Chapter No. 2
"Configuring Your BA Server Instance"
In this package, you will find:

The author’s biography

A preview chapter from the book, Chapter no.2 "Configuring Your BA Server Instance"

A synopsis of the book’s content

Information on where to buy this book

About the Author

Sergio Ramazzina is an experienced software architect/trainer with more than 25 years of experience in the IT field. He has worked on a broad number of projects for banks and major Italian companies and has designed complex enterprise solutions in Java, JavaEE, and Ruby. He started using Pentaho products from the very beginning in late 2003. He gained thorough experience by deploying Pentaho as an open source BI solution, standalone or deeply integrated in other applications as the analytical engine of choice.

In 2009, due to his experience in the Java/JavaEE world and appreciation for the open source world and its main ideas, he began participating actively as a contributor to some of the Pentaho projects such as JPivot, Saiku, CDF, and CDA and rose to the Pentaho Active Contributor level. At that time, he started participating as a BI architect and Pentaho expert on a wide number of projects where open source BI and Pentaho were the main players. In late 2010, he founded Serasoft, a young Italian consulting firm that specializes in delivering high value open source Business Intelligence solutions. With the team in Serasoft, he shared his passion and experience in designing and delivering highly innovative enterprise solutions to help users make their work more effective. In July 2013, he published his first book, Instant Pentaho Data Integration Kitchen, Packt Publishing. He is also passionate about skiing, tennis, and photography, and he loves his young daughter, Camilla, very much.

For More Information:
You can follow him on Twitter at @sramazzina. You can also look at his profile on LinkedIn at http://it.linkedin.com/in/sramazzina/.

Acknowledgments

Firstly, I want to thank my little daughter, Camilla, because every time she would see her dad working on the book, either late in the evening or early in the morning, she would always plant a wonderful kiss and say some words of encouragement.

Thanks to my colleagues and friends who continuously encouraged me in writing this book.

Thanks to my wonderful friends from the Pentaho Community who, during these years, helped me understand the inner workings of the product. A big, special thanks to Pedro Alves, Pentaho SVP for Community and Webdetails founder, for the help he gave me in getting access to a Pentaho EE license for the time required to write this book and for quickly answering me, on a Sunday afternoon, about an unexpected issue I had on CDE while writing its recipe. Thanks a lot, Pedro!

Another big thanks to all my technical reviewers for the wonderful work they did in reviewing my book and in suggesting areas to be improved. Thanks to Packt Publishing for trusting me with this new adventure and thanks to all of the staff at Packt Publishing that supported and assisted me during the writing of the book.
Pentaho Business Analytics Cookbook

Pentaho has become one of the most commonly used open source BI platforms during the last few years. In recent times, a lot of different books came out that covered topics on the Pentaho platform, but none of these gave a complete overview of the platform and its tools in one place to help users become productive quickly.

_Pentaho Business Analytics Cookbook_ is the first book to go deep in Pentaho with a reasonable level of detail of all the pieces of the platform in one single book. By going through all of the book's recipes, you will gain the necessary knowledge to be productive in a very short period of time in order to start using this platform effectively. The book also covers topics such as Pentaho Metadata Editor and Pentaho Mobile, making this book the first comprehensive source of information on Pentaho.

**What This Book Covers**

**Chapter 1**, _Getting Familiar with Pentaho User Console_, introduces the reader to the new Pentaho User Console. Because of the new look and feel of the Pentaho User Console, this chapter is a good overview for novice users and also for navigated users who would like to quickly familiarize with the new user interface.

**Chapter 2**, _Configuring Your BA Server Instance_, goes into the details of the new Administration perspective, the place where administrative tasks should be carried out.

**Chapter 3**, _Defining BA Server Data Sources_, explains the new way to define data sources in Pentaho BA 5. We will go deep in the definition all of the major data source types by giving a complete and detailed description.

**Chapter 4**, _Defining Business Models with the Pentaho Metadata Editor_, describes the advantages of implementing a metadata domain model and explains, at a good level of detail, how to define a Pentaho metadata domain model from the ground up as well as shows how to deploy it.

**Chapter 5**, _Creating Reports Using Pentaho Interactive Reporting_, shows how to use a metadata domain model easily and how we can define a tabular report using the Pentaho User Console.

**Chapter 6**, _Creating Analysis Reports_, starts by giving a brief recap about what a Mondrian schema is and how to define it using Pentaho Schema Workbench. Then, it goes through the details of defining an analysis report by using Pentaho Analyzer and Saiku.

For More Information:

Chapter 7, *Creating Reports Using Pentaho Report Designer*, shows how to use the powerful Pentaho Report Designer to create wonderful reports easily and without difficulty.

Chapter 8, *Creating Dashboards*, goes through the design of interactive dashboards by using Pentaho Dashboard Designer and CDE.

Chapter 9, *Scheduling Content*, takes us through the details of the new scheduler interface and shows how to easily schedule our recurring jobs.

Chapter 10, *Working with Pentaho Mobile BI*, is the first instance where we have an overview of the Pentaho Mobile application, showing how our content can be easily accessed from a mobile device.

Chapter 11, *Customizing Pentaho BA to Meet Your Business Needs*, gives a brief introduction about how to customize the Pentaho User Console by defining new themes and presents some interesting plugins taken from Pentaho Marketplace that can help us in our everyday tasks.

For More Information:
Configuring Your BA Server Instance

In this chapter, we will cover the following topics:

- Accessing the administration perspective
- Creating a new user
- Deleting an existing user
- Editing an existing user
- Creating a new role
- Deleting an existing role
- Editing an existing role
- Managing system roles
- Configuring authentication using the LDAP Server (EE version)
- Configuring authentication using the LDAP Server (CE version)
- Managing the mail server configuration
- Cleaning up aged generated files immediately
- Scheduling the cleanup of aged generated files

For More Information:
Introduction

In this chapter, we continue where Chapter 1, Getting Familiar with Pentaho User Console, left off by providing recipes related to the BA Server administration and configuration. For anyone used to administrative tasks with the previous Pentaho releases, this is a part of the new BA Server where we can see a major change with previous versions of Pentaho BI Server. Any time we were involved in administrative tasks with older Pentaho releases, we needed to start a different, separate web application:

- In case we were dealing with BI Server EE (Enterprise Edition), we needed to start Enterprise Console
- In case we were dealing with BI Server CE (Community Edition), we needed to start Administration Console

Starting from Version 5, everything changed. All administrative tasks and operations have been organized in a new perspective called the Administration perspective. This perspective is accessible from the Pentaho User Console to every member of the administrator role.

Recipes in this chapter are given assuming that we are able to successfully log in to Pentaho User Console as a user who is part of the administrator role. The administrator role is the role associated with all the Pentaho super users, and for that reason, it has full access to any functionality that is related to the administration of Pentaho BA Server.

In case we want to use demo users, remember that we can use the administrator username and password for the demo users' username and password. This user is the new Pentaho's demo administrator, after the famous user Joe (the Pentaho-recognized administrator until Pentaho 4.8) has been dismissed starting from Version 5.

Accessing the Administration perspective

To have everything at our fingertips, we are going to introduce you to how to get into the Administration perspective.

How to do it...

To access the Administration perspective, you must perform the following steps:

1. Pull down the perspective combo box in the upper-left area of Pentaho User Console.
2. Select the entry named Administration.
3. You will immediately be taken to the Administration perspective.

For More Information:
The Administration perspective is the new place where all the administrative tasks take place. This perspective, accessible from the upper-left combo in Pentaho User Console, is organized through a left-side menu that contains the main administrative areas:

- For Pentaho BA Server 5 CE, we have functions to manage users and roles, a place to configure settings for the mail server (until Version 4.8, this was created through external configuration files), and general settings such as scheduling the deletion of unneeded content files.
- For Pentaho BA Server 5 EE, we have added menus to configure the authentication through an LDAP sever and another menu to configure the server components' licensing.

We will work through any of these functionalities in the following recipes of this chapter.

For More Information:
Creating a new user

Now that we understand how to get into the new Administration perspective, we are going to see how we can easily define a new user in Pentaho BA Server. The user will be saved to the internal Pentaho user database.

How to do it...

The following steps will show us how we can define a new user in Pentaho BA Server:

1. The Users / Roles entry of the Administration perspective's left menu is automatically selected by default.
2. On the right part of the screen, the Users / Roles tab is selected by default.
3. Click on the plus (+) icon in the upper-right corner of the Users list. The New User dialog box opens, as shown in the following screenshot:

![New User Dialog Box](image)

4. In the User Name field, type the name of the user we are going to add. This field is mandatory.
5. In the Password field, type the password of the user we are going to add. This field is mandatory.
6. In the Confirm Password field, retype the password of the user we are going to add as a confirmation. This field is mandatory.
7. As soon as the Confirm Password field is filled and the content inserted herein is equal to the content in the Password field, the OK button appears.
8. If we click on the Cancel button, the dialog box closes and the new user data is not saved.

For More Information:
9. If we click on the OK button, the New User dialog box closes, the new user is saved, and it appears in the Users list.

10. Now that we have our new user, we must assign that user to one or more roles. Select the user inserted so far from the Users list.

11. Look at the Roles lists shown in the following screenshot. Select the role we want to assign to this user from the Available list and click on the > button. If we want, we can assign more than one role at a time by pressing Ctrl + right-clicking on any role you are going to assign to the user.

12. The role we just selected moves to right Roles list.

13. In case of an error, we can remove the role from right Roles list by selecting one or more wrong roles and clicking on the < button.

14. If we want to assign all the roles available to this user in one shot, we can click on the >> button without selecting an individual role from the Available list. The roles set will move from the Available list to the Selected list.

15. If we want to remove all roles from the current user in one shot, click on the << button. The roles set will move from the Selected list back to the Available list, as shown in the following screenshot:

For More Information:
Confi
fi
guring Your BA Server Instance

How it works...

Defining a new user is almost the same procedure as the one used in the older version. After
we access the Administration perspective, the Users / Roles menu entry is already selected
and we are ready to start inserting a new user. By clicking on the plus (+) icon in the upper-right
corner of the Users list, the New User dialog box opens and we are ready to fill the required
fields. After any field is properly filled, click on the OK button and close the dialog box. The new
user is immediately visible in the Users list. Now we must select the user and assign them a set
of roles. To do this, select the roles we want to assign to our new user by clicking on them in the
Roles list box and then clicking on the > button to move them to the right-hand side list box.
We can select more than one role at a time by pressing Ctrl + right-clicking on any of the
selected roles.

See also

Following this recipe, the user will be created in the Pentaho user database. We might be
interested in knowing how to delete a user in the Deleting an existing user section or how
to update a user in the Editing an existing user section. If we are interested in how to create
a new role for this user and how to associate it with a set of users, look at the Creating a new
role recipe later in this chapter.

Deleting an existing user

After seeing how to create a new user in Pentaho BA Server, this recipe is going to show us
how we can delete an existing user.

How to do it...

The following steps will show us how we can delete a user from the set of available users in
Pentaho BA Server:

1. The Users / Roles entry of the left menu is automatically selected by default.
2. On the right part of the screen, the Users / Roles tab is selected by default.
3. Select the user we want to delete from the Users list and click on the x icon in the
upper-right corner of the Users list.
4. A warning dialog box pops up asking us whether we are really sure about deleting
the selected user.
5. If we click on the Yes button, the user will be deleted and we will be immediately
taken back to the Users list. The deleted user will never appear anymore in the list
of users.
6. If we click on the No button, the selected user will not be removed from the Users list,
and we will immediately be taken back to the Users list.

For More Information:
How it works...

Deleting an existing user is easy as as creating a new one. After we access the administration perspective, the Users / Roles menu entry is already selected and we are ready to delete the user. To do this, select it from the Users list, and then delete it by clicking on the x icon in the upper-right corner of the Users list. The selected user is immediately deleted and is no longer available in the system.

See also

Following this recipe, our user will be deleted from the Pentaho user database. You might be interested in learning how to either create a new user in the Creating a new user recipe or about how to update a user in the Editing an existing user recipe.

Editing an existing user

Finally, here are some last words on how to update an existing user. Updating a user in Pentaho means updating the user's password or adding or removing roles from or to the user's roles set.

How to do it...

Let's start with changing a user's password. To do this, you must perform the following steps:

1. The Users / Roles entry of the Administration perspective's left menu is automatically selected by default.
2. On the right part of the screen, the Users / Roles tab is selected by default.
3. Select the user whose password we want to change from the User's list.
4. Click on the Edit button located on the left-hand side of the Password field. The Change Password dialog box opens.
5. In the New Password field, type a new password for this user. This field is mandatory.
6. In the Confirm Password field, retype the password for this user as a confirmation. This field is mandatory.
7. As soon as the Confirm Password field is filled and the content inserted herein is equal to the content in the Password field, the OK button appears.
8. If we click on the Cancel button, the dialog box closes and the updated password is not saved. The user continues to use their old password.
9. If we click on the OK button, the Change Password dialog box closes and the new password for this user is saved.

Configuring Your BA Server Instance

To add a new role to a user by updating the list of existing roles, you must perform the following steps:

1. The Users / Roles entry of the left menu is automatically selected by default.
2. On the right part of the screen, the Users / Roles tab is selected by default.
3. Select the user we want to change by updating the set of roles; the user is the member from the Role list.
4. From the Available roles list, select the roles we want to assign to the user and click on the > button. If we want, we can assign more than one role at a time by pressing Ctrl + right-clicking on any role we are going to assign to this user.
5. The users we just selected move from the Available to the Selected users list.
6. In case of an error, we can remove the role from the Selected list and reassign it to the Available list by selecting the wrong role and clicking on the < button. If we want, we can remove more than one role at a time by pressing Ctrl + right-clicking on any of the roles we want to remove.
7. If we want to assign all available roles to this role in one shot, we can click on the >> button without selecting any individual role from the Available list. The roles set will move from the Available list to the Selected list.
8. In case of an error, if you were to remove all users from the current role in one shot, press the << button. The users set will move from the Selected list back to the Available list.

To remove an existing role from a user's role set, we must perform the following steps:

1. The Users / Roles entry of the left menu is automatically selected by default.
2. On the right part of the screen, the Users / Roles tab is selected by default.
3. Select the user we want to change to update the roles from the User's list.
4. From the Selected roles list, select the roles we want to remove from the user and press the > button. If we want, we can select more than one role at a time by pressing Ctrl + right-clicking on any role we are going to remove from this user.
5. The roles we just selected move from the Selected to the Available users list.
6. In case of an erroneous selection, we can remove the role from the Available list and reassign it to the Selected list by selecting the wrong role and pressing the < button. If we want, we can remove more than one role at a time by pressing Ctrl + right-clicking on any of the roles we want to remove.
7. If we want to remove all the roles from the current user in one shot, press the << button. The roles set will move from the Selected list back to the Available list.
How it works...

Managing existing users is a matter of changing the user's password and/or changing the set of roles assigned to a user.

To change the user's password from the Users list, we select the user whose password we want to change, and then we click on the Edit button located to the left of the Password field. The Change Password dialog box opens and gives us the ability to insert the new password by filling the New Password and Change Password fields. After we have filled the two fields, we can click on the OK button to confirm the new password we just set.

By updating the list of Roles a user is a member of is very simple; procedure is almost similar in cases of adding and removing user's membership from a role. After selecting the user we want to act upon, the list to the left contains the set of available roles, and the list to the right contains the set of roles assigned to this user. If we want to add a user's membership for a role, select the role we want to make the user a member of, and press the > button. If we want to remove a user's membership from a role, select the role we want to remove the user membership from, and click on the < button.

See also

We might be interested in knowing how to create a new user in the Creating a new user recipe or how to delete an existing user in the Deleting an existing user recipe. If we are interested in how to create a new role for this user and how to associate that role to a set of users, look at the Creating a new role recipe later in this chapter.

Creating a new role

We opened this chapter with a set of recipes on how to manage users in Pentaho BA Server. Now, in this recipe, we are going to see how to create a new role and how to associate it with a predefined set of operation permissions. Operation permissions are the set of things a user can or cannot do if they would be a member of this role. That said, the role is a way to associate a set of users with the same collection of operation permissions.
Configuring Your BA Server Instance

How to do it...

The following steps will show us how to define a new role and associate it with a set of Operation Permissions:

1. From the Users / Roles entry of the left menu, select the Manage Roles tab.

2. Click on the plus (+) icon in the upper-right corner of the Roles list and the New Role dialog box will open, as shown in the following screenshot:

3. In the Name field, type the name of role we are going to create. This field is mandatory. As soon as we start filling the field with some characters, the OK button appears.

4. If we click on the Cancel button, the dialog box closes and a new role is not created.

For More Information:
5. If we click on the **OK** button, the **Change Password** dialog box closes and a new role is created.

6. The **Roles** list is updated with the new role we just created in a selected state.

7. The new role does not have any permission assigned by default. As shown in the following screenshot, select the permissions we want to assign to a new role by clicking on items in the **Operation Permissions** checkboxes list:

8. Now that we have created our new role, we can make some users members of this new role. Select the role inserted so far from the **Roles** list.

9. Look at the **Users** lists. Select the users we want to assign to the role and press the **>** button. If we want, we can assign more than one user at a time by pressing **Ctrl** + right-clicking on any user we are going to assign to this role.

10. The roles we just selected move from the **Available** to the **Selected** roles list.

11. In case of an error, we can remove the user from the **Selected** list by selecting the wrong users and pressing the **<** button. If we want, we can remove more than one user at a time by pressing **Ctrl** + right-clicking on any of the roles we want to remove.

12. If we want to assign all the users available to this role in one shot, we can press the **>>** button without selecting any individual users from the **Available** list. The users set will move from the **Available** list to the **Selected** list.

13. If we want to remove all users from the current role in one shot, press the **<<** button. The users set will move from the **Selected** list back to the **Available** list.

---

For More Information:

Configuring Your BA Server Instance

How it works...

**Operation Permissions** relates to giving a class of users (all the users who are members of a specific role) the ability to manage certain operations when authenticated to the Pentaho platform. As we will see in the *Managing system roles* recipe, we can also give Operation Permissions to unauthenticated users by associating permissions to Anonymous System Role.

Operation Permissions are basic permission items that we can assign to a specific role. The resulting users' permissions depend on a combination of the Operation Permissions' items we have assigned to a particular role that we are going to define. We have several permission items and they are summarized as follows:

- **Read Content**: This is the basic permission item level we can assign to a specific role. By giving this permission, a user can only browse files in the solution, access the content they are enabled to access, and start the execution of a report, dashboard, or other executable items. As an example, when we try to create a new folder, the system gives us a warning message that we do not have any rights to do this. Lastly, the user can't do the following things:
  - Copy, paste, and rename anything both in the Home and Public section of the solution
  - Move to trash any content item both in the Home and Public section of the solution
  - Assign or manage any privilege on the solution's content items
  - Upload or download any item from the solution
  - Create any interactive report, dashboard, analyzer report, and data source in the Pentaho User Console

  The **Administration** perspective is not accessible. The **Schedule** perspective gives you only the ability to view your schedules. In the **Home** perspective, the toolbar displays only the **Browse Files** and the **Documentation** buttons to the user.

- **Create Content**: This item grants the permissions to create new content of any type. By adding this permission content, you are enabled to do the following:
  - Copy, paste, and rename anything in the Home section of the solution
  - Create new folders in the solution
  - Create new data sources
  - Create any interactive report, dashboard, analyzer report, and data source in Pentaho User Console
The user can't do the following things:

- Copy, paste, and rename anything in the Public section of the solution
- Move to trash any content item both in the Home and the Public section of the solution
- Assign or manage any privilege in the solution's content items
- Upload or download any content item

Other things that are valid when this operational permission is assigned are as follows:

- The File Actions menu displays a Schedule menu item, but as soon as we try to access it, we get a message that warns us that we don't have the right to do that kind of action.
- The Administration perspective is not accessible. The Schedule perspective gives us only the ability to view our schedules. In the Home perspective, the toolbar displays all of the possible buttons to the user.

- **Schedule Content**: This item only grants the permissions to schedule content by enabling all of the related features in the Schedule perspective. Permissions to access the content items are not implicitly assigned by granting this permission item because they depend on the combination of the Read and Create operational permissions that we're going to define.

- **Publish Content**: This item only grants the permissions to publish any content to the solution. Permissions to the content items are not implicitly assigned by granting this permission item because they depend on the combination of the Read and Create operational permissions we're going to define.

- **Administer Security**: This item only grants permissions to assign privileges to the content items by enabling the Share tab in the content item's Properties dialog box. Permissions to access the content items are not implicitly assigned by granting this permission item because they depend on the combination of the Read and Create operational permissions we're going to define.

### See also

As soon as we install your brand new instance of Pentaho BA Server and we get to the Administration perspective to manage users and roles, we notice that few default roles that have already been defined exist. For details about these out-of-the-box roles, take a look at the article Define Security for the BA Server in Pentaho Infocenter at the following URL: http://infocenter.pentaho.com/help/index.jsp?topic=%2Fconfig_ba_server%2Ftask_managing_users_and_roles.html.

For More Information:

Deleting an existing role

This recipe will show us how we can easily delete a role from the existing set of roles.

How to do it...

The following steps will give us an idea about how we can easily delete a role from an existing set of roles:

1. The Users / Roles entry of the left menu is automatically selected by default.
2. Select the Manage Roles tab and then select the role we want to delete from the Roles list.
3. Click on the x icon in the upper-right corner of the Roles list.
4. A warning dialog box opens, asking if we are really sure that we want to delete the selected role.
5. If we click on the Yes button, we will immediately be taken back to the Roles list, the selected role will be deleted, and it won't appear anymore in the Roles list.
6. If we click on the No button, we will immediately be taken back to the Roles list and the selected role will not be removed from the Roles list.

How it works...

Deleting an existing role follows more or less the same procedure as the one we saw while deleting an existing user. After we access the Administration perspective, we see that the Users / Roles menu entry is already selected by default. Choose the Manage Roles tab, and then select the role we want to delete from the Roles list. Then, after the role has been selected, delete it by clicking on the x icon in the upper-right corner of the Roles list. The selected role is immediately deleted, and it is no longer available in the system. Any reference to users that are members of this role are automatically deleted.

See also

Maybe we are interested in creating or updating an existing role. See the Creating a new role or Editing an existing role recipes to get details on this. In the There's more... section of Creating a new role recipe, we can find a detailed illustration of Operation Permissions, which is a good topic to get comfortable with in order to properly configure Pentaho roles.
Editing an existing role

Finally, here are some words on how to update an existing role. Updating a role in Pentaho means either updating the set of users assigned to this role or changing the operation permissions for this role, or both. This recipe shows us how we can do this.

How to do it...

To update a role by adding a new user or a new set of users to this role, we must perform the following steps:

1. Select the Manage Roles tab from the Users / Roles menu entry.
2. From the Role list, select the role we want to change by updating the set of users who are members of that role.
3. From the Available users list, select the users we want to assign to the role and click on the > button. If we want, we can assign more than one user at a time by pressing Ctrl + right-clicking on any user we are going to assign to this role.
4. The roles we just selected move from the Available to Selected roles list.
5. In case of an error, we can remove the user from the Selected list and reassign it to the Selected list by selecting the wrong user and pressing the < button. If we want, we can remove more than one user at a time by pressing Ctrl + right-clicking on any of the users we want to remove.
6. If we want to assign all the users available to this role in one shot, we can click on the >>> button without selecting any individual users from the Available list. The user set will move from the Available list to the Selected list.
7. In case of an error, if we want to remove all the users from their current role in one shot, click on the << button. The user set will move from the Selected list back to the Available list.

To update this role by removing an existing user or an existing set of users from this role, we must perform the following steps:

1. Select the Manage Roles tab from the Users / Roles menu entry.
2. From the Roles list, select the role we want to change by removing a user or a set of users who are members of that role.
3. From the Selected users' list, select the users we want to remove from the role and click on the > button. If we want, we can assign more than one user at a time by pressing Ctrl + right-clicking on any user we are going to remove from this role.
4. The roles we just selected move from the Selected to the Available roles list.

For More Information:
5. In case of an error, we can remove the user from the Available list and reassign it to the Selected list by selecting the wrong user and clicking on the < button. If we want, we can remove more than one user at a time by pressing Ctrl + right-clicking on any of the roles we want to remove.

6. If we want to remove all the users from the current role in one shot, click on the << button. The users set will move from the Selected list back to the Available list.

7. In case of an error, if we want to reassign all the users available to this role in one shot, we can click on the >> button without selecting any individual user from the Available list. The users set will move from the Available list to the Selected list.

To update this role by changing Operation Permissions, we must perform the following steps:

1. Select the Manage Roles tab from the Users / Roles menu entry in the Administration perspective.
2. From the Roles list, select the role we want to change by updating Operation permissions.
3. Change the permissions currently assigned to the role by checking or unchecking the items in the Operation Permissions checkboxes list.
4. The new set of Operation Permissions for the selected role are immediately saved and applied.

**How it works...**

Editing an existing role means changing the set of Operation Permissions assigned to a role or updating the set of users who are members of that role.

To change Operation Permissions for an existing role, just select the role and either check or uncheck the Operation Permissions checkbox until we reach the desired configuration for the selected role.

Updating the list of Users members of a selected role is a very simple procedure. After selecting the role we want to act upon, we see that the list to the left of Role contains the set of available Users, and the list to the right contains the set of Users assigned to this user. If we want to add the user membership for a role, we select the user we want to make a member of selected Role and click on the > button. If we want to remove the Users membership from selected Role, we select the user we want to remove from the Users membership and click on the < button.

**There's more...**

Unfortunately, a rather useful thing that is missing from the list is the ability to rename a role whenever required. If we need to rename a role, the only thing we can do is delete the wrong role and recreate it. This is not so straightforward, but it is the only way to do this.
See also

If we are interested in creating a new role or going through the details of the Operation Permissions settings, take a look at the Creating a new role recipe.

Managing system roles

As soon as any user logs into Pentaho, the system grants a set of predefined roles called the System roles. Starting from Pentaho BA Server 5.0, the management of permissions for these roles is in the Administration perspective. This recipe shows us how we can manage the permissions for these two roles.

How to do it...

The following steps will detail how we can change Operation Permissions to predefined System roles:

1. Select the System Roles tab from the left menu entry, Users / Roles, in the Administration perspective. The following screenshot shows us the set of System roles that are predefined in the system and their assigned operational permissions:

2. Select the role we want to change by updating Operation permissions from the Roles list.

3. Change the permissions currently assigned to the selected role by checking or unchecking items in the Operation Permissions checkboxes list.

4. The new set of permissions are immediately saved and applied to the current role.

For More Information:

How it works...

System roles are particular roles that are predefined in the system and we can only manage the assignment of Operation Permissions. To change Operation Permissions assigned to a specific system role, select the role we want to make the changes to and check or uncheck the Operation Permissions flags until we get the desired configuration.

There's more...

Let's go deep into these two roles and see which role they play in the Pentaho authentication process.

Things to notice about the authenticated role

The authenticated role is the system role that is injected into the set of user roles during the authentication process. It is extremely important to know that it exists because it adds a set of default Operation Permissions for a user who is going to log in to Pentaho User Console. Therefore, any time we are considering the permissions associated to a specific user, don't forget this hidden contribution to the final result!

How to bypass the Pentaho BA Server security

In Pentaho BA Server, it is impossible to remove completely the security mechanisms of the Pentaho platform. For this reason, the only thing we can do is bypass the user authentication mechanisms by introducing an Anonymous role. Anonymous is System Roles that is automatically assigned to any unauthenticated user that is going to log in to the BA server platform.

To bypass the BA server security and allow unauthenticated users to connect to Pentaho, we first need to stop the BA server and apply a set of configuration changes to wire Pentaho Spring Security beans in a different way. By wiring Spring beans correctly, we can assign users an Anonymous role with the correct permissions for our particular use case by choosing from the set of available Operation Permissions.

For a detailed description about how to remove the security and allow anonymous access, follow the guidelines detailed in the article Remove Security by Allowing Anonymous Access in Pentaho Infocenter at the following URL: http://infocenter.pentaho.com/help/index.jsp?topic=%2Fsecurity_guide%2Ftask_removing_security.html.

See also

It could be a good idea for you to refresh your knowledge about the Operation Permissions settings by going through the details in the Create a new role recipe.
Configuring authentication through the LDAP server (EE version)

The Configuring authentication through the LDAP server (EE version) recipe covers one of the hottest topics when configuring Pentaho. Usually, as soon as we introduce a new application to our network, that application must be integrated enterprise-wide with other systems. The first thing we care about is the security and because of this, the first thing we are required to take great care of is the integration with our customer or our own company's enterprise authentication system. This, for the vast majority of cases, is an LDAP server or an MS Active Directory.

This recipe will show us how to configure the Pentaho BA server EE to authenticate users to an LDAP server (OpenLDAP for the current example) without pain. It is a critical configuration procedure, partially made through a wizard implemented in the Administration perspective by partially editing some files by hand.

How to do it...

The following steps detail how we can easily configure the Pentaho BA server EE (Enterprise Edition) to connect to an LDAP server:

1. Select the Authentication entry from the Administration perspective's left-side menu. As we can see in the following screenshot, the Authentication configuration form opens by showing our actual authentication mechanism. If this is a brand new installation and we didn't change anything, the default authentication method's radio button is selected as Local – use basic Pentaho authentication.

For More Information:
2. Select the **External – Use LDAP / Active Directory server** authentication method.

3. As shown in the following screenshot, a message box warns us that by switching the authentication method, we are going to start a new configuration and may change users, roles, and the login password:

4. If we click on **No**, we are taken back to the main **Authentication** page without starting the switching process. Our Pentaho BA server authentication's source remains unchanged.

5. If we click on **Yes, Continue**, we are going to start the reconfiguration of the authentication system to use **External – Use LDAP / Active Directory server**.

6. The server tries to connect to the LDAP server that was defined at that time.

7. If this is our first time configuring the connection to the LDAP server, Pentaho will try to connect to a default LDAP location and, most probably, it will fail. If so, a message box will warn us about that. Do not worry about this and click on the **Close** button to continue.

8. As shown in the following screenshot, after we click on the **Close** button, the **LDAP Server Connection** form appears:

For More Information:

9. Type LDAP Server URL in the Server URL field. This field is mandatory.
10. Type the user's distinguished name in the User Name field. This field is mandatory.
11. Type the user's password in the Password field. This field is mandatory.
12. Click on the Test Server Connection button to verify that Pentaho connects successfully with your LDAP Server.
13. If the connection test does not work properly, a message box warns us about this and we will be taken back to LDAP server configuration parameters to apply the needed corrections.
14. If the LDAP server connection works properly as configured, the LDAP configuration form expands vertically by adding two new sections: Pentaho System Administrator and LDAP Configuration.
15. Take a look at the **Pentaho System Administrator** section as shown in the following screenshot:

16. In the **Select user from LDAP server** field, type the complete name of the LDAP user, which we will consider as the Pentaho server administrator. In our case, the distinguished name is `cn=Pentaho Admin, ou=users, dc=pentaho-cookbook, dc=com`. This field is mandatory.

17. In the **Select roles from LDAP server** field, type the name for the LDAP group that we will consider as a group that contains users who we will consider as the Pentaho server administrator. This is a group in LDAP Server that will be mapped as the **Administrator** role. In our case, the complete group name is `cn=pentahoAdmin Roles, ou=users, dc=pentaho-cookbook, dc=com`. This field is mandatory.

18. Look at the **LDAP Configuration** section of the form, as shown in following the screenshot:

---

For More Information:

19. Select **LDAP Provider** from the related drop-down list. The default value, **Apache Directory Server**, is good enough in any standard case.

20. In the **User Base** field, type the complete path to consider as the base path for all of the user searches. In our case, the base path for users is `ou=users,dc=pentaho-cookbook,dc=com`. This field is mandatory.

21. In the **Group Base** field, type the complete path to consider as the base path for all of the group searches. In our case, the base path for groups is `ou=roles,dc=pentaho-cookbook,dc=com`. This field is mandatory.

22. Click on the **Save** button to confirm the settings.

23. A message box informs you that the changes have been saved successfully. Remember that new changes will not take effect until you restart your Pentaho server.

Now that we have completed the LDAP configuration, we need to refine some things before having everything fully working.

24. Go to the `<biserver_home>/pentaho-solution/system` directory.

25. Edit the `Context-security-ldap.properties` file application. This property file is generated when we click on the **Save** button at the end of the **LDAP Server Connection** configuration.

26. The file is divided into five sections, as specified in the *There's more...* section of this recipe.

**For More Information:**

27. Go to the **Populator** section identified by keys with the `populator` prefix. Verify that the `populator.groupSearchFilter` key is defined as `populator.groupSearchFilter=(&(objectClass=posixGroup)(memberUid={1}))`. If it is not, apply changes according to the sample provided.

28. Go to the **All Authorities Search** section identified by keys with the `allAuthoritiesSearch` prefix. Verify that the `allAuthoritiesSearch.searchFilter` key is defined as `allAuthoritiesSearch.searchFilter=(objectClass=posixGroup)`. If it is not, apply the changes according to the sample that is provided.

29. Go to the **All Username Search** section identified by keys with the `allUsernamesSearch` prefix. Verify that the `allUsernamesSearch.searchFilter` key is defined as `allUsernamesSearch.searchFilter=(objectClass=posixAccount)`. If it is not, apply the changes accordingly to the sample that is provided.

30. Save the file and close the editor.

```
    The configuration steps listed here are valid considering the connection of the Pentaho BA server to an OpenLDAP server. Assume a similar configuration in case we want to connect to an MS Active Directory server with the only exception of names of MS Active Directory server attributes used.
```

The LDAP configuration is finished. Remember that we have to restart our BA server before the new configuration changes take effect.

**How it works...**

The following is a definition that we can find on Wikipedia:

"LDAP stands for Lightweight Directory Access Protocol and is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate e-mail directory."

```
    See the Wikipedia link at http://en.wikipedia.org/wiki/LDAP.
```

In large organizations, an LDAP server is typically a good way to map all of the company's organizational structure in terms of domains (they can differentiate various branches or internal organization or other), roles, and users who relate to those domains. Because of this, it is a good rule of thumb to use this approach to have all of this information and the management of this information in one place in a centralized repository. To agree to this enterprise schema, any application must map its authentication and authorization mechanisms on such an enterprise security architecture to be fully compliant with the company policies.

---

**For More Information:**

To access a particular object in the LDAP tree, a client has to submit a so-called LDAP query to search for a specific object or a specific set of objects located in the tree. The query is composed of the following three main elements at least:

- A base object that sets the position in the tree relative to which we are going to perform the query
- A scope that sets the level of depth the query will act upon (singleLevel or wholeSubtree)
- A filter that helps us point rightly to the element or set of elements that we are looking for

After we complete the LDAP configuration wizard as explained in the recipe body, the wizard process generates a set of LDAP property configuration files located in the system configuration directory. They collect all the possible configuration properties for the entire LDAP configuration in one place.

The file we are referring to is named `applicationContext-security-ldap.properties` and is located in the `<biserver-home>/pentaho-solutions/system` directory.

This file is divided into five sections as follows:

- **Connection information:** This is identified by all keys with the `contextSource` prefix. It defines the connection to the LDAP server and the information about the user that can perform the searches over the LDAP tree (typically an LDAP user, not necessarily an administrator).
- **Users:** This is identified by all the keys with the `userSearch` prefix. It defines how the LDAP tree is searched for by users who are going to log in to Pentaho to authenticate them.
- **Populator:** This is identified by all the keys with the `populator` prefix. It defines how to match fully distinguished user names coming from `userSearch` to distinguished role names for the roles those users belong to.
- **All Authorities Search:** This is identified by all the keys with the `allAuthoritiesSearch` prefix. The entries that we get from this search populate the BA server Access Control List (ACL) roles.
- **All Username Search:** This is identified by all the keys with the `allUsernamesSearch` prefix. The entries that we get from this search populate the BA server Access Control List (ACL) users.

While going to configure this file, we will notice that in search filters, we will often have the `{0}` or `{1}` tokens. Basically, they let us parametrically build a dynamic filter based on the value of the login information typed by the user, specifically the following:

- `{0}` will be replaced by the user DN (Domain Name) found during a given search
- `{1}` will be replaced by the login username typed by the user

For More Information:

Configuring Your BA Server Instance

See also

If we are using Pentaho BA server CE, we may be interested in understanding how to configure the LDAP connection manually by looking at the Configuring authentication through the LDAP server (CE version) recipe. To get all of the required information about the LDAP properties and their meanings, look at Pentaho Infocenter at the following URL http://infocenter.pentaho.com/help/index.jsp?topic=%2Fsecurity_guide%2FReference_ldap_properties.html.

Configuring authentication through the LDAP server (CE version)

In case we are going to use Pentaho BA server CE, things are almost the same as for the EE version. This recipe will show us how to configure Pentaho BA server CE to authenticate it using an LDAP server (OpenLDAP for the current example) without pain. In this case, the procedure is completely manual but everything will become simple by following the recipes correctly.

How to do it...

1. Go to the <biserver_home>/pentaho-solution/system directory.
2. Open the applicationContext-security-ldap.properties file with your favorite editor. If this is the first time we are playing with the LDAP authentication, this property file is filled with its default values.
3. Look at the following excerpt; this is a complete configuration to connect and make searches over a typical LDAP server. We can find it in the resource files distributed with this book; it is a fully valid example that we can use to configure our configuration:

```
contextSource.providerUrl=ldap://ldap.acme.com
contextSource.userDn=cn=admin,dc=pentaho-cookbook,dc=com
contextSource.password=password

userSearch.searchBase=ou=users,dc=pentaho-cookbook,dc=com
userSearch.searchFilter=(uid={0})

providerType=ldapApacheConfiguration

populator.rolePrefix=
populator.groupSearchBase=ou=roles,dc=pentaho-cookbook,dc=com
populator.convertToUpperCase=false
populator.searchSubtree=false
populator.groupRoleAttribute=cn
populator.groupSearchFilter= (&(objectClass=posixGroup)(memberUid={1}))
```

For More Information:

adminUser=uid=pentaho_admin,ou=users,dc=pentaho-cookbook,dc=com
adminRole=cn=pentahoAdminsRole,ou=roles,dc=pentaho-cookbook,dc=com

allAuthoritiesSearch.roleAttribute=cn
allAuthoritiesSearch.searchBase=ou=roles,dc=pentaho-cookbook,dc=com
allAuthoritiesSearch.searchFilter=(objectClass=posixGroup)

allUsernamesSearch.searchFilter=objectClass=posixAccount
allUsernamesSearch.searchBase=ou=users,dc=pentaho-cookbook,dc=com

allUsernamesSearch.usernameAttribute=cn

4. As a general case, in case we are going to use this file as a starting point to configure a Pentaho BA server connection to an LDAP server, remember to change the fully qualified domain name (in our case, dc=pentaho-cookbook,dc=com) provided in the sample with the fully qualified domain name for our LDAP server.

5. Look at the contextSource.providerUrl key. Change the value according to the configuration specified for our LDAP server.

6. Look for contextSource.userDn. Change the content with the distinguished name of a valid LDAP user for our LDAP server. Typically, this could be an LDAP user who has the right to make queries all over the user's tree, not necessarily an LDAP administrator.

7. Look for contextSource.password. This is the password for the user mentioned at the previous step. Change it accordingly.

8. Do not forget to make any other appropriate changes either in search expressions or in configuration flags or both; they are needed in case we use different attributes to describe the same things.

9. Save the file and close the editor.

The configuration in the preceding excerpt is valid considering the connection of Pentaho BA Server to an OpenLDAP Server. Assume a similar configuration in case you want to connect to an MS Active Directory Server with the only exception of names the attributes used.

Now that we have completed the manual configuration of the LDAP properties file, we need to activate the newly configured LDAP provider. Pentaho is a Spring application with a lot of configuration files so it is very easy to do this. Of course, we need to know where we can make the required changes.

For More Information:
10. Go to the `<biserver_home>/pentaho-solution/system` directory.

11. Open the `security.properties` file with your favorite editor.

12. Change the value for the key provider from Jackrabbit (the default) to LDAP. This enables the LDAP provider to start working by connecting your BA server to your LDAP server.

13. Save the file and close the editor.

The LDAP configuration is finished. Remember that we have to restart our BA server before the new configuration changes take effect.

**How it works...**

If someone ever tried to configure LDAP connections to the old BI server CE, it will be very easy to understand that something changed in this new release. Anything about Pentaho's LDAP configuration files was already said in the *Configuring authentication through the LDAP server (EE version)* recipe, so now is a good time to analyze which are the main points where we can expect some differences.

As soon as anyone used to manually configuring LDAP connections in older releases starts to manually configure an LDAP connection in this new release, it will be clear how this procedure is different and easier in the new release.

Let’s go over the different sections of the LDAP configuration file. In old releases, we enabled the usage of a new authentication provider by properly wiring up an appropriate set of spring beans by reconfiguring the `pentaho-spring-beans.xml` file. Now it’s really easier; all the required beans are already wired properly and, by configuration, we can select the authentication provider to be used. To select the right authentication provider, we just need to change the `security.properties` configuration file located in the `<biserver-home>/pentaho-solutions/system` directory by specifying the name of the provider to be enabled (LDAP, in our case). This is a very easy and clean approach with respect to the past where we had to go through the reworking of a spring file to wire up different authenticator beans. This approach was hard because it required knowledge of how to properly manage spring files and the names of the files to wire up.

Then, the major change happened. As soon as we changed the authentication provider by mapping the security to the LDAP provider, we set the following two things:

- We mapped an existing enterprise LDAP group to the role of the Pentaho administrator
- We also mapped a set of default ACLs to specific Enterprise LDAP groups that will be recognized as Pentaho roles

**For More Information:**

Before Pentaho BA 5.0, these things were created by changing some lines in the pentaho.xml file and specifically changing the following two things:

- Change the value of the `pentaho-system/acl-voter/admin-role` element to the LDAP group name you want to consider as the Pentaho administrators role.
- Change values of the `pentaho-system/acl-publisher` children elements (default-acls or overrides) to assign default or overrides to certain LDAP groups.

Now, things radically changed by prioritizing the ease of configuration.

- There is no need to explicitly map the name of the LDAP group that will contain the Pentaho administrators because it is implicitly mapped to the default Pentaho's role administrator. While we configure the `applicationContext-security-ldap.properties` file located in `<biserver-home>/pentaho-solutions/system`, we automatically set the fully qualified name of the LDAP group that will be considered as the Pentaho administrators' role. We do this implicitly by setting the value of the `adminRole` key.
- The default ACLs are implicitly set by setting the appropriate set of Operations Permissions from the Manage Roles tab in the Users / Roles wizard of the Administration perspective.

So what else can we say except that the exact same thing seems easier to do?

**There's more...**

As soon as we connect our security to an LDAP server, the management of our users and roles becomes completely different.

The users' creation and maintenance is completely delegated to the LDAP server as a central unified place in our network that will accomplish this task. Usually, it is the responsibility of our system administrator to manage the task of creating and maintaining users. They know better than us how to manage these kind of things (and we will be very happy to delegate this task). Apart from this, the management of Pentaho roles takes a bit more of our time because even if we associate users to Pentaho roles in the LDAP Server by using LDAP groups, we need to assign to any inherited LDAP group (that will act as a Pentaho role) the related Pentaho Operation Permissions as in any other case.
To do this, we always follow the *Editing an existing role* recipe, look at paragraph where it talks about setting **Operation Permissions**, and do what is described to assign **Operation Permissions** to the roles we get from LDAP server. The interesting thing to notice in this case is that (as shown in the following screenshot) as soon as we go in the **Users / Roles** section of the **Administration** perspective, Pentaho will show us a different **Users / Roles** wizard.

As we can see, the following points are clear:

- The **Manage Users** tab is not present
- The **Manage Roles** tab dialog box contains only the set of roles we get from LDAP with the option to manage **Operation Permissions**

A lot of this is because the real user management is delegated to our LDAP Server. The only thing we can do in Pentaho is manage Pentaho security.

**See also**

Look at the *Configuring authentication through the LDAP server (EE version)* recipe for a detailed description about sections of the *applicationContext-security-ldap.properties* file and its intended use.
Managing the mail server configuration

Pentaho, as a Business Analytics platform, gives us all the tools needed to analyze and get insights from our data. A useful functionality is using the platform to monitor our KPIs and send a set of alerts or notifications as soon as these KPIs are going or have already gone out of acceptable threshold values. To do this, we can use e-mail and send out messages to warn users about these unacceptable conditions. Until Version 4.8, e-mail configuration for Pentaho was a cumbersome task because in the CE version, for example, we had to work directly with configuration files. Starting from this new version, the e-mail configuration wizard has been unified both for the CE and EE version in the Administration perspective.

How to do it...

These steps will show us how we can easily configure the e-mail subsystem in Pentaho BA Server:

1. The Users / Roles entry of the left menu is automatically selected by default.
2. Select the Mail Server entry from the left menu and the Mail Server configuration form opens in the Administration perspective.
3. If it is the first time we are configuring a connection to a Mail Server, the configuration form will be empty. If this is not first time we are going to configure the Mail Server connection, the form will display the current Mail Server configuration as shown in the following screenshot:

For More Information:
4. In the SMTP Host field, type the hostname or the IP address of the Mail Server that we are going to connect to. This field is mandatory.

5. In the Port field, type the hostname or the IP address of the Mail Server that we are going to connect to. The field is already filled with a value, 25, (the default port number for an SMTP server) but we are free to change it according to our needs. This field is mandatory.

6. If our Mail Server is an authenticated mail server, please check the Use Authentication checkbox. Uncheck it in case our server does not require any authentication. The default value for the checkbox is checked. This field is mandatory.

7. In case we checked the Use Authentication checkbox, in the Username field, type the name of the user to be used to get authenticated to the Mail Server to which we are going to connect. This field is mandatory.

8. In case we checked the Use Authentication checkbox, in the Password field, type the password of the user to use to be authenticated to the Mail Server to which we are going to connect. This field is mandatory.

9. From the Protocol drop-down list, select the type of protocol we want to use to communicate with the Mail Server. You can choose either SMTP or SMTPS.

10. In the Address all emails from server will come from the field, type the e-mail address of all of the incoming e-mails received by our users with whom we want to be associated. This is the e-mail address that will be displayed by our e-mail client as the From e-mail address. This field is mandatory.

11. Check Use Start TLS if our server requires Start TLS connection.

12. Check Use SSL if our server requires SSL connection.

13. Press the Test SSL connection to verify that everything is correct in the configuration that we have defined so far.

14. If something in the configuration is wrong, the server returns with a warning that suggests us to review our configuration, correct any errors, and try to test it again.

15. If everything is correct, the server returns with a success message and informs you to check your inbox for the account specified in the Address field all the e-mail from the server will come from for a confirmation message.

16. Press the Close button to close the information dialog box.

17. If the configuration is correct, click on the Save button to confirm our configuration.

Unfortunately, in this case, the server does not inform us about the success of the save operation; it only gives us an exception in case the operation fails.

For More Information:
Chapter 2

How it works...

Starting from this release, e-mail configuration has become a bit friendlier because Pentaho developed a configuration form wizard to assist us with this in any version (either CE or EE). Until the release of Version 4.8, to configure the e-mail in the CE version, a user had to edit an XML configuration file named email-config.xml, which is located in <biserver_home>/pentaho-solution/system/smtp-email. Even if the file was well commented, it was always a little bit trickier for a normal user, and it required quite a bit of technical knowledge to locate the file on Pentaho BA Server directories and also to know the meaning of the various properties and their values. Only the EE version had the wizard to help the user configure the Mail Server connection. Now, the wizard is present in the CE version too and requests for the same information that we found in the file we mentioned so far but in a friendlier way. Lastly, when the user clicks on the Save button, the server updates that same file.

There's more...

Many users use Google's Gmail as the e-mail provider of choice so it is a good idea to spend a few words talking about this.

Configuring e-mail to connect to Gmail

The SMTP e-mail configuration has a few things to take into consideration as detailed in the following steps:

1. Remember that the name of Google's SMTP Host is smtp.gmail.com. Type this name in the SMTP Host field.
2. Gmail requires an authenticated connection so be sure that the Use Authentication checkbox is checked.
3. Insert a valid Gmail username and password. Remember to type the username followed by its domain (for example, sample.username@domainame.com) in order for it to be correctly understood by Google.
4. The port to connect to Google's SMTP server is 587. Type this value in the Port field.
5. From the Protocol drop-down list, select SMTPS.
6. Set the value for the Use Start TLS checkbox to the checked value.
7. Set the value for the Use SSL checkbox to the checked value.

See also

If you are a newbie looking for details about the SMTP protocol, look at the article at http://en.wikipedia.org/wiki/SMTP. For details on how to configure a Gmail account with POP3 or IMAP, see the article at https://support.google.com/mail/troubleshooter/1668960?rd=1#ts=1665119,1665162.

For More Information:
Cleaning up aged generated files immediately

In any case where we run the execution of a content item, we have the production of temporary files (either iPDF, Excel, images, or any other thing). This content is produced in a specified location and must be regularly cleaned up so it doesn’t fill the disk at a level that could be dangerous for the system. This recipe shows us how we can run a task from the Administration perspective to immediately clean up that kind of content.

How to do it...

The following steps detail how we can run a task from the Administration perspective to immediately clean up aged generated files:

1. Select the Settings entry from the left menu in the Administration perspective.
2. The Settings configuration form is opened, as shown in the following screenshot:

   ![Configuration Form Screenshot]

3. Look at the form’s Delete generated files now section as shown in the previous screenshot.

For More Information:

4. Set the maximum age of the files in the Delete generated files older than field.
5. Click on the Delete Now button.
6. The task of deletion starts immediately and the temporary content is immediately deleted.

**How it works...**

Cleaning up aged generated files is an important operation to keep the usage of our disk under control. By going in the Administration perspective and choosing the Settings entry, we can set an aging value for our files by filling the Delete generated files older than field. By clicking on the Delete Now button, a background task will immediately delete the older content files.

**See also**

We can take a look at the Scheduling cleanup of aged generated files recipe if we are interested in scheduling the maintenance and deletion of aged files.

**Scheduling the cleanup of aged generated files**

The previous recipe showed us how we can delete temporary files immediately. The current recipe shows us how we can do the same thing but by scheduling the task that deletes the temporary files so that it can automatically be executed periodically and maintain the temporary directory cleanup without any effort.

**How to do it...**

The following steps detail how we can schedule the cleanup of aged generated files:

1. Select the Settings entry from the left menu from the Administration perspective.
Configuring Your BA Server Instance

2. The **Settings** configuration form opens as shown in the following screenshot:

3. Look at the **Schedule deletion of generated files** section of the form as shown in the previous screenshot.

4. Initially, if we never set a schedule, a label will inform us that no schedules are defined to delete temporary files.

5. Click on the **Schedule Deletion** button.

6. The **Edit Schedule** dialog box opens to let us set the properties and launch the deletion task according to our needs.

For More Information:
7. Set the maximum age of the files to delete by typing a value in the **Delete generated files other than** field. The default value is **180** days.

8. Fill in all the parameters needed to rightly schedule the files' deletion.

9. Click on the **Cancel** button to close the dialog box without confirming the new schedule. In this case, no schedules are created at all.

10. Click on the **OK** button to confirm the schedule and close the dialog box. A detail of the schedule we just set is shown in the **Settings** screen as shown in the previous screenshot.

11. If we want to reset the schedule that we just created, we click on the **Cancel Schedule** button shown in the previous screenshot.

### How it works...

Managing the deletion of aged files using the schedule is very simple. It creates a new schedule behind the scenes to automatically start the execution of the deletion task. The task started is the same task that we start if we want to immediately delete the temporary files, and you can start it by pressing the **Delete Now** button (see the previous recipe for details about this). Remember that this schedule will not be visible to users because it is considered a system schedule.

### See also

To see how we can delete aged temporary files immediately, see the *Cleaning up aged generated files immediately* recipe.
Where to buy this book


Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.