

invis-Server Upgrade von Version 14.1 auf 14.2

Der wichtige Hinweis vorweg: invis-Server Version 14.2 ist sowohl unter openSUSE Leap 15.1 als auch 15.2 lauffähig. Eingeschränkt wird dies allerdings dadurch, dass es noch keine offiziellen Kopano Pakete für Leap 15.2 gibt. D.h. wer eine subskribierte Kopano-Version nutzt, kann zwar auf 14.2 upgraden, muss aber bei Leap 15.1 bleiben. D.h. Das Distributions-Upgrade muss zunächst ausgelassen werden.

Vorbereitung

Sichern Sie alle Datenbanken des Servers. Sie können dafür die Tools des invis-Servers nutzen:

Kopano

Führen Sie hier beide Sicherungswege durch:

```
invis:~ # kdbdump
...
invis:~ # kbackup
```

Weitere Datenbanken

```
invis:~ # alldump
```

Dokuwiki

```
invis:~ # dwdatasnapshot
```

Da mit der neuen auf MIT-Kerberos basierenden Samba-Version 4.7, die im Laufe des Upgrades installiert wird, werden überarbeitete AppArmor Profile notwendig. Um negative Effekte auf das Upgrade durch mögliche AppArmor-Blockaden vorzubereiten wird AppArmor vor dem Upgrade deaktiviert.

```
invis:~ # systemctl stop apparmor.service
...
invis:~ # systemctl disable apparmor.service
```

Im späteren Verlauf des Upgrades wird AppArmor mit neuen Profilen wieder aktiviert.

Auch der Email-Abruf sollte vor dem Upgrade deaktiviert werden:

```
invis:~ # systemctl stop fetchmail.service
invis:~ # systemctl disable fetchmail.service
```

Auch der Samba Domain-Controller wird abgeschaltet.

```
invis:~ # systemctl stop samba-ad-dc.service
```

Sichern Sie jetzt noch das ActiveDirectory:

ActiveDirectory

```
invis:~ # adbackup
```

Linux-Updates & Software-Upgrades

Spielen sie zunächst anstehende Sicherheits-Updates für openSUSE Leap ein:

```
invis:~ # zypper ref
...
invis:~ # you
...
```

Aktualisieren Sie anschließend entscheidende Software des Servers. Allem voran Kopano und ownCloud. Gehen Sie entsprechend der Anleitungen hier im Wiki vor.

Samba Upgrade

Beginnend mit Samba-Version 4.13 stellen wir für jede von uns erfolgreich getestete Samba-Version ein eigenes Sub-Repository im Stable-Zweig unserer openSUSE-Build-Server Repositories zur Verfügung. Dies verhindert versehentliche Upgrades und ermöglicht das Upgraden von Samba weitgehend unabhängig vom Rest des invis-Servers.

D.h. vor dem Upgrade muss das Samba-Repository ausgetauscht werden. Ermitteln Sie zunächst die Nummer des vorhandenen Samba-Repositories:

```
invis:~ # zypper repos |grep samba
17 | spins_invis_15_stable_samba | Samba 4.10 with Heimdal Kerberos
(openSUSE_Leap_15.1) | Ja | ( r )
Ja | Ja
```

Dieses Repository, im Beispiel Repository Nummer **17**, muss zunächst entfernt werden:

```
invis:~ # zypper rr 17
```

Fügen Sie jetzt das aktuelle Repository hinzu:

```
invis:~ # zypper ar
https://download.opensuse.org/repositories/spins:/invis:/15:/stable:/samba:/
413/openSUSE_Leap_15.1/spins:invis:15:stable:samba:413.repo
invis:~ # zypper ref
```

Überprüfen Sie jetzt erneut die Nummer des Samba-Repositories, gut möglich, dass das neue Repository eine andere Nummer trägt:

```
invis:~ # zypper repos |grep samba
16 | spins_invis_15_stable_samba_413 | Stable Samba Packages with Heimdal
Kerberos V. 4.13 (openSUSE_Leap_15.1)
```

Jetzt können Sie die Samba Pakete upgraden:

```
invis:~ # zypper dup --from 16 --allow-vendor-change
```

Danach kann der Samba-Domain-Controller wieder gestartet werden:

```
invis:~ # systemctl start samba-ad-dc.service
```

Vermutlich wird der Samba-Domain-Controller nicht starten. Das liegt daran, dass die Pakete einen neueren Kernel erwarten als openSUSE 15.1 liefert. D.h.: Jetzt ist zunächst das Distributions-Upgrade durchzuführen. Das läuft nach bekanntem Schema ab:

```
invis:~ # sed -i 's/15\.1/15\.2/g' /etc/zypp/repos.d/*
invis:~ # zypper dup
```

Nach dem obligatorischen Reboot sollte auch Samba wieder laufen. Testen Sie einfach mit:

```
invis:~ # systemctl status samba-ad-dc.service
```

Danach prüfen Sie, ob das Active-Directory wieder zur Verfügung steht. Am einfachsten geht das indem die vorhandenen Benutzer und Gruppen abgefragt werden:

```
invis:~ # wbinfo -u
141-NET\administrator
141-NET\guest
141-NET\krbtgt
141-NET\dns-invis
141-NET\ldap.admin
141-NET\junk
141-NET\postmaster
141-NET\heinzb
....
invis:~ # wbinfo -g
141-NET\cert publishers
141-NET\ras and ias servers
141-NET\allowed rodc password replication group
141-NET\denied rodc password replication group
141-NET\dnsadmins
141-NET\enterprise read-only domain controllers
141-NET\domain admins
141-NET\domain users
141-NET\domain guests
141-NET\domain computers
```

141-NET\domain controllers

...

Liefere beide Kommandos brauchbare Ergebnisse sieht das Upgrade schon mal gut aus. Jetzt muss der sssd-Dienst neu gestartet werden:

```
invis:~ # systemctl restart sssd.service
```

In unseren Tests hat der Neustart zwar problemlos funktioniert, allerdings weigerte sich der sssd beharrlich Benutzer und Gruppen aus dem AD abzufragen. Getestet wird dies mit:

```
invis:~ # getent passwd
```

Liefert dieses Kommando auch nach einer Weile lediglich die Benutzer aus „/etc/passwd“ ist ein Neustart des Servers erforderlich. Danach hat in unseren Tests alles funktioniert. „Reboot tut gut“ gilt nicht nur unter Windows.

From: <https://wiki.invis-server.org/> - **invis-server.org**

Permanent link: https://wiki.invis-server.org/doku.php?id=invis_server_wiki:upgrade:14.1_to_14.2&rev=1641294847

Last update: **2022/01/04 11:14**

