OPEN-XCHANGE™ Whitepaper

keep in touch

OX
OPEN·XCHANGE
SERVER 5.0
• Outlook-Echtzeitanbindung
• Integration einer WebDAV-Schnittstelle
• Dediziertes Lösch-/Besitzrecht
• Flexible Frameplatzierung
• Instant Messaging- Komponente
• Implementierung „Öffentlicher Ordner"
• Anlage von Sichtvorlagen
• Erweiterung der Terminserienfunktion
• Teamansicht

Open-Xchange™ Server

Directory Integration

Concepts to integrate Open-Xchange Server 5

into Company Directory Services

v1.00

The information contained in this book was compiled with the utmost care. Nevertheless, erroneous statements cannot be excluded altogether. Open-Xchange Inc., the authors and the translators are not liable for possible errors and their consequences.

The names of software and hardware used in this book may be registered trademarks; they are used without guarantee of free usability. Open-Xchange Inc. generally follows the spelling conventions of the manufacturers. The reproduction of brand names, trade names, logos etc. in this book (even without special marking) does not justify the assumption that such names can be considered free (for the purposes of trademark and brand name regulations).

Please direct any recommendations or comments to
documentation@open-xchange.com

Author: Stephan Martin

Editors: Robert Colombara, David Cuthbert, Stephan Martin

Layout: Robert Colombara

Contents

1. Introduction

The Open-Xchange Server 5 is an Open Source-based, full featured Messaging and Collaboration solution that runs on Red Hat Enterprise Linux 4 and SUSE Linux Enterprise Server 9.

The architecture of Open-Xchange Server 5 is completely based on open standards and open protocols and makes use of well known open source services, which are included in the Linux enterprise distributions, as back ends.

Due to the use of standard protocols, there are many possibilities to exchange the back end services and to integrate Open-Xchange into existing infrastructure services in a company's IT structure.

There are many reasons for deciding to integrate the Open-Xchange Server into an existing company wide directory service. Such integration derives benefits from reuse of the pre-existing user base and allows central administration and sharing of the same authentication data with other services. In addition it overcomes certain limitations inherent in the OpenLDAP server, like scalability and replication.

This whitepaper describes several ways to integrate Open-Xchange Server 5 into existing company directories. These different concepts offer a wide range of flexibility on the one hand and of complexity on the other hand.

This whitepaper is not meant as a complete How-To with in depth documentation of configuration files or programming examples. This paper describes the concepts on an architectural level. Obviously a System Administrator requires deep knowledge of Open-Xchange Server and the Linux Operating System as well as of the existing company directory service in order to implement a successful integration.

2. Architecture Overview

This chapter gives a brief overview of the architecture of the Open-Xchange Server and its back end services.

In general the Open-Xchange Server 5 consists of the Open-Xchange Application Server, which contains the application logic and which does the main processing work, a collection of daemons which handle specific tasks.

All data is handled by back-end services, which are specially designed to store exactly these types of data.

Essentially, there are four types of data storage:

- Directory Service (LDAP)
- Database (SQL)
- E-Mail (IMAP/SMTP)
- File System

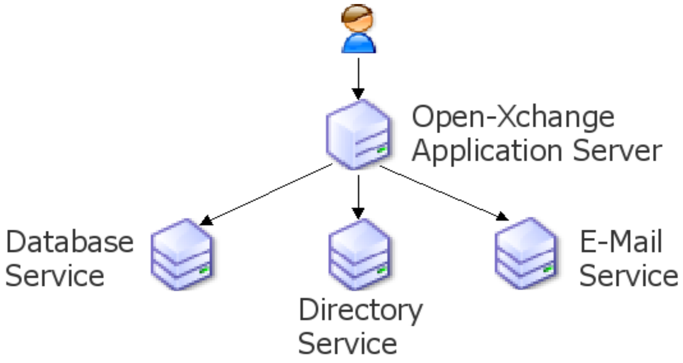

Figure 1: Subsystems inside of the Open-Xchange Server

2.1. The Open-Xchange Administration Framework

This chapter describes the standard setup used to administer an Open-Xchange Server when it is integrated with its back-end services.

In the standard setup, the Open-Xchange Server's administrative front-end is used to administer all users through the Open-Xchange Server.

In the maintained version of the Open-Xchange Server, the administrative front-end communicates with the server through the XML-RPC interface, which allows access to all administrative tasks. On the Open-Xchange Server there is a daemon running which will listen for XML-RPC calls and which coordinates necessary actions with the relevant back-end services to respond to them. Any necessary XML-RPC commands can also be generated through command line tools which are included in the Open-Xchange Server package. So it is possible to trigger all actions needed for server administration.

In short this means that while data is stored by backend services, calls to those services are handled by the Open-Xchange server itself rather than directly through the administrative front-end.

The main advantage of this concept is that the Open-Xchange Server acts as an abstraction layer between the administrative front-end and the back-end services. If one backend service is changed, the database component for example, only the relevant interface in the Open-Xchange Server needs to be adapted and the other components don't need to be changed.

3. Directory Integration

This chapter presents several ways to integrate the Open-Xchange Server into existing Company Directory services.

3.1. Reasons for Directory Integration

There could be many reasons why the Open-Xchange Server should be integrated into existing Company Directories.

Some of them are related to our, Open-Xchange's, belief that it is important to integrate our software into existing structures, as opposed to forcing a company to develop its IT infrastructure in a way that is convenient for our product development group. It is brash to presume that a messaging and collaboration solution should define the way a company administers its employees and its whole IT infrastructure. On the contrary, Open-Xchange believes that a collaboration solution should be administered in exactly the way a company wants to administer their employees.

- Single Point of Administration
  The users are created only once in the Company Directory and don't need to be created in the Open-Xchange Servers directory as well. A single repository contains all usernames and passwords.

- Single Authentication
  The user has one username and one password for all applications in the company. If he changes his password in one place, the new password is automatically valid for all other applications as well

- Inherit Administration Delegation
  In many companies personnel are not administered by IT administrators, their user accounts are created by the Human Resources department when they enter the company and HR deletes the accounts when they leave the company. In many cases HR departments use provisioning software which is connected to the company directory server. Integration into this company directory will provide the ability for Open-Xchange Server to be administered through HR.

- Inherit Decentralized Administration
  Many companies require decentralized user administration. This means that there is a dedicated administrator for department A and another one for department B. This type of decentralized administration often requires a highly sophisticated and flexible permission model which cannot be built into a directory service in a standard way and still fulfill the requirements of every company. If the company's directory administration tool provides this type of

decentralized administration, it will be inherited transparently by the Open-Xchange Server.

3.2. Integration Concepts

There are several different methods through which directory integration can be achieved. It is very important to find the right solution for the project. The concepts range from simple offline replication to a deep online integration with the use of the native information from the company directory. Another consideration is that implementation of these methods ranges from a 1 hour task to a large and complex IT project.

3.2.1. Simple Offline Replication with Connector

The simplest integration method is relies on a connector which will read the information from the company directory and will write it to the Open-Xchange Server’s internal directory service.

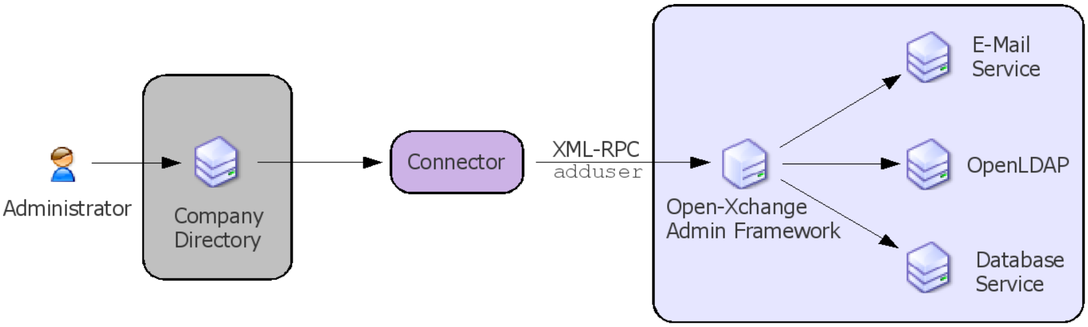

Figure 2: Integration of Company Directory Services via a Connector

This concept is very easy to implement, as the simplest version of the connector may be just a shell or Perl script which does the search for a given username in the company directory and then uses the returned values to call the command line tool `adduser` in order to create the user on the Open-Xchange Server. Of course, this type of connector could be enhanced to run regularly and to automatically scan the company directory for changes. This scenario is typically a one way process, the data is read from the company directory and is written to the Open-Xchange Server.

One huge drawback of this concept is that it is normally impossible to read passwords from the company directory in a way which would permit synchronize with the Open-Xchange Server. Therefore the users would have to be created with a standard password and would be forced to change the password during the first login.

Pros and Cons:

- **Pro:** No need for changes (Schema, Permissions) in company directory
- **Pro:** Very easy to implement
- **Con:** No transparent online integration, different repositories

3.2.2. Enhanced Offline Replication with Connector

The inability to synchronize the password mentioned above can be solved by adopting a slightly more complex methodology: the Open-Xchange internal LDAP directory can be configured in such a way that it authenticates against the company directory and not against its own password data store.

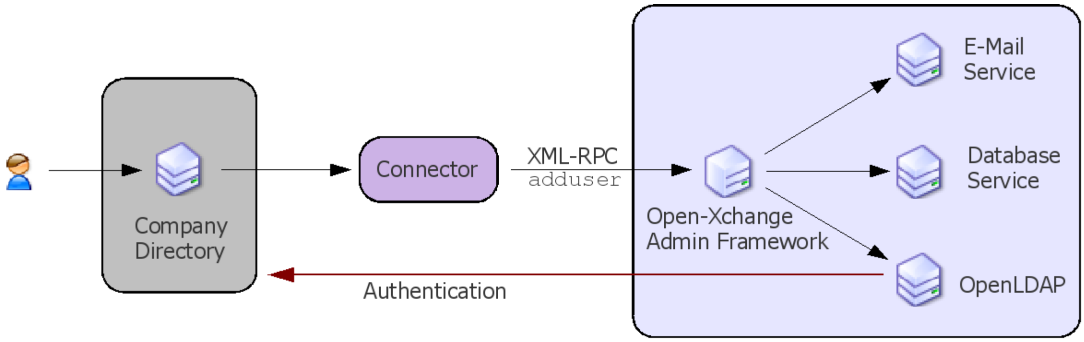

Figure 3: Offline Replication using a Connector

This concept also makes it possible to use other authentication methods like `kerberos` to authenticate against the company directory, which is useful if the company directory is an ADS (Active Directory Server).

The main drawback of this concept is that it requires some deep knowledge to tweak OpenLDAP to use another directory service as authentication source.

Pros and Cons:

- **Pro:** No need for changes (Schema, Permissions) in Company Directory
- **Pro:** Use Company directory for authentication, no password sync necessary
- **Con:** No transparent online integration, different repositories
- **Con:** Implementation of transparent authentication quite complex

3.2.3. Advanced Transparent Online Integration

The most advanced form of system integration is a complete and transparent integration of the Open-Xchange Server into the company directory. In this concept, the standard Open-Xchange internal OpenLDAP directory would be completely replaced by the existing company directory.

The complexity and the effort required to implement this advanced integration are heavily dependent on the type and structure of the company directory.

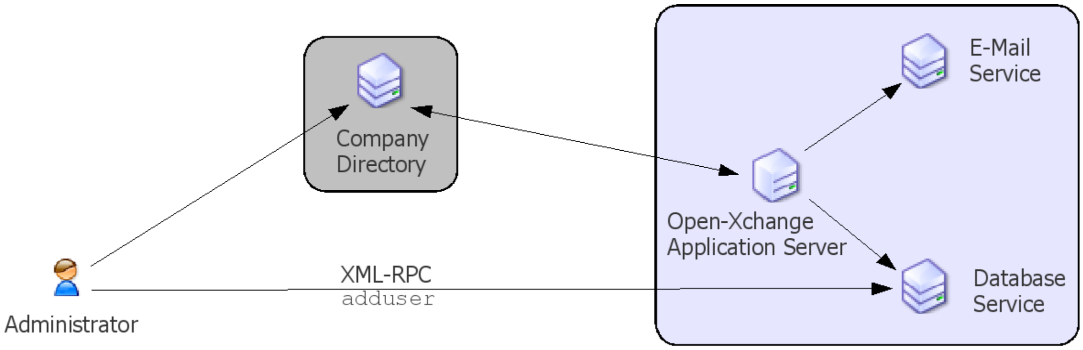

Figure 4: Transparent Online Integration

To implement this concept, there are three major adaptations which must be put into effect:

- The company’s directory schema needs to be enhanced to hold the additional information that is required by the Open-Xchange Server (e.g. user settings like time zone and language) The administrative front-end for the company directory also needs to be enhanced to edit/update this additional information
- The Open-Xchange Server’s LDAP interface configuration needs to be adapted to work with the company directory, e.g. to map several LDAP attributes to the names that are already present in the company directory or to use the structure of the company directory, which may be complex, to represent the organizational structure of the company.
- The administration front-end for the company directory, or the company directory itself, needs to be adapted to trigger the required actions on the Open-Xchange Server when a user is created or deleted. This is necessary, e.g., to have the correct permission mappings in the database for the different groupware modules. This trigger can be done through the XML-RPC interface mentioned above or through the relevant command line tools.

Pros and Cons:

- **Pro:** Complete, transparent integration
- **Pro:** Decentralized Administration possible through Company Directory
- **Pro:** Scalability through Company Directory
- **Con:** Quite complex to implement
- **Con:** Company Directory / Admin Front-end needs to be adapted:
    - Open-Xchange Schema
    - Trigger user deployment to database

3.2.4. Advanced Online Integration through a Meta Directory

The last concept is the one which, on the one hand, is the most flexible but, on the other hand, is the most complex.

Implementing a Meta Directory between the company directory and the Open-Xchange Server will bring all advantages of the advanced integration mentioned above, without the need to modify the company directory.

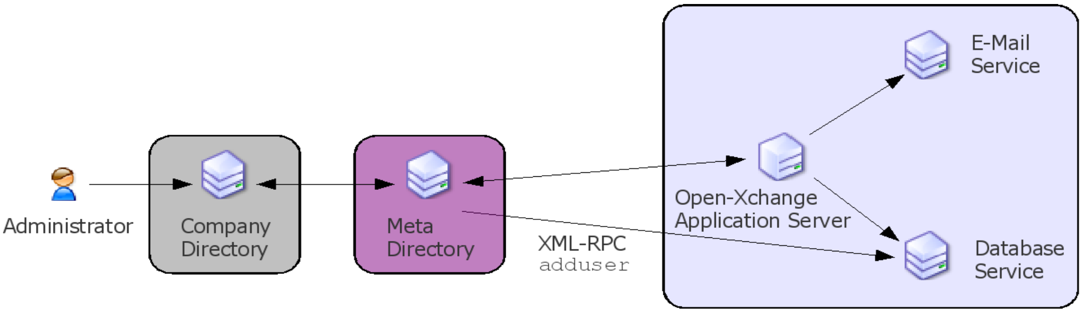

Figure 5: Directory Integration via a Meta Directory

The Open-Xchange Server will integrate completely and transparently into the meta directory. The meta directory is responsible for mapping attributes and the directory structure between the company directory and the Open-Xchange Server.

Pros and Cons:

- **Pro:** Decentralized Administration through Company Directory
- **Pro:** Scalability through Company Directory
- **Pro:** Very flexible through the Meta Directory as abstraction layer
- **Con:** Quite complex to implement
- **Con:** Third system introduced (maintenance)