IBM Information Server Administration Guide
Before using this information and the product that it supports, read the information in "Notices" on page 145.
Chapter 1. Administration overview

In IBM® Information Server, you can administer and manage users, roles, sessions, security, logs, and schedules. Both the console and the Web console provide global administration capabilities.

**Security administration**

You can administer security in the following areas:

**Access control**
Provide role assignments and specify what the user can do.

**User and group creation or update**
If the IBM Information Server internal user directory is used, you can create or update users and groups.

**Active session management**
View current active sessions, manage session limits, and force one or all users to disconnect.

IBM Information Server leverages WebSphere® Application Server for the directory and authentication process. IBM Information Server uses the WebSphere Application Server configuration for user and group access and authentication and supports all user registries that are supported by WebSphere Application Server.

IBM Information Server also provides a custom WebSphere Application Server user registry. To store users and groups in the repository, you can use this custom registry instead of external directories.

**WebSphere Information Analyzer, WebSphere DataStage™, and WebSphere QualityStage users**

WebSphere Information Analyzer, WebSphere DataStage, and WebSphere QualityStage require that there is a valid operating system user id on the computer where the engine tier is installed. For each IBM Information Server user that needs to access the IBM Information Server engine, you must map the IBM Information Server user credentials to valid operating system user credentials that exist on the engine tier. To administer security for these users, you can either specify that the user registry is shared between the operating system user registry and the internal user registry, or you can map the credentials for each user.

**Sharing the user registry**
If the IBM Information Server user registry is the same as the engine tier user registry, you can share the user registry. You must configure and ensure that the operating system where the engine tier is installed uses the same user registry as IBM Information Server. If IBM Information Server is configured to use the internal user registry, you cannot share the user registry.

**Credential mapping**
If the operating system where the engine tier is installed is not using the same user registry as the WebSphere Application Server, you must map the credentials on a user by user basis or by specifying a default engine tier local operating system user name and password that is used for all users who do not have defined credential mappings.
Licensing administration

In the Web console, you can administer the installed licenses and view a list of the features and unit counts that are associated with a licensed component of IBM Information Server. Additionally, you can update the licenses for certain suite components.

Logging administration

You can manage logs across all of the IBM Information Server suite components. The consoles provide a central place to view logs and resolve problems. Logs are stored in the metadata repository, and each IBM Information Server suite component defines relevant logging categories. Logging administration includes the following areas:

Logging configuration
A suite administrator specifies which logging categories and severity levels of logging events are logged in the metadata repository.

Logging query
Create log views to retrieve and query the logged events that have been stored in the metadata repository.

Scheduling administration

Many of the suite components use scheduling capabilities. For example, a report run and an analysis job in WebSphere 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 a WebSphere Information Analyzer project in the 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.

To administer scheduling for IBM Information Server, 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.

When administering scheduling, you cannot create new schedules or update the schedule frequency. These tasks can be performed only from the suite component and consoles.

Related concepts

- Supported WebSphere Application Server registries
Chapter 2. IBM WebSphere DataStage administration

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

Table 1. WebSphere DataStage administration guides

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Client Guide</td>
<td>Describes the WebSphere DataStage administrator client and provides instructions about performing setup, routine maintenance operations, and administration on the WebSphere DataStage engine.</td>
</tr>
<tr>
<td>Designer Client Guide</td>
<td>Describes the WebSphere DataStage designer client and gives a general description of how to create, design, and develop a WebSphere DataStage application.</td>
</tr>
<tr>
<td>Director Client Guide</td>
<td>Describes the WebSphere DataStage director client and instructs the user how to validate, schedule, run, and monitor WebSphere DataStage parallel jobs and server jobs.</td>
</tr>
<tr>
<td>National Language Support Guide</td>
<td>Contains information about using the national language support (NLS) features that are available in WebSphere DataStage when NLS is installed.</td>
</tr>
</tbody>
</table>

By default, when you install the documentation in Windows®, it is available from the Start menu. In UNIX® and other platforms, the PDF documentation for the suite is installed in \IBM\InformationServer\Documentation. You can also find a complete set of the PDF documentation for the suite on the IBM Information Server PDF CD that is included with the installation software.
Chapter 3. IBM WebSphere Application Server administration

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

You can find information about WebSphere Application Server at publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp

For detailed IBM 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>Configuring WebSphere Application Server user registries</td>
<td>publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/ com.ibm.websphere.base.doc/info/aes/ae/tsec_useregistry.html</td>
</tr>
</tbody>
</table>
Chapter 4. Opening the IBM Information Server console

The IBM 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 WebSphere Information Analyzer, enabling information services with IBM WebSphere Information Services Director, and running reports. To open the console, double-click the desktop icon or select the program from the start menu.

To start the IBM Information Server console:
1. From the Windows start menu, select Start → All Programs → IBM Information Server → IBM Information Server Console.
2. In the login window, type your user name and password.
3. Click OK.
Chapter 5. Opening the IBM Information Server Web console

The IBM 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 WebSphere Business Glossary and the Information Services catalog. To open the Web console, you type the URL into a Web browser.

**Prerequisites**

- A Web browser. For a information about supported browsers, see the IBM 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)
- "Configuring your Web browser to work with the Web console"

To start the IBM Information Server Web console:

1. In the Web browser, enter the URL for the Web console. The URL is in the form `host_server:port`. `host_server` is the URL or IP address of the computer where WebSphere Application Server is installed and `port` is the port number that is assigned to the Web console. The default port number is 9080.
2. In the login page of the Web console, type your user name and password.
3. Click OK to open the Home tab.

**Configuring your Web browser to work with the Web console**

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

**Prerequisites**

- For details about Web browsers versions that are supported, see the IBM 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)

**Configuring Microsoft Internet Explorer 6.0 and 7.0 to work with the Web console**

To configure Microsoft Internet Explorer to work with the Web console:

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

   **Note:** Third-party pop-up blockers might also need to be disabled or
   configured to allow pop-ups for this site.

4. Specify that pages refresh with every visit to the page:
   a. Choose Tools → Internet Options and on the General tab, click Settings. In
      Microsoft Internet Explorer version 6, select Settings in the Temporary
      Internet files section. In Microsoft Internet Explorer version 7, 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. Choose Tools → Internet Options.
   b. On the Advanced tab, clear Browsing → Show friendly HTTP error
      messages.

**Configuring Internet Explorer to work with the Web console**

**on Microsoft Windows Server 2003**

If you are running Microsoft Internet Explorer on a computer that has Microsoft
Windows Server 2003 running, you might need to complete an additional step. In
this scenario, if you are browsing to a Web console by using its host name, such as
http://<hostname>:9080, you must add the Web site (http://<hostname>) to the
trusted site zones in Internet Explorer.

To add the website to the trusted site zones:
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 as http://<hostName> and click
   Add.

You do not need to complete this step if your client computer is also your server
and you are browsing to the server by using the URL http://localhost:9080, or if
you are using Mozilla Firefox.

**Configuring Mozilla Firefox to work with the Web console**

To configure Mozilla Firefox version 2.x to work with the Web console:
1. Enable JavaScript:
   a. Choose Tools → Options, and on the Content tab, click Enable JavaScript.
2. Set the browser to accept cookies for the IBM Information Server host site.
   a. Choose 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
      hostname and clicking Allow.
3. Enable pop-ups for the URL of the Web console:
   a. Choose 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 hostname and clicking **Allow**.

**Viewing report results in a Web browser**

To ensure that report results open correctly in Microsoft Internet Explorer, modify the following settings:

1. In the Internet Explorer toolbar, click **Tools → Internet Options**.
2. On the Security tab, click **Internet**.
3. On the Security tab, click **Custom Level**.
4. In the Security Settings dialog box, scroll to **Automatic prompting for file downloads** under **Downloads** and select **Enable**.
5. Click **OK**.
6. Click **OK**.
Chapter 6. IBM Information Server console overview

The IBM 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 WebSphere Information Analyzer, enabling information services with IBM WebSphere Information Services Director, and running reports.

The IBM Information Server console (the "console") is a rich-client-based interface that you can use for activities such as profiling data and developing service-oriented applications.

In the IBM Information Server console, you can complete the following tasks:
• Create a project
• Set up project-level security
• Analyze information
  – Analyze columns
  – Analyze primary keys and foreign keys
  – Analyze across domains
• 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

Related tasks
"Customizing the console" on page 31

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

Main areas of the console

The IBM 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 WebSphere Information Analyzer and WebSphere Information Services Director were installed. Some features might not be available if you have only one product module installed.

Related tasks
"Customizing the console" on page 31

The IBM Information Server console integrates multiple suite components into a unified user interface. To customize the console, you can set user preferences, create shortcuts, create notes, and change your password.
Chapter 7, “Setting up a project in the console,” on page 27

In the console, a project is a logical container for all of the tasks that can be performed in a suite component. Multiple users can contribute to a project and view the status of a project over time.

My Home workspace

When you open the 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.

![My Home workspace in the IBM Information Server console](image)

Figure 1. The My Home workspace in the IBM Information Server console

This workspace contains the following sections:

Getting Started pane

The Getting Started pane describes how to work in a product module, such as how to work in IBM Information Server WebSphere 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.

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

**Related tasks**

"Customizing the My Home workspace" on page 31

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 suite components that are installed.

**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.

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 WebSphere 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 WebSphere 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 WebSphere 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.

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.

Related tasks
Chapter 7, “Setting up a project in the console,” on page 27
In the console, a project is a logical container for all of the tasks that can be performed in a suite component. Multiple users can contribute to a project and view the status of a project over time.

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.

Related tasks

"Working with palettes" on page 32
Palettes are containers for console shortcuts, workspace history, open workspaces, and notes. You can dock, float, and anchor the palettes.

Project dashboard  
When you open a project, the project dashboard is displayed.
WebSphere Information Analyzer and WebSphere Information Services Director projects both contain a dashboard. The following figure shows an example of the WebSphere Information Analyzer dashboard.

![Dashboard example](image)

*Figure 7. The Project dashboard for WebSphere Information Analyzer*

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.

**Related tasks**

```
“Customizing the project dashboard” on page 28
```

You can customize the Dashboard workspace in the console to add or remove content panes. For some suite components, 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.

Figure 8. The Shortcuts tab

Related tasks
“Creating shortcuts” on page 32
You can create shortcuts to quickly access frequently used workspaces or tasks.

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.

Related tasks
“Creating notes” on page 33
In some suite components, you can create notes to comment on an object, provide information to other users, and flag issues for further investigation.
Basic task flow in the workspaces

Even though you perform different types of tasks in a WebSphere Information Analyzer project and a WebSphere 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 WebSphere Information Analyzer. The types of tasks and options that are available will vary between WebSphere Information Analyzer projects and WebSphere 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.

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.

Select the task that you want to perform from that menu

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

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.

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.

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.

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.

![Image of the Run Column Analysis task pane](image)

*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.

**Figure 14. Status bar showing the progress of the column analysis job**

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

The IBM 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.

**Related concepts**

[Chapter 15, "Managing schedules," on page 121](#)

In the 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.

### 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.

**Related concepts**

[Chapter 14, "Managing logs," on page 111](#)

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.

**Related tasks**

["Managing logging views in the console" on page 113](#)

In the console, you can create logging views, access logged events from a view, edit a log view, and purge log events.

---

**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 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.

![Image of instruction icon highlighted](image)

**Figure 15. The instruction icon highlighted**

To show the instructional text, click [i](instruction icon) (instruction pane).

To hide the instructional text, click the instruction icon again.
Chapter 7. Setting up a project in the console

In the console, a project is a logical container for all of the tasks that can be performed in a suite component. Multiple users can contribute to a project and view the status of a project over time.

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

**Related concepts**

"Project menu" on page 17
Above the Workspace Navigator, you can access the project menu to open a project, move between open projects, and create projects.

"Main areas of the console" on page 13
The IBM Information Server console provides workspaces that you use to investigate data, deploy applications and Web services, and monitor schedules and logs.

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 suite component.

**Prerequisites**

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

To create a project:
1. On the File menu in the console, select **New Project**.
2. In the New Project window, select the type of project that you want to create.
   The *Type* field appears only if more than one suite component is installed.
3. Type a name for the project.
4. Click **OK**. The Project Properties workspace opens.

You can now perform the following tasks:
* "Modifying project properties”
* "Assigning users to a project and assigning roles” on page 75

Modifying project properties

You can view and modify the properties of your project.

**Prerequisites**

You must have project administrator authority.

To modify project properties:
1. On the **Overview** navigator menu in the 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 console to add or remove content panes. For some suite components, you can also configure the dashboard to show a set of charts and graphs that are based on underlying project information.

To customize the dashboard for your project:
1. On the Overview navigator menu in the console, select Dashboard.
2. In the Dashboard workspace, click (Configure).
3. Optional: Click Add to add content panes to the Content list. The content panes that are available depend on the suite components 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 or not it appears on the workspace. Some content panes have additional configuration properties.
6. Click OK to save your changes.

Related concepts

“Project dashboard” on page 18
When you open a project, the project dashboard is displayed.
Chapter 8. Opening a project in the console

You can open a project to perform tasks that are associated with the project’s suite component, such as information analysis or information services enablement.

Prerequisites

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

To open a project:
1. In the Projects pane of the My Home workspace, select a project from the list.
2. Click Open Project. The Dashboard workspace opens.

You can also open projects from the File menu or the Workspace Navigator menu.
Chapter 9. Customizing the console and the Web console

You can customize both the IBM Information Server console and the IBM Information Server Web console to best suit your way of working.

Customizing the console

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

Related concepts

"Main areas of the console” on page 13
The IBM Information Server console provides workspaces that you use to investigate data, deploy applications and Web services, and monitor schedules and logs.

Chapter 6, “IBM Information Server console overview,” on page 13
The IBM 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 WebSphere Information Analyzer, enabling information services with IBM WebSphere Information Services Director, and running reports.

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 suite components that are installed.

To customize the My Home workspace:
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 suite components that are installed. Suite component panes might have additional configurable details.
5. For each content pane, you can modify the label of the pane and specify whether it appears on the My Home workspace.
6. Click OK to close the window.

Related concepts

"My Home workspace” on page 14
When you open the console, the My Home workspace is shown. In this workspace, you can access getting started information and you can access projects.

Modifying user preferences

You can modify user preferences to best suit your way of working. For example, you can specify preferences for startup, change the behavior of panes, and customize the status bar.
To modify user preferences:
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.

To create a shortcut:
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.

You can now access your shortcut on the Shortcuts palette.

Related concepts
“Shortcuts” on page 20
To quickly return to a task at a later time, you can create a shortcut.

Working with palettes
Palettes are containers for console shortcuts, workspace history, open workspaces, and notes. You can dock, float, and anchor the palettes.

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

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

To pin the palette to stay open, click (pin).

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

Related concepts
“Palettes” on page 17
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.

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

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.
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.

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.

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 suite components, you can create notes to comment on an object, provide information to other users, and flag issues for further investigation.

To create a note:

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.

After you create the note, you and other users can access the note by clicking (Note).

**Related concepts**

"Notes" on page 20
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.

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

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 Information Server is configured to authenticate against an external directory, passwords cannot be changed.

To change your password, select File → Change Password.
Customizing the Web console

You can access suite administration and reporting tasks, information about deployed information services, and glossaries of information assets in the IBM Information Server Web console. To customize the Web 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.

To customize the Home workspace:
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 Web console.

To change your password, click **Change Password** and type the required information.
Chapter 10. Setting up security

To administer security, you configure the user registry, control access levels, create or update users and groups, and map credentials for IBM WebSphere DataStage and IBM WebSphere QualityStage users.

You must also assign user roles to all users who want to use IBM Information Server. If you are using the internal registry, you must create users and assign privileges to those users. If you are using an external registry, the users automatically show up in the user list and you must assign roles to those users.

IBM Information Server security overview

The security features of IBM Information Server ensure that users have access to the features that they need, while also ensuring that users do not have access to features that are restricted. For example, user access can be controlled so that users have access to only certain product modules.

Login

When a user opens an IBM Information Server client application, such as the IBM Information Server console or the IBM WebSphere DataStage and QualityStage Designer client, the user is prompted for a user name and password.
IBM Information Server leverages the WebSphere Application Server user registry support for directory access. To log in to IBM Information Server, a user must have a user name and password in the user registry.

**Directory Service**

The directory service is part of the IBM Information Server services tier. This services tier is comprised of a set of services that are specific to IBM Information Server, all running in IBM WebSphere Application Server.
The services tier is the control center of IBM Information Server. It provides core functionality for many suite components and controls user access to the suite components. For example, it ensures that only users with IBM WebSphere Information Analyzer roles are able to perform information analysis. The services tier also controls communication between suite components.

**Metadata repository access**

The services tier is the gatekeeper for access to the metadata repository, which is where all of the suite components store and share essential project and runtime information. The client applications and the IBM Information Server engine access the metadata repository through the services tier. This enables IBM Information Server to control access at a central location.

**Engine access**

The engine starts processes that run under operating system users, and therefore requires that at least one operating system user exists.
Security setup

Setting up a secure environment in IBM Information Server involves configuring the user registry that will be used, creating users, and assigning security roles to those users. If you are not sharing the user registry between the service tier and engine tier, you must also map credentials between the registry that is used by the IBM Information Server directory service and the registry that is used by the engine. Finally, some suite components also require that you assign project-specific roles to users.

The following figure shows the main tasks that are involved in setting up security.

![Diagram showing the main tasks for setting up security]

**User registries**

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

To set up a user registry, you can choose one of the following options:

- The internal user directory provided by IBM Information Server.
- An external registry, such as the operating system registry, LDAP, or a custom registry.

**Internal directory**

The IBM Information Server user directory stores users and groups in the metadata repository.

The following figure shows IBM Information Server and WebSphere Application Server that are both configured to use the internal directory provided by IBM Information Server. The internal directory is stored in the IBM Information Server.
metadata repository. Typically, the metadata repository is co-located with the services tier, as shown in the following figure.

In the figure, IBM Information Server’s directory service points directly to the internal directory. WebSphere Application Server also points to that same internal directory. WebSphere Application Server can access IBM Information Server’s internal directory by using a custom user registry, which is provided with IBM Information Server. WebSphere Application Server performs the underlying authentication.

When you use the internal directory, you create users directly through the IBM Information Server console or Web console. Those users and their passwords are stored in the internal directory. You can also create groups and assign users to those groups. In addition to user name, password, and group membership, the internal directory stores the associations between users and their security roles, as well as attributes such as e-mail address and business address. The internal directory also provides the rest of IBM Information Server with the proper registry abstraction so that each component does not have to specify whether it uses an internal or external directory.

The internal directory stores only digested (one-way encryption) passwords for increased security.
External directory
You can use an external directory to authenticate users based on existing user registries, such as an operating system registry, or a Lightweight Directory Access Protocol (LDAP) server.

The following figure shows IBM Information Server and IBM WebSphere Application Server that are both configured to use an external user registry, such as the operating system registry, an LDAP registry, or a custom registry.

![Figure 20. Example of IBM Information Server architecture that uses an external directory](image)

When you use an external user registry, WebSphere Application Server points directly to that registry. The IBM Information Server directory service points to the WebSphere Application Server user registry. It does not point directly to the external registry. By going through WebSphere Application Server to access the external user registry, IBM Information Server takes advantage of the capabilities in WebSphere Application Server for handling various kinds of external user registries.

When you use an external registry, you create users through the administration tools for that registry. IBM Information Server looks to that external registry for user names, passwords, group definitions, and group memberships.
Even when you configure IBM Information Server to use an external registry, certain user information is still maintained in the internal directory. Specifically, the internal directory always stores the associations between users and their security roles, as well as attributes that are not passed through by WebSphere Application Server, such as e-mail address and business address. The internal directory is always available and working in the background.

**Engine security**

The IBM Information Server engine requires a local operating system user registry or an LDAP registry such as Windows Active Directory. The processes that are started by the engine run under these operating system or LDAP user accounts.

To coordinate security across the IBM Information Server services tier and the engine, you share the user registry or you map credentials between registries.

**Shared registry**

If you configure IBM Information Server to use an external registry, you can potentially share the user registry between IBM Information Server and the engine.

You might want to share the user registry when the engine tier and the services tier are installed on the same computer or if they both use the same LDAP directory for authentication. Note that you should only share the user registry if an external registry, such as an operating system or LDAP registry, is used and that registry is one that is used by both the engine tier and the services tier.

If the engine and services tiers cannot both use the same user registry, credential mapping is required.

The following figure shows a shared user registry and includes the engine. The engine can be on the same computer as the services tier or on another computer.
In the figure, the engine uses the local operating system user registry or an LDAP registry and the administrator has ensured that the WebSphere Application Server user registry is the same as the one that is being used by the IBM Information Server engine. WebSphere Application Server is configured to use a local operating system or LDAP registry and IBM Information Server is configured to use the WebSphere Application Server registry and then access the same operating system or LDAP registry.

As a result, WebSphere Application Server, IBM Information Server, and the IBM Information Server engine all have access to the same user names, passwords, and group definitions. By sharing the user registry, authentication to the engine occurs silently by using the same credentials (user ID and password) that the user uses to authenticate with IBM Information Server. In this mode, no credential mapping is required.

**Credential mapping**

If you are not sharing the user registry between the services tier and the engine tier, you must map user credentials between the IBM Information Server services tier and the engine tier to associate the user ID on the engine server.

When users authenticate to IBM Information Server, IBM Information Server automatically authenticates to the engine. In order for this automatic engine
authentication to occur, the system must know which engine credentials (user ID and password) to use for a specific engine and a specific user. You map user’s credentials to create this automatic authentication for your users.

In the following figure, IBM Information Server and WebSphere Application Server both use the IBM Information Server internal directory.

![Diagram](image)

**Figure 22. Example of IBM Information Server architecture that uses credential mapping**

The engine can be on the same computer as the services layer, or on another computer. In this example, the engine uses the local operating system user registry.

You coordinate security across IBM Information Server by mapping credentials between the internal directory and the operating system user registry on the engine computer. The credential mappings are stored with the internal directory in the IBM Information Server metadata repository. The passwords are strongly encrypted for increased security.

You can create individual user mappings, so that each IBM Information Server user is associated with exactly one engine user. You also can create a default user mapping, so that all IBM Information Server users who do not have individual credential mappings can access the engine through a shared engine user name.
Default and preconfigured users

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

The first two users that must be created are the administrator users for IBM Information Server and IBM WebSphere Application Server. These users are typically called “admin” and “wasadmin.” You can choose to create them during installation. The users must be created in the user registry that is used by the IBM Information Server directory service and WebSphere Application Server.

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

Next, there must be at least one user account for the engine. This user ID is typically called “dsadm.” On Linux® and UNIX, you can choose to create this account during installation. It must be created in the user registry that is used by the engine.

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

Finally, there are three users that you must define. The following users must be local OS users where DB2® is installed:

- If you use DB2 for the metadata repository, you must have a DB2 instance owner. This user is typically called “db2admin.” On Linux and UNIX, you also must have users for the fenced and non-fenced instances of DB2.
- All installations must have an owner for the metadata repository. This account is typically called “xmeta.”
- IBM WebSphere Information Analyzer administrators must have an owner for the information analysis repository. This account is typically called “iauser.” You can choose to create these accounts during installation.

<table>
<thead>
<tr>
<th>Sample user name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db2admin</td>
<td>DB2 instance owner</td>
</tr>
<tr>
<td>xmeta</td>
<td>Metadata repository owner</td>
</tr>
<tr>
<td>iauser</td>
<td>Information analysis repository owner</td>
</tr>
</tbody>
</table>

User roles

User roles determine which features of IBM Information Server users can use. For some suite components, it also determines which projects a user can access.
User roles can be defined at several levels that build on one another. Users derive authority from the union of their role in IBM Information Server (the suite role), their role in the suite component (for example, IBM WebSphere Information Analyzer or IBM Information Server FastTrack), and the role that they perform in an assigned project (the project role).

**Suite**

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

**Component**

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

**Project**

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

**Assigning user roles**

Typically, an IBM Information Server administrator assigns suite-level roles and component-level roles. Both roles are assigned by using the IBM Information Server console or Web console.
After the security roles are configured, the administrator of each component further defines the project-level roles in the console, Web console, or the WebSphere DataStage Administrator client. To perform the actions of a particular project-level role, you must also have suite-level access and access to the component that owns the project. For example, to be a DataStage developer, you must be assigned the roles of suite user and component-level DataStage user, as well as the DataStage developer project role.

The following figure shows the security roles.

![IBM Information Server Security Roles](image)

Figure 24. IBM Information Server security roles

**Tips for setting up security**

Refer to these additional tips when you are setting up security.

When setting up security, keep these tips in mind:

- If you plan to change the directory configuration, careful planning is needed for your installation so that the correct configuration can be selected during installation or you can configure the user directory directly after installation. Attempting to change the user directory after IBM Information Server components have been used by multiple users will cause the loss of all of the previous security information and is not recommended.

- Active administrator user accounts must exist for IBM Information Server and WebSphere Application Server. The WebSphere Application Server administrator user will be an IBM Information Server administrator by default.

- If you use an external user registry, password restrictions are imposed by that registry. If you use the IBM Information Server internal registry, passwords can contain any letters or digits, including the following special characters: _-\$:
Configuring user registries for IBM Information Server

A user registry contains valid user names and passwords. To log in to IBM Information Server, a user must have a user name and password in the user registry.

IBM Information Server uses the user registry that is configured in WebSphere Application Server for directory access.

After you install IBM Information Server, you can change to a different user registry or configure an LDAP-compliant user registry. Change user registries as a post-installation task; do not change user registries after the system has been in production. For production systems, you might want to migrate to a new installation to avoid any security issues and risks. Otherwise, there might be a mismatch between the users of the old and new registries.

To configure the user registries, you must perform two configuration tasks:

1. **Configure the user registry in WebSphere Application Server**
2. **Run the AppServerAdmin command to update the new credentials across your configuration**

If you must switch the user registry after the system has been in production, refer to "Switching the user registry configuration for a system in use" on page 55.

To switch user registries after installation, select one of the following options:

**Related tasks**

- [Using specific directory servers as the LDAP server](#)

**Running the AppServerAdmin command**

After you configure the user registry in IBM WebSphere Application Server, you must run the AppServerAdmin command to update the new credentials across your configuration.

If you change the default WebSphere administrator user name and password, this command updates the user name and password throughout the WebSphere Application Server configuration. You must run this command to complete the WebSphere Application Server configuration changes.

To run the AppServerAdmin command:

From the command line, enter the following command:

**Windows**

```
AppServerAdmin.bat -was -user <was admin username> -password <was admin password>
```

**Linux**

```
AppServerAdmin.sh -was -user <was admin username> -password <was admin password>
```

Where `<was admin username>` and `<was admin password>` are the default WebSphere Application Server user name and password specified during the WebSphere Application Server user registry configuration.
This command is available in the ASBServer\bin directory of your IBM Information Server directory, for example C:\IBM InformationServer\ASBServer\bin.

Related reference

“AppServerAdmin command” on page 89
If you change the default WebSphere Application Server administration credentials or the repository credentials, use the AppServerAdmin command to update the new credentials across your configuration.

Switching to the local operating system user registry

When you install IBM Information Server, the internal user registry is selected by default. After installation is complete, you can configure the suite to use the local operating system user registry.

You might want to change user registries if you want user credentials to be verified against the local operating system or if you test your installation with the internal registry and want to use a local operating system in production. Refer to the IBM WebSphere Application Server documentation topic [local operating system user registries] for more information.

Related tasks

“Switching the user registry configuration for a system in use” on page 55
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 complete this procedure.

Related reference

“AppServerAdmin command” on page 89
If you change the default WebSphere Application Server administration credentials or the repository credentials, use the AppServerAdmin command to update the new credentials across your configuration.

Configuring WebSphere Application Server to use the local operating system user registry

To switch from an internal user registry to use a local operating system user registry, you must first update the WebSphere Application Server security settings and configure WebSphere Application Server to use the local operating system user registry.

To switch to the local operating system user registry:

1. Log in to the WebSphere Application Server Administrator console. The URL for the console takes the following form: http://[hostname:WSadminport]/IBM/console.
2. In the WebSphere Application Server Administration console, click Security → Global Security.
3. Ensure that the Use domain-qualified user IDs option is not selected.
4. In the User registries list, click Local OS.
5. Type the WebSphere Application Server administrator credentials in the Server ID and Server user password fields. The credentials that you specify must match an existing user account on the local operating system of the computer where the application server is running. WebSphere Application Server has a number of restrictions with regard to local operating system user registries on both UNIX and Windows such as the WebSphere Application Server processes must be run as root, NIS on UNIX is not supported, and use of domain...
accounts on Windows imposes access rights on the users that are running WebSphere processes. You must refer to the WebSphere Application Server documentation for specific details.

6. Click **OK**.
7. Click the **Save** link at the top of the page, and click the **Save** button.
8. On the Global Security page, ensure that **LTPA** is selected for the **Active authentication mechanism** setting.
9. From the Active user registry menu, select **Local OS in the Active user registry**, and click **OK**. If an error occurs, the application server is unable to authenticate with the local operating system by using the credentials that were provided on the Local OS page.
10. Click the **Save** link, and click the **Save** button.

Related tasks

- [Configuring local operating system user registries](#)

### Modifying the IBM Information Server security configuration to support the local operating system user registry

After you configure WebSphere Application Server to use the local operating system user registry, you must stop WebSphere Application Server, update the new administrator credentials across your configuration, and then restart WebSphere Application Server.

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

To modify the security configuration:

1. Stop WebSphere Application Server.
2. From the command line, enter the following command. This command is available in the ASBServer\bin directory of your IBM Information Server directory, for example C:\IBM InformationServer\ASBServer\bin.

   - **Windows:**
     
     ```
     AppServerAdmin.bat -was -user <was admin user id> -password <was admin password>
     ```

   - **UNIX:**
     
     ```
     AppServerAdmin.sh -was -user <was admin user id> -password <was admin password>
     ```

   Where `<was admin user id>` and `<was password>` must match the credentials provided in the WebSphere Application Server console in "Configuring WebSphere Application Server to use the local operating system user registry" on page 48.
3. Restart WebSphere Application Server.

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

### Switching to the internal user registry

You can configure the IBM Information Server internal user registry during installation or after installation. The IBM Information Server internal user registry stores users and groups in the metadata repository.
To switch to the internal registry after installation, complete the following steps:

**Creating the WebSphere Application Server default administrator in the internal registry**

If you switch from an external registry to an internal registry, you must run the DirectoryAdmin command to create the WebSphere Application Server default administrator in the internal registry.

The default WebSphere administrator is also automatically configured as the initial new IBM Information Server default administrator. After the user registry configuration change, you can open the IBM Information Server Web console and grant suite administrator privileges to other users as needed.

To create the WebSphere Application Server default administrator in the internal registry:

From the command line, enter the following command. This command is available in the ASBServer\bin directory of your IBM Information Server directory, for example C:\IBM InformationServer\ASBServer\bin.

On Windows:

```
DirectoryAdmin.bat -user -userid <was admin username> -password <was admin password> -admin
```

On UNIX:

```
DirectoryAdmin.sh -user -userid <was admin username> -password <was admin password> -admin
```

Where `<was admin user id>` is the default WebSphere Application Server administrator user id and `<was password>` is the password of the default WebSphere Application Server administrator.

You can now configure WebSphere Application Server to use the internal user registry.

**Related reference**

[“AppServerAdmin command” on page 89](#)

If you change the default WebSphere Application Server administration credentials or the repository credentials, use the AppServerAdmin command to update the new credentials across your configuration.

[Creating a user in the IBM Information Server user registry](#)

Use the following command to create a user in the IBM Information Server internal user registry. This command should only be used for troubleshooting or recovery.

**Configuring WebSphere Application Server to use the internal user registry**

To switch to the internal user registry, you must configure the application server to use the internal user registry.

An IBM WebSphere Application Server custom user registry is installed when you install the suite. The custom registry must be configured as the active user registry for the application server for it to work with the IBM Information Server internal user registry.

To configure the application server to use the internal user registry:
1. Log in to the WebSphere Application Server Administrator console. The URL
for the console takes the following form: http://[hostname:WSadminport]/
IBM/console.
2. In the WebSphere Application Server Administration console, click Security →
Global Security.
3. Ensure that the Use domain-qualified user IDs option is not selected.
4. In the list of user registries, click Custom User Registry.
5. Enter the WebSphere Application Server administrator credentials in the
Server ID and Server user password fields. The credentials that you specify
must match an existing user account in the custom registry. The user
credentials that you provide must match the user ID and password that you
used when running the DirectoryAdmin command in "Creating the
WebSphere Application Server default administrator in the internal registry" on page 50.
6. Ensure that the custom registry class name is
com.ascential.acs.security.directory.custom.websphere.ASBUserRegistry.
7. Click OK.
8. Click the Save link at the top of the page, and click the Save button.
9. On the Global Security page, ensure that LTPA is selected for the Active
authentication mechanism setting.
10. Select Custom user registry in the Active user registry, and click OK. If an
error occurs, the application server is unable to authenticate with the local
operating system using the credentials that were provided under Custom User
Registry on the Global Security page. Ensure that you specified the same
credentials under Custom User Registry as you specified when you created
the default WebSphere Application Server administrator user by using the
DirectoryAdmin command.
11. Click the Save link, and click the Save button.
12. Stop WebSphere Application Server.
13. From the command line, enter the following command. This command is
available in the ASBServer\bin directory of your IBM Information Server
directory, for example C:\IBM InformationServer\ASBServer\bin.
   On Windows:
   AppServerAdmin.bat -was -user <was admin user id> -password
   <was admin password>
   On UNIX:
   AppServerAdmin.sh -was -user <was admin user id> -password
   <was admin password>
   Where <was admin user id> and <was password> matches the user credentials
   that you provided when you ran the DirectoryAdmin command.
14. Restart WebSphere Application Server, and verify that the application server
log files contain no errors.

Related tasks
"Switching the user registry configuration for a system in use" on page 55
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 complete this procedure.

Related reference
If you change the default WebSphere Application Server administration credentials or the repository credentials, use the AppServerAdmin command to update the new credentials across your configuration.

Switching to an LDAP user registry


To switch to an LDAP user registry, you must modify the WebSphere Application Server user registry and then modify the IBM Information Server security configuration.

About this task

You can configure any LDAP-compliant user registry for IBM Information Server. For more information on supported LDAP servers, refer to WebSphere Application Server V6.0.2 detailed system requirements.

Before you begin

If you change the user registry, start with a clean registry to prevent security issues and risks.

Configuring WebSphere Application Server to use LDAP

To switch from an internal user registry to use an LDAP user registry, you must first update the WebSphere Application Server security settings and configure WebSphere Application Server to use the LDAP user registry.

To configure WebSphere Application Server to use LDAP:

1. Log in to the WebSphere Application Server Administrator console. The URL for the console takes the following form: http://[hostname:WSadminport]/IBM/console.
2. Click Security → Global Security.
3. Ensure that the Use domain-qualified user IDs option is not selected.
4. In the User registries section, click the LDAP link.
5. Enter the information for connecting to your LDAP server including the following fields. The server user ID and password must be valid for connecting to the LDAP server. If you provide a base distinguished name or bind distinguished name, the distinguished names must use LDAP syntax. For example, CN=John Doe,OU=Rochester,O=IBM,C=US.

Server user ID

Type the WebSphere Application Server username. You can either enter the complete distinguished name (DN) of the user or the short name of the user, as defined by the user filter in the Advanced LDAP settings panel.

Server user password

Type the WebSphere Application Server password.

Type

Select the type of LDAP server from the list. The type of LDAP server determines the default filters that are used by WebSphere Application Server.
Host Enter the fully qualified host name of the LDAP server. You can enter either the IP address or the domain name system (DNS) name.

Port Enter the LDAP server port number. The default value is 389.

Base distinguished name (DN) Enter the base distinguished name (DN) of the directory service, which indicates the starting point for LDAP searches of the directory service. For example, for a user with a DN of cn=John Doe, ou=Rochester, o=IBM, c=US, specify the Base DN as any of the following options: ou=Rochester, o=IBM, c=US or o=IBM c=US or c=US. For authorization purposes, this field is case sensitive. This field is used to limit search scope.

Optional: Bind distinguished name (DN) Enter the bind DN name. The Bind DN is required only if anonymous access to the LDAP server is not allowed.

Optional: Bind password Enter the password that corresponds to the bind DN.

Reuse connection Ensure that this option is selected. This option specifies that the server should reuse the LDAP connection. Clear this option only in rare situations where a router is used to send requests to multiple LDAP servers and when the router does not support affinity. Leave this option selected for all other situations.

Optional: SSL enabled Select this option if you want to use Secure Sockets Layer communications with the LDAP server.

Optional: SSL configuration Select the Secure Sockets Layer configuration to use for the LDAP connection. This configuration is used only when SSL is enabled for LDAP. The default is DefaultSSLSettings. To modify or create a new SSL configuration, click Security → SSL.

Note: The DN that you provide in this screen must be carefully typed and checked. It must match the default casing that the LDAP server uses.

6. Click Apply.
7. To modify advanced settings, such as which ID the user can use to authenticate, click Advanced Lightweight Directory Access Protocol (LDAP) user registry settings in the Additional Properties section. For more information, refer to [publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/usec_advldap.html](publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/usec_advldap.html)
8. Click OK and on the next page click the Save link.
9. On the Global Security panel, select Lightweight Directory Access Protocol (LDAP) user registry from the Active User Registry field. Validation is only done when you click OK or Apply in the Global Security panel.
10. Click Apply. After you click Apply, WebSphere Application Server attempts to authenticate the user against the LDAP registry. This authentication tests the information that you entered and, if any information is incorrect, the authentication fails. If the authentication fails, check the information in Step 5.
11. Click the Save button to confirm your changes to your configuration. The registry changes take effect when you restart WebSphere Application Server later in the procedure.
For additional instructions on configuring WebSphere Application Server to use LDAP, refer to Configuring WebSphere Application Server for LDAP.

**Related tasks**

"Determining the LDAP distinguished name (DN)"

If you are configuring IBM Information Server to use an LDAP user registry, the full LDAP distinguished name (DN) of the suite administrator is required. If you cannot get the LDAP DN from your LDAP administrator, you might be able to use the following procedures to determine the LDAP DN.

**Determining the LDAP distinguished name (DN):**

If you are configuring IBM Information Server to use an LDAP user registry, the full LDAP distinguished name (DN) of the suite administrator is required. If you cannot get the LDAP DN from your LDAP administrator, you might be able to use the following procedures to determine the LDAP DN.

To determine the LDAP DN by using the WebSphere Application Server Administrator console:

1. Log in to the WebSphere Application Server Administrator console. The URL for the console takes the following form: `http://[hostname:WSadminport]/IBM/console`.
2. From the console, select Applications → Enterprise Applications → `application_name`.
3. Under Detail properties, click Security role to user/group mapping.
4. Select the Suite Admin role and click Look up users.
5. In the Search String field, enter an “*” (asterix) and click Search.

*By using a Windows computer that is registered with the Active Directory domain:*

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

To determine the LDAP DN by using a Windows computer that is registered with the Active Directory domain:

2. Open the Groups folder and double-click one of the groups.
3. In the Administrators Properties window, click Add.
4. In the Select users window, click Advanced.
5. In the Select Users window, perform a search for the 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.

**Modifying the IBM Information Server security configuration to support the LDAP user registry**

After you configure WebSphere Application Server to use an LDAP user registry, you must stop WebSphere Application Server, update the new administrator credentials across your configuration, and then restart WebSphere Application Server.

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

1. Stop WebSphere Application Server.
2. From the command line, enter the following command. This command is available in the ASBServer\bin directory of your IBM Information Server directory, for example C:\IBM InformationServer\ASBServer\bin.
   On Windows:
   
   AppServerAdmin.bat -was -user <was admin user id> -password <was admin password>
   
   On UNIX:
   
   AppServerAdmin.sh -was -user <was admin user id> -password <was admin password>
   
   Where <was admin user id> is the default WebSphere Application Server administrator user id and <was password> is the password of the default WebSphere Application Server administrator.

3. Restart WebSphere Application Server.

Note that the WebSphere Application Server administrator user name and password can be used to log into the IBM Information Server Web console. The WebSphere Application Server administrator is granted IBM Information Server administrator privileges by default. After you change the user registry, you can open the Web console and grant suite administrator access to additional users as needed.

**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 complete this procedure.

It is strongly recommended that you only switch the user registry as a post-installation task. If you must switch the user registry for a system that is in production, the following tasks will clean up all previous security configurations, such as role assignments, credential mappings, and access rights. These configurations are deleted from the repository and you must configure them again manually for the new users of the new registry.

All commands are available in the ASBServer\bin directory of your IBM Information Server directory, for example C:\IBM InformationServer\ASBServer\bin.

To switch the user registry configuration for a system in use:

1. **[Configuring user registries for IBM Information Server](#)** on page 47.
2. Save the WebSphere Application Server user registry changes and stop WebSphere Application Server. Do not restart WebSphere Application Server yet.
3. From the command line, enter the following command:
   On Windows:
   
   AppServerAdmin.bat -was -user <was admin username> -password <was admin password>
   
   On UNIX:
AppServerAdmin.sh -was -user <was admin username> -password
<was admin password>

Where the <was admin username> and <was admin password> are the default WebSphere Application Server user name and password that have been specified in Step 1. You must run this command to complete the WebSphere Application Server configuration changes.

4. From the command line, enter the following command to clean up all of the groups related to the security configuration:
   On Windows:
   DirectoryAdmin.bat -delete_groups
   On UNIX:
   DirectoryAdmin.sh -delete_groups

5. From the command line, enter the following command to clean up all of the users related to the security configuration:
   On Windows:
   DirectoryAdmin.bat -delete_users
   On UNIX:
   DirectoryAdmin.sh -delete_users

6. If you switch to the IBM Information Server internal user registry, you must run the following command from the command line again:
   On Windows:
   DirectoryAdmin.bat -was -user <was admin username> -password
   <was admin password>
   On UNIX:
   DirectoryAdmin.sh -was -user <was admin username> -password
   <was admin password>

7. Start WebSphere Application Server and ensure that the WebSphere SystemOut.log file contains no errors. This file is located in the following directory by default: IBM/WebSphere/AppServer/profiles/default/logs/server1/SystemOut.log.

   Related tasks
   "Switching to the local operating system user registry" on page 48
   When you install IBM Information Server, the internal user registry is selected by default. After installation is complete, you can configure the suite to use the local operating system user registry.

   "Configuring WebSphere Application Server to use the internal user registry" on page 50
   To switch to the internal user registry, you must configure the application server to use the internal user registry.

   Related reference
   "AppServerAdmin command" on page 89
   If you change the default WebSphere Application Server administration credentials or the repository credentials, use the AppServerAdmin command to update the new credentials across your configuration.

   Creating a user in the IBM Information Server user registry
   Use the following command to create a user in the IBM Information Server internal user registry. This command should only be used for troubleshooting or recovery.
Creating users and groups

If the IBM Information Server internal user registry is used, you can create users and groups by using the console or the Web console.

If you are using an external directory, such as the local operating system or LDAP, you must create users and groups by using the registry-specific administration tools.

Creating users in the console

If the IBM 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 IBM Information Server.

Prerequisites

You must have Administrator authority.

To create a user:
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 WebSphere 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.

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

Related concepts

"WebSphere Business Glossary roles” on page 66
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

"WebSphere DataStage and WebSphere QualityStage roles” on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

"WebSphere Information Analyzer roles” on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

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

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

You can assign operational metadata component roles to a user.

Creating groups in the console
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.

Prerequisites

You must have Administrator authority.

To create a group:
1. On the Home navigator menu, select Configuration → Groups.
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 user.
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 WebSphere 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.

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

Related concepts

For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.
“WebSphere DataStage and WebSphere QualityStage roles” on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

“WebSphere Information Analyzer roles” on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

“WebSphere Information Services Director roles” on page 71
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

“IBM Information Server FastTrack roles” on page 64
For IBM Information Server FastTrack, administrators can further define user authority by assigning suite component roles to IBM Information Server FastTrack users.

“IBM Metadata Workbench roles” on page 65
The suite administrator assigns roles that define the tasks that users of IBM Metadata Workbench can perform.

“Operational metadata roles” on page 69
You can assign operational metadata component roles to a user.

Related tasks

“Assigning groups to a project and specifying roles” on page 76
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.

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

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

To add users to a group:
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.

Related tasks

“Creating groups in the console” on page 58
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.
Creating users in the Web console
If the IBM 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 IBM Information Server.

Prerequisites
You must have suite administrator authority.

To create a user:
1. In the Web console, click the Administration tab.
2. In the Navigation pane, select Users and Groups → Users.
3. In the Users pane, click New.
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. 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 WebSphere Information Analyzer, you must assign the Information Analyzer Project Administrator, Data Administrator, or User role.
7. Click Save and Close to save the user information in the metadata repository.

Related concepts
“WebSphere Business Glossary roles” on page 66
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

“WebSphere DataStage and WebSphere QualityStage roles” on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

“WebSphere Information Analyzer roles” on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

“WebSphere Information Services Director roles” on page 71
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

“Security roles” on page 63
IBM Information Server supports role-based access control. Users derive authority from the union of their roles in IBM Information Server (the suite roles), their roles in the suite component, such as WebSphere Information Analyzer (the suite component roles), and the roles that they perform in an assigned project (the project roles).

Creating groups in the Web console
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group.

Prerequisites
You must have suite administrator authority.

To create a group:
1. In the Web console, click the Administration tab.
2. In the Navigation pane, select Users and Groups → Groups.
3. In the Groups pane, click New.
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 group to access. For example, if you are creating a group that will access WebSphere 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 Search. To view all users, do not enter any text in the fields and click Search.
   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.

Related concepts

“WebSphere Business Glossary roles” on page 66
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

“WebSphere DataStage and WebSphere QualityStage roles” on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

“WebSphere Information Analyzer roles” on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

“WebSphere Information Services Director roles” on page 71
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

“Security roles” on page 63
IBM Information Server supports role-based access control. Users derive authority from the union of their roles in IBM Information Server (the suite roles), their roles in the suite component, such as WebSphere Information Analyzer (the suite component roles), and the roles that they perform in an assigned project (the project roles).

Related tasks

“Adding users to a group in the Web console” on page 62
If the IBM Information Server internal user registry is used, you can add users to a group to quickly assign and reassign user roles.
Adding users to a group in the Web console

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

To add users to a group:
1. In the 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.
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 Search.</td>
</tr>
<tr>
<td>To view all users:</td>
<td>Do not enter any text in the fields and click Search.</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.

Related tasks

“Creating groups in the Web console” on page 60

Assigning 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, you can assign security roles to a user or group.

There are two levels of roles that are used to provide access to suite components and product modules:

The suite and product level roles

These roles can be assigned from the console or Web console. The roles are used to grant top-level and administrative access to IBM Information Server and its product modules, such as who can log in to IBM Information Server, who has IBM Information Server administrative rights, and who can access WebSphere DataStage, WebSphere QualityStage, or WebSphere Information Analyzer with regular user privileges or as administrators.

Project level roles

These roles can be assigned on a project basis from the project management area of the console or, for WebSphere DataStage and WebSphere QualityStage, from the WebSphere DataStage Administrator client. The roles are product module specific, such as DataStage developer or Information Analyzer Data Steward.
Typically, in the console or Web console, an IBM Information Server administrator configures which users can log in to IBM Information Server, which product modules the users have access to, and whether the users are regular users or administrators of these product modules.

After those security roles are configured, the administrator of each product module further defines the security configuration in the console, Web console, or the WebSphere DataStage Administrator client by assigning project roles to the users.

**Security roles**

IBM Information Server supports role-based access control. Users derive authority from the union of their roles in IBM Information Server (the suite roles), their roles in the suite component, such as WebSphere Information Analyzer (the suite component roles), and the roles that they perform in an assigned project (the project roles).

Security configuration is performed by two levels of administrators:

**IBM Information Server administrators**

Administrators who 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. IBM Information Server administrators can also configure credential mappings for IBM WebSphere Information Analyzer, IBM WebSphere DataStage, and IBM WebSphere QualityStage users. IBM Information Server administrators must have, at least, the Suite Administrator and Suite User role assigned to their user names. During installation, a default IBM Information Server administrator is created to perform the initial installation tasks and configure the user registry. Note that the default WebSphere Application Server administrator is always automatically configured as an IBM Information Server administrator when you restart WebSphere Application Server.

**IBM Information Server suite component administrators**

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

**Suite roles**

**Suite Administrator**

Provides maximum IBM Information Server administration privileges.

**Suite User**

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

The following figure shows the IBM Information Server security roles.
Related tasks

"Creating users in the Web console” on page 60

If the IBM 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 IBM Information Server.

"Creating groups in the Web console” on page 60

If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group.

"Assigning security roles to a user in the Web console” on page 76

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

"Assigning security roles to a group in the Web console” on page 77

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

"Viewing the roles that are assigned to a user or a group” on page 78

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.

IBM Information Server FastTrack roles

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

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

FastTrack User
A FastTrack User can use IBM Information Server FastTrack functions.
Users must be authorized to projects before they can use functions for creating, managing, and viewing mapping specifications.

Related tasks
“Creating users in the console” on page 57
If the IBM 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 IBM Information Server.

“Creating groups in the console” on page 58
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.

“Assigning security roles to a user in the console” on page 73
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

“Assigning security roles to a group in the console” on page 74
You can assign one or more suite and suite component roles to a group of users.

“Viewing the roles that are assigned to a user or a group” on page 75
In the 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.

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

IBM 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 Metadata Workbench users can perform.

The Metadata Workbench administrator should be familiar with the enterprise database metadata and data file metadata that is imported into the repository and 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.

Related tasks
“Creating users in the console” on page 57
If the IBM 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 IBM Information Server.
"Creating groups in the console" on page 58
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.

"Assigning security roles to a user in the console" on page 73
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

"Assigning security roles to a group in the console" on page 74
You can assign one or more suite and suite component roles to a group of users.

"Viewing the roles that are assigned to a user or a group" on page 75
In the 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.

WebSphere Business Glossary roles
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere 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.

Business Glossary Author
Can create and edit terms and categories and use terms to classify objects.

Business Glossary User
Can examine the metadata assets in the metadata repository, including the terms and the categories that contain terms.

Related tasks
"Creating users in the console" on page 57
If the IBM 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 IBM Information Server.

"Creating groups in the console" on page 58
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.

"Assigning security roles to a user in the console" on page 73
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

"Assigning security roles to a group in the console" on page 74
You can assign one or more suite and suite component roles to a group of users.

"Viewing the roles that are assigned to a user or a group" on page 75
In the 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.

"Creating users in the Web console" on page 60
If the IBM 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 IBM Information Server.

“Creating groups in the Web console” on page 60
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group.

“Assigning security roles to a user in the Web console” on page 76
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

“Assigning security roles to a group in the Web console” on page 77
You can assign one or more suite and suite component roles to a group of users.

“Viewing the roles that are assigned to a user or a group” on page 78
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.

**WebSphere DataStage and WebSphere QualityStage roles**
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere 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 WebSphere DataStage Administrator client.

**Suite component roles**

**DataStage and QualityStage Administrator**
Can perform the following tasks: assign project roles to WebSphere DataStage suite users in the WebSphere DataStage Administrator client, use the Administrator client to create, delete, and configure projects, mark projects as protected, unprotect projected projects, 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, and import objects into protected projects.

This role cannot edit jobs or other objects in protected projects.

**DataStage and QualityStage User**
Provides access to WebSphere DataStage and WebSphere QualityStage. Additionally, this role is used to filter the lists of users and groups that are shown in the WebSphere DataStage Administrator client. If an IBM Information Server user does not have this role, that user cannot access any of the WebSphere DataStage or WebSphere QualityStage product modules, even if that user has WebSphere DataStage or WebSphere 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, and view entire job log messages. This role can also use the Administrator client to perform limited tasks including changing project NLS settings, issuing server side DSEngine commands, and changing project properties (not protect/unprotect).
This role 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 WebSphere 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. This role can also use the DataStage Administrator client to perform limited tasks including changing the project NLS settings, issuing server side DSEngine commands, and changing project properties.

This role cannot edit jobs or other objects in protected projects, create, delete, or configure projects (can perform limited configuration tasks), or assign project roles to WebSphere DataStage suite users in the Administrator client.

**DataStage Operator**

Can perform the following tasks: use the Director client to run and schedule jobs and view entire job log messages (unless set to read first line only by WebSphere DataStage Administrator). This role can also use the Administrator client to perform limited tasks including changing project NLS settings, issuing server side DSEngine commands, 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, and 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, issuing server side DSEngine commands, and changing project properties (not protect/unprotect).

This role 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 WebSphere DataStage suite users in the Administrator client, or import objects into protected projects.

For more information, refer to the *IBM WebSphere DataStage Administrator Client Guide.*

**Related tasks**

- "Creating users in the console" on page 57
  If the IBM 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 IBM Information Server.

- "Creating groups in the console" on page 58
  If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.

- "Assigning security roles to a user in the console" on page 73
  All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.
"Assigning security roles to a group in the console” on page 74
You can assign one or more suite and suite component roles to a group of users.

"Viewing the roles that are assigned to a user or a group” on page 75
In the 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.

"Creating users in the Web console” on page 60
If the IBM 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 IBM Information Server.

"Creating groups in the Web console” on page 60
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group.

"Assigning security roles to a user in the Web console” on page 76
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

"Assigning security roles to a group in the Web console” on page 77
You can assign one or more suite and suite component roles to a group of users.

"Viewing the roles that are assigned to a user or a group” on page 78
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.

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.

Related tasks

"Creating users in the console” on page 57
If the IBM 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 IBM Information Server.

"Creating groups in the console” on page 58
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

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

In the 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.

**WebSphere Information Analyzer roles**

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

You can assign suite component roles in the console or the 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 WebSphere Information Analyzer, view the dashboard, and open a project.

**Project roles**

**Information Analyzer Business Analyst**

Reviews analysis results. This role 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. This role can run or schedule all analysis jobs.

**Information Analyzer Data Steward**

Provides read-only views of analysis results. This role can also view the results of all analysis jobs.

**Related tasks**

If the IBM 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 IBM Information Server.

If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.
"Assigning security roles to a user in the console" on page 73
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

"Assigning security roles to a group in the console" on page 74
You can assign one or more suite and suite component roles to a group of users.

"Assigning security roles to a user in the console" on page 75
In the 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.

"Creating users in the Web console" on page 60
If the IBM 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 IBM Information Server.

"Creating groups in the Web console" on page 60
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group.

"Assigning security roles to a user in the Web console" on page 76
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

"Assigning security roles to a group in the Web console" on page 77
You can assign one or more suite and suite component roles to a group of users.

"Assigning security roles to a user in the Web console" on page 78
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.

WebSphere Information Services Director roles
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

Suite component roles

Information Services 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 Information Services Director Administrator is automatically granted Information Services Catalog Manager authority.

Information Services Director Administrator
Provides access to all of the WebSphere Information Services Director design time functions, including the ability to manage projects, applications, and services. This role also provides the authority to import applications, export applications, and manage providers.

Information Services Director Consumer
Provides ability to invoke secured services.

Information Services Director Operator
Provides access to all of the WebSphere Information Services Director functions but does not have the authority to add, delete, or update projects, applications, or services.
**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**
Provides access to create, delete, and edit services, bindings, and operations. Also provides access to import and export projects.

**Information Services Director Project Administrator**
Provides access to create and delete applications, add and remove users and groups to projects, and edit project properties.

**Related tasks**

“Creating users in the console” on page 57
If the IBM 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 IBM Information Server.

“Creating groups in the console” on page 58
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group in a batch process.

“Assigning security roles to a user in the console” on page 73
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

“Assigning security roles to a group in the console” on page 74
You can assign one or more suite and suite component roles to a group of users.

“Viewing the roles that are assigned to a user or a group” on page 75
In the 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.

“Creating users in the Web console” on page 60
If the IBM 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 IBM Information Server.

“Creating groups in the Web console” on page 60
If the IBM Information Server internal user registry is used, you can create a group of users to assign security settings and roles to that group.

“Assigning security roles to a user in the Web console” on page 76
All users require authorization to access components and features of IBM Information Server. You can assign one or more suite and suite component roles to a user.

“Assigning security roles to a group in the Web console” on page 77
You can assign one or more suite and suite component roles to a group of users.

“Viewing the roles that are assigned to a user or a group” on page 78
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.
Assigning security roles in the 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.

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

Prerequisites
You must have suite administrator authority.

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.

To assign security roles to a user:
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.

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

Related concepts
"WebSphere Business Glossary roles“ on page 66
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

"WebSphere DataStage and WebSphere QualityStage roles“ on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

"WebSphere Information Analyzer roles“ on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

"WebSphere Information Services Director roles“ on page 71
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.
For IBM Information Server FastTrack, administrators can further define user authority by assigning suite component roles to IBM Information Server FastTrack users.

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

You can assign operational metadata component roles to a user.

Assigning security roles to a group in the console

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

Prerequisites

You must have suite administrator authority.

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.

To assign security roles to a group:

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.

Related concepts

For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

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

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

For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

For IBM Information Server FastTrack, administrators can further define user authority by assigning suite component roles to IBM Information Server FastTrack users.
”IBM Metadata Workbench roles” on page 65
The suite administrator assigns roles that define the tasks that users of IBM Metadata Workbench can perform.

”Operational metadata roles” on page 69
You can assign operational metadata component roles to a user.

Viewing the roles that are assigned to a user or a group
In the 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.

Prerequisites
You must have suite administrator authority.

To view the roles that are assigned to a user or group:
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 WebSphere DataStage, or in the IBM Information Server console.

Related concepts
”WebSphere Business Glossary roles” on page 66
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

”WebSphere DataStage and WebSphere QualityStage roles” on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

”WebSphere Information Analyzer roles” on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

”WebSphere Information Services Director roles” on page 71
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

”IBM Information Server FastTrack roles” on page 64
For IBM Information Server FastTrack, administrators can further define user authority by assigning suite component roles to IBM Information Server FastTrack users.

”IBM Metadata Workbench roles” on page 65
The suite administrator assigns roles that define the tasks that users of IBM Metadata Workbench can perform.

”Operational metadata roles” on page 69
You can assign operational metadata component roles to a user.

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.
To add users to a project and assign roles:

1. In the console, open the project that you want to assign users and roles to.
2. On the Overview navigator menu in the 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.

To assign groups to a project and select roles:

1. In the console, open the project that you want to assign groups to.
2. On the Overview navigator menu in the 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.

Related tasks

“Viewing the roles that are assigned to a user or a group” on page 78

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.

Assigning security roles in the 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.

In the 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 Web console

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

Prerequisites

You must have suite administrator authority.
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.

To assign security roles to a user:
1. In the 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 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 and Close to save the authorizations in the metadata repository.

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

Related concepts

“WebSphere Business Glossary roles” on page 66
For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

“WebSphere DataStage and WebSphere QualityStage roles” on page 67
For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

“WebSphere Information Analyzer roles” on page 70
For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

“WebSphere Information Services Director roles” on page 71
For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

“Security roles” on page 63
IBM Information Server supports role-based access control. Users derive authority from the union of their roles in IBM Information Server (the suite roles), their roles in the suite component, such as WebSphere Information Analyzer (the suite component roles), and the roles that they perform in an assigned project (the project roles).

Assigning security roles to a group in the Web console
You can assign one or more suite and suite component roles to a group of users.

Prerequisites

You must have suite administrator authority.

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.
To assign security roles to a group:

1. In the 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 **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 and Close** to save the authorizations in the metadata repository.

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

**Related concepts**

- "WebSphere Business Glossary roles" on page 66
  For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

- "WebSphere DataStage and WebSphere QualityStage roles" on page 67
  For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

- "WebSphere Information Analyzer roles" on page 70
  For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

- "WebSphere Information Services Director roles" on page 71
  For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

- "Security roles" on page 63
  IBM Information Server supports role-based access control. Users derive authority from the union of their roles in IBM Information Server (the suite roles), their roles in the suite component, such as WebSphere Information Analyzer (the suite component roles), and the roles that they perform in an assigned project (the project roles).

**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.

**Prerequisites**

You must have suite administrator authority.

To view the roles that are assigned to a user or group:

1. In the 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**.
5. In the Roles pane, view the list of assigned suite, suite component, or project roles. Project roles are assigned in the context of a project in WebSphere DataStage or in the IBM Information Server console.

**Related concepts**

- "WebSphere Business Glossary roles" on page 66
  For WebSphere Business Glossary, administrators can further define user authority by assigning suite component roles to WebSphere Business Glossary users.

- "WebSphere DataStage and WebSphere QualityStage roles" on page 67
  For WebSphere DataStage and QualityStage, administrators can further define user authority by assigning suite component and project roles to WebSphere DataStage and WebSphere QualityStage users.

- "WebSphere Information Analyzer roles" on page 70
  For WebSphere Information Analyzer, administrators can further define user authority by assigning suite component and project roles to WebSphere Information Analyzer users.

- "WebSphere Information Services Director roles" on page 71
  For WebSphere Information Services Director, administrators can further define user authority by assigning suite component roles to WebSphere Information Services Director users.

- "Security roles" on page 63
  IBM Information Server supports role-based access control. Users derive authority from the union of their roles in IBM Information Server (the suite roles), their roles in the suite component, such as WebSphere Information Analyzer (the suite component roles), and the roles that they perform in an assigned project (the project roles).

**Related tasks**

- "Assigning groups to a project and specifying roles" on page 76
  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.

### Configuring credential mappings

WebSphere Information Analyzer, WebSphere DataStage, and WebSphere QualityStage require that there is a valid operating system user id on the computer where the engine tier is installed. For each IBM Information Server user that needs to access the IBM Information Server engine, you must map the IBM Information Server user credentials to valid operating system user credentials that exist on the engine tier.

The operating system user id must have modify permissions for all the subdirectories of the IBM Information Server directory. To grant IBM Information Server users access to the IBM Information Server engine, you can share the user registry, specify default credentials, or map the credentials on a user by user basis.

Based on your configuration environment, you can select one of the following methods for configuration mapping. Note that the method is specified on a per IBM Information Server engine basis.

**Related tasks**

- "Granting access to WebSphere DataStage and WebSphere QualityStage users" on page 83
  After you share the user registry or define credential mappings, you must give your users access to WebSphere DataStage and WebSphere QualityStage.
Sharing a user registry

If the IBM Information Server user registry is the same as the engine tier user registry, you can share the user registry.

You must configure and ensure that the operating system where the engine tier is installed uses the same user registry as IBM Information Server. If IBM Information Server is configured to use the internal user registry, you cannot share the user registry. You must configure the credential mapping on a per user basis or specify a default mapping for all users that do not have a specific mapping.

The following list provides examples of deployment configurations in which you can share a user registry.

- WebSphere Application Server and the IBM Information Server engine are installed on the same computer. IBM Information Server is configured to use the local operating system user registry.
- WebSphere Application Server is installed on one computer and configured to use an LDAP server for the user registry. The engine tier is installed on a separate computer with the operating system configured to use the same LDAP server. For example, if this configuration is a Windows environment that uses Windows Active Directory, the IBM Information Server engine can be installed on the same or different Windows computer that is registered in the domain of the same Windows Active Directory.

After you share the user registry, you must still grant the engine tier operating system users the required permissions. Refer to the WebSphere DataStage Administrator Client Guide for more information.

Specifying a shared user registry

If you configure and ensure that the operating system where the engine tier is installed uses the same user registry as IBM Information Server, you can share the user registry to grant IBM Information Server users access to the IBM Information Server engine.

**Prerequisites**

- You must have suite administrator authority.
- You must ensure that the user registries that you are sharing are the same and that no credential mapping is required.

To specify a shared user registry:

1. In the Web console, click the Administration tab.
2. In the Navigation pane, select Domain Management > DataStage Credentials.
3. Select the WebSphere DataStage server that you want to configure to use the same user registry as the metadata server.
4. Click Open Configuration.
5. In the Server Configuration pane, select Share User Registry between IBM Information Server and DataStage Server.
6. Click Save and Close.

After you share the user registry, you can grant WebSphere DataStage and WebSphere QualityStage access to your users. After you mark the user registry 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 IBM Information Server will be used to run data integration jobs in the engine.
Mapping individual credentials

If the operating system where the engine tier is installed is not using the same user registry as the WebSphere Application Server, you must map the credentials on a user by user basis or provide default credentials.

WebSphere Information Analyzer, WebSphere DataStage, and WebSphere QualityStage require that there is a valid operating system user id on the computer where the engine tier is installed. For each IBM Information Server user that needs to access the IBM Information Server engine, you must map the IBM Information Server user credentials to the engine tier operating system user credentials.

An administrator can perform credential mappings for a group of users or users can map their own credentials.

**IBM Information Server suite administrators and WebSphere DataStage and WebSphere QualityStage administrators**

Can define a default engine tier operating system credential to use for all users that are trying to connect to IBM Information Server engine and that do not have a specific credential mapping defined.

For each individual IBM Information Server user, these administrators can define specific engine tier operating system credentials to map to the IBM Information Server user credentials.

**WebSphere DataStage and WebSphere QualityStage users**

Can define their own credential mappings in the Web console. These users can only define credentials for their user name.

---

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.

**Prerequisites**

You must have suite administrator authority or WebSphere DataStage and WebSphere QualityStage administrator authority.

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.

To define the default engine tier operating system user credentials:
1. In the Web console, click the **Administration** tab.
2. In the Navigator pane, select **Domain Management** → **DataStage Credentials**.
3. Select the WebSphere DataStage server that you want to specify the default credentials for.
4. Click **Open Configuration**.
5. In the **User Name** field, type the default WebSphere DataStage credential user name.
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 is 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.

To configure your credentials:
1. In the Web console, click the **Administration** tab.
2. In the Navigation pane, select **Domain Management** → **DataStage Credentials**.
3. Select the WebSphere DataStage server that you want to work with.
4. Click **Open My Credentials**.
5. Type the user name and password that you want to use to connect to the IBM 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 is installed.
6. Click **Save and Close**.

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

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

You can allow suite users to configure their own credential mappings.

To configure credential mappings:
1. Log in to the IBM Information Server Web console by using Administrator credentials.
2. On the Administration tab, expand the **Domain Management** section and click **DataStage Credentials**.
3. Select the server where the services layer is installed.
4. Click **Open User Credentials**.
5. Click **Browse** to search for suite users.
6. Specify additional search criteria, and click **Search** 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 is installed.

10. Click Apply.

11. To map additional suite users, repeat Steps 5 through 11.

After you map the credentials and the suite user or group is added to a User role in the WebSphere DataStage and QualityStage Administrator client, you can log in to the WebSphere DataStage and QualityStage Administrator Designer client.

**Granting access to WebSphere DataStage and WebSphere QualityStage users**

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

To grant access to WebSphere DataStage and WebSphere QualityStage users:

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

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 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 Assign Roles.
   e. In the Assign Roles pane, assign the following roles to the user.

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

   **DataStage and QualityStage User**
   
   Required for any user that needs to log in to any of the WebSphere DataStage and WebSphere QualityStage product modules.

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

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

**Related tasks**

- "Specifying a shared user registry" on page 80
  If you configure and ensure that the operating system where the engine tier is installed uses the same user registry as IBM Information Server, you can share the user registry to grant IBM Information Server users access to the IBM Information Server engine.

- "Mapping individual credentials" on page 81
  If the operating system where the engine tier is installed is not using the same user registry as the WebSphere Application Server, you must map the credentials on a user by user basis or provide default credentials.
Configuring IBM Information Server for use with PAM/LDAP

The IBM WebSphere DataStage and WebSphere QualityStage server and can be configured to use the local operating system authentication or an external authentication mechanism (such as LDAP) through support for Pluggable Authentication Module (PAM).

You can configure the WebSphere DataStage and WebSphere QualityStage server to use the same user registry as the user registry that is used by IBM Information Server. If you share the same user registry and that user registry is not using the local operating system authentication services, then you must use the WebSphere DataStage and WebSphere QualityStage server PAM support. When the WebSphere DataStage and WebSphere QualityStage server and IBM Information Server are using the same user registry, no credential mapping is required between the suite users and the WebSphere DataStage and WebSphere QualityStage server users.

To configure the WebSphere DataStage and WebSphere QualityStage server to use PAM:
1. "Configuring the WebSphere DataStage and WebSphere QualityStage server through PAM (Linux, UNIX)."
2. "Configuring WebSphere Application Server to use LDAP" on page 52

Configuring the WebSphere DataStage and WebSphere QualityStage server through PAM (Linux, UNIX)

PAM is currently supported on AIX®, HP-UX, and Linux platforms.

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

To configure PAM on WebSphere DataStage and WebSphere QualityStage server:
1. Add to or create the PAM configuration file on your platform.
2. Stop the IBM Information Server engine by running the following command:
   
   $DHOME/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, dsepm, to the PAM configuration file. The name and the location of the PAM configuration file are platform dependant.

5. Regenerate the WebSphere DataStage configuration file by running the following command:
```bash
$DSHOME/bin/uv -admin -regen
```

6. Restart the WebSphere DataStage Server by running the following command:
```bash
$DSHOME/bin/uv -admin -start
```

**Examples of PAM configuration files**

### Linux

On a Linux system, you must create a file named dsepm in the `/etc/pam.d` directory. The following example shows the possible contents of the dsepm file on a 32-bit Linux system:

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

---

**Configuring Windows Server 2003**

After you install IBM Information Server on Microsoft Windows 2003 Server, you must perform an additional task to configure users. The following configuration is required for the engine tier computer and is only applicable to the users of the operating system where the engine tier is installed.

Which task you use depends on whether Microsoft Windows Server 2003 is or is not configured to be a domain controller.

The first time that an IBM Information Server client, such as the IBM WebSphere DataStage client or the IBM Information Server console, successfully logs in to the IBM Information Server services tier the server is added to the `registered-servers.xml` file. This file is located, by default, in the `InformationServer\ASBNode\eclipse\plugins\com.ibm.isf.client_configuration_8.1.0.0` directory.

When logging in to an IBM Information Server services tier for the first time, the operating system user on that client must have file system write permission to the `registered-servers.xml` file to enable the file to be updated. If the user does not have the required permission, the login fails.

System administrators can choose to limit access to specific IBM Information Server services tiers from any client by removing the file system write permission to the `registered-servers.xml` file. The administrator, or any one who has write permission, can log in ahead of time to each server that they want the user of the client to be able to 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, refer to "Configuring write permission to the `registered-servers.xml` file" on page 88.
Configuring permissions and groups (Windows Server 2003)

You must complete these tasks to configure users and groups to access to IBM 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 is installed.

To configure permissions and groups:
2. Configure users to log in.
   a. From the Start menu, click Control Panel → Administrative Tools → Local Security.
   b. From the main directory of the Local Security window, expand Local Policies → User Rights Assignment to display the policies.
   c. In the Local Security window click the policy Allow Log on Locally, and click Actions → Properties.
   d. In the Allow Log on Locally Properties window, click the Add User or Group button.
   e. In the Select Users, Computers, or Groups window, click the Locations button, click the name of your local computer, and click OK.
   f. In the Select Users, Computers, or Groups window, click the Advanced button, and then click the Find Now button.
   g. From the results of the search, click Authenticated Users, and then click OK three times to save the results and to return to the Local Security window.
   h. Close the Local Security Policy window.
3. Create a group of users.
   a. From the Start menu, click Control Panel → Administrative Tools → Computer Management.
   b. From the main directory of the Computer Management window, expand System tools → Local Users and Groups → Groups.
   d. In the New Group window, type the name for the group, click Create, and click Close.
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.
   c. Click Actions → Add to Group.
   d. In the User Properties window, click the Add button.
   e. In the Select Users, Computers, or Groups window, click the Location button.
   f. Click the name of your local computer, and then click OK.
   g. In the Select Users window, click the Advanced button.
   h. In the window that opens, click the Find Now button.
   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 server folder.
a. In Windows Explorer, locate the server folder. The default location is c:\IBM\Information Server\Server.

b. Click File → Properties.

c. In the Properties window, click the Security tab, and click Add.

d. In the Select Users, Computers, or Groups window, click Locations, click the name of the local computer, and click OK.

e. In the Select Users window, click Advanced.

f. In the window that opens, click Find Now.

g. Click the name of the group that you want to set permissions for.

h. Click OK twice.

i. In the Permissions list, click Modify, click Write in the Allow column, and click OK.

j. 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 2003 domain controller)**

If Windows Server 2003 is a domain controller, you must complete these tasks to configure users and groups to access IBM 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 is installed.

Because you cannot add the built-in authenticated users group to a group that you create in steps 2 and 3, you might prefer to skip steps 2 and 3 and use the authenticated users group directly.


2. Configure the server to allow local users to log in.

   a. From the Start menu, click Control Panel → Administrative Tools → Domain Security Policy.
   
   b. From the main directory of the Domain Security Policy window, expand Local Policies → User Rights Assignment to display the policies.
   
   c. In the Domain Security window, click the policy Allow Log on Locally and click Actions → Properties.
   
   d. In the Allow Log on Locally Properties window, click the Add User or Group button.
   
   e. Click Browse.
   
   f. In the Select Users, Computers, or Groups window, click Advanced and then click the Find Now button.
   
   g. From the results of the search, click Authenticated Users, and then click OK three times to return to the Domain Security Policy window.
   
   h. Close the Domain Security Policy window.

3. Create a group.

   a. From the Start menu, click 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 the name for the group.
   
   e. Leave Group scope as Global and Group type as Security, and click OK.
4. Add users to the group.
   a. From the Users in the current domain window, click the name of the group that you want to add users to, 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.

5. Set permissions on the server folder.
   a. In Windows Explorer, locate the server folder. The default location is c:\IBM\Information Server\Server.
   b. Click File ⇒ Properties.
   c. In the Properties window, click the Security tab, and click Add.
   d. In the Select Users, Computers, or Groups window, click the Locations button.
   e. In the window that opens, click the Advanced button, and then click the Find Now button.
   f. Click the name of the group that you want to set permissions for.
   g. Click OK, and then click OK again.
   h. Click the name of the group that you want to set permissions for.
   i. In the Permissions list, click Modify, click Write in the Allow column, and click OK.
   j. 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

To enable a successful client login to an IBM Information Server services tier for the first time, you can add or remove file system write permission to the registered-servers.xml file.

To configure write permission to the registered-servers.xml file:

1. In Microsoft Windows Explorer, locate the registered-servers.xml file. By default, this file is located in the following directory: \Information Server\ASBNode\eclipse\plugins\ibm.isf.client_configuration_8.1.0.0.
2. Select the file.
4. In the Properties window, click the Security tab.
5. Click Add.
6. In the Select Users, Computers, or Groups window, click Locations.
7. Select the name of your local computer and click OK.
8. In the Select Users window, click Advanced.
9. Click Find Now.
10. Select the name of the group or the user that you want to set permissions for.
11. Click OK.
12. Click OK.
13. In the Permissions list, click Allow or Deny in the Write column.
14. Click OK.
15. If you receive a message to confirm your changes, confirm by clicking Apply changes to this folder, subfolders and files.

Administration commands and tools

Use the following 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 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 two options: -was and -db.

-was option

If you change the default 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 Administration 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 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 xmeta or repository user credentials are used by WebSphere Application Server to connect to the IBM Information Server repository. If you change the xmeta or repository user name and password, this command updates the user name and password throughout WebSphere Application Server and the IBM Information Server configuration.

You might have to change the repository credentials if the original user was deleted from the registry or if that user’s password changed or expired. You must run this command each time the xmeta or repository user credentials are changed.

Syntax
The command syntax for the -was option:

Windows
AppServerAdmin.bat -was -user <username> -password <password>

UNIX Linux
AppServerAdmin.sh -was -user <username> -password <password>

The command syntax for the -db option:

Windows
AppServerAdmin.bat -db -user <repository_userid> -password <repository_password>

UNIX Linux
AppServerAdmin.sh -db -user <repository_userid> -password <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
The new password of the WebSphere Application Server user.

-db
Updates the new user credentials throughout the WebSphere Application Server configuration and the IBM 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 new repository user name.

-password
The new password of the repository user.

Related tasks

“Switching to the local operating system user registry” on page 48
When you install IBM Information Server, the internal user registry is selected by default. After installation is complete, you can configure the suite to use the local operating system user registry.

“Creating the WebSphere Application Server default administrator in the internal registry” on page 50
If you switch from an external registry to an internal registry, you must run the DirectoryAdmin command to create the WebSphere Application Server default administrator in the internal registry.

“Running the AppServerAdmin command” on page 47
After you configure the user registry in IBM WebSphere Application Server, you must run the AppServerAdmin command to update the new credentials across your configuration.

“Configuring WebSphere Application Server to use the internal user registry” on page 50
To switch to the internal user registry, you must configure the application server to use the internal user registry.

“Switching the user registry configuration for a system in use” on page 55
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 complete this procedure.

**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 Information Server directory service tasks. You should only use this tool and these commands for advanced configuration, such as configuring the IBM 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 IBM Information Server directory, for example C:\IBM\InformationServer\ASBSERVER\bin.

By using this tool, you can complete the following tasks:

**Creating a user in the IBM Information Server user registry**

Use the following command to create a user in the IBM Information Server internal user registry. This command should only be used for troubleshooting or recovery.

WebSphere Application Server does not need to be up and running to run this command.

**Syntax**

**Windows**

DirectoryAdmin.bat -user -userid <username> -password <password>

**UNIX**

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.

**Related tasks**

"Creating the WebSphere Application Server default administrator in the internal registry" on page 50

If you switch from an external registry to an internal registry, you must run the DirectoryAdmin command to create the WebSphere Application Server default administrator in the internal registry.

"Switching the user registry configuration for a system in use" on page 55

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 complete this procedure.
**Resetting the password of a user**

If you use the IBM 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.

WebSphere Application Server does not need to be up and running to run this command.

**Syntax**

**Windows**

DirectoryAdmin.bat -user -userid <username> -password <password>

**UNIX**

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.

**Assigning the IBM Information Server administrator role to a user**

Use the following command to add the IBM Information Server Suite Administrator role to a user. Only use this command if you are fixing your directory service configuration.

WebSphere Application Server does not need to be up and running to run this command unless the checkid option is also used.

**Syntax**

**Windows**

DirectoryAdmin.bat -user -userid <username> -admin

**UNIX**

DirectoryAdmin.sh -user -userid <username> -admin

**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 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 "Determining the LDAP distinguished name (DN)" on page 54.

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 IBM Information Server Suite Administrator role to the user.

You can also use this command with the -checkid parameter to check the existence of the user before applying the Suite Administrator role to that user. Use the following syntax:
DirectoryAdmin -user -userid <username> -admin -checkid

Checking to see if a user exists in the configured registry
Use this command to see if a user name exists in the configured registry. This command should only be used for troubleshooting or recovery.

Prerequisites
•  WebSphere Application Server must be up and running to run this command.

Syntax
DirectoryAdmin.bat -user -userid <username> -checkid

DirectoryAdmin.sh -user -userid <username> -checkid

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. Note that the user ID syntax differs depending on the user registry that is configured in 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 "Determining the LDAP distinguished name (DN)" on page 54.

**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.

**-checkid**
Checks to see if the user exists in the configured registry. If the user does not exist, you will receive a message that the user id is not found.

You can also use this command with the -admin parameter to check the existence of the user before applying the Suite Administrator role to that user. Use the following syntax:
```
DirectoryAdmin -user -userid <username> -admin -checkid
```

**Configuring the IBM Information Server directory service to use the internal user registry**
Use this command to point the IBM Information Server user registry to the internal user registry.

WebSphere Application Server does not need to be up and running to run this command. If 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 WebSphere Application Server startup, you can use the DirectoryAdmin command to force the provider change. This command can be used as a recovery or workaround mechanism.

**Syntax**

Windows
```
DirectoryAdmin.bat -set_provider ISF
```

UNIX
```
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 IBM Information Server directory service to use the internal user registry.

**Configuring the IBM Information Server directory service to use the WebSphere Application Server user registry**
Use this command to point the IBM Information Server user registry to the WebSphere Application Server user registry.

WebSphere Application Server does not need to be up and running to run this command. If it is up and 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 WebSphere Application Server startup, you can use the DirectoryAdmin command to force the provider change. This command can be used as a recovery or workaround mechanism.

**Syntax**

Windows

DirectoryAdmin.bat -set_provider WAS

UNIX Linux

DirectoryAdmin.sh -set_provider WAS

**Parameters**

The following options are available for the DirectoryAdmin command.

**-set_provider**

- The command line option that sets a provider to active.

**WAS**

- Indicates that the tool should configure the IBM Information Server directory service to use the WebSphere Application Server user registry.

**Deleting users from the IBM Information Server user registry**

Use this command to delete users from the IBM Information Server user registry. This command deletes all the users in the IBM Information Server user registry. If you are using an external registry, such as LDAP or a local OS, this command deletes only the proxies of the users that were created in the internal repository and their role assignments.

WebSphere Application Server does not need to be up and 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.

**CAUTION:**

This command deletes all the users in the IBM Information Server user registry. From the IBM Information Server Web console, you can delete users selectively.

Use this command only for troubleshooting.

**Syntax**

Windows

DirectoryAdmin.bat -delete_users

UNIX Linux

DirectoryAdmin.sh -delete_users

**Parameters**

The following options are available for the DirectoryAdmin command.

**-delete_users**

- Deletes all the users in the IBM Information Server user registry.
Deleting groups from the IBM Information Server user registry

Use this command to delete groups from the IBM Information Server user registry. This command deletes all the groups in the IBM Information Server user registry. If you are using an external registry, such as LDAP or a local OS, this command deletes only the proxies of the groups that were created in the internal repository and their role assignments.

WebSphere Application Server does not need to be up and 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.

CAUTION:
This command deletes all the groups in the IBM Information Server user registry. From the IBM Information Server Web console, you can delete groups selectively.

Use this command only for troubleshooting.

Syntax

Windows
DirectoryAdmin.bat -delete_groups

UNIX Linux
DirectoryAdmin.sh -delete_users

Parameters

The following options are available for the DirectoryAdmin command.

-delete_groups
   Delets all the groups in the IBM 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.

Prerequisites
- WebSphere Application Server must be up and running to run this command.

Syntax

Windows
DirectoryAdmin.bat -user -search -idp <userid_pattern> -max_count <maxcount>

UNIX Linux
DirectoryAdmin.sh -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 that you want 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 pre-pended 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.

Prerequisites
- WebSphere Application Server must be up and running to run this command.

Syntax

Windows
DirectoryAdmin.bat -user -search -idp <groupid_pattern> -max_count <maxcount>

UNIX  Linux
DirectoryAdmin.sh -user -search -idp <groupid_pattern> -max_count <maxcount>

Parameters
The following options are available for the DirectoryAdmin command.

-group
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 that you want 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 pre-pended 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.

Prerequisites
- WebSphere Application Server must be up and running to run this command.
Syntax

DirectoryAdmin.bat -user -userid <username> -display

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 that you want to look up the details of. Note that the user ID syntax differs depending on the user registry that is configured in 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 "Determining the LDAP distinguished name (DN)" on page 54.

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.

-display
Displays the detailed information associated with that user name.

Troubleshooting examples that use the DirectoryAdmin tool

If you run into the following problems while administering IBM 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

Note: If you have multiple IBM Information Server Suite Administrators, you could instead ask one of those administrators to log in to the IBM Information Server Web console and reset the lost user password in the Web console.

User registry configuration is not working and you cannot log in to the Web console

To reset the user registry configuration to use the IBM Information Server internal user registry:
1. From the command line, set the IBM Information Server to use the IBM Information Server internal user registry by entering the following command:
   `DirectoryAdmin.bat -set_provider ISF`

2. Create the default IBM Information Server Suite administrator user by using the following command:
   `DirectoryAdmin.bat -user -userid <default isadmin userid> -password <password> -admin`

3. Log in to the WebSphere Application Server Administrator console and set the WebSphere Application Server user registry to the IBM Information Server internal user registry.

To reset the user registry configuration to use the WebSphere Application Server user registry:
1. Ensure that the WebSphere Application Server user registry is configured to use the local OS or LDAP user registry of your choice.
2. From the command line, set IBM Information Server to use the WebSphere Application Server user registry by entering the following command:
   `DirectoryAdmin.bat -set_provider WAS`

3. Assign a user the necessary security roles to make that user the default IBM Information Server Suite Administrator by entering the following command:
   `DirectoryAdmin.bat -user -userid <default isadmin> -admin`

   The default IBM Information Server administrator user syntax differs depending on the user registry that is configured in 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 “Determining the LDAP distinguished name (DN)” on page 54.
Chapter 11. Deploying IBM Information Server assets

You can deploy IBM Information Server assets with IBM Information Server Manager, and you can use IBM WebSphere Business Glossary to move categories and terms from one IBM Information Server repository to another, such as from a development environment to a production environment.

Each deployment package you create by using the IBM Information Server Manager comprises a number of WebSphere DataStage and QualityStage objects. When you are ready, you deploy the package that you have built to the specific project on the specified domain.

In a basic deployment scenario, a set of WebSphere DataStage objects is moved from a development environment to a test or production environment. The objects make up some or all of an application, but are not necessarily dependent on each other. The objects that make up the set might be developed by different users, possibly in different WebSphere DataStage projects.

You can deploy any selected items in the Repository view to the target server if you created the package and have the authority to attach to the target domain. You can also deploy from the package when connectivity does not exist between the source and target systems.

For IBM WebSphere Business Glossary, you can export your entire glossary from one instance of IBM Information Server, and import it to the metadata repository on another instance.

The contents of a glossary are exported to an archive file that is in XML Metadata Interchange (XMI) format. You can then import the archive file into a metadata repository on a different instance of IBM Information Server. The import and export utilities preserve the relationships between terms and categories, their links to related IT assets, and their links to stewards. The IT assets and stewards themselves are not exported or imported.

During the import, if the IT assets and stewards exist in the metadata repository, the relationships are re-established. If you later import IT assets and stewards into the repository, the relationships are re-established to the categories and terms that you imported.
Chapter 12. Managing licenses

In the Web console, you can view a list of the features and unit counts that are associated with a licensed component of IBM Information Server and you can upload a new license file. A new license file can modify any of the licensed components.

Viewing a list of licensed components in the suite

You can view a list of licensed components in the suite and the features and unit counts that are associated with a licensed component.

To view a list of licensed components in the suite:
1. In the Web console, click the Administration tab.
2. In the Navigation pane, select Domain Management → Licensing
3. Select the component that you want to view.
4. Click View. The Licensing Features pane shows the features and unit counts that are associated with that license.

The unit count for each type of feature is measured differently. Server features are measured in numbers of licensed processor value units (PVUs) or central processor units (CPUs). Client features are measured in numbers of seats, concurrent connections, or authorized users. A client feature can specify a certain number of seats, concurrent connections, or authorized users or an unlimited quantity.

Updating the license before adding new product modules and components

The suite installation wizard registers your license when you install IBM Information Server. If you purchase additional product modules or components after you install the suite, you must update the license in the services tier before you can install the new modules.

Prerequisites
- You must have suite administrator authority.
- Obtain a new license from the IBM Information Server License Portal or your IBM Sales Administrator. A license file always contains all of the products that you are licensed to use. When you add new products to your license, the license file must include all of the existing licensed products as well as the newly acquired products.

About this task

Obtain a license file and complete this task if any of the following conditions apply:
- You are adding additional product modules.
- You are upgrading from IBM Information Server FastTrack Version 8.0.1. *
- You are upgrading from IBM Metadata Workbench Version 8.0.1. *
- You are upgrading from IBM Information Server Business Glossary Anywhere, Version 8.0.1. *
If the current license has a date that is before May 20, 2008 and if you previously installed this product, you can use the IBM Information Server installation program to upgrade the product. However, you must obtain and upload a new license file that includes this product. You can obtain and upload the updated license file either before or after you upgrade to IBM Information Server Version 8.1. If the current license has a date prior to May 20, 2008 but you did not previously install the product, you must obtain and upload a new license file that includes this product before you can use the IBM Information Server Version 8.1 installation program.

**Procedure**

To update the license:

1. Ensure that your new license file is on a computer that can run the Information Server Web console.
2. Use one of the following methods to log in to the Web console as a suite administrator:
   - Click **Start** → **IBM Information Server** → **IBM Information Server Web Console**.
   - Open a Web browser and go to the URL for the Web console. The URL takes the form, `services_host:port`, where `services_host` is the URL or IP address of the server where the services tier is installed and `port` is the port that is assigned to the Web console. The default port is 9080.
3. On the Administration tab, click **Domain Management** → **Licensing**.
4. Click "Upload a Licensing File."
5. Select your .xml license file and click **Upload**.

**Accessing the license file**

The .xml license file controls which product modules you can install, which features are available in each client, and whether a client can connect to the services for IBM Information Server.

**About this task**

When you install the services tier, you must specify the location of a license file. When you install additional product modules, the installation program reads the license information that is stored at services tier. If you later obtain additional products, you must obtain a new license file and upload the file to the services tier.

The license file controls which features are enabled in the clients. For example, if you have a license for IBM WebSphere Information Analyzer, after you install the client and start the IBM Information Server console, the user interface that you use to analyze data is available. For a client to connect to a services tier, the services that correspond to the client must be installed and licensed for that services tier.

You must obtain a license file before you start the installation.

**Procedure**

To access the license file:

1. Obtain your license file from your IBM Sales Administrator or directly through the IBM Information Server License Key Portal as described in your product Proof Of Entitlement.
2. Before you install the suite, ensure that the computer where you perform the installation can access the license file. After you install the suite, the license information is stored at the services tier, and the original .xml file is no longer used.

3. After you install the suite, use the IBM Information Server Web console to update the license.
Chapter 13. Managing active sessions

In the Web console, you can view a list of all the users that are currently connected to the server that you logged on to.

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 Web console, you can view and manage the active user sessions.

Prerequisites

You must have suite administrator authority.

A user session is an instance of a user with a connection to the metadata 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.

To view all active sessions:
1. In the Web console, click the Administration tab.
2. In the Navigation pane, select Session Management → Active Sessions. The Active Sessions pane shows the users that are currently connected to the server.

Related tasks

“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.

“Opening user details” on page 108
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.

“Disconnecting a session” on page 109
You can disconnect an individual user session.

“Disconnecting all sessions” on page 108
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.

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.

Prerequisites

You must have suite administrator authority.
To set session limits:
1. In the 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.

Related tasks

“Viewing all active sessions” on page 107
In the Web console, you can view and manage the active user sessions.

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.

Prerequisites
You must have suite administrator authority.

To open user details:
1. In the 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.

Related tasks

“Viewing all active sessions” on page 107
In the Web console, you can view and manage the active user sessions.

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.

Prerequisites
You must have suite administrator authority.

To disconnect all sessions:
1. In the 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 OK. All sessions are immediately ended.

Related tasks

“Viewing all active sessions” on page 107
In the Web console, you can view and manage the active user sessions.
Disconnecting a session

You can disconnect an individual user session.

**Prerequisites**

You must have suite administrator authority.

To disconnect a session:
1. In the 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**. The session is immediately ended.

**Related tasks**

“Viewing all active sessions” on page 107

In the Web console, you can view and manage the active user sessions.
Chapter 14. 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 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 IBM Information Server suite component defines relevant logging categories.

**Related concepts**

“Logging” on page 25

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

**Logging components**

A logging component is a named entity that represents a suite component in IBM Information Server or a shared service, such as the sessions or scheduling, 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 ASCL-ASB-AGENT-RA has one set of logged messages for the Resource Adapter, which is a functional aspect of the logging component called the WebSphere Metadata Server agent.

**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
You can use the debug level and trace level to troubleshoot problems at runtime that involve specific logging categories.

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>
<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>
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.

Related concepts

“Logging” on page 25
You can configure log views to manage the log messages that are generated when activities run in the suite.

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.

Prerequisites

You must have suite administrator or suite user authority.

To create a view of logged events:
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. 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.

To view logged events:
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.

To edit a log view:
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. 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.

To copy a log view:
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. 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.

Prerequisites

You must have suite administrator authority.

To purge logged messages:
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.

Managing logging views in the Web console

In the Administration tab of the 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 Web console

You can create views of events that suite component users and shared services initiate. These events are stored in the metadata repository.
Prerequisites

You must have suite administrator or suite user authority.

To create a view of logged events:
1. In the 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</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To specify a date range:</td>
<td>1. Select <strong>Range</strong>.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>To schedule real-time update:</td>
<td>1. Select <strong>Real-Time Logging</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Specify the number of events to include and the refresh rate, in seconds.</td>
</tr>
<tr>
<td>To specify elapsed time:</td>
<td>1. Select <strong>Interval</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Specify an interval number and select the type of interval, such as 5 days.</td>
</tr>
</tbody>
</table>

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 Web console**

You can open a log view to inspect the events that the view captured.

To view log events:
1. In the 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 Web console**
You can edit a view of logged events to modify which events are included in the log view.

To edit a log view:
1. In the 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 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.

To copy a log view:
1. In the 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 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.

**Prerequisites**
You must have suite administrator authority.

To purge logged messages:
1. In the 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.
Managing logging by component

For each logging component in IBM 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.

A logging component is a named entity that represents a suite component in IBM 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.

Prerequisites

You must have suite administrator authority.

To create a logging configuration:

1. In the 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.
6. In the New pane, type a name for the configuration.
7. Optional: In the Threshold menu, select a threshold level for writing logging events to the metadata repository.
8. Optional: Add 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. Modify the severity levels for the included categories.
10. Click Save and Close to save the configuration in the metadata repository.

Editing a logging configuration

If you want to change the logging categories and the filtering of the views, you can edit a logging configuration.

Prerequisites

You must have suite administrator authority.

To edit a logging configuration:

1. In the 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.

**Prerequisites**
You must have suite administrator authority.

To copy a logging configuration:
1. In the 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.

**Prerequisites**
You must have suite administrator authority.

To set a default logging configuration:
1. In the 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.

**Prerequisites**
You must have suite administrator authority.

You can create multiple logging configurations for each suite component. Only active logging configurations log events in the metadata repository.

To activate a logging configuration:
1. In the 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 15. Managing schedules

In the 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 WebSphere 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 a WebSphere Information Analyzer project in the IBM 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.

Related concepts

"Scheduling" on page 24

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

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 7. 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.

Prerequisites
You must have suite administrator or suite user authority.

To create a schedule view:
1. In the 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.
4. Specify the name, description, and access level of the view.
5. In the Filters pane, specify criteria for filtering schedules.
6. Click Save and Close to save the schedule view.

You can now view all of the schedules that are captured by this schedule view.

Related tasks
"Viewing the schedules that are captured by a schedule view" on page 123
You can view the schedules that are captured by a schedule view. From this view, you can then manage the schedules and scheduled tasks.
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.

Prerequisites

You must have suite administrator or suite user authority.

To create a schedule view from a copy:
1. In the 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. 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.

To view the schedules that are captured by a schedule view:
1. In the 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.

Related tasks

“Working with the scheduled tasks in a view” on page 124
After you create a schedule view, you can access the individual schedules and scheduled tasks that are captured by the view. You can start 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.

“Creating a schedule view” on page 122
You create a schedule view to access and manage a list of schedules and scheduled tasks.

Pausing all of 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.

To pause all of the schedules in a schedule view:
1. In the 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.

Related tasks
"Resuming all of 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.

---

### Resuming all of 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.

To reuse all of the schedules in a schedule view:

1. In the 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.

**Related tasks**

"Pausing all of the schedules in a view” on page 123

To pause a set of schedules, you can pause all of the schedules that are captured by a schedule view.

---

### Purging the history for all of 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.

To purge the history for all of the schedules in a view:

1. In the 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>To purge all run history:</td>
<td>Select All.</td>
</tr>
</tbody>
</table>
| To purge run history in a date range: | 1. Select Range.  
                                      | 2. Type dates and times or use the calendar to specify a start date and an end date. |

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 start 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.

**Related tasks**

"Viewing the schedules that are captured by a schedule view” on page 123

You can view the schedules that are captured by a schedule view. From this view, you can then manage the schedules and scheduled tasks.
Stopping a scheduled task

While you are viewing the schedules that are captured by a schedule view, you can stop a scheduled task.

To stop a scheduled task:
1. In the 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.

To purge the history of a scheduled task:
1. In the 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.

To view a list of completed schedules:
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.

To view a list of running schedules:
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.

To view a list of upcoming scheduled tasks:
1. In the View Schedules pane, select a schedule.
2. Click View Forecast.
Chapter 16. Backing up and restoring IBM 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 Information Server.

The services tier and engine tier consist of a variety of elements that require backup. The procedures documented here do not cover backup and restoring IBM Information Server clients that are running on Microsoft Windows computers. Backup 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.

Backup and Restore Synchronization

The engine installation contains files and configuration data that are linked to elements stored in the metadata repository. WebSphere DataStage and QualityStage projects are stored in the engine installation directory or elsewhere on the same computer and are linked to elements stored in the metadata repository. There is also information stored in files in the WebSphere Application Server directory that is linked to elements stored in the metadata repository. Finally, while the WebSphere Information Analyzer analysis database and WebSphere QualityStage Match Designer databases are separate from the metadata repository database, there are cross-database references between them.

Because of these interdependencies, to guarantee a successful backup, the metadata repository, WebSphere DataStage and WebSphere QualityStage projects, the WebSphere QualityStage Match Designer database, WebSphere Information Analyzer analysis database, and all of the file system-based elements that change after installation must be backed up simultaneously and the backup must occur while all services and WebSphere Application Server are shut down.

When you restore an installation, all of the same elements that were backed up need to be restored simultaneously before starting WebSphere Application Server or the WebSphere DataStage and QualityStage services.

The paths in the following tables assume that the product is installed in the default location. Your path will vary if you installed IBM Information Server in a different location.
# File system elements

**Table 8. File system elements that change after installation (Windows)**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\IBM\InformationServer</td>
<td>The base installation directory for IBM Information Server. Includes all files that are associated with the IBM Information Server installation instance. By default, this directory also stores WebSphere DataStage and WebSphere QualityStage projects.</td>
<td>All IBM Information Server installation actions, running of analysis jobs, WebSphere DataStage and QualityStage activities, configuration changes such as application of license files, and various other activities.</td>
</tr>
<tr>
<td>C:\Program Files\Common Files\InstallShield\Universal\IBM\InformationServer</td>
<td>Installation registry, latest version required for any future installation actions such as adding components to the installation or installing fix packs or patches.</td>
<td>Any installation done with the IBM Information suite installer. Fix pack and patch installs do not modify this file element.</td>
</tr>
<tr>
<td>C:\IBM\WebSphere\AppServer</td>
<td>The base installation directory for WebSphere Application Server which includes all installed services tier components of IBM Information Server.</td>
<td>All IBM Information Server installation actions, configuration changes made through the WebSphere Application Server or IBM Information Server administration consoles or external tools that modify configuration values.</td>
</tr>
<tr>
<td>WebSphere DataStage and QualityStage server project directories. By default: C:\IBM\InformationServer\Server\Projects However, you might choose to create project directories anywhere on the server’s file system.</td>
<td>Stores compiled WebSphere DataStage and QualityStage jobs and routines and metadata associated with running WebSphere DataStage and QualityStage jobs.</td>
<td>Whenever a user creates a new WebSphere DataStage and QualityStage project, a corresponding server directory is created to hold its runtime metadata.</td>
</tr>
</tbody>
</table>

**Table 9. File system elements that change after installation (Linux, UNIX)**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/IBM/InformationServer</td>
<td>The base installation directory for IBM Information Server. Includes all files that are associated with the IBM Information Server installation instance. By default, this directory also stores WebSphere DataStage and QualityStage projects.</td>
<td>All IBM Information Server installation actions, running of analysis jobs, WebSphere DataStage and QualityStage activities, configuration changes such as application of license files, and various other activities.</td>
</tr>
</tbody>
</table>
### Table 9. File system elements that change after installation (Linux, UNIX) (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux, UNIX: /root/InstallShield/Universal/IBM/InformationServer</td>
<td>Installation registry, latest version required for any future installation actions such as adding components to the installation or installing fix packs or patches.</td>
<td>Any installation done with the IBM Information suite installer. Fix pack and patch installs do not modify this file element.</td>
</tr>
<tr>
<td>AIX: /usr/lib/objrepos/InstallShield/Universal/IBM/InformationServer</td>
<td></td>
<td>All IBM Information Server installation actions, configuration changes made through the WebSphere Application Server or IBM Information Server administration consoles or external tools that modify configuration values.</td>
</tr>
<tr>
<td>/opt/IBM/WebSphere/AppServer</td>
<td>The base installation directory for WebSphere Application Server which includes all installed services tier components of IBM Information Server.</td>
<td>Whenever a user creates a new WebSphere DataStage or QualityStage project, a corresponding server directory is created to hold its runtime metadata.</td>
</tr>
<tr>
<td>DataStage server project directories. By default: /opt/IBM/InformationServer/Server/Projects However, you might choose to create project directories anywhere on the server’s file system.</td>
<td>Stores compiled WebSphere DataStage and QualityStage jobs and routines and metadata associated with running WebSphere DataStage and QualityStage jobs.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 10. File system elements that do not change or rarely change after installation (Windows)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Documents and Settings\installation user\WASRegistry</td>
<td>WebSphere Application Server installation and port registries. These are located under the user name of the user that performed the initial installation.</td>
<td>Not changed by use of IBM Information Server. Might be changed if WebSphere Application Server fixes or fix packs are installed separately. The vpd.properties file in the Windows directory might contain entries for other products unrelated to IBM Information Server if you use an InstallShield MultiPlatform-based installer.</td>
</tr>
<tr>
<td>C:\Documents and Settings\installation user\portdef.props</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\WINDOWS\vpd.properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C:\IBM\SDDLIB</td>
<td>The base installation directory for DB2 when installed as part of IBM Information Server.</td>
<td>Not changed by use of IBM Information Server. Installation of DB2 fixes or fix packs will modify files in this directory.</td>
</tr>
</tbody>
</table>

---

Chapter 16. Backing up and restoring IBM Information Server 129
Table 10. File system elements that do not change or rarely change after installation (Windows) (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\MKS Toolkit</td>
<td>UNIX emulation tools used by IBM Information Server</td>
<td>Not changed by use of IBM Information Server. Installation of IBM Information Server fixes or fix packs that identify they update MKS Toolkit will modify files in this directory.</td>
</tr>
</tbody>
</table>

Table 11. File system elements that do not change or rarely change after installation (Linux, UNIX)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>/root/.WASRegistry</td>
<td>WebSphere Application Server installation and port registries. These are located under the user name of the user that performed the initial installation.</td>
<td>Not changed by use of IBM Information Server. Might be changed if WebSphere Application Server fixes or fix packs are installed separately. The vpd.properties file in the Windows directory might contain entries for other products unrelated to IBM Information Server if you use an InstallShield MultiPlatform-based installer.</td>
</tr>
<tr>
<td>/root/portdef.props</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/root/vpd.properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/etc/services</td>
<td>Port assignments for the computer. When DB2 or WebSphere DataStage and QualityStage are installed the following entries are added: DB2_db2inst1 60000/tcp DB2_db2inst1_1 60001/tcp DB2_db2inst1_2 60002/tcp DB2_db2inst1_END 60003/tcp dsrpc 31538/tcp # RPCdaemon DSEngine@/u1/IBM/InformationServer/Server/DSEngine</td>
<td>Not changed after initial installation of IBM Information Server. Port assignments might be different in your installation.</td>
</tr>
</tbody>
</table>
Table 11. File system elements that do not change or rarely change after installation (Linux, UNIX) (continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/inittab</td>
<td>Services to be started on system boot. If you have installed DB2 as part of IBM Information Server this file is modified to add the following entry: fmc:234:respawn:/u1/IBM/db2/V9/bin/db2fmcd #DB2 Fault Monitor Coordinator</td>
<td>Not changed after initial installation of IBM Information Server.</td>
</tr>
</tbody>
</table>

| Start up and shutdown scripts.  | Scripts that are used to start and shut down the services associated with IBM Information Server. The ISFAgent script and DSEngine scripts are present only when the engine tier is installed. The ISFServer script is present only when the services tier is installed. | Not changed after initial installation of IBM Information Server. |

| /opt/IBM/db2/V9              | The base installation directory for DB2 when installed as part of IBM Information Server. | Not changed by use of IBM Information Server. Installation of DB2 fixes or fix packs will modify files in this directory. |

| /home/dasusr1                | The home directory of the DB2 Database Administrator account. Contains files required to run DB2. | Not changed by use of IBM Information Server. Installation of DB2 fixes or fix packs might modify files in this directory. |

| /home/db2inst1               | The home directory of the DB2 Database instance owner. Contains files required to run DB2. | Not changed by use of IBM Information Server. Installation of DB2 fixes or fix packs might modify files in this directory. |

Databases

Table 12. Databases that must be backed up

<table>
<thead>
<tr>
<th>Product module</th>
<th>Database</th>
<th>Default database name</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Metadata repository</td>
<td>xmeta</td>
</tr>
<tr>
<td>WebSphere Information Analyzer</td>
<td>Analysis results</td>
<td>iadb</td>
</tr>
<tr>
<td>WebSphere QualityStage</td>
<td>Match designer</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Other
On Windows installations, the registry stores a variety of values used by IBM Information Server. Backing up and restoring the registry must be done in conjunction with a full system backup.

The registry entries used by IBM Information Server do not change after initial installation.

---

**Backing up IBM Information Server components**

You can back up the components of IBM Information Server to ensure that you can recover your data in the event of hardware failure or other disaster.

**Prerequisites**

Stopping services might cause unexpected errors if clients are connected. You can determine if there are active connections and optionally terminated the connections in the IBM Information Server Web console. For more information, refer to Managing active sessions.

Although clients might not be connected, the server might still be in use if WebSphere DataStage and QualityStage jobs or WebSphere Information Analyzer analysis jobs are currently running or might start running before all server components can be stopped. You can use the IBM Information Server Web console to determine if any jobs are running or are scheduled to run in the near future. For more information, refer to Managing schedules.

**Procedure**

To back up IBM Information Server components:

1. Disconnect all user sessions.
2. [Shut down the IBM Information Server and WebSphere Application Server services](#).
3. Back up the metadata repository by using database management tools. See the vendor documentation for your database. Refer to the IBM DB2 Database for Linux, UNIX and Windows Information Center for the backup overview for IBM DB2.
4. If WebSphere Information Analyzer is installed, back up the analysis database used by WebSphere Information Analyzer. See the vendor documentation for your database. Refer to the IBM DB2 Database for Linux, UNIX and Windows Information Center for the backup overview for IBM DB2.
5. If WebSphere QualityStage is installed, back up the results database used for the WebSphere QualityStage Match Designer output. See the vendor documentation for your database. Refer to the IBM DB2 Database for Linux, UNIX and Windows Information Center for the backup overview for IBM DB2.
6. Ensure that you have backed up all system elements listed in Chapter 16, "Backing up and restoring IBM Information Server," on page 127.
7. Back up external files or libraries that are used by WebSphere DataStage and QualityStage jobs.
8. [Restart the IBM Information Server and WebSphere Application Server services](#).
Restoring IBM Information Server components

If you backed up the files, directories, and databases that are associated with IBM Information Server, you can restore these components to recover your data in the event of hardware failure or other disaster.

Restrictions

When you restore an installation, all of the same elements that were backed up need to be restored simultaneously before you start the IBM Information Server and WebSphere Application Server services.

About this task

This task assumes that you are recovering IBM Information Server on a system where IBM Information Server was previously installed and that a good backup was previously performed. It also assumes that the host name of the computer is identical to that of the computer on which the backup was performed and that all components are being restored in the exact same location that they originally were in. If a different host name is used, the system will be inoperable.

Procedure

To restore IBM Information Server components:

1. Disconnect all user sessions. Users should not be allowed to log in to the system at any point during the restore. Otherwise, it is possible that the restore might fail or users might lose data which will be overwritten when the metadata repository is restored.
2. Shut down the IBM Information Server and WebSphere Application Server services.
3. Restore the metadata repository by using database management tools. See the vendor documentation for your database platform. Refer to the IBM DB2 Database for Linux, UNIX and Windows Information Center for the restore overview for IBM DB2.
4. If WebSphere Information Analyzer was installed, restore the analysis database used by WebSphere Information Analyzer. See the vendor documentation for your database platform. Refer to the IBM DB2 Database for Linux, UNIX and Windows Information Center for the restore overview for IBM DB2.
5. If WebSphere QualityStage was installed, restore the results database used for the WebSphere QualityStage Match Designer output. See the vendor documentation for your database platform. Refer to the IBM DB2 Database for Linux, UNIX and Windows Information Center for the restore overview for IBM DB2.
6. Restore the system elements that are listed in Chapter 16, “Backing up and restoring IBM Information Server,” on page 127.
7. Restore external files or libraries that are used by WebSphere DataStage and QualityStage jobs.
8. Restart the IBM Information Server and WebSphere Application Server services.
Shutting down the IBM Information Server and WebSphere Application services

You must shut down IBM Information Server services and WebSphere Application Server services before backing up or restoring your system.

To shut down the IBM Information Server services and WebSphere Application Server services:

1. Stop the following services: ASB Agent, Logging Agent, DataStage Telnet Service, DSRPC Server, and DataStage Engine Resource Service. The engine services will only be present if you installed both the services tier and the engine tier on the same machine.

**Microsoft Windows**

To stop the services:

a. Log in with a user that has local administrator privileges.

b. Stop these services in the order that they appear in the table.

**Note:** On Windows, you can use the Services Administrative Tool or the sc command line tool to stop services.

<table>
<thead>
<tr>
<th>Service Full Name</th>
<th>Service Short Name</th>
<th>Process Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSRPC Service</td>
<td>dsrpc</td>
<td>dsrpced.exe</td>
</tr>
<tr>
<td>DataStage Telnet Service</td>
<td>dstelnet</td>
<td>tl_dsservice.ex</td>
</tr>
<tr>
<td>DataStage Engine Resource Service</td>
<td>DSEngine</td>
<td>dsservice.exe</td>
</tr>
<tr>
<td>ASB Agent</td>
<td>ASBAgent</td>
<td>ASBAgent.exe</td>
</tr>
<tr>
<td>Logging Agent</td>
<td>LoggingAgent</td>
<td>LoggingAgent.exe</td>
</tr>
</tbody>
</table>

**Linux or UNIX**

To stop the services:

a. Login as root.

b. Run the following command to source the dsenv file. The paths shown in this command assumes that the product is installed in the default location. Your path will vary if you installed IBM Information Server in a different location.

```
./opt/IBM/InformationServer/Server/DSEngine/dsenv
```

The /.dshome file contains the current engine location. Because UNIX systems support multiple instances of WebSphere DataStage, ensure that /.dshome contains the engine that you want to back up. Otherwise, the bin/uv -admin -stop command stops the instance of WebSphere DataStage that is in the /.dshome file.

c. Run the following commands to stop the WebSphere DataStage services. The paths shown in these commands assume that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

```
cd ./opt/IBM/InformationServer/Server/DSEngine
bin/uv -admin -stop
```
d. Run the following commands to stop the ASB Agent and the Logging Agent. The paths shown in these commands assume that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

```
  cd /opt/IBM/InformationServer/ASBNode/bin
  ./NodeAgents.sh stop
```

2. Stop WebSphere Application Server.

**Windows**

Click All Programs → IBM WebSphere → Application Server v6 → Profiles → default → Stop the server. If you installed IBM Information Server in a different WebSphere Application Server profile, you will need to select the correct profile.

**Note:** Additionally, you can stop WebSphere Application Server by using the command below. The path shown in this command assumes that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

```
C:\IBM\WebSphere\AppServer\bin\stopServer.bat
  -username <WAS_Username> -password <WAS_Password>
```

**Linux or UNIX**

The path shown in this command assumes that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

```
/opt/IBM/WebSphere/AppServer/profiles/default/bin/stopServer.sh
  -username <WAS_Username> -password <WAS_Password>
```

---

**Starting IBM Information Server and WebSphere Application services**

You must restart IBM Information Server services and WebSphere Application Server services after backing up or restoring your system.

To start IBM Information Server and WebSphere Application services:

1. Start WebSphere Application Server.

**Windows**

Click All Programs → IBM WebSphere → Application Server v6 → Profiles → default → Start the server. If you installed IBM Information Server in a different WebSphere Application Server profile, you must select the correct profile.

**Note:** Additionally, you can start WebSphere Application Server by using the command below. The path shown in this command assumes that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.
C:\IBM\WebSphere\AppServer\bin\profiles\default\bin\startServer.bat
server1 -username <WAS_Username> -password <WAS_Password>

Linux or UNIX

The path shown in this command assumes that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

/opt/IBM/WebSphere/AppServer/profiles/default/bin/startServer.sh
 username <WAS_Username> -password <WAS_Password>

Note: When restarting WebSphere Application Server, regardless of method used, the startup method will return prior to the server being fully started. Monitor the SystemOut.log file until the following entry is shown:
[5/1/08 15:10:20:591 EDT] 0000000a WsServerImpl A WSVR0001I: Server server1 open for e-business

You can find the SystemOut.log file in the locations listed below. The paths shown assume that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

Windows
C:\Program Files\IBM\WebSphere\AppServer\profiles\default\logs\server1\SystemOut.log

Linux or UNIX
/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1/
SystemOut.log

Typically, the server will be fully started in 2 to 4 minutes after the startup method indicates that startup has completed.

2. Start the following services: ASB Agent, Logging Agent, DataStage Telnet Service, DSRPC Server, and DataStage Engine Resource Service. The engine services will only be present if you installed both the services tier and the engine tier on the same machine.

Microsoft Windows

Start these services in the order that they appear in the table.

Note: On Windows, you can use the Services Administrative Tool or the sc command line tool to start the services.

<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>DataStage Engine Resource Service</td>
<td>DSEngine</td>
</tr>
<tr>
<td>DataStage Telnet Service</td>
<td>dstelnet</td>
</tr>
<tr>
<td>DSRPC Service</td>
<td>dsrpc</td>
</tr>
</tbody>
</table>

Linux or UNIX

To start the services:
a. Run the following command to source the dsenv file. The paths shown in this command assume that the product is installed in the default location. Your path will vary if you installed IBM Information Server in a different location.

```
. /opt/IBM/InformationServer/Server/DSEngine/dsenv
```

The /.dshome file contains the current engine location. Because UNIX systems support multiple instances of WebSphere DataStage, ensure that /.dshome contains the engine that you want to restore. Otherwise, the bin/uv -admin -start command starts the instance of WebSphere DataStage that is in the /.dshome file.

b. Run the following commands to start the WebSphere DataStage services. The paths shown in these commands assume that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

```
cd ./opt/IBM/InformationServer/Server/DSEngine
bin/uv -admin -start
```

c. Run the following commands to start the ASB Agent and the Logging Agent. The paths shown in these commands assume that the product is installed in the default location and uses the default WebSphere Application Server profile. Your path will vary if you installed IBM Information Server in a different location or used a different profile.

```
cd /opt/IBM/InformationServer/ASBNode/bin
./NodeAgents.sh start
```
Product documentation

Documentation is provided in a variety of locations and formats, including in help that is opened directly from the product interface, in a suite-wide information center, and in PDF file books.

The information center is installed as a common service with IBM Information Server. The information center contains help for most of the product interfaces, as well as complete documentation for all product modules in the suite.

A subset of the product documentation is also available online from the product documentation library at [publib.boulder.ibm.com/infocenter/iisinfsv/v8r1/index.jsp](publib.boulder.ibm.com/infocenter/iisinfsv/v8r1/index.jsp)

PDF file books are available through the IBM Information Server software installer and the distribution media. A subset of the information center is also available online and periodically refreshed at [www.ibm.com/support/docview.wss?rs=14&uid=swg27008803](www.ibm.com/support/docview.wss?rs=14&uid=swg27008803)

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 [www.ibm.com/shop/publications/order](www.ibm.com/shop/publications/order)

You can send your comments about documentation in the following ways:
- E-mail: comments@us.ibm.com

Contacting IBM

You can contact IBM for customer support, software services, product information, and general information. You can also provide feedback on products and documentation.

Customer support

For customer support for IBM products and for product download information, go to the support and downloads site at [www.ibm.com/support/us/](www.ibm.com/support/us/)

You can open a support request by going to the software support service request site at [www.ibm.com/software/support/probsub.html](www.ibm.com/software/support/probsub.html)

My IBM

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 [www.ibm.com/account/us/](www.ibm.com/account/us/)
Software services


IBM Information Server support


General information

To find general information about IBM, go to [www.ibm.com](http://www.ibm.com).

Product feedback

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).

Documentation feedback

You can click the feedback link in any topic in the information center to comment on the information center.

You can also send your comments about PDF file books, the information center, or any other documentation in the following ways:

- E-mail: comments@us.ibm.com
How to read syntax diagrams

The following rules apply to the syntax diagrams that are used in this information:

- Read the syntax diagrams from left to right, from top to bottom, following the path of the line. The following conventions are used:
  - The >>--- symbol indicates the beginning of a syntax diagram.
  - The --- > symbol indicates that the syntax diagram is continued on the next line.
  - The >--- symbol indicates that a syntax diagram is continued from the previous line.
  - The --- > < symbol indicates the end of a syntax diagram.
- Required items appear on the horizontal line (the main path).

<table>
<thead>
<tr>
<th>Required_item</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;---</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Optional items appear below the main path.

<table>
<thead>
<tr>
<th>Required_item</th>
<th>Optional_item</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;---</td>
<td></td>
</tr>
<tr>
<td></td>
<td>---------------</td>
</tr>
</tbody>
</table>

If an optional item appears above the main path, that item has no effect on the execution of the syntax element and is used only for readability.

<table>
<thead>
<tr>
<th>Required_item</th>
<th>Optional_item</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;---</td>
<td></td>
</tr>
<tr>
<td></td>
<td>---------------</td>
</tr>
</tbody>
</table>

- If you can choose from two or more items, they appear vertically, in a stack.
  If you must choose one of the items, one item of the stack appears on the main path.

<table>
<thead>
<tr>
<th>Required_item</th>
<th>Required_choice1</th>
<th>Required_choice2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If choosing one of the items is optional, the entire stack appears below the main path.

<table>
<thead>
<tr>
<th>Required_item</th>
<th>Optional_choice1</th>
<th>Optional_choice2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If one of the items is the default, it appears above the main path, and the remaining choices are shown below.

<table>
<thead>
<tr>
<th>Required_item</th>
<th>Default_choice</th>
<th>Optional_choice1</th>
<th>Optional_choice2</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;&gt;---</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- An arrow returning to the left, above the main line, indicates an item that can be repeated.
If the repeat arrow contains a comma, you must separate repeated items with a comma.

A repeat arrow above a stack indicates that you can repeat the items in the stack.

- Sometimes a diagram must be split into fragments. The syntax fragment is shown separately from the main syntax diagram, but the contents of the fragment should be read as if they are on the main path of the diagram.

**Fragment-name:**

```
required_item fragment-name
```

- Keywords, and their minimum abbreviations if applicable, appear in uppercase. They must be spelled exactly as shown.
- Variables appear in all lowercase italic letters (for example, column-name). They represent user-supplied names or values.
- Separate keywords and parameters by at least one space if no intervening punctuation is shown in the diagram.
- Enter punctuation marks, parentheses, arithmetic operators, and other symbols, exactly as shown in the diagram.
- Footnotes are shown by a number in parentheses, for example (1).
Product accessibility

You can get information about the accessibility status of IBM products.

The IBM Information Server product modules and user interfaces are not fully accessible. The installation program installs the following product modules and components:

- IBM Information Server Business Glossary Anywhere
- IBM Information Server FastTrack
- IBM Metadata Workbench
- IBM WebSphere Business Glossary
- IBM WebSphere DataStage and QualityStage
- IBM WebSphere Information Analyzer
- IBM WebSphere Information Services Director

For more information about a product’s accessibility status, go to [http://www.ibm.com/able/product_accessibility/index.html](http://www.ibm.com/able/product_accessibility/index.html)

Accessible documentation

Accessible documentation for IBM 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.
Notices

This information was developed for products and services offered in the U.S.A.

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:

IBM World Trade Asia Corporation
Licensing 2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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. 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.
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 trademarks and certain non-IBM trademarks are marked on their first occurrence in this information with the appropriate symbol.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" 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, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium 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, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

The United States Postal Service owns the following trademarks: CASS, CASS Certified, DPV, LACSLink, ZIP, ZIP + 4, ZIP Code, Post Office, Postal Service, USPS and United States Postal Service. IBM Corporation is a non-exclusive DPV and LACSLink licensee of the United States Postal Service.

Other company, product, or service names may be trademarks or service marks of others.
Index

Special characters
.xml files 104

A
accessibility 139
active sessions disconnecting 108, 109
view 107
administration commands 89
troubleshoot 89
DataStage 3
troubleshoot administration 89
WebSphere Application Server 5
administrator creating the default 50
AppServerAdmin 47, 89
authentication configuring PAM 84

B
backup 127
Business Glossary
security 66

C
column analysis viewing charts and graphs 28
command AppServerAdmin 47
commands
AppServerAdmin 89
assign administrator role 92
check if a user exists 93
configure to use internal registry 94
configure to use WebSphere Application Server user registry 94
create a user 91
delete groups 96
delete users 95
directory service 91
display user details 97
reset credentials 92
search for groups 97
search for users 96
troubleshoot default WebSphere credentials 89
components enabling 103
logging 111
configuration
logging views 115
schedule views 122
configuration files examples
PAM 85
configuring Internet Explorer 9
console 13
areas 13
dashboard 19
history 17
menus 15, 17
My Home workspace 14
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 21
task list 22
task pane 23
walkthrough 21
workspaces 22
creating
project 27
credential mapping 42
configuring your own 82
credential mappings configure 79
credentials
map 81
server default 81
customer support 139
customizing
Home tab 34

dashboard 19
customizing 28
DataStage security roles 67
Debug severity level 111
directories 38
directory external 40
internal 38
directory service 35
DirectoryAdmin assign administrator role 92
check if a user exists 93
configure to use internal registry 94
configure to use WebSphere Application Server user registry 94
create a user 91
delete groups 96
delete users 95
display user details 97
reset credentials 92
search for groups 97
DirectoryAdmin (continued)
search users 96
troubleshoot 98
DirectoryAdmin tool 91
disconnecting users 108, 109
distinguished name determine 54
documentation accessible 139

E
eengine secure 41
security 41, 42
events
logging 111
purging 114, 116
snapshot 115

F
FastTrack security 65
Fatal severity level 111
forecasts scheduled tasks 125

G
group roles 76
groups 58, 60
assigning users to 59, 62

H
history 17
Home tab customizing 34

I
IBM Information Server backup 132
console 13
data recovery 133
logging 1
prepare for data recovery 132
restore 133
scheduling 1
security 1
IBM Information Server console components 13
object list 22
project dashboard 19
shortcuts 20
status bar 19
task flow 21
task list 22
IBM Information Server console
(continued)
  walkthrough 21
  workspaces 22
IBM support 139
inactivity limit 107
information analysis
  graphics 28
Information Analyzer
  security 70
Information Services Director
  security 71
  internal registry
  creating default administrator 50
  internal user registry
  configuring 50
  switch to 50
Internet Explorer, configuring 9

logging views
  creating 113, 115
  criteria 112
logs 25

M
maximum active sessions 107
metadata repository
  access 35
  criteria for logging events 111
  engine
  access 35
Metadata Workbench Administrator
  role 65
Metadata Workbench User role 65
My Home workspace 14

N
notes 17
  note icons 20

O
object list 22
  open workspaces 17
opening a project 29
Operational metadata
  security roles 69
operators
  enabling 103

P
PAM
  configuring for WebSphere DataStage
  and QualityStage 84
  example configuration files 85
passwords
  changing in the Web console 34
plug-ins
  enabling 103
  pop-ups, enabling in Internet Explorer 9
private views
logging 112, 122
product accessibility
  accessibility 143
project
  adding groups 76
  adding users 76
  assigning group roles 76
  assigning user roles 76
  creating 27
  creating groups 58, 60
  creating users 57, 60
details 27
  opening 29
overview 27
  security 57, 60
  setting up 27
project details 27
project menu 17

R
recovery 127
registries
  overview 38
  user 47
registry
  shared 41
reports
  create 24
  view 24
reports workspace 24
restore 127
roles
  DataStage 67
  Metadata Workbench Administrator 65
  Metadata Workbench User 65
  Operational metadata 69

S
schedule views
  copying 123
  creating 122
  criteria 121
scheduled tasks
  forecasts 125
  purging run histories 125
  stopping 125
schedules
  completed 125
  pausing 123
  purging run histories 125
  reactivating 124
  restarting 124
  running 125
  stopping 123
  viewing 123
scheduling 1
  schedule requests 24
scheduling jobs 24
screen readers 139
security
  1
  assigning groups to a project 76
  assigning users to a project 76
  configuring PAM 84
  creating groups 58, 60
  creating users 57, 60
  engine 41
  example PAM configuration files 85
  external directory 40
  how to set up 35
  internal directory 38
  modify configuration 49
overview 35, 38, 44
  roles 63
  setting up 73
setup 38, 46
tips 46
user roles 45
security configuration
  modify to support LDAP 54
  switching user registry 55
security roles
  assign 62
Business Glossary 66

JavaScript, enabling in Internet Explorer 9

LDAP
  configure WebSphere Application Server to use 52
  determine DN 54
  modify security configuration to support 54
  switch to 52
legal notices 145
licenses
  .xml files 104
  installing 103
  using 104
licensing
  viewing available 103
local operating system
  user registry 48
local operating system user registry
  configure WebSphere Application Server 48
log view
  copying 114, 116
logged events
  accessing 113, 115
  purging 114, 116
views 113, 115
logged messages
  purging 114, 116
logging
  1
  log views
    log messages 25
logging components
  overview 111
logging configurations
  active 118
  copying 118
  default 118
  editing 117
  overview 111
logging view
  modifying 114, 116
security roles (continued)
  FastTrack  65
  Information Analyzer  70
  Information Services Director  71
  viewing assigned  75, 78
session limits
  setting  107
sessions
  active  107
  disconnecting  108, 109
severity levels
  logging criteria  111
shared views
  logging  112, 122
shortcuts  17, 20
software services  139
status  19
status bar  19
suite component roles
  assigning users  73, 74, 76, 77
  suite roles  63
suite users
  group assignments  59, 62
support, customer  139

T
  task list  22
  trademarks  147
troubleshoot
  DirectoryAdmin tool  91
troubleshooting
  delete groups  96
  delete users  95
  display user details  97
  search for groups  97
  search for users  96

U
  user credentials
    map individual  81
  user directories  38
  user name and password
    update  47
  user registries  38
    configure for local operating system  48
    configure internal  50
    configure LDAP  52
    configure local operating system  48
    configuring  47
    credential mapping  42
    LDAP  52, 54
    modify security configuration  49
    shared  41
    sharing  80
    switching for a system in use  55
    switching to internal  50
user registry
  sharing  80
user roles  76
  mapping  79
  overview  45
users  57, 60
  assigning security roles  73, 76
users (continued)
  assigning suite component roles  74, 77
default and preconfigured  44
define default WebSphere DataStage and QualityStage  81
disconnecting  108, 109
grant access to WebSphere DataStage and WebSphere QualityStage  83
group assignments  59, 62
mapping credentials  82
security
  granting access  83
  sharing a registry  80

V
  views
    creating  113, 115, 122
    logged events  112

W
  Web console
    changing passwords  34
  WebSphere Application Server
    administering  5
  WebSphere DataStage
    administering  3
  WebSphere DataStage server
    mapping credentials  82
workspace
  completing tasks  21
  workspace navigator  15, 21