OXSE4UCS 6.22 / 7.2

Open-Xchange Server Edition 6.22 / 7.2 for Univention Corporate Server 3.1

Table of contents

1 Introduction

The Open-Xchange Server Edition for Univention Corporate Server (OXSE4UCS) includes the groupware Open-Xchange and the integration packages for Univention Corporate Server (UCS).

OXSE4UCS is tailored to professional users looking for a tried-and-tested solution for the management of their entire IT infrastructure including groupware or companies which already employ UCS and wish to expand their infrastructure with innovative groupware functions.

More detailed information on UCS can be found on the Univention GmbH website:
http://www.univention.de/

2 Installation

As OXSE4UCS is an expansion pack for the Univention Corporate Server, one or more UCS server(s) must be installed first.

There are several possible different installation scenarios. In principle, OXSE4UCS can be installed on all UCS domain controller server roles: DC master, DC backup or DC slave. Installation on the server roles *member server* or *base system* is currently not possible.

To start, the UCS systems are installed as usual with UCS 3.1. If several systems are in the UCS domain, a check must be performed that the join procedure has been run on all servers. This is usually done at the end of the installation procedure. Further information on the installation of UCS can be found in the UCS manual: http://docs.univention.de/.

Please ensure that the latest UCS errata updates are installed on all systems (with the UMC module *Online Update → Package Updates* or the command line tool *univention-upgrade*).

2.1 Single server installation on a DC master, DC Backup or DC Slave

Since UCS 3.1 the Open-Xchange Server Edition has to be installed via the Univention App Center. To start the Univention App Center, log into Univention Management Console and open the UMC module **App Center**. In the Univention App Center you need to select the application ***Open-Xchange Server Edition*** and click on *Install*.

Download, installation and configuration of OXSE4UCS may take several minutes. Please do not shut down or restart the UCS system until the installation is complete.

To get access to the newest updates for OXSE4UCS, username and password for a valid LDB account may be configured. The configuration is explained in section 4.1 in detail.

2.2 Installation in a distributed environment

When installing a distributed environment, integration in the UCS management system must be performed firstly by installing packages on DC Master.

```
$ univention-upgrade
$ univention-add-app -l oxseforucs
$ univention-install univention-ox-directory-integration univention-ox-common python-univention-ox-common
$ univention-upgrade
```

If DC backup systems are present within the UCS domain, the package **python-univention-ox-common** has to be installed on all DC backup systems.

```
$ univention-upgrade
$ univention-add-app -l oxseforucs
$ univention-install python-univention-ox-common
$ univention-upgrade
```

The following services can then be distributed on the other UCS systems:

- IMAP server and spam and virus filtering
- MySQL server (*mysql-server*)
- OX instance (*univention-ox*)

2.2.1 MySQL server

On the MySQL server the package **mysql-server** has to be installed:

```
$ univention-upgrade
$ univention-add-app -l oxseforucs
$ univention-install mysql-server
$ univention-upgrade
```

The configuration of the MySQL server should be set so that the MySQL service can be accessed via the external network interfaces. To achieve this, for example, the *bind-address* option can be set to *0.0.0.0* in the MySQL configuration file */etc/mysql/my.cnf*.

```
bind-address 0.0.0.0
```

After the change, the MySQL service needs to be restarted:

```
$ invoke-rc.d mysql restart
```

and the MySQL port has to be configured in the local firewall settings:

```
$ ucr set security/packetfilter/tcp/3306/all=ACCEPT
$ invoke-rc.d univention-firewall restart
```

In addition, the OX instances must be authorized to access the database. The following gives an example, which must be adapted to the environment at hand.

```
$ mysql
mysql> GRANT ALL PRIVILEGES ON *.* TO \
 'openexchange'@'ox-instance1.ucs.local' \
 IDENTIFIED BY 'secret';
mysql> GRANT ALL PRIVILEGES ON *.* TO \
 'openexchange'@'ox-instance2.ucs.local' \
 IDENTIFIED BY 'secret';
mysql> GRANT ...
mysql> FLUSH PRIVILEGES;
mysql> exit
$
```

2.2.2 Active OX instance

Before installing the active OX instance certain environment variables must be set to ensure that the join scripts run later receive the corresponding permissions. The following gives an example, which must be adapted to the environment at hand. The variable OXDB defines the MySQL server to be used by the OX instance. The corresponding password should be saved in the variable OXDBPW. The

standard IMAP server must be specified in the variable OXIMAPSERVER. Hostnames need to be specified as fully qualified domain names (FQDN). It is not possible to use IP addresses.

```
$ export HISTIGNORE="export*"
$ export OXDB=oxdbserver.ucs.local
$ export OXDBPW="secret"
$ export OXIMAPSERVER=oximapserver.ucs.local
```

Then the **univention-ox** package must be installed on the active OX instance.

```
$ univention-upgrade
$ univention-add-app -l oxseforucs
$ univention-install univention-ox
$ univention-upgrade
```

Then the join scripts need to run:

```
$ univention-run-join-scripts
```

The responsible Sieve server has to be configured via UCR variables:

```
$ ucr set ox/cfg/groupware/mailfilter.properties/SIEVE_SERVER=“$OXIMAPSERVER“
```

Finally, the environment variable *OXDBPW* with the password can be unset using the following command:

```
$ unset OXDBPW
```

2.2.3 IMAP server

On the IMAP server the package **univention-mail-cyrus-ox** has to be installed:

```
$ univention-upgrade
$ univention-add-app -l oxseforucs
$ univention-install univention-mail-cyrus-ox
```

Please note: The installation of the IMAP server has to be performed **after** the installation of the active OX instance. Otherwise the installation will fail.

The spam and virus check via *amavis, spamassassin* and *clamav* will be installed and activated automatically.

A check should then be performed to see whether all join scripts have been run successfully:

```
$ univention-upgrade
$ univention-run-join-scripts
```

The fully qualified domain name (FQDN) of the active OX instance has to be configured in the configuration file **/etc/postgrey/whitelist_clients.local**, otherwise mails cannot be sent by the OX instance.

```
$ vim /etc/postgrey/whitelist_clients.local
$ ucr commit /etc/default/postgrey
$ invoke-rc.d postgrey restart
```

Please note:
The Cyrus spool directory /var/spool/cyrus must not be placed on a NFS share. Otherwise data consistency problems might occur with the index files.

2.2.4 Additional passive OX instances

First, the **univention-ox** package must also be installed on the additional passive OX instances.

```
$ univention-upgrade
$ univention-add-app -l oxseforucs
$ univention-install univention-ox
$ univention-upgrade
```

Then the settings can be copied from the active OX instance. This can be done, for example, using the following command:

```
$ rsync -a root@ox-instance1.ucs.local:/opt/open-xchange/.   /opt/open-xchange/
```

Finally, the groupware must be restarted on the passive OX instance:

```
$ invoke-rc.d open-xchange restart
```

2.3 OXtender for business mobility

The Open-Xchange OXtender for Business Mobility is an optional component for OXSE4UCS which enables the connection of mobile devices. Prior to the installation of the OXtender, username and password of a valid LDB account has to be configured. The configuration steps are described in section 4.1.

On the OX system (active OX instance) the package **univention-ox-usm-ox** has to be installed:

```
$ univention-install univention-ox-usm-ox
```

If the target system is neither a DC master or a DC backup system, the **univention-ox-usm-udm** package should also be installed on all DC master and DC backup systems.

```
$ univention-install univention-ox-usm-udm
```

3 Updating

The following steps are necessary to update a UCS 3.0-2 system with OXSE4UCS 6.20 to UCS 3.1 with OXSE4UCS 7.2:

- **Update to UCS 3.1-1:** The update can be started by the UMC module *Online update* or by the command line tool *univention-upgrade*. Further details about the update are described in the UCS manual. After the update to UCS 3.1, the OXSE4UCS installation will be automatically reconfigured to use the Univention App Center for further updates.
- **Installation of the latest UCS errata updates:** The errata updates can be installed with UMC module *Online update → Package Updates* or by the command line tool *univention-upgrade*.

- **Update of the “Open-Xchange Server Edition” via the App Center:** Now the “Open-Xchange Server Edition” can be updated to version 7.2 with the UMC module *App Center*. Where necessary, a key identification (Key ID) has to be added to the the UCS license. This is done via a special wizard when updating or installing the “Open-Xchange Server Edition” in the *App Center*.
- **Installation of Package Updates:** The last step is to ensure, that the latest package updates are installed (with the UMC module *Online Update → Package Updates* or via the command line tool *univention-upgrade*).

All further updates for OXSE4UCS will be available in Univention App Center. Please check the UMC module *App Center* for updates of the application *Open-Xchange Server Edition.*

4 Administration

4.1 UMC module “OX Licence management”

The license management module supports you in the configuration of an Open-Xchange account and the selection of a suitable Open-Xchange license key. It is necessary to specify an Open-Xchange account to be able to select a license key previously saved in the account and install the UCS license. In addition, the account is also required for the installation of version and security updates from the Open-Xchange online repository, as this requires authentication.

For this account, the same combination of username and password is required which was also used for the license database http://ldb.open-xchange.com.

On an unconfigured system, the license management module displays the first configuration step directly, as shown in the figure. In all other cases, an overview of the current configuration is displayed.

The first step involves entering the username and password of the Open-Xchange account. After continuing to the second configuration step via the **Next** button, the entered account information is automatically verified. Should it prove necessary to reset the password for an account, the **Reset password** button can be used to reset the password for an account. The username must be entered in the dialogue which opens; the password must be entered twice. On confirmation, an e-mail is sent to the e-mail address specified for the account containing a confirmation link, which can be opened in the browser of your choice to complete the process.

The second and final step requires to select a suitable Open-Xchange license key. A variety of information is stored in the license database for a license key (e.g., the primary mail domain or the number of licensed users). In addition, a UCS license is saved for every license key in the license database, which is downloaded from the LDB server and installed on the local system when this wizard is finished.

If several keys are saved in the specified account, it is important to select the correct key, as it will otherwise not be possible to complete the configuration if the information saved in the license database does not correspond to the local system.

When performing the configuration for the first time, you may be prompted to confirm the end user license agreement (EULA) for the selected product via the checkbox.

After clicking on the **Finish** button, the UCS license is downloaded and installed. The Open-Xchange license key is then configured on the local system. This procedure can take a few seconds.

Once the configuration is complete, the module redirects to the overview page. This page displays the currently configured Open-Xchange account, the status of the specified user data (valid/invalid), the license key selected for this system and the LDAP base of the installed system.

Following successful configuration, it is possible to directly **Switch to the Online Update module** from here and install the available updates.

If it proves necessary to change the Open-Xchange account or it has been relicensed, you can open the configuration wizard again using the **Change settings** button. For relicensing, it is necessary to perform the configuration procedure anew so that the modified license information is adopted on the local system.

4.2 User and group management

New users and groups can be created using the Univention Management Console (UMC). The UMC can be accessed on the DC master via a web browser at `https://<IP address of DC master>/umc/`. It is possible to log in as the Administrator user using the password specified during the installation.

When creating a user, the **open-xchange groupware account** user template should be selected. This preselects all Open-Xchange specific settings.

4.3 Frontend selection

During installation two versions of the Open-Xchange frontend have been configured: OX6 and AppSuite. In default configuration these frontends are shown on the overview page (`https://<IP address of the OX system>/`) and may be used simultaneously.

By setting UCR variables either of those frontends may be deactivated. For disabling the AppSuite frontend run the following command:

```
$ ucr set ox/frontend/appsuite/enabled=no
```

and for disabling the OX6 frontend the following command has to be called:

```
$ ucr set ox/frontend/ox6/enabled=no
```

4.4 System messages

The *mail/alias/root* UCS variable must be set so that system messages can be delivered. To do this, either a new account can be created or, alternatively, oxadmin@DOMAIN is provided for this purpose:

```
$ ucr set mail/alias/root=oxadmin@ucs.local
$ newaliases
$ invoke-rc.d postfix reload
```

It is possible to log in as the oxadmin user in the Open-Xchange web interface using the password from the */etc/ox-secrets/context10.secret* file.

4.5 Greylisting

Greylisting is a method of defending e-mail users from spam in which e-mails are temporarily rejected. By default, the SMTP server is obliged to retry to send the e-mail later. As this renewed attempt at sending is often not provided by the simple implementations of the SMTP clients used by spammers, a portion of the spam e-mails can be filtered out without creating loads by placing complex filter programs on the server.

4.5.1 Installation

The **univention-ox-meta-singleserver** or **univention-mail-cyrus-ox** package installs and activates the greylisting function automatically. The `postfix/greylisting` UCR variable is used to activate and deactivate the greylisting function.

After installation, the variable is set to **enabled** by default, which activates the greylisting. It can be deactivated by changing this value to **disabled**. Once the variable has been changed, the system services *postgrey* and *postfix* must be restarted. This can be performed via the *System services* UMC module or the command line:

```
$ invoke-rc.d postgrey restart
$ invoke-rc.d postfix restart
```

4.5.2 Configuration

The following UCR variables influence the actions of postgrey. The can be changed via the *Univention Configuration Registry* UMC module or the command line. Once the variables have been changed, the system service *postgrey* must be restarted in order to activate the changes. This can be performed via the *System services* UMC module or the command line.

UCR variables	**Default**	**Description**
mail/postfix/greylisting/delay	300	This value specifies the period for which an e-mail is temporarily rejected. The e-mail is only delivered once the server attempts to resend the e-mail after this period has expired. The value is specified as a numerical value in seconds.
mail/postfix/greylisting/lookup	host	Specifies whether e-mail servers are identified by their complete IP address (value: **host**) or only by the first 24 bits of the address (value: **subnet**).
mail/postfix/greylisting/max-age	35	This value specifies the period after which old entries are removed from the greylisting database. The value is specified as a numerical value in days.
mail/postfix/greylisting/privacy	true	Specifies whether the entries in the database are masked with a one-way function in order to make it difficult to discover sensitive data. The possible values are **true** for masking and **false** for plain text.

mail/postfix/greylisting/recipient/whitelist	*See text*	This value is a list of files separated by blank spaces which contain recipient addresses for which greylisting should not be performed. It is also possible to specify regular expressions in the files. The default value already includes two files: The list supplied by *postgrey* and a file for local changes. The file for local changes is called */etc/postgrey/whitelist_recipients.local* and can be adapted for additional entries.
mail/postfix/greylisting/retry-window	48	The variable defines the time period within which the server must attempt to resend the rejected e-mail in order not to be temporarily rejected again. The value is specified as a numerical value in hours.
mail/postfix/greylisting/text		If required, the variable includes a text deviating from the default, which is sent to the server as a reason when e-mails are temporarily rejected. This message is shown to users of defective mail servers which do not try to resend the e-mail after the temporary failure and is thus not normally seen by users.
mail/postfix/greylisting/client/whitelist/auto	5	This value specifies after how many successfully delivered e-mails the respective server is automatically accepted in the whitelist in order not to delay further e-mails. The value is specified as a numerical value.
mail/postfix/greylisting/client/whitelist	*See text*	This value is a list of files separated by blank spaces which contain server addresses for which greylisting should not be performed. It is also possible to specify regular expressions in the files. The default value already includes two files: The list supplied by *postgrey* and a file for local changes. The file for local changes is called */etc/postgrey/whitelist_clients.local* and can be adapted for additional entries.

More comprehensive documentation on the configuration possibilities can be found in the postgrey man page.