Upgrade von Version 13.5 auf 14.0

Beginnen wir mit einem ernst gemeinten Hinweis:

Hinweis: *Die folgende Anleitung setzt voraus, dass Ihr Server definitiv auf dem Stand von Version 13.5 ist, also bereits PHP7 und ownCloud 10.0 verwendet. Ist das nicht der Fall müssen Sie zunächst auf Version 13.5 aktualisieren. Eine Anleitung dazu finden Sie* ***hier****.*

Vorbereitung

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

ActiveDirectory

```
invis:~ # adbackup
```

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 und deaktiviert.

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

Die neue Samba-Version bringt ohnehin ein eigenes Service-Unit-File mit.

Distributions-Upgrade

Mit dem Sprung auf invis-Server 14.0 muss auf openSUSE Leap 15.0 aktualisiert werden. Die Vorgehensweise dazu ist denkbar einfach. Zunächst müssen Sie Ihre Software-Repositories daran anpassen. Es kann auch nicht schaden zunächst mal alles zu sichern, so wie es ist:

```
invis:~ # cp -R /etc/zypp/repos.d /etc/zypp/repos.d.bak
```

Prüfen wir jetzt, ob ein CD/DVD Repository bei der Installation verwendet wurde. Ist das der Fall, kann es gelöscht werden:

```
invis:~ # grep "cd://" /etc/zypp/repos.d/*
/etc/zypp/repos.d/openSUSE-42.3-0.repo:baseurl=cd:///?devices=/dev/disk/by-
id/ata-TSSTcorp_CDDVDW_SH-224BB_R8WS68BCB00TYX
invis:~ # rm /etc/zypp/repos.d/openSUSE-42.3-0.repo
```

Bis einschließlich invis-Server 13.5 kamen zur Realisation des ActiveDirectories von uns selbst gepflegte Pakete der Software Samba zum Einsatz. Mit Veröffentlichung von openSUSE Leap 15.0 bringt openSUSE jetzt selbst AD-fähige Samba-Pakete mit, die vom invis-Server ab Version 14.0 genutzt werden. Entsprechend kann das von uns beigesteuerte Samba-Repository entfernt werden. Suchen Sie nach diesem Repository:

```
invis:~ # zypper repos |grep Samba
16 | spins_invis_stable_samba46      | Samba AD Packages
(openSUSE_Leap_42.3)                          | Ja        | (r ) Ja
| Ja
```

Im gezeigten Beispiel trägt das Samba-Repository die Nummer 16, damit kann es entfernt werden:

```
invis:~ # zypper rr 16
```

Weiterhin verfügt Ihr invis-Server über zwei weitere Repositories unseres Projektes. Da wir für Version 14.0 des Servers eine neue Repository-Struktur aufgebaut haben, können diese beiden Repositories nach dem gleichen Schema, wie oben entfernt und dann durch die neuen Repositories ersetzt werden:

```
invis:~ # zypper repos |grep spins_invis
14 | spins_invis_common              | Common packages for invis-Server
stable & unstable (openSUSE_42.3) | Ja        | (r ) Ja         | Ja
25 | spins_invis_stable              | Stable Packages for invis-servers
```

```
(openSUSE_Leap_42.3)              | Ja        | (r ) Ja         | Ja
```

Zu entfernen sind hier also die Repositories Nr. 14 und 15:

```
invis:~ # zypper rr 15
Repository 'Production Project for the openSUSE invis-Server Spin
(openSUSE_Leap_42.3)' entfernen
.....................................[fertig]
Repository 'Production Project for the openSUSE invis-Server Spin
(openSUSE_Leap_42.3)' wurde entfernt.
invis:~ # zypper rr 14
Repository 'Common packages for invis-Server stable & unstable
(openSUSE_42.3)' entfernen
.........................................[fertig]
Repository 'Common packages for invis-Server stable & unstable
(openSUSE_42.3)' wurde entfernt.
invis:~ #
```

Fügen wir jetzt die neuen Repositories hinzu:

```
invis:~ # zypper ar
https://download.opensuse.org/repositories/spins:/invis:/15:/common/openSUSE
_Leap_15.0/spins:invis:15:common.repo
...
invis:~ # zypper ar
https://download.opensuse.org/repositories/spins:/invis:/15:/stable/openSUSE
_Leap_15.0/spins:invis:15:stable.repo
```

Wenn Sie Kopano auf Basis einer offiziellen Kopano-Subskription einsetzen müssen Sie eine der Repository-Dateien manuell anpassen. Editieren Sie die Datei:

```
/etc/zypp/repos.d/Kopano-openSUSE_limited.repo
```

, indem Sie die mit „baseurl=“ beginnende Zeile auf folgende URL abändern:

```
...
baseurl=https://download.kopano.io/limited/core:/final/SLE_15/
...
```

Dieses Kopano-Repository verlangt Zugangsdaten, diese wurden während des Server-Setups eingegeben und in

```
/root/.zypp/credentials.cat
```

hinterlegt. Sie können in dieser Datei ebenfalls die URL zum Repository anpassen oder die Zugangsdaten beim nächsten ***zypper ref*** Kommando erneut eingeben. In der genannten Datei muss die erste Zeile geändert werden:

```
[https://download.kopano.io/limited/core:/final/SLE_15/]]
username = FSP Computer und Netzwerke
```

```
password = supergeheim
...
```

Abschließend sind noch die openSUSE Versionsnummern in den verbleibenden Repository-Dateien zu ersetzen:

```
invis:~ # sed -i 's/42\.3/15\.0/g' /etc/zypp/repos.d/*
```

Jetzt kann das Distributions-Upgrade durchgeführt werden:

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

Stimmen Sie dem Vorschlag den ***zypper dup*** macht zu, danach beginnt das Paket-Upgrade.

Achtung: *Starten Sie den Server im Anschluss an das Distributionsupgrade noch* ***nicht*** *neu. Wann der Neustart zu erfolgen hat, wird hier im weiteren Verlauf der Upgrade-Anleitung mitgeteilt.*

Wiederinbetriebnahme des Samba Active-Directories

Beim Upgrade von Samba 4.6.x auf 4.7.x kann es durch den Wechsel der Kerberos-Bibliotheken von Heimdal zu MIT dazu kommen, dass Teile des ActiveDirectories beschädigt werden. Dies betrifft sogenannte verknüpfte Attribute, wie sie bei Gruppenmitgliedschaften genutzt werden. Um dies zu beheben kann das Samba-Tool genutzt werden. Zunächst ein Trockenlauf um das AD auf Fehler zu prüfen:

```
invis:~ # samba-tool dbcheck --cross-ncs 2>&1 | tee dbcheck.txt
```

Hinweis: *Derzeit treten beim Prüflauf auf jeden Fall ein paar Fehler auf. Diese betreffen das LDAP-Schema bzw. die LDAP-Daten des DHCP-Servers. Wir werden versuchen das Auftreten der Fehler von vorneherein zu beseitigen. Dies ist bisher noch nicht geschehen.*

Werden Fehler gefunden, können diese wie folgt behoben werden:

```
invis:~ # samba-tool dbcheck --cross-ncs --fix
```

Das Tool fragt bei jedem Fehler, ob er behoben werden soll. Quittieren Sie dies jeweils mit „**y**“.

Alternativ zum manuellen Bestätigen der Reparaturschritte können Sie dem Befehl auch die Option „–yes“ anhängen, was die Sache etwas einfacher gestaltet. Wiederholen Sie die Reparatur mehrfach, bis keine Fehler mehr gemeldet werden.

Anders als bisher mit dem integrierten Heimdal Kerberos KDC (Kerberos Distribution Center - Der Kerberos Server) nutzt Samba ab Version 4.7. mit MIT Kerberos einen externen KDC. Dessen Konfigurationsdatei muss beim Wechsel manuell angelegt werden. Erstellen Sie im Verzeichnis

```
/var/lib/samba/private
```

die Datei **kdc.conf** nach folgendem Schema:

```
[kdcdefaults]
        kdc_ports = 88
        kdc_tcp_ports = 88
        kadmind_port = 464

[realms]
        INVIS-NET.LOC = {
        }

        invis-net.loc = {
        }

        INVIS-NET = {
        }

[dbmodules]
        db_module_dir = /usr/lib64/krb5/plugins/kdb

        INVIS-NET.LOC = {
                db_library = samba
        }

        invis-net.loc = {
                db_library = samba
        }

        INVIS-NET = {
                db_library = samba
        }

[logging]
        kdc = FILE:/var/log/samba/mit_kdc.log
        admin_server = FILE:/var/log/samba/mit_kadmin.log
```

Passen Sie die REALM (respektive Domänennamen) an Ihre Umgebung an. Achten Sie dabei auf Groß- und Kleinschreibung.

Jetzt können Sie den Samba-Domain-Controller starten und anschließend prüfen, ob Ihr ActiveDirectory wieder in Betrieb ist.

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

Die Abfrage sollte ein „active (running)“ ergeben. Weiterhin sollte in der Liste der zugehörigen Prozesse auch der KDC-Prozess zu finden sein:

```
...
           ├─26507 /usr/lib/mit/sbin/krb5kdc -n
...
```

Fragen Sie jetzt, nur um sicher zu gehen noch Ihre Benutzer und Gruppen ab:

```
invis:~ # wbinfo -u
...
invis:~ # wbinfo -g
...
```

Liefern beide Abfragen Fehlermeldungen anstelle von Listen der Benutzer und Gruppen, sollten Sie zunächst das AD aus der zuvor erstellten Datensicherung wiederherstellen und es erneut versuchen. Das sollte aber nicht der Fall sein. In unseren Tests lief das Upgrade problemlos.

Starten Sie jetzt den SSSD neu und kontrollieren Sie, ob die Benutzer des AD auch unter Linux zur Verfügung stehen:

```
invis:~ # systemctl restart sssd.service
invis:~ # getent passwd
....
heinzb:*:21115:20513:Heinz Becker:/home/heinzb:/bin/bash
klarab:*:21117:20513:Klara Becker:/home/klarab:/bin/bash
```

In der Ausgabe sollten Benutzer auftauchen, der UID größer 21000 ist.

Sorgen Sie jetzt dafür, dass das AD mit dem Systemstart automatisch gestartet wird:

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

Damit ist die Wiederherstellung des AD abgeschlossen.

Reinstallieren des invis-Server Setup-Pakets

Während des Distributions-Upgrades wurde das invis-Server Setup-Paket deinstalliert. Sie müssen jetzt die aktuelle Version wieder installieren:

```
invis:~ # zypper in invisAD-setup-14
```

Im nächsten Schritt müssen die Konfigurationsdateien des invis-Servers und des invis-Portals wieder hergestellt und aktualisiert werden.

invis-pws.conf

An dieser Datei hat sich strukturell nichts geändert, sie kann einfach in ihrer vorherigen Version wieder hergestellt werden:

```
invis:~ # cp /etc/invis/invis-pws.conf.rpmsave /etc/invis/invis-pws.conf
```

invis.conf

Diese Datei wurde für invis-Server Version 14.0 erweitert, daher müssen Sie die soeben neu installierte Version zunächst sichern:

```
invis:~ # old /etc/invis/invis.conf
moving /etc/invis/invis.conf to /etc/invis/invis.conf-20190119
```

Stellen Sie jetzt die alte Datei der vorherigen Installation wieder her:

```
invis:~ # cp /etc/invis/invis.conf.rpmsave /etc/invis/invis.conf
```

Ändern Sie zunächst die Version des invis-Servers in Ihrer Konfigurationsdatei auf 14.0 ab. Die gesuchte Stelle finden Sie am Anfang der Datei:

```
...
#invis-server Version
invisVersion:14.0
...
```

Fügen Sie jetzt die neu hinzu gekommenen Komponenten in die wiederhergestellte Datei ein. Aus (ca. Zeile 40):

```
...
# Sollen die Fileserver-Freigaben regelmäßig auf Viren überprüft werden?
# [j/n]
avCheck:j
...
```

wird:

```
...
# Wo liegen die Windows-Profile
profileDir:/srv/shares/profiles

# Sollen die Fileserver-Freigaben regelmäßig auf Viren überprüft werden?
# [all|profiles|none]
avCheck:none
...
```

Damit wird festgelegt ob und in welcher Form regelmäßige Virenscans auf dem Server durchgeführt werden sollen. Bis Version 13.5 konnte lediglich festgelegt werden ob solche Scans durchgeführt werden sollen oder nicht. Ab Version 14.0 kann festgelegt werden, ob alle Datenverzeichnisse, nur die Windows-Benutzerprofile gescannt werden oder keine Scans durchgeführt werden sollen.

Das ganze ist letztlich eine Frage der Datenmenge und der Rechenleistung des Servers. Auf schwächeren Geräten mit großer Datenmenge sehen wir von solchen Scans ganz ab. Voraussetzung

(und das sollte selbstverständlich sein) ist, dass auf allen Clients Virenscanner installiert sind.

Ab invis-Version 14.0 ist es möglich bei Gruppenverzeichnissen die vom invis-Portal beim erstellen neuer Gruppen erzeugt werden mit Verzeichnisvorlagen zu arbeiten. In der invis-Konfigurationsdatei wird festgelegt, wo die Verzeichnisvorlagen zu finden sind. Fügen Sie den folgenden an beliebiger Stelle in die Konfigurationsdatei ein:

```
...
# Pfad zu den Verzeichnisvorlagen der Gruppenverzeichnisse
groupDirTemplatePath:/srv/shares/media/portal/verzeichnisvorlagen
...
```

config.php (invis-Portal)

Passen Sie in

```
/etc/invis/portal/config.php
```

zunächst die Versionsnummern am Beginn der Datei an. Aus:

```
...
$INVISVERSION = '13.5';
$OPENSUSEVERSION = '42.3';
...
```

wird:

```
...
$INVISVERSION = '14.0';
$OPENSUSEVERSION = '15.0';
...
```

Auch in der Konfiguration des invis-Portals muss der Pfad zu den Gruppenverzeichnisvorlagen eingefügt werden. Fügen Sie in (ca.) Zeile 44 nach „$SFU_GUID_BASE =“ folgende Zeile hinzu:

```
...
$SFU_GUID_BASE = '20000';
$GROUP_DIR_TEMPLATE_PATH = '/srv/shares/media/portal/verzeichnisvorlagen';
...
```

Im Block „SAMBA“ (ab Zeile 72) muss die Gruppe „diradmins“ in der Variablen „$GROUPSTOEXTEND“ eingefügt werden:

```
...
$SMB_GROUPSTOEXTEND = array("Domain Users", "Domain Admins", "Domain
Guests", "Archiv", "Verwaltung", "diradmins");
...
```

Durch das Upgrade hat sich auch die Liste der Dienste, die durch das invis-Portal verwaltet werden geändert. Hinzugekommen ist „firewalld“ und aus „samba“ wurde „samba-ad-dc“. Erweitern bzw. ändern Sie die Variable „$SERVER_SERVICES“ ab Zeile 85 wie folgt ab:

```
...
        array('fetchmail','Emails abholen'),
        array('firewalld','Firewall'),
        array('freshclam', 'Virenscanner Updater'),
        array('mysql', 'MariaDB Datenbank'),
        array('named','DNS Namensauflösung'),
        array('ntop', 'Netzwerkanalyse'),
        array('ntpd', 'Zeitserver'),
        array('postfix','Email-Versand'),
        array('postgresql', 'PostgreSQL Datenbank'),
        array('samba-ad-dc', 'Active Directory'),
...
```

Damit ist auch dieser Schritt abgeschlossen.

Neue AppArmor Profile ausrollen

Ebenfalls durch den Wechsel der Kerberos-Bibliotheken müssen die Samba-Profile des Security-Frameworks AppArmor, welches auf invis-Server standardmäßig aktiv ist angepasst werden. Angepasste Profile bringt das neue invis-Server Setup-Paket bereits mit. Kopieren Sie diese einfach an Ort und Stelle:

```
invis:~ # cp /usr/share/sine/templates/samba_ad/apparmor/* /etc/apparmor.d/
```

Starten Sie jetzt AppArmor und sicherheitshalber gleich noch Samba neu:

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

Aktivieren Sie AppArmor wieder für den Systemstart:

```
invis:~ # systemctl enable apparmor.service
```

Damit ist auch dieser Schritt abgeschlossen.

Inbetriebnahme des Firewall-Daemons (firewalld)

Mit Erscheinen der openSUSE Leap Version 15.0 ist SUSE vom jahrelang selbst entwickelten Firewall-System „**SuSEfirewall2**“ auf den von RedHat entwickelten „**firewalld**“ umgestiegen. Diesen Umstieg müssen Sie mit Hilfe von ***sine2*** vollziehen.

Um das fine2-Firewall-Modul aufrufen zu können bedarf es eines Tricks. Normalerweise ist dieses

Modul kein optionales Modul, kann also nicht einzeln aufgerufen werden. Genau das muss für den nächsten Schritt geändert werden. Öffnen Sie dazu in Ihrem Editor folgende Datei:

```
/usr/share/sine/registered-modules.txt
```

Ändern Sie darin die Zeile:

```
...
13:d:firewall
...
```

auf

```
...
13:o:firewall
...
```

ab.

Jetzt können Sie das Firewall-Modul direkt aufrufen. Es kümmert sich um alles weitere:

```
invis:~ # sine2 firewall
```

Dass der neue Firewall-Daemon den Start mit einem Fehler verweigert und sich auch nicht starten lässt, kann an dieser Stelle getrost ignoriert werden. Ursache dafür ist, dass der Server nach dem Distributionsupgrade noch nicht neu gestartet wurde. Dieser noch ausstehende Neustart des Server sollte jetzt durchgeführt werden:

```
invis:~ # reboot
```

Dabei zeigt sich, dass das Boot-Menü im openSUSE Look erscheint und auch noch die vorherige invis-Server Version angezeigt wird. Dies wird im nächsten Schritt behoben.

Grub Theme

Stellen wir der Form halber auch unser Grub-Theme wieder her. Kann ja nicht schaden auch so etwas mal gemacht zu haben.

Das invis-Theme liegt in Form eines tar.gz-Archivs im Dokumentationsverzeichnis des invisAD-setup Paketes. Von dort können Sie es direkt an Ort und Stelle entpacken:

```
invis:~ # tar -xzf /usr/share/sine/templates/check/grub/invis8.tar.gz -C
/boot/grub2/themes/
```

Während des Upgrades wurde eine Kopie der alten Grub-Konfigurationsdatei erstellt. Stellen Sie diese wieder her. Wenn Sie möchten können Sie ja die neue von openSUSE generierte Datei ebenfalls sichern.

```
invis:~ # cp /etc/default/grub /etc/default/grub.suse
invis:~ # cp /etc/default/grub.old /etc/default/grub
```

Ändern Sie jetzt in Datei

```
/etc/default/grub
```

die Versionsnummer Ihres invis-Servers auf die Nummer ab, auf die aktualisieren möchten:

```
...
GRUB_DISTRIBUTOR="invisAD Server 14.0"
...
```

Jetzt muss die Änderung noch in eine aktive Grub2-Konfiguration umgesetzt werden:

```
invis:~ # grub2-mkconfig -o /boot/grub2/grub.cfg
```

Starten Sie zur Kontrolle jetzt den Server noch einmal neu.

Kopano & Postfix Probleme beseitigen

Aktuelle Kopano-Versionen kennen das Verschlüsselungsprotokoll SSLv2 nicht mehr. Dieses ist aus allen Kopano-Konfigurationsdateien unter

```
/etc/kopano
```

zu entfernen. Aktiv verwendet wird es ohnehin nicht mehr, das Kürzel „SSLv2“ taucht in den Konfigurationsdateien (`server.conf`, `ical.conf` und `gateway.conf`) ohnehin nur auf um SSLv2 zu blockieren, also mit vorangestelltem Ausrufezeichen (Negation). Es ist beim entfernen des Kürzels jeweils auch das Ausrufezeichen zu entfernen. Gleichzeitig können Sie die Sicherheit ein wenig erhöhen, indem Sie das inzwischen als unsicher geltende Protokoll TLSv1 ausschließen. In allen drei Dateien sieht das identisch aus. Ändern Sie den folgenden Block einfach von:

```
...
# SSL protocols to use, space-separated list of protocols
# (SSLv3 TLSv1 TLSv1.1 TLSv1.2); prefix with ! to lock out a protocol.
ssl_protocols = !SSLv2 !SSLv3

# SSL ciphers to use, set to 'ALL' for backward compatibility
ssl_ciphers = ALL:!LOW:!SSLv2:!EXP:!aNULL:!3DES
...
```

nach:

```
...
# SSL protocols to use, space-separated list of protocols
# (SSLv3 TLSv1 TLSv1.1 TLSv1.2); prefix with ! to lock out a protocol.
ssl_protocols = !SSLv3 !TLSv1
```

```
# SSL ciphers to use, set to 'ALL' for backward compatibility
ssl_ciphers = ALL:!LOW:!SSLv3:!EXP:!aNULL:!3DES
...
```

Danach sind alle Kopano Dienste neu zu starten:

```
invis:~ # runkopano stop
invis:~ # runkopano start
```

~~Postfix wurde während des Distributions-Upgrades auf Version 3.3.0 aktualisiert. Dies erfordert eine zusätzliche Konfigurationsoption in der Datei <file>/etc/postfix/main.cf</file> Fügen Sie am Ende der Datei folgende Zeile ein: <code> smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, defer_unauth_destination </code> und Starten Sie Postfix dann neu: <code> invis:~ # systemctl restart postfix.service </code>~~

Weitere Anpassungen

Für die noch fehlenden Schritte und Tests benötigen wir einen laufenden Client-PC und Zugriff auf das invis-Portal. Starten Sie einen PC im Netzwerk und melden Sie sich daran als Domänen-Administrator an.

Neue Gruppenverwaltungsfunktion einrichten

Öffnen Sie einem Browser das invis-Portal und melden Sie sich auch dort als Administrator an. Wechseln Sie in die Rubrik „administration“. Bei unseren Versuchen ist es vorgekommen, dass der verwendete Browser diese Seite noch im Cache hatte und die neuen Funktionen beim Anlegen von Gruppen nicht zur Verfügung standen. Laden Sie die Seite einmal neu und klicken Sie dann auf „Gruppen“. Legen Sie eine neue Gruppe unter dem Namen „diradmins“ an. Diese Gruppe soll vom Typ „Team“ sein und nicht über ein Gruppenarbeitsverzeichnis verfügen.

Führen Sie anschließend auf der Root-Konsole Ihres Servers das Script ***afterup*** aus.

```
invis:~ # afterup
```

Damit wird das Verzeichnis für Vorlagen der Gruppenarbeitsverzeichnisse der neuen Gruppe „diradmins“ übereignet. Mitglieder der Gruppe können dadurch in der Freigabe „Media“ im Unterverzeichnis '\portal\verzeichnisvorlagen' Vorlagen für Gruppenarbeitsverzeichnisse anlegen.

Kimai aktualisieren

Wenn Sie die Zeiterfassungssoftware Kimai auf dem invis-Server nutzen, muss dessen Datenbank an die während des Upgrades installierte neue Kimai-Version angepasst werden. Dieser Vorgang läuft völlig automatisch ab. Öffnen Sie Kimai einfach wie gewohnt und folgen Sie den Anweisungen.