OXSE4UCS 6.22 / 7.2

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

Inhaltsverzeichnis

1 Einführung

Open-Xchange Server Edition für Univention Corporate Server (OXSE4UCS) beinhaltet die Groupware Open-Xchange und die Integrationspakete für die Einbindung in Univention Corporate Server (UCS).

OXSE4UCS richtet sich an professionelle Anwender, die eine bewährte Lösung zur Verwaltung ihrer gesamten IT-Infrastruktur inklusive Groupware suchen, oder an Unternehmen, die bereits UCS einsetzen und ihre Infrastruktur um innovative Groupware-Funktionen erweitern möchten.

Erweiterte Beschreibungen zu UCS sind auf der Webseite der Univention GmbH zu finden: http://www.univention.de/

2 Installation

Da OXSE4UCS eine Erweiterung zu Univention Corporate Server ist, müssen zunächst ein oder mehrere UCS-Server installiert werden.

Es sind unterschiedliche Installationsszenarien denkbar. Grundsätzlich kann OXSE4UCS dabei auf allen Domaincontroller-Serverrollen von UCS installiert werden, also *DC Master*, *DC Backup* oder *DC Slave*. Eine Installation auf den Serverrollen *Memberserver* oder *Basissystem* ist derzeit nicht vorgesehen.

Zunächst können die UCS-Systeme wie gewöhnlich mit UCS 3.1 installiert werden. Sollten mehrere Systeme beteiligt sein, so sollte sichergestellt werden, dass der Join-Vorgang in die UCS-Domäne stattgefunden hat. Dieser erfolgt in der Regel automatisch am Ende der Installation. Weitere Hinweise zur Installation von UCS sind im UCS-Handbuch zu finden: http://docs.univention.de/.

Die Installation setzt voraus, dass auf allen beteiligten Systemen die aktuellen UCS Errata-Updates installiert sind (mit dem UMC-Modul „Online Update“ → „Paket-Aktualisierungen“ oder dem Kommandozeilen-Befehl „univention-upgrade“).

2.1 Einzelinstallation auf einem DC Master, DC Backup oder DC Slave

Die Installation von OXSE4UCS erfolgt seit UCS 3.1 über das Univention App Center. Dazu ist eine Anmeldung an der Univention Management Console des Zielsystems und das Öffnen des UMC-Moduls „App Center“ erforderlich. Im Univention App Center muss dann die Applikation „Open-Xchange Server Edition“ ausgewählt und auf „Installieren“ geklickt werden.

Das Herunterladen der OXSE4UCS-Pakete sowie deren Installation und Konfiguration kann je nach

Internetanbindung mehrere Minuten benötigen. Das UCS-System darf in diesem Zeitraum nicht neugestartet oder heruntergefahren werden.

Um die neuesten OX-Updates für OXSE4UCS zu erhalten, können Benutzername und Passwort eines gültigen LDB-Kontos konfiguriert werden. Dieser Schritt wird in Abschnitt 4.1 näher erläutert.

2.2 Installation einer verteilten Umgebung

Bei der Installation einer verteilten Umgebung muss zunächst durch die Integration in das UCS-Managementsystem auf dem DC Master durchgeführt werden:

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

Zusätzlich muss auf allen DC Backup-Systemen das Paket **python-univention-ox-common** installiert werden:

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

Auf die anderen UCS-Systeme können dann die folgenden Dienste verteilt werden:

- IMAP-Server sowie Spam- und Virenfilter
- MySQL-Server (*mysql-server*)
- OX-Instanz (*univention-ox*)

2.2.1 MySQL-Server

Die Installation des MySQL-Server erfolgt durch die Installation des Pakets **mysql-server**.

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

Die Konfiguration des MySQL-Server sollte so eingestellt werden, dass der MySQL-Dienst über die externen Netzwerk-Interfaces erreichbar ist. Dazu kann beispielsweise in der MySQL-Konfigurationsdatei */etc/mysql/my.cnf* die Einstellung für die Option *bind-address* auf *0.0.0.0* gesetzt werden:

```
bind-address 0.0.0.0
```

Nach der Änderung muss der MySQL-Dienst neu gestartet werden:

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

und die Firewall-Einstellungen für MySQL erweitert werden:

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

Zusätzlich müssen die OX-Instanzen berechtigt werden auf die Datenbank zuzugreifen. Das nachfolgende Beispiel ist an die jeweilige Umgebung anzupassen:

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

2.2.2 Aktive OX-Instanz

Vor der Installation der aktiven OX-Instanz müssen einige Umgebungsvariablen gesetzt werden, damit die später ausgeführten Join-Skripte die entsprechenden Berechtigungen erhalten. Im folgenden ein Beispiel, welches an die jeweilige Umgebung anzupassen ist. Die Variable *OXDB* definiert den MySQL-Server, der von der OX-Instanz verwendet werden soll. Das zugehörige Passwort ist in der Variablen

OXDBPW abzulegen. Der Standard-IMAP-Server ist in der Variable *OXIMAPSERVER* anzugeben. Die Rechnernamen müssen als vollständiger Rechnername (FQDN) angegeben werden. Die Angabe von IP-Adressen ist nicht möglich.

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

Auf der aktiven OX-Instanz ist anschließend das Paket **univention-ox** zu installieren.

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

Danach sind die Join-Skripte auszuführen:

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

Anschließend kann mit folgendem Befehl die Umgebungsvariable OXDBPW mit dem enthaltenen Passwort wieder entfernt werden:

```
$ unset OXDBPW
```

Abschließend muss der zuständige Sieve-Server gesetzt werden:

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

2.2.3 IMAP-Server

Die Installation des IMAP-Servers muss **nach** der Installation der aktiven OX-Instanz durch die Installation des Pakets **univention-mail-cyrus-ox** erfolgen. da die Installation des IMAP-Servers eine installierte, aktive OX-Instanz voraussetzt.

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

Die Spam- und Viren-Prüfung durch *amavis*, *spamassassin* und *clamav* wird automatisch mitinstalliert und konfiguriert. Anschließend sollte geprüft werden, ob alle Join-Skripte erfolgreich ausgeführt sind:

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

Der vollständige Rechnername (FQDN) der aktiven OX-Instanz muss auf dem IMAP-System in der Datei **/etc/postgrey/whitelist_clients.local** eingetragen werden, damit Mails von diesem System sofort angenommen werden:

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

Hinweis:
Das Cyrus-Laufzeitverzeichnis `/var/spool/cyrus` darf nicht auf einer NFS-Freigabe betrieben werden, da ansonsten Konsistenzprobleme in den Index-Dateien auftreten können.

2.2.4 Weitere passive OX-Instanzen

Auf den weiteren passiven OX-Instanzen muss zunächst ebenfalls das Paket **univention-ox** installiert werden.

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

Anschließend können die Einstellungen von der aktiven OX-Instanz kopiert werden, bspw. mit dem folgenden Aufruf:

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

Anschließend sollte die Groupware auf der passiven OX-Instanz neu gestartet werden:

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

2.3 Installation OXtender für Business Mobility

Der Open-Xchange OXtender für Business Mobility ist eine optionale Komponente für OXSE4UCS, durch die eine Anbindung mobiler Endgeräte ermöglicht wird. Für die Installation des OXtenders müssen Benutzername und Passwort eines gültigen LDB-Kontos konfiguriert werden. Dieser Schritt wird in Abschnitt 4.1 näher erläutert.

Installiert wird der OXtender über das Paket **univention-ox-usm-ox**:

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

Falls das Zielsystem kein DC Master oder DC Backup System ist, muss zuvor auf dem DC Master sowie allen DC Backup-Systemen zusätzlich das Paket **univention-ox-usm-udm** installiert werden.

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

3 Aktualisierung von OXSE4UCS

Für die Aktualisierung eines UCS 3.0-2-Systems mit OXSE4UCS 6.20 auf UCS 3.1 OXSE4UCS 7.2 sind folgende Schritte notwendig:

- **Update auf UCS 3.1-1:** Über „Release-Aktualisierungen“ im UMC-Modul „Online Update“ oder den Kommandozeilen-Befehl „univention-upgrade“ kann wie im UCS-Handbuch beschrieben, das Update auf UCS 3.1-1 durchgeführt werden. Während des Updates wird die manuelle OXSE4UCS-Installation automatisch auf eine App-Center-Installation umgestellt.
- **Installation der neuesten Errata-Updates:** Über „Paket-Aktualisierungen“ im UMC-Modul „Online Update“ oder den Kommandozeilen-Befehl „univention-upgrade“ können die aktuellen Errata-Updates eingespielt werden.
- **Aktualisierung der „Open-Xchange Server Edition“ über das App Center:** Über das UMC-Modul „App Center“ kann nun auf die Version 7.2 aktualisiert werden. Ggf. muss der UCS-Lizenzschlüssel noch um eine sogenannte Schlüsselidentifikation (Key-ID) erweitert werden. Dies geschieht über den Dialog „Bereitstellung eines aktualisierten UCS-Lizenzschlüssels“ direkt bei der Aktualisierung bzw. Installation von „Open-Xchange Server Edition“ über das App Center.

- **Einspielen weitere Paket-Aktualisierungen:** Als letzte Schritt müssen über das UMC-Modul „Online Update“ oder den Kommandozeilen-Befehl „univention-upgrade“ nochmals die „Paket-Aktualisierungen“ geprüft und ggf. eingespielt werden.

Weitere Updates sind ab UCS 3.1 über das Univention App Center zu installieren. Sobald für eine Applikation ein Update zur Verfügung steht, wird dies im Univention App Center angezeigt.

4 Administration

4.1 UMC-Modul „OX-Lizenz-Verwaltung“

Das Lizenzmanagement-Modul hilft bei der Konfiguration eines Open-Xchange-Kontos und der Auswahl eines passenden Open-Xchange-Lizenzschlüssels. Die Angabe eines Open-Xchange-Kontos ist notwendig, um einen der zuvor am Konto hinterlegten Lizenzschlüssel auswählen und die UCS-Lizenz einspielen zu können. Darüber hinaus wird das Konto für das Einspielen von Versions- und Sicherheits-Updates aus dem Open-Xchange-Online-Repository benötigt, da dieses eine Authentifizierung erfordert.

Bei dem Konto handelt es sich um die gleiche Kombination aus Benutzernamen und Passwort, welche auch für die Lizenzdatenbank (http://ldb.open-xchange.com) verwendet wurde.

Auf einem unkonfigurierten System zeigt das Lizenzmanagement-Modul direkt den ersten Konfigurationsschritt an. Anderenfalls wird eine Übersicht der aktuellen Konfiguration angezeigt. Im ersten Schritt sind Benutzername und Passwort des Open-Xchange-Kontos anzugeben. Beim Wechsel zum zweiten Konfigurationsschritt über die Schaltfläche **Weiter** werden die angegebenen Kontodaten automatisch auf Korrektheit geprüft. Sollte es notwendig sein, das Passwort eines Kontos zurückzusetzen, kann über die Schaltfläche **Passwort zurücksetzen**, das Zurücksetzen des Passworts für ein Konto angestoßen werden. Im sich öffnenden Dialog ist der Benutzername sowie zweimal das neue Passwort einzugeben. Nach der Bestätigung wird an die Email-Adresse des Kontos eine Mail mit einem Bestätigungslink versendet, welcher in einem Browser Ihrer Wahl geöffnet werden muss, um den Vorgang abzuschließen.

Im zweiten und letzten Schritt muss ein passender Open-Xchange-Lizenzschlüssel ausgewählt werden. Für einen Lizenzschlüssel wurden in der Lizenzdatenbank diverse Informationen (z.B. primäre Maildomäne oder die Anzahl der lizenzierten Benutzer) gespeichert. Darüber hinaus wurde für jeden Lizenzschlüssel in der Lizenzdatenbank eine UCS-Lizenz hinterlegt, welche mit dem Abschluss dieses Assistenten vom LDB-Server heruntergeladen und im lokalen System installiert wird. Falls mehrere Schlüssel an dem angegebenen Konto hinterlegt wurden, ist die Auswahl des korrekten Schlüssels wichtig, da die Konfiguration nicht abgeschlossen werden kann, falls die in der Lizenzdatenbank

hinterlegten Informationen nicht zu dem lokalen System passen.

Wird die Konfiguration das erste Mal durchgeführt, kann es notwendig sein, über die Auswahlbox die Endbenutzer-Lizenzvereinbarung (EULA) für das ausgewählte Produlct zu bestätigen. Nach dem Auswählen der Schaltfläche **Fertigstellen** wird die UCS-Lizenz heruntergeladen und eingespielt. Weiterhin wird der Open-Xchange-Lizenzschlüssel im lokalen System konfiguriert. Dieser Vorgang kann einige Sekunden in Anspruch nehmen. Nach Abschluss der Konfiguration wechselt das Modul direkt auf die Übersichtsseite. Auf ihr wird das aktuell konfigurierte Open-Xchange-Konto, der Status der angegebenen Benutzerdaten (gültig/ungültig), der für dieses Open-Xchange-System ausgewählte Lizenzschlüssel sowie die LDAP-Basis des installierten Systems angezeigt.

Nach einer erfolgreichen Konfiguration kann man von dieser Stelle aus direkt **Zum Online-Update-Modul wechseln** und dort die verfügbaren Updates einspielen.

Ist der Wechsel des Open-Xchange-Kontos notwendig oder es wurde nachlizensiert, kann der Konfigurationsassistent über den Schaltfläche **Einstellungen ändern** erneut geöffnet werden. Beim Nachlizensieren ist es erforderlich, dass der Konfigurationsvorgang erneut durchgeführt wird, damit die geänderten Lizenzinformationen in das lokale System übernommen werden.

4.2 Benutzer- und Gruppenverwaltung

Neue Benutzer und Gruppen können mit der Univention Management Console (UMC) angelegt werden. Die UMC ist auf dem DC Master per Webbrowser unter der Adresse `https://<IP-Adresse des DC Master>/umc/` erreichbar. Die Anmeldung kann als Benutzer *Administrator* mit dem bei der Installation vergebenen Passwort erfolgen.

Beim Anlegen eines Benutzers sollte die Benutzervorlage **open-xchange groupware account** ausgewählt werden. Durch diese Vorlage werden alle Open-Xchange-spezifischen Einstellungen vorausgewählt.

4.3 Auswahl der Oberflächen

Während der Installation wurden zwei Versionen der Open-Xchange-Oberfläche eingerichtet: OX6 und AppSuite. Diese werden in der Standardkonfiguration beide auf der Übersichtsseite (`https://<IP-Adresse des OX-Systems>/`) angezeigt und können parallel verwendet werden.

Es ist jedoch möglich, wahlweise eine der Oberflächen zu deaktiveren. Dies kann über das Setzen einer der beiden folgenden UCR-Variablen erreicht werden. Zum Deaktivieren der AppSuite:

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

oder zum Deaktivieren von OX6:

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

4.4 Systemmeldungen

Damit Systemmeldungen zugestellt werden können, sollte die UCS-Variable *mail/alias/root* gesetzt werden. Es kann hierfür entweder ein neuer Account angelegt werden. Alternativ steht *oxadmin@DOMAIN* dafür bereit:

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

Die Anmeldung als Benutzer *oxadmin* an der Open-Xchange Weboberfläche erfolgt mit dem Passwort aus der Datei */etc/ox-secrets/context10.secret*.

4.5 Greylisting

Greylisting ist eine Technik zur Abwehr von Spam-E-Mails, bei der E-Mails temporär abgelehnt werden. Die SMTP-Server sind laut Standard verpflichtet, in solch einem Fall den Versand der E-Mail später erneut zu versuchen. Da der erneute Zustellversuch durch die einfachen Implementierungen der von Spammern genutzten SMTP-Clients häufig nicht erfolgt, kann so ein Teil der Spam-E-Mails ausgefiltert werden, ohne Last durch komplexe Filterprogramme auf dem Server zu erzeugen.

4.5.1 Installation

Durch die Installation des Pakets **univention-ox-meta-singleserver** oder **univention-mail-cyrus-ox** wird automatisch die Greylisting-Funktionalität installiert und aktiviert. Mittels der UCR-Variable `postfix/greylisting` kann die Greylisting-Funktionalität aktiviert oder deaktiviert werden.

Nach der Installation ist die Variable standardmäßig auf den Wert **enabled** gesetzt, wodurch das Greylisting aktiviert wird. Zum Deaktivieren kann sie auf den Wert **disabled** gesetzt werden. Nach dem Ändern der Variable müssen die Systemdienste *postgrey* und *postfix* neu gestartet werden. Dies kann über das UMC-Modul *System-Dienste* oder die Kommandozeile geschehen:

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

4.5.2 Konfiguration

Die folgenden UCR-Variablen beeinflussen das Verhalten von postgrey. Sie können über das UMC-Modul *Univention Configuration Registry* oder über die Kommandozeile geändert werden. Nach dem Ändern der Variablen muss der Systemdienst *postgrey* neu gestartet werden, um die Änderungen zu aktivieren. Dies kann über das UMC-Modul *System-Dienste* oder die Kommandozeile geschehen.

UCR-Variable	**Standard**	**Beschreibung**
mail/postfix/greylisting/delay	300	Dieser Wert gibt an, für wie lange eine E-Mail temporär abgelehnt wird. Erst wenn der Server nach Ablauf dieser Zeit den E-Mail-Versand erneut probiert wird die E-Mail zugestellt. Die Angabe erfolgt als Zahlenwert in Sekunden.
mail/postfix/greylisting/lookup	host	Stellt ein, ob E-Mail-Server über ihre komplette IP-Adresse (Angabe **host**) oder nur über die ersten 24 Bit der Adresse (Angabe **subnet**) identifiziert werden.
mail/postfix/greylisting/max-age	35	Dieser Wert gibt an, nach welcher Zeit alte Einträge aus der Greylisting-Datenbank entfernt werden. Die Angabe erfolgt als Zahlenwert in Tagen.
mail/postfix/greylisting/privacy	true	Stellt ein, ob die Einträge der Datenbank mit einer Einwegfunktion maskiert werden, um ein Ausspähen von sensitiven Daten zu erschweren. Die möglichen Angaben sind **true** für Maskierung und **false** für Klartext.
mail/postfix/greylisting/recipient/whitelist	*siehe Text*	Dieser Wert ist eine mit Leerzeichen getrennte Liste von Dateien, die Empfänger-Adressen enthalten, für die kein Greylisting durchgeführt werden soll. Die Angabe von regulären Ausdrücken in den Dateien ist ebenfalls möglich. Der Standardwert enthält bereits zwei Dateien: Die von *postgrey* mitgelieferte Liste und eine Datei für lokale Änderungen. Die Datei für lokale Änderungen heißt */etc/postgrey/whitelist_recipients.local* und kann für zusätzliche Einträge angepasst werden.
mail/postfix/greylisting/retry-window	48	Die Variable definiert, innerhalb welcher Zeitspanne der Server den E-Mail-Versand einer abgelehnten E-Mail erneut probieren muss, um nicht abermals temporär abgelehnt zu werden. Die Angabe erfolgt als Zahlenwert in Stunden.

mail/postfix/greylisting/text		Die Variable enthält, sofern gewünscht, einen vom Standard abweichenden Text, der dem Server bei der temporären Ablehnung der E-Mail als Grund gesendet wird. Diese Meldung wird Benutzern von defekten Mail-Servern die nach dem temporären Fehlschlag den E-Mail-Versand nicht erneut probieren angezeigt, und wird deshalb normalerweise nicht von Benutzern gesehen.
mail/postfix/greylisting/client/whitelist/auto	5	Dieser Wert gibt an, nach wie vielen erfolgreich übertragenen E-Mails der entsprechende Server automatisch auf eine Whitelist gesetzt wird, um weitere E-Mails nicht zu verzögern. Die Angabe erfolgt als Zahlwert.
mail/postfix/greylisting/client/whitelist	*siehe Text*	Dieser Wert ist eine mit Leerzeichen getrennte Liste von Dateien, die Server-Adressen enthalten, für die kein Greylisting durchgeführt werden soll. Die Angabe von regulären Ausdrücken in den Dateien ist ebenfalls möglich. Der Standardwert enthält bereits zwei Dateien: Die von *postgrey* mitgelieferte Liste und eine Datei für lokale Änderungen. Die Datei für lokale Änderungen heißt */etc/postgrey/whitelist_clients.local* und kann für zusätzliche Einträge angepasst werden.

Eine ausführlichere Dokumentation der Konfigurationsmöglichkeiten findet sich in der Manpage zu postgrey.