You cannot combine implemented data resources, business intelligence assets, and
physical data model assets in the same file.

You are prompted for confirmation before each asset is deleted. You can suppress
the confirmation message by specifying the `-force` option.

The `deletecm` command has the following syntax:

```
istool deletecm
authentication parameters
[generic parameters]
[-preview]
[-force]
[-inputfile "filename"]
-commonmetadata '-[base "path"] [identity_string...]'
```

**Parameters**

*authentication parameters*

All asset management commands use authentication parameters to connect to a
specific installation of InfoSphere Information Server.

*generic parameters*

The generic parameters are available to all asset management commands. Use
the generic parameter to request help on command syntax, or to specify silent
or verbose operation.

*preview or -pre*

Specify this option to see a preview of the deletion. The preview lists the RIDs
and the identity strings of the assets that will be deleted when you run the
deletecm command. You can use the preview option to ensure that the scope of
the deletion is what you expect. Use the force option to suppress the
confirmation prompts when you run a preview. Otherwise, the same
confirmation prompts for each asset are displayed as if you are running the
deletion. No assets are actually deleted by the preview option.

*force or -f*

Specify this option to suppress prompting for confirmation. The command
silently deletes assets without requesting confirmation. Otherwise, you are
prompted to confirm deletion of each individual asset.

*inputfile "filename" or -if "filename"*

Specify the -inputfile option with a file name to provide a list of assets to
delete. Create this file by running the query command with the -outputfile
option. If you specify an input file you cannot specify an identity string.

*commonmetadata or -cm*

Specifies that implemented data resources are to be deleted. If you specify an
input file instead of an identity string you must still specify this option.

*identity_string*

Specifies individual assets to delete or to preview. If you specify an identity
string, you cannot specify an input file. If you specify more than one identity
string, then the identity strings and associated options must be enclosed in
single quote characters ('). If you specify only one identity string, then the
single quote characters are optional.
**-base path**

You can optionally use the -base argument to specify a base path. This path is then prefixed to all the asset identity strings that you specify.

**Example**

The following command deletes all the implemented data resources listed in the file c:\to_delete_commonmetadata.txt:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd
-inputfile "c:\to_delete_commonmetadata.txt"
-cm ''
```

The following command deletes the table1 and table2 database tables in the databases db1 and db2:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd
-cm '/myhost/db1/schema1/table1.tbl /myhost/db2/schema1/table2.tbl'
```

The following command deletes the table7 and table8 database tables in the database db1:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd
-cm '-base "/myhost/db1/schema1" table7.tbl table8.tbl'
```

The following command previews a deletion operation that deletes two tables:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd -preview
-cm '/myhost/db1/schema1/table1.tbl /myhost/db2/schema1/table2.tbl'
```

The following command deletes the two tables that were previewed in the previous command:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd
-cm '/myHost/db1/schema1/table1.tbl /myhost/db2/schema1/table2.tbl'
```

The following command deletes the BI report queries that are contained by the BI report "bi_report1" in the specified BI folder and BI server:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd –cm
'/bi_server1/bi_folder_name1/bi_report1/*/.*.rds'
```

The following command uses the -base option to specify a base path for the asset identity string that specifies the assets to delete:

```
istool deletecm –dom ABC:9080 –u xmetauser –p xmetapwd –cm
'base="/bi_server1/bi_folder1/model_name2/collection_namespace1"
collection_name01.ocl collection_name02.ocl'
```

**Delete command for disconnected assets**

Use the istool deletecm command with the -orphanedNonSeeds parameter to delete assets in the metadata repository of IBM InfoSphere Information Server that are disconnected from their required containing assets, such as database tables that have no relationship to a database schema.

Disconnected assets do not have valid identities in the metadata repository and can cause errors when you use them in suite tools.

You must have the Common Metadata Administrator role to delete disconnected assets.

You can also delete disconnected assets by using the Repository Management tab of the IBM InfoSphere Information Server Web console.
Syntax

The `deletecm` command has the following syntax when it is used to delete disconnected assets:

```
istool deletecm
authentication parameters
[generic parameters]
-orphanedNonSeeds
```

Parameters

authentication parameters

All asset management commands use authentication parameters to connect to a specific installation of InfoSphere Information Server.

generic parameters

The generic parameters are available to all asset management commands. Use the generic parameter to request help on command syntax, or to specify silent or verbose operation.

-orphanedNonSeeds or -orphanedNS

Specify this option to delete all disconnected assets.

Example

The following command deletes the disconnected assets (non-seed objects), such as database columns that have no relationship to a database table:

```
istool deletecm -dom ABC:9080 -u xmetauser -p xmetapwd
-orphanedNonSeeds
```

Reporting assets

Reporting assets are designs for reports that are made in the IBM InfoSphere Information Server console.

You can interchange the designs for reports, and the results that were obtained from running the reports. The reports and associated results are exported from the source metadata repository to an archive file. The archive file has the suffix .isx.

You can specify the name of the report to export, or you can specify that the reports associated with a particular product are exported. The following products can have reports associated with them:

- InfoSphere DataStage
- InfoSphere Information Analyzer
- InfoSphere QualityStage
- Administration reports for the suite.

You can include the report results for a specific named report, include the reports results for the last \( n \) runs of that report, or include all the results for the specified reports.

Export command for reporting assets

You can use the istool command line interface (CLI) to export your IBM InfoSphere Information Server reporting assets. These assets can include both report designs and report results.
Purpose

The reporting asset interchange commands export reports from your InfoSphere Information Server installation. You can identify the reports to export by using the following methods:

- Export all the reports associated with a particular suite component. For example, you can export all your IBM InfoSphere Business Glossary reports.
- Export reports by name. You can specify wildcards as part of the report name.

You can also specify that the export includes the report results as well as the design details of a report.

To export a report or report results, you must have administration, read, and update permissions for that report. The creator of a report automatically has administration, read, and update permissions, and can grant permissions to other users or groups. A user with the Suite Administrator role can export any reports.

Command syntax

```
istool export
  [authentication]
  [generic parameters]
  -archive "pathname" [-updatearchive]
  [-AbortIfError number_of_errors]
  -report
  ["-reportName "report_name"
    [-ownedByProduct "product_name"]
    [-includeLastReportResults number |
     -IncludeAllReportResults]
    -IncludeReportResultName report_result_name]
  ]
  ["-ownedByProduct "product_name"
    [-reportName "report_name"]
    [-includeLastReportResults number |
     -IncludeAllReportResults]
    -IncludeReportResultName report_result_name]
```

Parameters

export
   The export command specifies an export operation.

authentication
   All asset interchange commands use authentication parameters to connect to a specific installation of InfoSphere Information Server installation.

generic parameters
   The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

-archive "pathname" or -ar "pathname"
   Specifies the path name for the file that the assets are exported to.

-updatearchive or -up
   Updates the archive file if it exists (otherwise it is overwritten if it exists).

-AbortIfError number_of_errors or -abort number_of_errors
   Stops the export if more than the specified number of errors occur.
-report
Specifies that report assets are exported.

-reportName "report_name" or -repName "report_name"
Exports reports by name. The argument report_name can include wildcard
characters. For example, the parameter:
   -reportName "MyRep*"

exports the reports MyRep1, MyRep2, and MyRepTues. If you specify this
parameter together with the -ownedByProduct parameter, reports that specify
both criteria are exported.

-ownedByProduct "product_name" or -prod "product_name"
Exports the reports that are associated with the specified suite component. If
you specify this parameter together with the -reportName parameter, reports
that satisfy both criteria are exported. Valid values for product_name are in the
following list:
   • "Administration"
   • "Business Glossary"
   • "DataStage"
   • "Information Analyzer"
   • "QualityStage"

-includeLastReportResults number or -incLastResult number
Exports the specified number of report results along with the report design
that you specified by using the reportName or prod parameters. For example,
the parameters:
   -reportName "MyRep1" -includeLastReportResults 20

export the report design for MyRep1 together with the 20 most recent results
for that report.

-includeAllReportResults or -incAllResults
Exports all results along with the report design that you specified by using the
-reportName or -prod parameters. For example, the parameters:
   -reportName "MyRep1" -includeAllReportResults

export the report design for MyRep1 together with all the results for that
report.

-includeReportResultName "report_name" or -incResultName "report_name"
Exports the most recent results for the report specified by report_name. You can
use wildcards in report_name to return results for a number of reports. For
example, the parameter:
   -includeReportResultName "MyRep*"

exports the most recent results for the reports MyRep1, MyRep2, and
MyRep15.

Exit status
A return value of 0 indicates successful completion; any other value indicates
failure.
Examples

This following command exports all the InfoSphere QualityStage reports on the qaqserv system to the archive, QSRAI_001.isx.

istool export -domain qaqserv:9080 -username user1 -password pass1 -archive "c:/QSRAI_001.isx" -report '-prod "QualityStage"'

The following command exports the report named FreqPat to the archive QSRAI_001.isx.

istool export -domain qaqserv:9080 -username user1 -password pass1 -archive "c:/QSRAI_002.isx" -report '-reportName "FreqPat"'

The following command exports all InfoSphere DataStage reports with names beginning with Mb to the archive MDBds_001.isx, together with all the results for those reports.

istool export -domain qaqserv:9080 -username user1 -password pass1 -archive "c:/MDBds_001.isx" -report '-prod "DataStage" -reportName "Mb*" -includeAllReportResults'

Import command for reporting assets

You can use the istool command line interface (CLI) to import your reporting assets from a file containing previously exported assets. These assets can include both report designs and report results.

Purpose

Use the -report command parameter with the istool import command to import reports from an archive that contains previously exported assets.

To import a report or report results, you must have the role of Suite Administrator, or have read permissions for the template that the report is based on. After the import, you are the owner of that report and have administration, read, and write permissions.

Command syntax

istool import [authentication] [generic parameters] [-AbortAfter number_of_errors] -report -archive pathname -preview | -replace

Parameters

import
The import command specifies an import operation.

authentication options
All asset interchange commands use authentication options to connect to a specific installation of IBM InfoSphere Information Server

generic options
The generic options are available by all asset interchange commands. Use the generic options to request help on command syntax, or to specify silent or verbose operation.
-AbortAfter number_of_errors or -abort number_of_errors
  Specifies that the import stops if more than the specified number of errors occur.

-report
  Specifies that report assets are imported.

-archive "pathname" or -ar "pathname"
  Specifies the path name of the file that the assets were previously exported to.

-preview or -pre
  Specify this option to preview the action of the command without changing the repository.

-replace
  Merges imported assets with existing assets if they have the same identity. The -replace parameter must be specified for all reporting imports, regardless of whether there are existing assets in the metadata repository.

Example

The following command previews reporting assets that were previously exported to the archive c:\MDBds_001.isx:

`istool import -domain qakserv:9080 -username user1 -password pass1
-report -archive "c:\MDBds_001.isx" -preview`

The following command imports reporting assets that were previously exported to the archive c:\MDBds_001.isx:

`istool import -domain qakserv:9080 -username user1 -password pass1
-report -archive "c:\MDBds_001.isx" -replace`

Importing multiple types of assets

If the archive file to be imported includes multiple types of assets, you must specify each type of included metadata on the command line when you import the archive file, otherwise only reporting assets are imported. For example, if the archive includes InfoSphere Information Analyzer you must specify the -ia and -cm and options in addition to the -rep options when you import the archive. You can use separate import commands for each type of asset.

Note: You must use the -replace option when you import report assets from an archive. If you do not want to use the -replace option for the other types of assets in the archive, you must use a separate command to import the reports. If you import assets without the -replace option and import their related reports with the -replace option, some of the reports might not be accurate for the unreplaced assets in the target environment. Check the reports and run them again in the new environment if necessary.

In the following example, the first command imports InfoSphere Information Analyzer assets and common metadata assets from the file ia_archive1.isx without using the -replace option. The second command imports reporting assets from the same archive file while using the required -replace option.

`import -u admin -p admin100 -dom EVEREST -ar ia_archive1.isx
-ia '' -cm ''`

`import -u admin -p admin100 -dom EVEREST -ar ia_archive1.isx
-replace -rep`
Exit status

A return value of 0 indicates successful completion; any other value indicates failure.

Merge and replace actions for reporting assets

If a reporting asset with the same identity exists in the target repository, then the new asset is merged with the existing asset.

A reporting asset has various attributes, and the merging process affects the attributes differently. A reporting asset has the following attributes:

- **Report design**
  If a matching Report exists in the target repository, the report is overwritten provided that the user importing the asset has update permission on the target report. Otherwise the import of that asset fails.

- **Report access control list**
  The access control list for the target report is retained.

- **Report results**
  Report results cannot change, and so a report result in an import file will not overwrite the target report result.

- **FavoriteUsers**
  If the report exists on the target and has a FavoriteUsers list, the imported FavoriteUsers list is merged with the existing list. Any users that the imported list contains are added to the list of the target report.

Security assets

Security assets comprise the user IDs, user groups, user roles, and associated credentials that you define in your IBM InfoSphere Information Server.

The InfoSphere Information Server suite contains a number of components. In a typical system, several users are defined. Each of these users might have access to all the suite, or only to certain components within the suite. Each of these users can have different roles that give them different rights in how they interact with suite components and associated data.

Configuring the users, groups, and their roles is an important part of configuring the suite. There can be several situations where you need to import or export the information from the suite. For example, when you back up your suite assets, you might want to include the users and roles with these assets. When you develop on one system and test on a different system, then you might want to include the users, groups, and roles with the other assets that you deploy. Similarly, when you deploy your project to the final target production system, you might need to move these assets to that system.

Export command for security assets

You can use the istool command line interface (CLI) to export your IBM InfoSphere Information Server security assets, such as users and roles.

Purpose

Use the -security parameter with the istool export command to export the following assets:
• Users and groups and their suite and product role assignments (including their credentials when relevant).
• Engine credential mappings.
• Project roles are not exported by using the -security parameter. They are exported by commands for the tools that create the project.

The export creates an archive file. By default the file has the suffix .isx.

You must have the Suite Administrator role to export security assets.

**Command syntax**

```bash
istool export
authentication
[general options]
-secure "pathname" [-updatearchive]
[-AbortIfError number_of_errors]
[-preview]
-secure
 ['-securityUser
  -userid user_pattern...
  [-includeUserGroupMemberships]
  [-includeCredential]
  [-includeCredentialMappings]
  [-includeRoles]]'
 |
 ['-securityGroup
  -groupid group_pattern...
  [-includeGroupUserMemberships]
  [-includeRoles]]'
```

**Parameters**

- **export**
  The export command specifies an export operation.

- **authentication**
  All asset interchange commands use authentication parameters to connect to a specific InfoSphere Information Server installation.

- **generic parameters**
  The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

- **-archive "pathname" or -ar "pathname"**
  Specifies the path name (including file name) for the archive that the assets are exported to.

- **-updatearchive or -up**
  Updates an existing archive file (otherwise overwrites it).

- **-AbortIfError number_of_errors or -abort number_of_errors**
  Stops the export if the specified number of errors occur.

- **-preview or -pre**
  Shows a preview of the export. The preview lists the assets that are exported when the export runs.

- **-security or -sec**
  The -security command parameter specifies that security assets are exported.

- **'-securityUser subparameters' or -su 'subparameters'**
  Specifies an export operation of security assets relating to users. The
-securityUser parameter is mutually exclusive with the -securityGroup parameter. The -securityUser parameter has the following subparameters:

-**userid** *user_pattern* or **-u** *user_pattern*
  Specifies user assets to export. *User_pattern* is a search pattern for locating users. You can use the asterisk (*) character to represent multiple characters, and the question mark (?) character to represent single characters. The following strings are examples of valid search patterns:
  - *dsadmin* - selects the user dsadmin
  - *dsuser?* - selects the users dsuser1, dsuser2, and dsuser3
  - *ds* - selects the users dsadmin, dsuser1, dsuser2, and dsuser3
  - "dsadmin dsuser2" - selects the users dsadmin and dsuser2

-includeUserGroupMemberships or **-incUsrGrpMems**
  Exports user group relationships, including the referenced groups, along with user details.

-includeCredential or **-incCred**
  Exports user credentials. Encrypted passwords are stored in the asset archive. Passwords are stored in digested form (SHA-1). If the InfoSphere Information Server installation is using an external directory, this parameter is ignored.

-includeCredentialMapping or **-incMap**
  Exports DataStage credential mapping. Encrypted passwords are stored in the asset archive (passwords are stored in XOR encrypted form).

-includeRoles or **-incRole**
  Specifies that user role relationships are also exported.

'-securityGroup subparameters' or **-sg** 'subparameters'
  Specifies an export operation of security assets relating to groups. The -securityGroup parameter is mutually exclusive with the -securityUser parameter. The -securityGroup parameter has the following subparameters:

-**groupid** *group_pattern* or **-grp** *group_pattern*
  Specifies user group assets to export. *Group_pattern* is a search pattern for locating user groups. You can use the asterisk (*) character to represent multiple characters, and the question mark (?) character to represent single characters. The following strings are examples of valid search patterns:
  - *dsadmins* - selects the group dsadmins
  - *dsgroup?* - selects the groups dsgroup1, dsgroup2, and dsgroup3
  - *ds* - selects the groups dsadmins, dsgroup1, dsgroup2, and dsgroup3
  - "dsadmins dsgroup1" - selects the groups dsadmins and dsgroup1

-includeGroupUserMemberships or **-incGrpUsrMems**
  Specifies that group user relationships, including the referenced users, are also exported.

-includeRoles or **-incRole**
  Specifies that group role relationships are also exported.
Exit status

A return value of 0 indicates successful completion; any other value indicates failure.

Examples

The following command exports DataStage users (whose user IDs begin with "ds" on this system), together with their credentials and credential mappings, to the file dsusers.isx.

```bash
istool export -archive "c:\dsusers.isx" -domain mysys:9080 -username myid -password mypasswd -security '-securityUser -userident ds* -includeCredentials -includeCredentialMappings'
```

The following command exports a group containing IA users, together with their roles, to the file ia_export.isx.

```bash
istool export -archive "c:\ia_export.isx" -domain mysys:9080 -username myid -password mypasswd -security '-securityGroup -groupident iaUsergp -includeRoles'
```

Import command for security assets

You can use the istool command line interface (CLI) to import IBM InfoSphere Information Server security assets, such as users and groups.

Purpose

Use the -security command parameter with the istool import command to import user, group, roles, and credential mappings from previously exported archive files.

If a security asset of the same name exists in the target metadata repository, then the imported asset is merged with the existing asset. If the imported asset has entries for fields that are empty in the target asset, the imported settings are added to the target asset. For example, if a user has additional roles defined in the import file, those roles are added to the existing user in the target user definition.

You must have the Suite Administrator role to import security assets.

Command syntax

```bash
istool import authentication [generic parameters] [-AbortAfter number_of_errors] -security -archive pathname -preview | -replace
```

Parameters

- **import**
  - The import command specifies an import operation.

- **authentication**
  - All asset interchange commands use authentication parameters to connect to a specific InfoSphere Information Server installation.
The generic parameters are available to all asset interchange commands. Use the generic parameters to request help on command syntax, or to specify silent or verbose operation.

- **-AbortAfter** number_of_errors or -**abort** number_of_errors
  Stops the import if more than the specified number of errors occur.

- **-preview** or -pre
  Previews the import. The preview lists the assets that will be imported when the import runs.

- **-security** or -sec
  Specifies that security assets are imported.

- **-archive** pathname or -ar pathname
  Specifies the pathname (including file name) for the archive that the assets are imported from.

- **-replace**
  Merges imported assets with existing assets if they have the same identity. The -replace parameter must be specified for all security imports, regardless of whether there are existing assets in the metadata repository.

**Exit status**

A return value of 0 indicates successful completion; any other value indicates failure.

**Example**

The following command previews the contents of the archive file /opt/IBM/InformationServer/exports/dsuserexport.isx:

```bash
istool import -domain server1:9080 -username user1 -password pass1
-archive "/opt/IBM/InformationServer/exports/dsuserexport.isx" -security -preview
```

The following command imports the users from the archive file /opt/IBM/InformationServer/exports/dsuserexport.isx:

```bash
istool import -domain server1:9080 -username user1 -password pass1
-archive "/opt/IBM/InformationServer/exports/dsuserexport.isx" -security -replace
```

**Merge and replace actions for security assets**

If a security asset with the same identity exists in the target repository, then the new asset is merged with the existing asset.

The merge rules depend on the type of the security asset:

**User**  
If a matching user exists in the target repository, the import implements the following merge rules:

- All empty or null attributes of the existing user are replaced by the attributes from the imported user.
- A union is made of all group memberships between the existing user and the imported user. That is, any group memberships of the imported user that do not already exist for the target user are added to the target user.
- A union is made of all user roles between the existing user and the imported user. That is, any user roles of the imported user that do not already exist for the target user are added to the target user.
• The user credentials of a target user are not overwritten by the user credentials of the imported user.

• The credential mappings of a target user are not overwritten by the credential mappings of the imported user. If the target user has no credential mappings, then the import creates the credential mappings of the imported user.

**Group**  If a matching user exists in the target repository, the import implements the following merge rules:

• All empty or null attributes of the existing group are replaced by the attributes from the imported group.

• A union is made of all user memberships between the existing group and the imported group. That is, any user memberships of the imported group that do not already exist for the target group are added to the target group.

• A union is made of all group roles between the existing user and the imported user. That is, any group roles of the imported group that do not already exist for the target group are added to the target group.
Appendix A. Product accessibility

You can get information about the accessibility status of IBM products.

The IBM InfoSphere Information Server product modules and user interfaces are not fully accessible. The installation program installs the following product modules and components:

- IBM InfoSphere Business Glossary
- IBM InfoSphere Business Glossary Anywhere
- IBM InfoSphere DataStage
- IBM InfoSphere FastTrack
- IBM InfoSphere Information Analyzer
- IBM InfoSphere Information Services Director
- IBM InfoSphere Metadata Workbench
- IBM InfoSphere QualityStage

For information about the accessibility status of IBM products, see the IBM product accessibility information at http://www.ibm.com/able/product_accessibility/index.html.

Accessible documentation

Accessible documentation for InfoSphere Information Server products is provided in an information center. The information center presents the documentation in XHTML 1.0 format, which is viewable in most Web browsers. XHTML allows you to set display preferences in your browser. It also allows you to use screen readers and other assistive technologies to access the documentation.

The documentation that is in the information center is also provided in PDF files, which are not fully accessible.

IBM and accessibility

See the IBM Human Ability and Accessibility Center for more information about the commitment that IBM has to accessibility.
Appendix B. Reading command-line syntax

This documentation uses special characters to define the command-line syntax.

The following special characters define the command-line syntax:

[] Identifies an optional argument. Arguments that are not enclosed in
brackets are required.

... Indicates that you can specify multiple values for the previous argument.

| Indicates mutually exclusive information. You can use the argument to the
left of the separator or the argument to the right of the separator. You
cannot use both arguments in a single use of the command.

{} Delimits a set of mutually exclusive arguments when one of the arguments
is required. If the arguments are optional, they are enclosed in brackets ([ ]).

Note:
• The maximum number of characters in an argument is 256.
• Enclose argument values that have embedded spaces with either single or
double quotation marks.

For example:

wsetsrc[-S server] [-l label] [-n name] source

The source argument is the only required argument for the wsetsrc command. The
brackets around the other arguments indicate that these arguments are optional.

wlsac [-l | -f format] [key...] profile

In this example, the -l and -f format arguments are mutually exclusive and
optional. The profile argument is required. The key argument is optional. The
ellipsis (...) that follows the key argument indicates that you can specify multiple
key names.

wrb -import {rule_pack | rule_set}...

In this example, the rule_pack and rule_set arguments are mutually exclusive, but
one of the arguments must be specified. Also, the ellipsis marks (...) indicate that
you can specify multiple rule packs or rule sets.
Appendix C. Contacting IBM

You can contact IBM for customer support, software services, product information, and general information. You also can provide feedback to IBM about products and documentation.

The following table lists resources for customer support, software services, training, and product and solutions information.

Table 57. IBM resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description and location</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Support Portal</td>
<td>You can customize support information by choosing the products and the topics that interest you at <a href="http://www.ibm.com/support/entry/portal/Software/Information_Management/InfoSphere_Information_Server">www.ibm.com/support/entry/portal/Software/Information_Management/InfoSphere_Information_Server</a></td>
</tr>
<tr>
<td>Software services</td>
<td>You can find information about software, IT, and business consulting services, on the solutions site at <a href="http://www.ibm.com/businesssolutions/">www.ibm.com/businesssolutions/</a></td>
</tr>
<tr>
<td>My IBM</td>
<td>You can manage links to IBM Web sites and information that meet your specific technical support needs by creating an account on the My IBM site at <a href="http://www.ibm.com/account/">www.ibm.com/account/</a></td>
</tr>
<tr>
<td>Training and certification</td>
<td>You can learn about technical training and education services designed for individuals, companies, and public organizations to acquire, maintain, and optimize their IT skills at <a href="http://www.ibm.com/software/sw-training/">http://www.ibm.com/software/sw-training/</a></td>
</tr>
</tbody>
</table>
Appendix D. Accessing and providing feedback on the product documentation

Documentation is provided in a variety of locations and formats, including in help that is opened directly from the product client interfaces, in a suite-wide information center, and in PDF file books.

The information center is installed as a common service with IBM InfoSphere Information Server. The information center contains help for most of the product interfaces, as well as complete documentation for all the product modules in the suite. You can open the information center from the installed product or from a Web browser.

Accessing the information center

You can use the following methods to open the installed information center.

• Click the Help link in the upper right of the client interface.

  Note: From IBM InfoSphere FastTrack and IBM InfoSphere Information Server Manager, the main Help item opens a local help system. Choose Help > Open Info Center to open the full suite information center.

• Press the F1 key. The F1 key typically opens the topic that describes the current context of the client interface.

  Note: The F1 key does not work in Web clients.

• Use a Web browser to access the installed information center even when you are not logged in to the product. Enter the following address in a Web browser: http://host_name:port_number/infocenter/topic/com.ibm.swg.im.iis.productization.iisinfsv.home.doc/ic-homepage.html. The host_name is the name of the services tier computer where the information center is installed, and port_number is the port number for InfoSphere Information Server. The default port number is 9080. For example, on a Microsoft® Windows® Server computer named iisdocs2, the Web address is in the following format: http://iisdocs2:9080/infocenter/topic/com.ibm.swg.im.iis.productization.iisinfsv.nav.doc/dochome/iisinfsrv_home.html.

A subset of the information center is also available on the IBM Web site and periodically refreshed at http://publib.boulder.ibm.com/infocenter/iisinfsv/v8r7/index.jsp.

Obtaining PDF and hardcopy documentation

• A subset of the PDF file books are available through the InfoSphere Information Server software installer and the distribution media. The other PDF file books are available online and can be accessed from this support document: https://www.ibm.com/support/docview.wss?uid=swg27008803&wv=1.

• You can also order IBM publications in hardcopy format online or through your local IBM representative. To order publications online, go to the IBM Publications Center at http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss.
Providing comments on the documentation

Your feedback helps IBM to provide quality information. You can use any of the following methods to provide comments:

- To comment on the information center, click the Feedback link on the top right side of any topic in the information center.
- **Send your comments by using the online readers' comment form at [www.ibm.com/software/awdtools/rcf/](http://www.ibm.com/software/awdtools/rcf/)**
- Send your comments by e-mail to comments@us.ibm.com. Include the name of the product, the version number of the product, and the name and part number of the information (if applicable). If you are commenting on specific text, include the location of the text (for example, a title, a table number, or a page number).
- **You can provide general product feedback through the Consumability Survey at [www.ibm.com/software/data/info/consumability-survey](http://www.ibm.com/software/data/info/consumability-survey)**
Notices and trademarks

This information was developed for products and services offered in the U.S.A.

Notices

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites.
sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to
IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

The following terms are trademarks or registered trademarks of other companies:

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The United States Postal Service owns the following trademarks: CASS, CASS Certified, DPV, LACS\textsuperscript{link}, ZIP, ZIP + 4, ZIP Code, Post Office, Postal Service, USPS and United States Postal Service. IBM Corporation is a non-exclusive DPV and LACS\textsuperscript{link} licensee of the United States Postal Service.

Other company, product or service names may be trademarks or service marks of others.
Index

A
active sessions
disconnecting 158
view 157
active-passive configuration
administration overview 179
failover 190
Tivoli System Automation for Multiplatforms administration
resources 179
administration commands 119
infoSphere DataStage 4
troubleshoot 119
WebSphere Application Server 5
analysis database
Information Analyzer analysis database 221
owner user name and password changing 117
AppServerAdmin 119
AppServerAdmin -was command
changing administrative privileges 121
changing the RunAs user 121
ASB agent
running as non-root user 95
asset interchange 252
export command 278, 296
exporting 278, 297
import command 280, 297
importing 280, 297
scenarios 253
asset types
DataStage 288
assets
business intelligence 320
implemented data resources 319
physical data models 320
auditing
audit configuration events 102
configuring 97, 98, 99, 100, 101, 102, 103, 105, 106, 107, 108
credential mapping events 100
events 98
log files 97, 106, 107, 108
user and group management events 98
user session management events 101
user, group and project security role assignment events 99
authentication
configuring PAM 43, 45
automatic client reroute (ACR) 190
backup
scenarios 218
BI collection 299, 307, 314, 320
BI folder 320
BI model 256, 299, 307, 314, 320
BI report 299, 307, 314, 320
BI report query 299, 307, 314, 320
BI report section 320
BI server 320
bi2bg 261
business intelligence 320
business intelligence assets 299, 307
Business intelligence assets 307
business intelligence model 256, 261
common metadata (continued)
delete 322, 324
delete overview 318
query command 321
security roles 69
common metadata assets
exporting 307
importing 314
components
logging 195
configuration
auditing 97, 98, 99, 100, 101, 102, 103, 105, 106, 107, 108
logging views 199
schedule views 206
configuration files
elements 46
configuring Microsoft Internet Explorer 9
configuring Mozilla Firefox 9
console 13
areas 13
dashboard 19
history 17
menus 15, 17
My Home workspace 13
notes 17
object list 22
open workspaces 17
palettes 17
project menu 17
projects 17
selecting a task 21
shortcuts 17, 20
status bar 19
task flow 20
task list 22
task pane 23
walkthrough 20
workspaces 22
contract libraries 307, 314
conversion of BI model to glossary content 261
conversion of logical data model to business glossary content 266
conversion, to business glossary 260
convert to category 260
convert to glossary 260
convert to terms and categories 260
convert, business intelligence model 256
creating
project 27
credential mapping 81
configuring your own 85
recreating after back up 221
credentials
recovery 212
server default 84
cube 299, 307, 314, 320
custom attributes
eploying 313
custom attributes (continued) importing 317  
customer support contacting 341  
customizing Home tab 32

dashboard 19  
customizing 28  
data file 299, 307, 314, 319  
data file structure 299, 307, 314, 319  
data item definition 299, 307, 314, 319  
database 299, 307, 314, 319  
database connection 299, 307, 314, 319  
database schema 299, 307  
database scripts 167  
database table 299, 307, 314, 319  
databases managing 161  
DataStage 291  
asset types 288  
DB2 password changing 118  
DB2 cluster 188  
db2admin changing metadata repository database owner password 115, 116  
password changing 118  
Debug severity level 196  
delete 318, 322, 324  
delete command, istool 294  
deploy package command 283  
Deployment Manager starting 237, 239  
progressing 232, 234  
deregistration options 171  
design stored procedure 320  
design table 320  
directories 34, 36  
DirectoryAdmin accessing LDAP attributes 130  
assign administrator role 123  
check if a user exists 124  
configure to use application server registry 126  
configure to use internal registry 125  
create a user 122  
delete groups 127  
delete users 126  
display user details 129  
reset credentials 123  
search for groups 128  
search users 128  
troubleshoot 132  
Directory-Command tool 134  
disconnecting users 158  
disk space requirements 212  
display repository details 163  
distinguished name (DN) determining by using WebSphere Application Server Administrative Console 49  
determining by using Windows Active Directory search 50  
dmgr shutting down 232, 234  
starting 237, 239  
status checking 245  

e  
encryption passwords 212  
gine secure 77  
security 81  
user registry 78  
engine tier 190  
backing up 220  
failover in active-passive configuration 190  
recovering from failover 191  
restore 220  
entitlements activating or deactivating 149  
activating or deactivating items 151  
LicensingServiceAdmin command 153  
viewing activated items 150  
events logging 195  
purging 198, 201  
snapshot 199  
Examples RepositoryAdmin 172, 175, 176  
export 256  
export command, istool 286  
exporting InfoSphere FastTrack assets by using the command line 274  

F  
failover  
DB2 clustered configuration 190  
defined 179  
engine tier 190  
high availability disaster recovery (HADR) 188, 189  
recovering from failover 191  
fatal severity level 196  
federated repository 130  
forecasts  

G  
generate terms and categories 260  
glossary 256  
conversion from business intelligence model 262  
conversion from logical data model 269  
export 256  
import 258  
glossary model 260  
group roles 75  
groups 56, 58  
assigning users to 57, 58  

H  
heartbeat 179  
high availability administering active-passive configuration 179  
high availability disaster recovery (HADR) 188  
failover overview 188  
failover recovery 189  
history 17  
Home tab customizing 32  
host 299, 307, 314, 319  

I  
IADB  
Information Analyzer analysis database 221  
iauser changing user name and password 117  
IBM InfoSphere DataStage activating or deactivating editions and feature packs 151  
activating or deactivating entitled canvases and features 149  
viewing activated editions and feature packs 150  
identity strings 299, 307, 314, 320  
implemented data resource assets 314  
implemented data resources 299, 307, 319  
import 258  
import command for InfoSphere FastTrack 275  
import command, istool 292  
inactivity limit 157  
information analysis graphics 28  
Information Analyzer back up 221  
restore 221  
Information Analyzer analysis database 221  
backing up DB2 database 221  
backing up Oracle database 221  
backing up SQL Server database 221  
restoring DB2 database 221  
restoring Oracle database 221  
restoring SQL Server database 221  
InfoSphere Business Glossary security 67  
InfoSphere Data Architect glossary model 260  
InfoSphere DataStage administering 4  
backing up projects 221  
restoring projects 221  
security roles 67  
updating projects 221  
InfoSphere FastTrack roles 70  
security 66
InfoSphere Information Analyzer
analysis database owner user name and password changing 117
roles 70
security 70
InfoSphere Information Server
add-on components, installing in a cluster 181
administration overview 1
back up 213
console 13
non-root user, system restart 94
prepare for data recovery 215, 216
restore 216
setting up non-root user, WebSphere Application Server 88
InfoSphere Information Server administrator
password changing 110
InfoSphere Information Server console components 13
object list 22
project dashboard 19
shortcuts 20
status bar 19
task flow 20
task list 22
workspaces 22
InfoSphere Information Server engine mapping credentials 85
InfoSphere Information Server Manager 291
InfoSphere Information Server recovery assistant back up wizard 211, 213
InfoSphere Information Server recovery assistant restore wizard 211
InfoSphere Information Server Web console changing passwords 111
configuring browsers for 9
determining URL for 8
navigating to 11
InfoSphere Information Services Director cluster deployment 181
security 71
InfoSphere Metadata Workbench Administrator role 66
User role 66
InfoSphere Streams assets istool command 296
migrating 296
internal user registry pros and cons 39
switch back to 50
isadmin password changing 110
ISALite password encryption 212
istool 252, 256, 299, 307, 325, 330
command-line syntax 248
import command 292
interchanging common metadata assets 307, 314
custom attributes 313, 317
logical data model assets 310, 315
reports 326, 328
istool (continued)
interchanging (continued)
security assets 330, 333
istool command 319, 320
istool command line 247
istool command modes 251
istool commands 282
istool delete command 294
istool export command 278, 286, 296
istool import command 280, 297
istool location 247
logging configurations active 204
copying 203
default 203
editing 202
overview 195
logical data model 266
logical data model assets exporting 310
importing 315
logs 25, 195
JavaScript
enabling in Microsoft Internet Explorer 9
enabling in Mozilla Firefox 9
jobs crashed 193
restarting crashed 193
LDAP
accessing attributes 130
determining DN by using WebSphere Application Server Administrative Console 49
determining DN by using Windows Active Directory search 50
switch to 47
user registry pros and cons 39
ldm2bg 266
LDR_CNTRL 241
legal notices 345
LicensingServiceAdmin activating or deactivating editions and feature packs 151
command reference 153
introduction 149
viewing activated editions and feature packs 150
list repositories 163
local operating system user registry 39, 41
log files
SystemOut.log 242, 243
WebSphere Application Server 245
log view
copying 198, 201
creating 197, 199
criteria 196
log messages 25, 195
modifying 198, 200
logged events
accessing 198, 200
purging 198, 201
views 197, 199
logged messages
purging 198, 201
logging agent running as non-root user 95
logging components overview 195
M
maintenance mode 228
managing repositories 161
maximum active sessions 157
merging
reporting assets 330
security assets 334
metadata repository changing owner password 115, 116
criteria for logging events 196
DB2 database recovery 218
deleting assets 318, 322, 324
migration 218
moving 218
Oracle database recovery 218
SQL Server database recovery 218
MetadataServer script running 238
Microsoft Internet Explorer, configuring 9
modes, istool command 251
Mozilla Firefox, configuring 9
My Home workspace 13
N	naming data model 260
ndm 260
NDM 260
node agents running as non-root user 95
nodes synchronizing 186
non-root administration
WebSphere Application Server 87
non-root user
running agents as 95
notes 17
note icons 20
O
object list 22
open workspaces 17
opening a project 28
operational metadata security roles 69
P

PAM
configuring for InfoSphere Information Server engine 43, 45
configuring for InfoSphere Information Server services 43
element configuration files 46
password changing
analysis database owner 117
DB2 118
InfoSphere Information Server administrator 110
InfoSphere Information Server Web console 111
metadata repository database owner 115, 116
Web console 32
WebSphere Application Server administrator 112, 113
passwords
recovery 212
permissions
Windows 2008 59, 61
physical data model 320
physical data model assets 307, 314
physical data models 320
physical domain 320
plugin-cfg.xml file
managing for WebSphere Application Server clusters 181
pop-up windows
enabling in Microsoft Internet Explorer 9
enabling in Mozilla Firefox 9
private views
logging 196, 206
product accessibility
accessibility 337
product documentation
accessing 343
project
adding groups 75
adding users 74
assigning group roles 75
assigning user roles 74
creating 27
creating groups 56, 58
creating users 55, 57
details 27
menu 17
opening 28
overview 27
recovering 192
security 55, 57
setting up 27
project directory
changing 221
default 221
projects
backing up 220
updating 220
R

recovering projects 192
recovery 211
credentials 212
password encryption 212
password strength 212
planning 212, 218, 221
recovery tool
command syntax 223
commands
-resp 223
restart 225
version 225
metadata repository properties 218
response file 218
register repositories 167, 169
registries
overview 34
user 34
reporting assets 325
reports
creating 24
exporting 326
importing 328
merging 328
view 24
workspace 24
repositories
managing 161
repository connection
test 171
RepositoryAdmin tool 161
changing connection properties 172
registering a repository 172, 176
relocating a repository 175
requirements
disk space 212
system 212
response command (recovery tool) 223
response file
Information Analyzer properties 221
migration tool 221
restart command (recovery tool) 225
restore 211
scenarios 218
roles
common data rules 70
Common metadata 69
InfoSphere DataStage 67
InfoSphere Metadata Workbench Administrator 66
Metadata Workbench User 66
Operational metadata 69
rule user 70
rwx permission
non-root user 89, 91
scheduled tasks
forecasts 209
purging run histories 208
stopping 208
schedules
completed 209
pausing 207
purging run histories 208
reactivating 207
restarting 207
running 209
stopping 207
viewing 207
scheduling
jobs 24
schedule requests 24
schema 307, 314, 319
scripts
database creation 167
security
assigning groups to a project 75
assigning users to a project 74
configuring PAM 43, 45
creating groups 56, 58
creating users 55, 57
gine 77
example PAM configuration files 46
external directory 36
internal user registry 34
managing 33
overview 33, 54
roles 65
set up 72
setup 33
user roles 64
security assets 330
exporting 330
importing 333
merging 333
security configuration
auditing 105
switching user registry 53
security roles
InfoSphere Business Glossary 67
InfoSphere FastTrack 66
InfoSphere Information Analyzer 70
InfoSphere Information Services Director 71
viewing assigned 74, 77
send package command 285
serverStatus command 242, 245
services
shutting down (Windows) 230
sessions
active 157
disconnecting 158
setting limits 157
severity levels
logging criteria 196
shared views
logging 196, 206
shortcuts 17, 20
software services
contacting 341
special characters
in command-line syntax 339
special characters in identity strings 305
S

save SQL scripts 167
scenarios
backup and restore 218
schedule views
copying 206
creating 206
criteria 205

Q

query command 321

352 Administration Guide