

Apache Directory Studio Apache DS

User's Guide

Apache Directory Studio Apache DS: User's Guide

Version 2.0.0.v20210213-M16

Copyright © 2006-2021 The Apache Software Foundation

Licensed to the Apache Software Foundation (ASF) under one or more contributor license agreements. See the NOTICE file distributed with this work for additional information regarding copyright ownership. The ASF licenses this file to you under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Table of Contents

| | |
|---|----|
| I. Getting started | 1 |
| 1. Download and installation | 1 |
| 2. LDAP Servers View | 1 |
| 3. Apache DS Configuration Editor | 2 |
| 3.1. Overview Page | 3 |
| 3.2. LDAP/LDAPS Servers Page | 4 |
| 3.3. Kerberos Server Page | 6 |
| 3.4. Partitions Page | 7 |
| 3.5. Password Policies Page | 8 |
| 3.6. Replication Page | 10 |
| II. Tasks | 12 |
| 1. Creating a new LDAP server | 12 |
| 2. Starting a server | 12 |
| 3. Stopping a server | 12 |
| 4. Editing the configuration | 13 |
| 5. Deleting a server | 13 |
| III. Reference | 14 |

Chapter I. Getting started

This part of the guide provides you a sum up of the basic concepts of the Apache DS plugin.

1. Download and installation

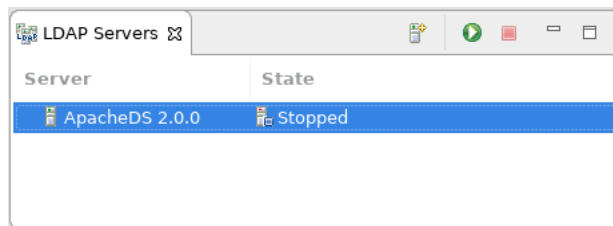
The latest version of Apache Directory Studio can be downloaded from the Apache Directory Studio Downloads page, at this address: <https://directory.apache.org/studio/downloads.html> [<https://directory.apache.org/studio/downloads.html>].

The download page also includes the installation instructions.

2. LDAP Servers View

The LDAP Servers view allows you to manage the servers. This view displays a list of all your servers. You can use this view to start or stop the servers.

Here is an example screenshot of the LDAP Servers view:



Use the LDAP Servers view to perform the following tasks:




- Create a server
- Rename a server
- Configure a server
- Start a server
- Create a connection to the server
- Stop a server
- Delete a server

The LDAP Servers view displays the current status of all the servers. The **State** column indicates whether or not a server has been started. The following lists the possible server status:

- Starting
- Started
- Stopping
- Stopped






Toolbar

The toolbar of the LDAP Servers view contains the following actions:

-  - *New server* : Creates a new LDAP server.
-  - *Run* : Starts the selected LDAP server.
-  - *Stop* : Stops the selected LDAP server.






Context Menu

The context menu of the LDAP Servers view contains the following actions:

-  - *New Server* : Creates a new LDAP server.
- *Open Configuration* : Opens the configuration editor.
-  - *Delete* : Deletes the selected LDAP server.
- *Rename...* : Renames the selected LDAP server.
-  - *Run* : Starts the selected LDAP server.
-  - *Stop* : Stops the selected LDAP server.
-  - *Create a Connection* : Creates a preconfigured connection to the selected LDAP server.
- *Properties* : Opens the properties dialog of the selected LDAP server which shows details like version and the path the to configuration folder.

Icons

The following icons can appear in the LDAP Servers view:

| Icon | Description |
|---|-----------------|
|  | Server |
|  | Starting server |
|  | Started server |
|  | Stopping server |
|  | Stopped server |

3. Apache DS Configuration Editor

The Configuration Editor for Apache DS consists in a six pages editor:

- The *Overview* gives you a quick overview about enabled protocols, ports, and configured partitions.

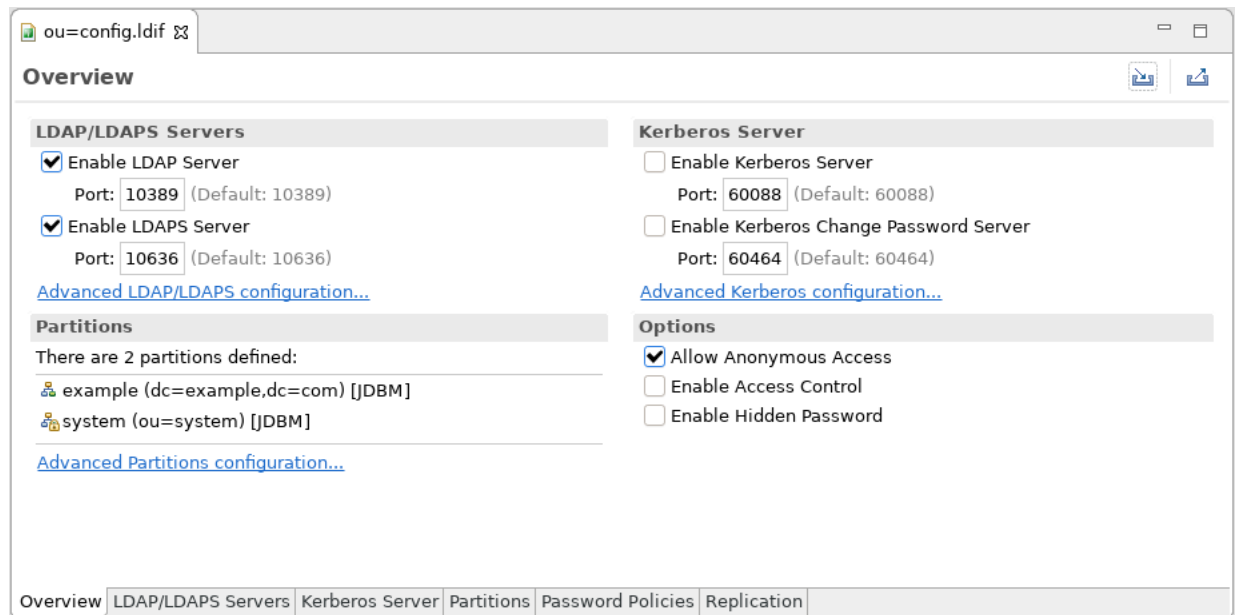
- The *LDAP/LDAPS Servers* page allows you to configure the LDAP server.
- The *Kerberos Server* page allows you to configure the Kerberos server.
- The *Partitions* page allows you to manage your server partitions.
- The *Password Policy* page allows you to manage password policies.
- The *Replication* page allows you to manage replication settings.

3.1. Overview Page

The **Overview** page gives you a quick overview about enabled protocols, ports, and configured partitions.

It contains four sections : **LDAP/LDAPS Servers** , **Kerberos Server** , **Partitions** and **Options** .

Here's what the **Overview** page looks like:



LDAP/LDAPS Servers

This section allows you to enable/disable each of the following protocols and specify the port it is running on:

- LDAP (default port: 10389)
- LDAPS (default port: 10636)

Kerberos Server

This section allows you to enable/disable each of the following protocols and specify the port it is running on:

- Kerberos (default port: 60088)
- Change Password (default port: 60464)

Limits

This section shows the partitions defined.

Options

Check the **Allow Anonymous Access** checkbox to allow anonymous access on the server.

Check the **Enable Access Control** to enable Access Control on the server.

Check the **Enable Hidden Password** to hide password attributes in search results.

3.2. LDAP/LDAPS Servers Page

The **LDAP/LDAPS Servers** page of the configuration editor allows you to edit all LDAP specific settings.

It contains the following sections : **LDAP/LDAPS Servers** , **Limits** , **SSL/Start TLS Keystore** , **SSL Advanced Settings** , **Supported Authentication Mechanisms** , **SASL Settings** and **Advanced** .

Here's what the **LDAP/LDAPS Servers** page looks like:

LDAP/LDAPS Servers

This section allows you to enable/disable the LDAP and LDAPS protocols. For each protocol you can specify

- Port: the TCP port the server should listen to
- Address: the IP address the server should bind to (default 0.0.0.0 means to bind to all network interfaces)
- NbThreads: the number of threads to use to serve requests

- **Backlog Size:** the number of requests to queue when all threads are busy

Limits

This section allows you to specify the Limits of the server.

Max. Time Limit lets you choose the maximum time that should last a request (in milliseconds).

Max. Size Limit lets you choose the maximum number of entries that should be returned.

Max. PDU Size lets you choose the maximum PDU size (in bytes).

SSL/Start TLS Keystore

This section allows you to specify keystore which contains the private key used for SSL and Start TLS sessions.

Keystore lets you select the path to the keystore file.

Password lets you enter the password of the keystore file.

SSL Advanced Settings

This section allows you to specify advanced settings for SSL and Start TLS.

Check the **Require Client Auth** checkbox to require client authentication.

Check the **Request Client Auth** checkbox to request client authentication.

Ciphers Suite lets you select which cipher suites are allowed to use.

Enabled Protocols lets you select which protocols are enabled (default: TLSv1, TLSv1.1, TLSv1.2).

Supported Authentication Mechanisms

This section allows you to specify the supported authentication mechanisms. You can choose between the following mechanisms:

- SIMPLE
- GSSAPI (SASL)
- CRAM-MD5 (SASL)
- DIGEST-MD5 (SASL)
- NTLM (SASL), including the provider
- GSS-SPNEGO (SASL), including the provider

SASL Settings

This section allows you to specify to the SASL settings.

The **SASL Host** field represents the name of the host.

The **SASL Principal** field represents the service principal name that the server-side of the LDAP protocol provider will use to "accept" a GSSAPI context initiated by the LDAP client. The SASL principal **MUST** follow the name-form "ldap/[fqdn]@[realm]".

The **Search Base DN** field represents the Distinguished Name where a subtree-scoped DIT search will be performed. This is **BOTH** where the LDAP service principal must reside, as well as where user principals must reside.

The **SASL Realms** field allows you specify to the SASL realms.

Use the **Add...** , **Edit...** and **Delete** buttons to set your SASL Realms.

Advanced

This section allows you to specify other advanced settings of the server.

Check the **Enable TLS** checkbox to enable the Start TLS extended operation.

Check the **Enable server-side password hashing** checkbox to instruct the server to hash modified user passwords on the server side. When checked this also allows you to select the hashing method to use.

The **Replication pinger sleep** field allows you to define the frequency how often the replication consumer pings the replication producer (in seconds).

The **Disk synchronization delay** field allows you to define the frequency how often data is synchronized to the disk (in milliseconds).

3.3. Kerberos Server Page

The **Kerberos Page** of the configuration editor allows you to edit all Kerberos specific settings.

It contains the following sections : **Kerberos Server** , **Kerberos Settings** and **Ticket Settings** .

Here's what the **Kerberos Server page** looks like:

The screenshot shows the 'Kerberos Server' configuration page. It is divided into three main sections:

- Kerberos Server**:
 - Enable Kerberos Server
 - Port: 60088 (Default: 60088)
 - Address: 0.0.0.0 (Default: 0.0.0.0)
 - Enable Kerberos Change Password Server
 - Port: 60464 (Default: 60464)
 - Address: 0.0.0.0 (Default: 0.0.0.0)
- Kerberos Settings**:
 - Primary KDC Realm: EXAMPLE.COM (Default: EXAMPLE.COM)
 - Search Base Dn: ou=users,dc=example,dc=com (Default: ou=users,dc=example,dc=com)
 - Encryption Types:
 - DES-CBC-MD5
 - DES3-CBC-SHA1-KD
 - AES128-CTS-HMAC-SHA1-96
- Ticket Settings**:
 - Verify Body Checksum
 - Allow Empty Addresses
 - Allow Forwardable Addresses
 - Require Pre-Authentication By Encrypted TimeStamp
 - Allow Postdated Tickets
 - Allow Renewable Tickets
 - Allow Proxiable Tickets
 - Max. Renewable Lifetime (ms): 604800000
 - Max. Ticket Lifetime (ms): 86400000
 - Allowable Clock Skew (ms): 300000

At the bottom, there is a breadcrumb trail: Overview | LDAP/LDAPS Servers | Kerberos Server | Partitions | Password Policies | Replication.

Kerberos Server

This section allows you to enable/disable the Kerberos and Change Password protocols. For each protocol you can specify

- Port: the TCP port the server should listen to

- Address: the IP address the server should bind to (default 0.0.0.0 means to bind to all network interfaces)

Kerberos Settings

This section allows you to specify the Kerberos server settings.

The **Primary KDC Realm** field represents the primary realm of the key distribution controller.

The **Search Base DN** field represents base DN in the LDAP server where principals are searched.

Encryption Types lets you select which encryption types are allowed to use.

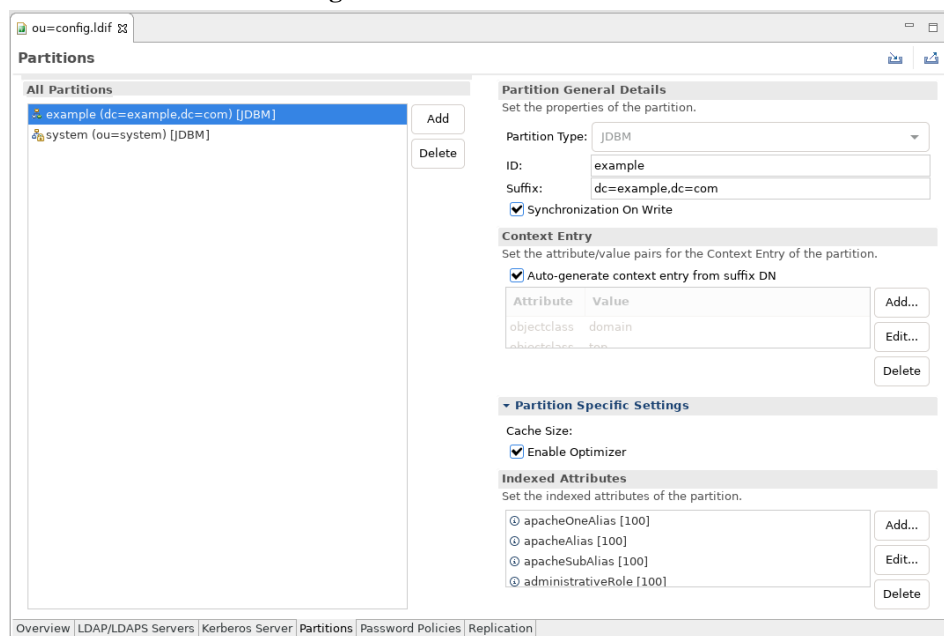
Ticket Settings

This section allows you to specify the Ticket specific settings. Please refer to RFC 1510 and RFC 4120 for detailed information about each setting.

3.4. Partitions Page

The **Partitions Page** of the configuration editor allows you to edit the server partitions.



Here's what the **Partitions Page** looks like:



The page is divided vertically in two parts.

The left side of the page shows the partitions defined on the server. This is where you can add or delete a partition.

The following icons appear:

-  : Standard Partition
-  : System Partition

The right side of the page display and lets you edit the details of the selected partition in the left side.

Partition General Details

Partition Type allows you to choose the partition type. Available options are JDBM or Mavibot.

An **ID** is mandatory for the partition.

A **Suffix** is mandatory for the partition and defines the context entry DN.

Check the **Synchronization On Write** checkbox to enable the synchronization on write for the partition.

Context Entry

Check the **Auto-generate context entry from suffix DN** to instruct the server to automatically generate the context entry on first startup.

If you disable the auto-generation you have to specify all attributes.

Partition Specific Settings

If you selected JDBM partition type the following settings are available.

The **Cache Size** defines the cache size of the partition.

Check the **Enable Optimizer** checkbox to enable the optimizer for the partition.

Indexed Attributes

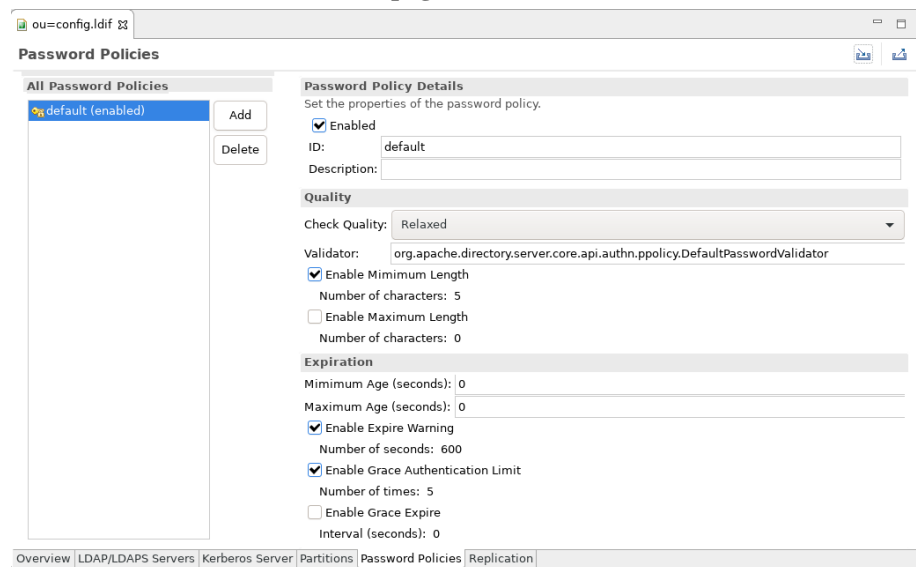
This section allows you to specify to the server the attributes that should be indexed and their cache size.

Use the **Add...**, **Edit...** and **Delete** buttons to set the indexed attributes.

3.5. Password Policies Page

The **Password Policies Page** of the configuration editor allows you to edit the server's password policies. See also IETF draft-behera-ldap-password-policy-10 for a detailed description of the password policy configuration.

Here's what the **Password Policies page** looks like:



The page is divided vertically in two parts.

The left side of the page shows the password policies defined on the server. This is where you can add or delete a policy.

The right side of the page display and lets you edit the details of the selected password policy in the left side.

Password Policy Details

Check the **Enabled** checkbox to enable the password policy.

An **ID** is mandatory for the password policy.

An **Description** is optional for the password policy.

Quality

Check Quality defines which quality level a new password must fulfil. One of the following options can be chosen:

- Disabled - Don't check the password
- Relaxed - Check the password and accept passwords that can't be checked (hashed passwords)
- Strict - Check the password but reject passwords that can't be checked (hashed passwords)

Validator Defines the class that implements PasswordValidator interface (default org.apache.directory.server.core.api.authn.ppolicy.DefaultPasswordValidator).

Check **Enable Minimum Length** to enable and specify the minimum password length.

Check **Enable Maximum Length** to enable and specify the maximum password length.

Expiration

Minimum Age defines the number of seconds that must elapse between modifications to the password.

Maximum Age defines the number of seconds after which a modified password will expire. Default value is 0, does not expire. If not 0, the value must be greater than or equal to the value of the minimum age.

Check **Enable Expire Warning** to enable and specify the number of seconds before password expiration a warning message will be returned to an authentication user.

Check **Enable Grace Authentication Limit** to enable and specify the how often an expired password can be used to authenticate.

Check **Enable Grace Expire** to enable and specify the number of seconds for the grace period.

Options

Check **Enable Must Change** to enforce that the password must be changed by the user after a password reset.

Check **Enable Allow User Change** to allow users to change their own password.

Check **Enable Safe Modify** to enforce that the existing password must be ent when changing the password.

Lockout

Check **Enable Lockout** to enable password lockout.

Lockout Duration defines the number of seconds that the password cannot be used to authenticate due to too many failed bind attempts.

Maximum consecutive Failures defines the number of consecutive failed bind attempts after which the password may not be used to authenticate.

Check **Enable Maximum Idle** to enable and specify the number of seconds an account may remain unused before it becomes locked.

Check **Enable In History** to enable and specify the maximum number of used password history is preserved.

Minimum Delay defines the number of seconds to delay responding to the first failed authentication attempt. Default value 0, no delay

Maximum Delay defines the maximum number of seconds to delay responding to the first failed authentication attempt.

3.6. Replication Page

The **Replication** of the configuration editor allows you to setup replication consumers. See also RFC 4533 for a detailed description of the parameters.

Here's what the **Replication Page** looks like:

The screenshot shows the 'Replication' configuration page. On the left, there is a list of 'All Replication Consumers' with one entry, 'consumer1', and 'Add' and 'Delete' buttons. The main area is divided into several sections:

- Replication Consumer Details:** Includes a checked 'Enabled' checkbox, an 'ID' field with 'consumer1', and a 'Description' field.
- Connection:** Includes 'Replication Mode' with radio buttons for 'Refresh And Persist' (selected) and 'Refresh Only'. Below it is a 'Refresh Interval (ms): 60000' field. Other fields include 'Remote Host: localhost', 'Remote Port: 10389', 'Bind DN: uid=admin,ou=system', 'Bind Password: *****' (with a 'Show password' checkbox), 'Size Limit: 0', 'Time Limit: 0', and a 'Use Start TLS' checkbox.
- Replication Consumer Details (Configuration):** Includes 'Base DN: dc=example,dc=com' with a 'Browse...' button, 'Filter: (objectClass=*)' with a 'Filter Editor...' button, 'Scope: Subtree' (selected), 'Attributes: All Attributes' (checked), and a list of attributes with 'Add...', 'Edit...', and 'Delete' buttons.
- Aliases and Dereferencing:** Includes checkboxes for 'Finding Base DN' and 'Search'.

The bottom of the page has a navigation bar with tabs: Overview, LDAP/LDAPS Servers, Kerberos Server, Partitions, Password Policies, and Replication.

The page is divided vertically in two parts.

The left side of the page shows the replication consumers defined on the server. This is where you can add or delete a replication consumer.

The right side of the page display and lets you edit the details of the selected replication consumer in the left side.

Replication Consumer Details

Check the **Enabled** checkbox to enable the replication consumer.

An **ID** is mandatory for the replication consumer.

An **Description** is optional for the replication consumer.

Connection

Replication Mode defines the replication mode to use. One of the following options can be chosen:

- Refresh And Persist - Push based replication using persisten search
- Refresh Only - Poll based replication


The reminder of the section allows to configure the connection parameters to the replication provider.

Configuration

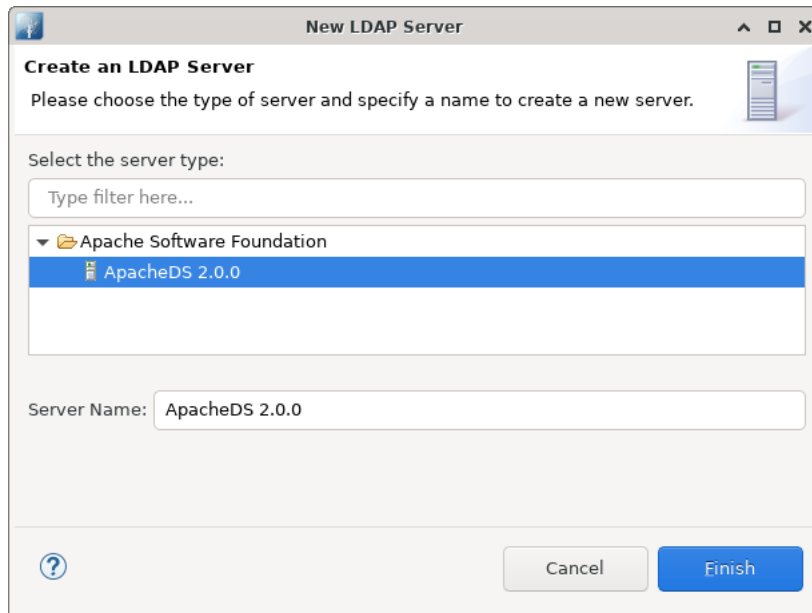
The configuration section allows to define the search parameters for the entries to replicate.

Chapter II. Tasks

1. Creating a new LDAP server

To create a new LDAP server, in the Servers view toolbar, click on the  **New Server** button, or use the **Strg-E** shortcut.


The following wizard appears:




Give a name to the server.

| Option | Description | Default |
|-------------|---|---------|
| Server Type | The type of the LDAP server. Currently only the Apache Directory Server (ApacheDS) is available. | empty |
| Server Name | The name of the LDAP server. In the LDAP Servers view the server is listed with this name. The name must be unique. | empty |

2. Starting a server

To start a server, in the Servers view, select the server you want to start and click the  **Run** button in the toolbar, or use the **Strg-R** shortcut.

3. Stopping a server

To stop a server, in the Servers view, select the server you want to stop and click the  **Stop** button in the toolbar, or use the **Strg-T** shortcut.

4. Editing the configuration

To edit the configuration of a server, in the Servers view, select the server and double-click on it, click the **Open Configuration** action in the context menu, or use the **F3** shortcut.

5. Deleting a server

To delete a server, in the Servers view, select the server you want to delete and click the **✖ Delete** action in the context menu, or use the **Delete** shortcut.

Chapter III. Reference