

Was ist nach der Nextcloudinstallation in UCS noch zu tun?

Getestet mit UCS 4.4

Nextcloud installiert man bequem auf UCS im Appcenter. Mit Collabora Online (Libre365) und Let's Encrypt ist dies ein unschlagbares Gespann. Nach der Installation der Anwendungen ist je nach Version noch einiges zu tun. Bevor man sich einloggen kann, muss man auf den Servern wo Nextcloud/Collabora oder was auch immer installiert wurde die Joinscripte (im Webinterface) ausführen die neu durch die Installation der Apps hinzugefügt wurden.

Nextcloud

Hier prüft man als „Administrator“ ob alle Voraussetzungen vorhanden sind. Ist dies nicht der Fall wird man drauf im Webinterface inkl. der Dokumentationslinks hingewiesen.

Für Apache sind noch folgende Einstellungen nötig. 3 UCS Variablen sind zu setzen. Dies geht im Webinterface, aber auch auf der CMD:

```
ucr set apache2/hsts=yes
ucr set apache2/hsts/includeSubDomains=yes
ucr set apache2/hsts/max-age=15552000
```

Und noch eine Config für die DAV Werte:

```
nano /etc/apache2/ucs-sites.conf.d/meine_config.conf
```

```
<IfModule mod_rewrite.c>
  RewriteEngine on
  RewriteRule ^/\.\well-known/host-meta /nextcloud/public.php?service=host-
meta [QSA,L]
  RewriteRule ^/\.\well-known/host-meta\.json
/nextcloud/public.php?service=host-meta-json [QSA,L]
  RewriteRule ^/\.\well-known/webfinger
/nextcloud/public.php?service=webfinger [QSA,L]
  RewriteRule ^/\.\well-known/carddav /nextcloud/remote.php/dav/ [R=301,L]
  RewriteRule ^/\.\well-known/calDav /nextcloud/remote.php/dav/ [R=301,L]
</IfModule>
```

Öffentliche Server sollten keinen Zugang zum UCS-Managementinterface von außen besitzen. Daher schränken wir deren Zugang hier ein.

```
nano /etc/apache2/conf-available/umc-access.conf
```

```
<Location ~ "/univention/(management|login)/">
  Require ip X.X.X.X
```

```
Require ip X.X.X.X
Require all denied
</Location>

<Location ~ "/univention/login/(main.js.*|LoginDialog.*)">
  Require all granted
</Location>
```

Nun noch Apache Modul aktivieren und neu laden.

```
a2enconf umc-access
systemctl reload apache2
```

LDAP Anbindung

Default kann sich jeder Benutzer zur Cloud verbinden. Dies möchte man selbstverständlich unterbinden. Man hat hier zwei Möglichkeiten. Einmal in der UMC das Häkchen rausnehmen, oder/und Filter im LDAPmodul zu setzen. Einen unter Benutzer:

```
(&(objectclass=nextcloudUser)(nextcloudEnabled=1)(memberOf=cn=tux-mitarbeiter,cn=tux-groups,cn=groups,dc=tux,dc=at))
```

Für mehrere Gruppen:

```
(&(objectclass=nextcloudUser)(nextcloudEnabled=1)(|(memberOf=cn=tux-mitarbeiter,cn=tux-groups,cn=groups,dc=tux,dc=at)(memberOf=cn=tux-mitarbeiter-admin,cn=tux-groups,cn=groups,dc=tux,dc=at)))
```

Und einen unter Anmeldeattribute:

```
(&(objectclass=nextcloudUser)(nextcloudEnabled=1)(uid=%uid)(memberOf=cn=tux-mitarbeiter,cn=tux-groups,cn=groups,dc=tux,dc=at))
```

Das Beispiel lässt nur Mitglieder der Gruppe **tux-mitarbeiter** zu. Nicht vergessen auch den Administrator in die Gruppe hinzu zufügen.

Oder auch für mehrere Gruppen:

```
(&(objectclass=nextcloudUser)(nextcloudEnabled=1)(uid=%uid)(|(memberOf=cn=tux-mitarbeiter,cn=tux-groups,cn=groups,dc=tux,dc=at)(memberOf=cn=tux-mitarbeiter-admin,cn=tux-groups,cn=groups,dc=tux,dc=at)))
```

==== Let's Encrypt ====

Für das muss zuerst Port 80 und 443 nach aussen frei geschaltet werden. Danach im Appcenter für Apache die FQDN's im Let's Encrypt Modul eintragen. Jetzt noch Apache neu starten und das Zertifikat auch für das System als gültig aktivieren. Fertig.

```
<code>
systemctl restart apache2
```

update-ca-certificates

Collabora Online

Für das Online Office ist weiters nichts zu tun. Dies integriert sich voll automatisch in die Cloud nach der Installation vom UCS Appcenter.

From:

<https://deepdoc.at/dokuwiki/> - DEEPDOC.AT - enjoy your brain

Permanent link:

https://deepdoc.at/dokuwiki/doku.php?id=prebuilt_systems:ucs:was_ist_nach_der_nextcloudinstallation_in_ucs_noch_zu_tun&rev=1712835839

Last update: **2024/04/11 13:43**

