invis-Server Infrastruktur

Das Projekt invis-Server besteht inzwischen aus mehr, als nur dem Server selbst. Hinzugekommen sind bereits vor einiger Zeit ein System zur Datensicherung und ein Setup-Paket zur Integration von openSUSE basierten Clients. Neu im Blumenstrauß ist der invis-Filialserver als ergänzendes Server-System für Außenstellen einer Organisation.

Funktionen des invis Servers

invis Server sind „voll ausgestattete“ Server für kleine Unternehmen. Ihre Leistungen umfassen von Aufgaben zur Netzwerkorganisation via DHCP und DNS über klassische Serverdienste wie Datei und Mail-Server bis hin zu Groupware und ERP Funktionen.

Im Einzelnen:

- Router/Gateway + Firewall (bis invis-Version 13.5 SuSEfirewall2, ab invis-Version 14.0 firewalld).
- Netzwerkorganisation: ISC DHCP/DNS mit ActiveDirectory als Datenbackend
- zentrale Benutzerverwaltung: Samba4 Active Directory mit RFC2307 Erweiterung (Unter Windows als SFU (Services for UNIX) bekannt)
- Druckserver: Samba + CUPS
- Dateiserver: Samba + NFS
- Mailserver/Groupware: dovecot IMAP oder Kopano + Postfix + amavisd-new + fetchmail + CorNAz
- Webserver: Apache2 + PHP usw.
- SQL-Server: MySQL + PostgreSQL. FirebirdSQL optional
- Faxserver: capisuite + Faxgate (Wird dank des ISDN Sterbens früher oder später entfallen)
- VPN: openVPN
- Groupware: Kopano 8.x
- ERP Kivitendo – ab invis-Server Version 8 auch waWision, ab invis-Server Version 14 auch invoiceplane
- User/Admin-Interface: invis Portal

Eine Diskussion darüber, ob die Konzentration dieser Fülle an Diensten auf nur einer einzigen Maschine sinnvoll ist, wird an dieser Stelle nicht geführt. Hier lade ich zur Nutzung unserer Foren unter https://progress.opensuse.org/projects ein (kostenlose Registrierung ist erforderlich).

invis Server erheben den Anspruch ihre Dienste weitestgehend unabhängig vom verwendeten Client-Betriebssystem anzubieten. Daher legen wir Wert darauf Nutzung und Administration im Browser zu ermöglichen.

invis-Filial-Server

invis-Filial-Server befinden sich noch in einem recht frühen Entwicklungsstadium. Trotzdem steht das System kurz vor Veröffentlichung als Version 1.0 mit einem bezogen auf unser Ziel eingeschränkten, aber dennoch recht praktischem Funktionsumfang. Dazu zählen:

- Firewall und Router für die Außenstelle
- Aufbau einer VPN-Verbindung zum zentralen invis-Server
- Lokaler Fileserver für die Außenstelle
- Datensynchronisation via ownCloud zwischen Zentrale und Außenstelle

Der Filialserver ist derzeit lediglich „Memberserver“ in der AD-Domäne der Unternehmenszentrale. Angedacht für die Zukunft ist, ihn zum Read-Only-Domain-Controller (RODC) auszubauen.

Für wen ist das System gedacht?

Zielgruppe sind in erster Linie kleine Unternehmen ohne eigene IT-Abteilung, Unternehmen mit evtl. bis zu 35 PC Arbeitsplätzen, unabhängig von der Branche in der sie tätig sind. In der Praxis leisten invis-Server ihre Dienste in kleinen Handwerks- und Industriebetrieben, Arztpraxen, Anwaltskanzleien, Jugendhilfe-Organisationen, Ingenieur- und Makler-Büros.

Allen gemein ist, dass sie auf externe IT-Dienstleister angewiesen sind, die sich um die komplexeren Aufgaben der IT und somit auch den invis-Server im Unternehmen kümmern. Es ist nicht ausgeschlossen, dass ein Unternehmen einen solchen Server gänzlich in Eigenregie betreibt, Voraussetzung dafür sind allerdings Kenntnisse rund um Netzwerktechnik, Linux, Windows und Active-Directory.

Aufgaben wie die Verwaltung von Benutzerkonten, Gruppen, Mail-Konten usw. können auch ohne Fachkenntnisse und externen IT-Dienstleister nach kurzer Anleitung in Eigenverantwortung erfolgen.

Bei der Entwicklung des Servers haben wir immer diese Zielgruppe im Fokus. **„Aus der Zielgruppe, für die Zielgruppe“** lautet unser Motto. Viele Funktionen des invis-Servers wurden auf Basis unserer praktischen Erfahrungen im Umfeld kleiner Unternehmen implementiert. Ebenfalls im Fokus haben wir die IT-Kosten im Unternehmen, das System soll kosteneffizient nutzbar sein, also IT-Budgets kleiner Unternehmen nicht überfordern.

Nicht im Fokus sind Unternehmen die sehr hohe Anforderungen hinsichtlich IT-Sicherheit und Hochverfügbarkeit haben. (Verstehen Sie das nicht falsch, Sicherheit liegt uns natürlich sehr am Herzen.) Auch die Verwaltung von mehr als 50 Client-PCs ist zwar mit einem invis-Server machbar, allerdings wünschen sich Administratoren solcher und größerer Umgebungen andere Werkzeuge der Server-Verwaltung, als sie der invis-Server mitbringt. Einem „Ein-Server-System“ sind hier Grenzen gesetzt, die sich nicht überschreiten lassen oder bei ihrem Überschreiten die eigentlich anvisierte Zielgruppe aus dem Auge verliert.

Derartige Anforderungen erfordern einen weit höheren finanziellen und technologischen Einsatz, als die von uns mit dem invis-Server-Projekt anvisierte Zielgruppe, zu leisten oder zu verstehen bereit ist. Die Verhältnismäßigkeit der Mittel soll gewahrt bleiben. Um ein wenig Sand von A nach B zu befördern brauche ich eine Schaufel und keinen Bagger.

Aus unserer Sicht ist es auch nicht zielführend invis-Server für Einzelfälle stark zu individualisieren. Der Aufwand dafür ist erheblich und bringt entsprechende Kosten mit sich. Dies, sowohl für die Individualisierung, als auch für die darauf folgende Systempflege. Wir konzentrieren uns bevorzugt auf die Entwicklung eines einheitlichen, gut zu pflegenden Systems.

Gute Ideen, die unser System verbessern nehmen wir, genauso wie Unterstützung zu deren Umsetzung, gerne an.

invis Server im Netz

Vor allem hinsichtlich der Integration eines invis-Servers in bestehenden Netzwerkstrukturen kommt es immer wieder zu Missverständnissen. Sie sind definitiv nicht dazu gedacht als einfacher Fileserver ihren Dienst zu verrichten. Auch eine Beschränkung auf die Nutzung als Groupware-Server, wird der in invis Servern steckenden Arbeit nicht gerecht. Solche Einzellösungen lassen sich ohnehin mit wenig Aufwand individuell installieren.

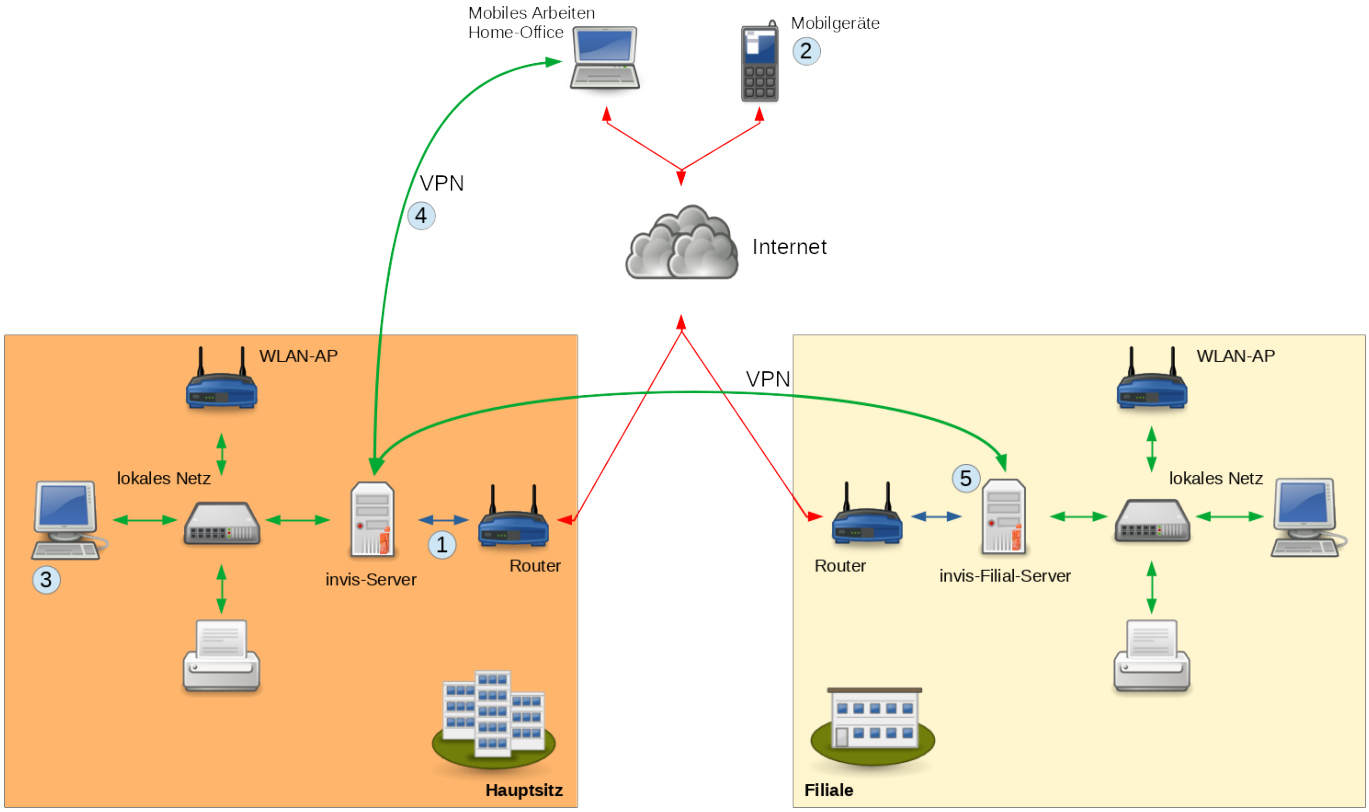
Intention des Systems ist es ein Netzwerk zu organisieren und zu verwalten, sie mit bestehenden Verwaltungsstrukturen wie DHCP-Server, zentralen Benutzerverwaltungen usw. zu kombinieren ist nicht das Ziel des Systems und praktisch kaum umsetzbar.

invis-Server sind tatsächlich als „rundum-sorglos Paket“ für kleine Unternehmen gedacht. Dabei liegt der Fokus auf hoher Funktionalität bei überschaubaren Kosten.

Überblick

invis Server arbeiten prinzipiell als Router/Gateway deren Firewall so ausgelegt ist, dass sie ein dahinter liegendes Netzwerk vor Zugriffen aus dem Internet schützen. D.h. es ist prinzipiell der invis Server, der den Zugang des gesamten Netzwerkes zum Internet regelt.

Die nachfolgende Abbildung zeigt die gesamte invis-Server-Infrastruktur im Überblick:



Auf ein paar Besonderheiten sollte hingewiesen werden:

Router

Punkt 1 in der Abbildung

invis Server müssen mit mindestens zwei Netzwerkschnittstellen/Netzwerkkarten ausgestattet sein, von denen eine „extern“ mit dem Router und die zweite „intern“ mit dem lokalen Netz verbunden ist.

Aus Sicht der Firewall des invis Servers ist „extern“ ihrem Namen entsprechend die externe und „intern“ die interne Zone. Die Einrichtung einer DMZ ist im Normalfall nicht notwendig, aber möglich.

Unabhängig davon, ob Sie ein eigenes oder ein Gerät Ihres Providers einsetzen. Der Internetzugang wird immer von einem Router hergestellt. D.h. die Internet-Zugangsdaten werden nicht im invis-Server sondern im vorgeschalteten Router hinterlegt. Die Nutzung eines einfachen DSL-Modems ist nicht mehr üblich und wird von invis-Servern auch nicht mehr unterstützt. Trotzdem existieren für das vorgeschaltete Gerät zwei Betriebsweisen.

- Im Router-Betrieb arbeitet ein solcher Router als DHCP- und DNS-Server, D.h. er stellt ein eigenes lokales Netzwerk bereit mit dem der invis-Server mit seiner „externen“ Netzwerkschnittstelle verbunden ist. Diese Betriebsart ermöglicht es das Netz zwischen invis-Server und vorgeschaltetem Router als Netzwerk für „Gäste“ anzubieten. D.h. Gastbenutzer können mit Ihren Geräten ins Internet, haben aber keine Möglichkeit auf Ressourcen des lokalen Unternehmensnetzes zuzugreifen.
- In der zweiten Betriebsart (üblich bei Business-Verträgen der Kabelnetzbetreiber wie etwa Unitymedia) stellt der Internet-Provider über den Router ein „kleines“ IP-Netzwerk mit echten im Internet gültigen IP-Adressen bereit. Eine dieser Adressen wird an der externen Schnittstelle des invis-Servers konfiguriert. Damit ist der invis-Server direkt mit dem Internet verbunden und der Betrieb eines Gastnetzes ist nicht möglich. In dieser Betriebsart entfällt die Einrichtung von Portweiterleitungen.

Achtung: *Es darf keine Verbindung zwischen Router und zentralem Netzwerk-Switch geben.*

Erhält die externe Schnittstelle des invis-Servers seine IP-Adresse per DHCP vom Router, muss am Router dafür Sorge getragen werden, dass der invis-Server immer die selbe IP-Adresse erhält → feste Reservierung. Dies ist die Grundvoraussetzung, dass die Dienste die ein invis-Server im Internet anbietet auch zuverlässig erreicht werden können. Die Adresse die der invis-Server vom Router erhält ist das Ziel einiger Portweiterleitungen am Router. Dazu später mehr.

Alternativ können manche Router eine nachgeschaltete IP-Adresse als "exposed Host" führen. In diesem Fall erübrigt sich die Einrichtung von Portweiterleitungen, ist aber weniger sicher.

Um einen invis Server möglichst einfach via Internet erreichbar zu machen ist ein fester im Internet gültiger Name für den Server erforderlich. Es bietet sich die Nutzung eines DynDNS-Dienstes an. Gängige Router unterstützen solche Dienste direkt.

Wer einen eigenen DNS-Server im Internet betreibt, kann sich alternativ eine Subdomain einrichten und diese direkt per DDNS bei der Internet-Einwahl aktualisieren. Das auf dem Server alle 10 Minuten ausgeführte Script ***inetcheck*** kann die Adresse automatisch im zuständigen Nameserver per DDNS

aktualisieren.

Achtung: *Einige ältere Router des Herstellers AVM blockieren im Standard-Setup manche ausgehenden DNS-Abfragen, was etwa Schwierigkeiten mit DDNS machen kann. Nicht bei allen Geräten kann die Konfiguration so geändert werden, dass der Betrieb eines invis-Servers nicht beeinträchtigt wird. Dieses Verhalten haben wir allerdings in den letzten Jahren nicht mehr beobachtet.*

Wird im lokalen Netzwerk ein WLAN benötigt, muss dieses mit WLAN-Accesspoints realisiert werden.

Mobile Geräte

Punkt 2 in der Abbildung

invis-Server bieten, je nach eingesetzter Groupware, die Synchronisation von Groupware-Daten (Email, Termine, Aufgaben und Kontakte) an. Zum Einsatz kommt dabei das ActiveSync Protokoll. ActivieSync wiederum nutzt HTTPs auf Port 443. D.h. Port 443 muss an den invis-Server weitergeleitet werden, damit die Synchronisation möglich ist.

Clients

Punkt 3 in der Abbildung

Lokale Clients werden mittels eines Domänenbeitritts mit der ActiveDirectory Domäne des invis-Servers verbunden. Möglich ist dies mit allen gängigen Betriebssystemen (Windows, Linux, MacOS). Speziell für Linux-Clients auf denen openSUSE Leap genutzt wird bieten wir ein eigenes **invis-Client-Paket** an, mit dem die Integration sehr einfach möglich ist. Das Paket unterstützt auch die Integration von zusätzlichen Linux-Fileservern als Memberserver in die Domäne.

Mobiles Arbeiten / Home-Office

Punkt 4 in der Abbildung

Notebooks oder PCs „zuhause“ können via VPN mit dem invis-Server und dem dahinter liegenden lokalen Unternehmensnetz verbunden werden um dessen Ressourcen zu nutzen. Zum Einsatz kommt hier OpenVPN. Clients dafür gibt es für alle gängigen Betriebssysteme.

Unabhängig von der VPN-Verbindung ist die Nutzung der auf einem invis-Server installierten Webapplikationen, wie etwa die Kopano-Webapp oder Dokuwiki. Diese können via HTTPs von einem Browser teils direkt, teils indirekt nach einer Anmeldung am invis-Portal genutzt werden.

Filial-Server

Punkt 5 in der Abbildung

Auch der Filial-Server ist, genau wie der invis-Server selbst, als Router ausgelegt. Sprich, für dessen Netzerk-Integration gilt das gleiche wie zuvor für den invis-Server beschrieben. Denkbar ist allerdings

auch ihn nicht als Router, sondern als einfaches Netzwerkmitglied hinter dem Hauptrouter zu betreiben. D.h. in dieser Betriebsart ist der Filial-Server selbst kein Router mehr. Inwieweit diese zweite Möglichkeit als Option in das Setup einfließt steht bisher nicht fest.

Fester Bestandteil des Setups ist der Aufbau einer VPN-Verbindung zum Netz des Hauptservers, sowie dessen Beitritt zur ActiveDrectory-Domäne des Hauptservers. Er arbeitet als lokaler Fileserver im Netz der Filiale, die Daten des Fileservers lassen sich via ownCloud mit Freigabe-Verzeichnissen des zentralen invis-Servers synchronisieren. D.h. Mitarbeiter die an beiden Standorten tätig sind können auf beiden Seiten mit Ihren Daten arbeiten.

Derzeit ist der Filialserver einfacher Memberserver der zentralen Domäne. D.h. damit der Zugriff auf dessen Fileserver-Freigaben klappt müssen auf allen PCs der Filiale Benutzerkonten angelegt werden, die denen der Domäne entsprechen. Für spätere Entwicklungsschritte ist angedacht, den Filial-Server als „Read-only-Domain-Controller“ (RODC) zu betreiben. Damit wäre es möglich alle PCs der Filiale in die AD-Domäne aufzunehmen, womit dann das Anlegen lokaler Benutzerkonten entfällt. Wie gesagt, ist noch Zukunftsmusik.

Zugang von "Außen"

Eine Warnung vorweg:

Achtung: *Manche Kabelnetzbetreiber (beispielsweise Unitymedia), die schnelle Internetanbindungen anbieten, fassen bei Privatkunden-Anschlüssen mehrere Kunden hinter einen Router in einem privaten IPv4 Netz zusammen. Ein invis-Server an einem solchen Anschluss wird niemals via Internet erreichbar sein. Wechseln Sie zu einem Business-Tarif und beantragen Sie eine feste IP-Adresse um dies zu beheben.*

invis Server sind dafür ausgelegt auf verschiedenen Wegen via Internet erreichbar zu sein. Vorgesehen sind 5 unterschiedlich Zugänge:

1. **SSH** – Administrativer Zugriff. Der Port des SSH-Servers wird während des Setups auf einen zufälligen hohen Port verschoben.
2. **HTTPs** – Zugriff auf das invis-Portal und installierte Webapplikationen. Auch der HTTPs Port wird während des Setups auf einen zufälligen hohen Port verschoben.
3. **OpenVPN** – VPN Zugang auf den Server und das dahinter liegende Netz.
4. **HTTPs** – ActiveSync/z-push auf Port 443
5. **HTTP** – dient rein technischen Zwecken. Über Port 80 wird die Nutzung offizieller Sicherheitszertifikate des Zertifizierers „Let's Encrypt“ ermöglicht.

Der Zugriff auf installierte Webapplikationen via Internet setzt den den vorherigen Zugriff auf das invis-Portal sowie die Mitgliedschaft in der Gruppe „**mobilusers**“ voraus. Deeplinking auf die Webapplikationen wird verhindert. Davon ausgenommen sind z-Push, die Kopano Webapp und ownCloud.

Im Zusammenhang mit ownCloud sollte folgender Umstand klar sein:

ownCloud muss sowohl aus dem lokalen Netz, wie auch aus dem Internet unter der gleichen URL erreichbar sein.

D.h. auch beim Zugriff aus dem internen Netz wird die extern gültige URL genutzt. Ansonsten wäre es nicht möglich konsistente URLs zu erzeugen über die Dritte auf freigegebene Dateien oder Ordner zugreifen können.

Achtung: *Dafür ist es erforderlich, dass der von Ihnen verwendete Router eingerichtete Portforwarding-Regeln auch dann anwendet, wenn der Zugriff aus dem lokalen Netz (interne Zone) erfolgt.* ***Einige Router der Telekom (Digibox), Vodafone (Easybox), Telefonica (One Access) sind dazu leider nicht in der Lage!*** *Verwenden Sie statt dessen Geräte der Hersteller AVM (FritzBox) oder LANCOM. Mit diesen Geräten treten keine Probleme auf.*

Als Hostname kommt prinzipiell ein im Internet gültiger Hostname (DDNS) in Frage. Die Verwendung einer festen IP-Adresse (muss vom Provider gestellt werden) ist zwar denkbar, sorgt aber in Verbindung mit Verschlüsselung immer für Probleme, da Sicherheitszertifikate nur auf Namen und nicht für IP-Adressen ausgestellt werden.

Sind diese Voraussetzungen nicht gegeben, wird der externe Zugriff auf den Server im Allgemeinen schwierig und die Nutzung von ownCloud beinahe unmöglich.

Ordnung im Netz

Vor der Integration eines invis Servers in ein Netzwerk, sollten Sie dort für Ordnung sorgen. So ist es sinnvoll sich ein einheitliches Namensschema für alle im Netzwerk vorhandenen Geräte und Computer auszudenken und umzusetzen. Praktisch ist, wenn aus dem Namen eines Gerätes bzw. Computers Rückschlüsse auf dessen Funktion oder Standort möglich sind. Weniger sinnvoll ist es PCs nach ihren Benutzern zu benennen, PCs wechseln gelegentlich ihren Platz und Benutzer können ihr Unternehmen verlassen.

Achtung: *Vorsicht ist bei der Umbenennung von PCs dann geboten, wenn darauf Dienste laufen, die fest an den Hostnamen gekoppelt sind, wie etwa Microsoft-SQL-Server. Klären Sie im Vorfeld einer Änderung, welche Auswirkung diese haben kann.*

Alle im Netz vorhandenen Computer und Geräte sollten Ihre IP-Adressen **unbedingt** per DHCP vom invis Server erhalten, sind also für den automatischen Adressbezug zu konfigurieren. Sind die MAC-Adressen der Geräte bekannt, können Sie über das invis-Portal Adress-Reservierungen (Leases) und Einträge im DNS Server anlegen.

Benutzerverwaltung

Eines der wesentlichen Merkmale der invis Server ist die zentrale Benutzerverwaltung. Der gesamte Datenbestand der Benutzerverwaltung (wie auch der von DNS, DHCP uvw.) liegt in einem LDAP-Verzeichnis. Als LDAP-Dienst nutzen invis-Server ein Active Directory auf Basis von Samba 4.

Die Anbindung von Linux-Clients wird mittels des Dienstes **sssd** realisiert. Je nach eingesetzter Linux Distribution kann **sssd** mit Bordwerkzeugen eingerichtet oder muss von Hand konfiguriert werden. Eine Anleitung ist hier im Wiki zu finden.

Windows Clients müssen zur Integration einen Domänenbeitritt durchführen. Auch dies steht hier im

Wiki beschrieben.

Achten Sie darauf, dass Sie **vor** einem Domänenbeitritt mit einem Windows-PC diesem seinen endgültigen Host-Namen gegeben und ihn bereits in die DHCP und DNS Konfiguration integriert haben.

Die sinnvolle Nutzung eines invis Servers setzt die Nutzung der zentralen Benutzerverwaltung voraus!

Email & Groupware

invis-Server können entweder mit einer Groupware (derzeit ausschließlich Kopano) oder einem einfachen IMAP-Server in Verbindung mit dem Webmailer Roundcubemail installiert werden. D.h. es steht entweder nur Email oder Email, Kontaktverwaltung, Terminverwaltung, Aufgabenverwaltung zur Verfügung. In beiden Fällen sind fest installierte Clients auf den angeschlossenen PC für die Nutzung der Funktionen nicht zwingend erforderlich. Der Zugang zu den Funktionen kann über vorinstallierte Web-Applikationen im Browser erfolgen.

Unterstützt werden gängige Mail- und Groupware-Clients wie Mozilla Thunderbird oder Microsoft Outlook. Für die Nutzung der Groupware Kopano steht bevorzugt die Kopano-DeskApp als Desktop-Client zur Verfügung. Um Microsoft Outlook als weitgehend vollwertigen Kopano-Client zu nutzen, ist die Verwendung des Plugins „Kopano Outlook Extension / KOE“ erforderlich. Dies setzt eine kostenpflichtige Kopano-Subskription voraus. Gleiches gilt für die Kopano-DeskApp. Wir empfehlen grundsätzlich den Abschluss eines Subskriptionsvertrages. Dieser ist nicht teuer und bringt Support durch Kopano, sowie Maintenance mit. Mit der genannten Maintenance können sie jederzeit die dieweils aktuelle Kopano-Version nutzen. Mit den Kopano-Community-Paketen aus der openSUSE Distribution ist dies nicht möglich und es steht auch kein Support zur Verfügung.

Grundsätzlich wird bei invis Servern davon ausgegangen, dass keine Internetverbindung via Standleitung und fester IP-Adresse vorhanden ist. Für den Mailserver bedeutet dies, dass für den email Versand jeweils eine Internet-Einwahl angestossen werden muss und der email-Empfang indirekt geschieht. emails können nicht direkt beim invis Server eingeliefert werden, sondern verbleiben zunächst in den jeweiligen Postfächern eines Mail-Providers im Internet. Sie werden dort zyklisch per ***fetchmail*** abgeholt und dann in lokale Postfächer eingeliefert.

Jeder auf einem invis Server angelegte Benutzer verfügt über eine lokales email-Konto (Postfach), dem eine Adresse nach dem Schema „*username@lokale-domain.loc*“ zugeordnet ist. Diese Adresse hat ausschließlich im lokalen Netzwerk Bedeutung und kann im Internet nicht verwendet werden. Diesem Mailkonto können mittels CorNAz (Eintrag „Mailkonten“ im invis-Portal) vom User selbst beliebig viele externe Mailkonten zugeordnet werden.

Alle Mail-Clients im Netzwerk (Thunderbird, Outlook usw.) kennen nur die lokale Mail-Adresse. Wird von einem Client aus eine Email versendet, prüft der invis-Server, ob sich der Empfänger im lokalen Netzwerk oder im Internet befindet. Trifft letzteres zu, tauscht der invis Server automatisch die in der Email verankerten lokalen Absender-Adresse gegen eine im Internet Gültige (sender address rewriting) aus.

Hat der Benutzer mehrere externe Mailkonten/Email-Adressen angegeben, kann er mit unserem Mail-Konten-Verwaltungs-Tool „CorNAz“ festlegen, welches seine bevorzugte Absender-Adresse ist.

Emails an lokale Empfänger werden direkt zugestellt, hier findet kein „address rewriting“ statt.

Wird eine email an eine externe Adresse eines lokalen Benutzer gesendet, findet ein „adress rewriting“ in umgekehrter Richtung statt (recipient address rewriting). Dies führt ebenfalls zu einer direkten Zustellung solcher emails ohne Umweg über einen externen Mail Provider.

Hinweis: *Die sinnvolle Nutzung der Groupware-Funktionen des Servers ist nur unter Verwendung der lokalen Mailserver-Funktion möglich!*

Versionen und Versionsnummerierung

invis-Server gab es in den Versionen „invis Classic“ und „invis ActiveDirectory“. Davon wird die Classic Version nicht mehr gepflegt und lässt sich auch allenfalls nicht mehr installieren.

Die letzte Version des invis-Classic trug die Versionsnummer 9.3.

Ab Version 10.0 wurde der invis-Server dank Samba 4 auf ActiveDirectory anstelle von OpenLDAP umgestellt. Dies entspricht einer Aktualisierung der Windows Domänenstruktur von NTLM (Windows Server NT 4.0) auf ActiveDirectory mit Kerberos Authentifizierung (ab Windows Server 2000). Notwendig war dies, da immer mehr Business-Applikationen das Vorhandensein eines ActiveDirectories voraussetzen und neuere Windows-Versionen nur noch mit zunehmend großem Aufwand zum Beitritt in eine NTLM-Domäne zu bewegen sind.

Die Versionen 10.0 bis 10.3 basierten auf openSUSE 13.1. Seit dem Auslaufen der Evergreen Maintenance für openSUSE 13.1 im November 2016 werden nur noch Installationen basierend auf der jeweils aktuellen openSUSE Leap unterstützt. Noch existierende alte Installationen sollten aktualisiert oder neu installiert werden. Erläuterungen zu den verschiedenen Upgrade-Pfaden sind hier im **Wiki** zu finden.

Die Versionsnummer eines invis-Servers besteht aus 3 Teilen bzw. Stellen:

„Major_Number-Minor_Number-Build-Number“

Eine Erhöhung der ersten Nummer kennzeichnet eine Veränderung des Paketes, die es inkompatibel mit dem Vorgänger macht. Das bedeutet, ein Upgrade auf ein solches Paket, erfordert immer händische Anpassungen am System. Wir werden uns Mühe geben, die notwendigen Anpassungen im Wiki zu dokumentieren. Es kann auch möglich sein, dass eine neue Major-Release eine Neuinstallation erfordert. Dies war beispielsweise beim Sprung von 9.x auf 10.x notwendig, da ein „Upgrade“ von Samba3 + openLDAP auf Samba4 ActiveDirectory die Struktur des invis-Servers grundlegend verändert hat.

Eine Erhöhung der zweiten Stelle bedeutet neue Features, die die Kompatibilität nicht brechen. Dabei kann es sein, dass diese Features auf einer bestehenden Installation händisch nachinstalliert bzw. konfiguriert werden können. Den Betrieb eines bestehenden invis-Servers sollte dies nicht stören.

Änderungen in der dritten Stelle deuten lediglich auf Bugfixes hin. Auch hier kann es sein, dass nach einem Update händische Eingriffe notwendig sind. Die Funktion eines in Betrieb befindlichen Servers wird bei einem Update nicht gestört.

Grundsätzlich werden wir (soweit es unsere Zeit erlaubt) versuchen alle erforderlichen Update bzw.

Upgrade Schritte hier im Wiki zu dokumentieren. Sollte etwas fehlen, bedenken Sie bitte, dass wir alle neben der Pflege und Entwicklung des invis-Servers auch noch die Jobs zu erledigen haben, die uns ernähren.

Seit Einführung von invis-Server 11.0 (August 2016) wurde die Major-Versionsnummer in den Namen des invis-Setup Paketes aufgenommen. Also wird aus **„invisAD-setup“** dann **„invisAD-Setup-11“**. Dies verhindert versehentliche Updates des Paketes bei dem ein bestehendes System beschädigt werden könnte. Um zur neuen Version zu kommen ist also immer ein Upgrade, entsprechend der Beschreibungen hier im Wiki, erforderlich.

invis Server und Benno Mailarchiv

Die revisionssichere, langfristige, elektronische und systematische Aufbewahrung (Archivierung) von Emails ist in Deutschland aufgrund von Vorschriften aus Handelsgesetzbuch (HGB), Abgabenordnung (AO) und der Grundsätze ordnungsgemäßer Buchführung (GoDB) verpflichtend. Davon ausgenommen sind Kleinstunternehmer und Freiberufler. Dabei orientiert sich „langfristig“ an die gesetzlichen Aufbewahrungsfristen (von 6 oder 10 Jahren) wie sie auch für steuerrelevante Papierdokumente gelten und „revisionssicher“ meint unveränderlich. D.h. archivierte Mails dürfen im Archiv nicht verändert oder gelöscht werden können.

Nicht zu archivieren ist potentiell eine Verletzung der Buchführungspflicht, die mit Geld- oder gar Gefängnisstrafen geahndet werden kann.

Archiviert werden müssen Emails die in ihrer Bedeutung Handels- oder Geschäftsbriefen entsprechen oder die steuerliche Erfassung eines Unternehmens betreffen oder kurz alle Mails, die in irgendeiner Form geschäftsrelevant sind.

Benno Mailarchiv ist ein gesetzeskonforme Open-Spource-Lösung zur Email-Archivierung, mit dem großen Vorteil, dass es für den Anwender zugänglich ist und eine hervorragende Suchfunktion bietet um auch alte Mails schnell zu finden.

Sowohl für die Aktivierung eines invis-Benutzers als Mailarchiv-Benutzer, wie auch für die Nennung von Mailadressen auf die ein Benutzer im Archiv leseberechtigt ist, enthält der invis-Server Kommandozeilen Scripts.

Der invis-Server selbst übernimmt allerdings nicht die Rolle des des Mail-Archivs, Benno Mailarchiv muss auf einem gesonderten System installiert werden.

Benno-Mailarchiv kann als reines, nicht zugängliches Archiv kostenfrei betrieben werden, für die Nutzung zum schnellen Auffinden von Mails muss es lizenziert werden. Näheres dazu erfahren Sie durch **FSP Computer & Netzwerke**

invis-Server arbeiten als vollständige interne Mailserver über die der gesamte Mailverkehr eines Unternehmens laufen kann. In der Mailserver-Komponente des invis-Servers kann eine „Weiche“ (always bcc) aktiviert werden, die alle ein und ausgehenden Mails parallel ans Archiv sendet. Alle Mails deshalb, weil es kaum entscheidbar ist welche Mails ein Steuerprüfer im Zweifelsfall als „geschäftsrelevant“ ansieht.

Eine wesentliche Funktion von Benno Mailarchiv ist die Möglichkeit darin sehr komfortabel zu suchen. D.h. Anwender müssen die Möglichkeit haben sich an einer Benno-Weboberfläche anmelden zu können und darin Mails zu finden, die Sie auch sehen dürfen und zwar nur diese.

Die Anbindung der Benno-Webapp an das ActiveDirectory des invis-Servers ist von Haus aus vorbereitet. Beim Anmelden wird gegen das AD authentifiziert, weiterhin ließt Benno aus dem AD auf welche Mails ein Benutzer zugriffsberechtigt ist. Das orientiert sich an Mail-Adressen die einem Benutzer zugeordnet werden. Dabei können einem Benutzer im AD auch Berechtigungen für Mailadressen zugeordnet werden, die über seine persönlichen Adressen hinaus gehen.