invis Server Administration

Ein komplexer Unternehmensserver wie der „invis-Server“ erfordert im laufenden Betrieb immer wieder Aufmerksamkeit. Es müssen gelegentlich Konfigurationen angepasst oder Online-Updates installiert werden. Diese Seite beschreibt wo und wie Sie an Ihrem Server arbeiten.

Hinweis: *Nicht Aufgabe dieser Seite ist die Vermittlung von IT-Basiswissen. System- und Netzwerkadministratoren sollten darüber verfügen, oder in der Lage sein es sich anzueignen. Dies ist kein Vorwurf, an die Leser dieser Zeilen, sondern der Hinweis darauf, dass Server-Produkte wie ein invis-Server hoch komplexe Systeme sind, deren Administration Fachwissen verlangen. Wenn ich beispielsweise eine neue Wasserleitung im Haus benötige, wende ich mich auch an einen Sanitärbetrieb und versuche nicht selbst meine Wohnung unter Wasser zu setzen.*

Zur Administration des Servers gehören Störungsbeistand und natürlich wiederkehrende Aufgaben, wie das Einspielen von Updates, das Verwalten von Benutzern und Gruppen oder das Verwalten von Mailkonten. Einige dieser Aufgaben lassen sich bequem über das invis-Portal andere hingegen lediglich auf der Kommandozeile des Servers erledigen. Sowohl das invis-Portal, inklusive weiterer installierter Administrationswerkzeuge als auch die Kommandozeile des sind sowohl aus dem lokalen Netzwerk als auch via Internet erreichbar. Letzteres setzt allerdings einen korrekt konfigurierten Router und funktionierendes DDNS voraus.

Hinweise dazu, wie Sie Ihren Router konfigurieren finden Sie **hier**.

Hinweis: *Die nachfolgenden Anleitungen werden immer wieder aktualisiert und erweitert, d.h. Sie beziehen sich primär auf die jeweils aktuellen Versionen des invis-Servers.*

invis Portal

Das invis-Portal ist eine Schnittstelle für einfache administrative Tätigkeiten, weiterhin ermöglicht es den Zugriff auf komplexere Administrations-Software. Die nachfolgend genannten Funktionen stehen im invis-Portal nur nach erfolgreicher Anmeldung mit einem administrativen Konto sichtbar. Auf invis-AD Systemen der Benutzer ***administrator***. (Auf invis-Classic Systemen war dies nach der Installation der Benutzer ***domadmin***)

Funktionen

- **Benutzerverwaltung:** Anlegen und Löschen von Benutzern. Das Portal unterscheidet zwischen fünf verschiedenen Benutzertypen (Mailkonto, Benutzerkonto, Benutzerkonto mit Groupware-Zugang, Administratorenkonto und Gastkonto). Die Benutzertypen auf Active Directory Versionen des invis-Servers unterscheiden sich von denen des Classic Servers.

- **Gruppenverwaltung:** Hinzufügen und Entfernen von Benutzergruppen und Zuordnen von Benutzern zu Gruppen. Werden hierüber Gruppen angelegt, wird automatisch ein Gruppenverzeichnis auf dem Fileserver angelegt.
- **Netzwerkorganisation:** Hinzufügen und Entfernen von Netzwerkgeräten zur DHCP- und DNS-Konfiguration. Das Portal unterscheidet zwischen vier verschiedenen Geräteklassen (Server, Drucker, Client-PC und IP-Gerät). In Abhängigkeit der Klassen werden IP-Adressen aus dafür reservierten Bereichen vergeben.
- **Dienste:** Ab invisAD 10.1 können über das Portal auch Dienste gestartet und gestoppt werden.
- **Funktionen:** Ab invisAD-Version 14.1 können hier ausgewählte administrative Scripte des Servers ausgeführt werden. Beispielsweise können hier mit einem Klick die Zugriffsberechtigungen der Gruppenverzeichnisse zurück gesetzt werden.

Zusätzliche administrative Werkzeuge

- **Verzeichnisdienst:** Das LDAP-Verzeichnis Ihres invis-Server ist der zentrale Speicherort einer Vielzahl von Konfigurationsdaten des Servers. Sie finden hier Daten zu DHCP, DNS, Benutzerverwaltung usw. Achtung der Umgang mit einem LDAP-Verzeichnis setzt entsprechende Grundkenntnisse voraus. Um phpLDAPAdmin administrativ nutzen zu können, melden Sie sich mit dem Konto des Domänen-Administrators daran an. Sie müssen Ihre lokale Domain an den Benutzernamen anhängen (administrator@invis-net.loc) damit die Anmeldung funktioniert. Die Anmeldung funktioniert natürlich auch mit allen anderen Benutzerkonten des ActiveDirectories, allerdings verfügen normale Benutzer über zu wenig Rechte um Veränderungen am LDAP-Datenbestandes vornehmen zu können.
- **MySQL Administration:** Administration der Datenbank-Engine MySQL. MySQL wird beispielsweise vom Groupware-System Ihres invis-Server genutzt. Sie können hiermit neue Datenbanken anlegen, sollten aber keine vorhandenen Löschen. Sie können phpMyAdmin auch zur Erstellung von Datensicherungen der Datenbanken nutzen. Das Passwort des MYSQL-Benutzers „root“ können Sie mit dem Kommando ***sine2 showpws*** auf der Kommandozeile erfragen.
- **PostgreSQL Administration:** Administration der Datenbank-Engine PostgreSQL. PostgreSQL wird beispielsweise vom Warenwirtschaftssystem Ihres invis-Server genutzt. Sie können hiermit neue Datenbanken anlegen, sollten aber keine vorhandenen Löschen. Sie können phpPGAdmin auch zur Erstellung von Datensicherungen der Datenbanken nutzen.
- **Server Administration:** Hinter diesem Link steht das Programm Shell-in-a-box, mit dem Sie

aus dem Browser heraus auf die Kommandozeile Ihres Servers zugreifen können. Dabei ist zu beachten, dass Shell-in-a-box keine direkten Zugriffe als Benutzer „root“ zulässt (***su -*** verwenden) und, dass es ein denkbar schlechte Idee ist in einer solchen Shell-Sitzung den Apache-Webserver zu stoppen. Angenehmer ist jedoch dass Arbeiten mit einer direkten SSH-Verbindung, als Notlösung taugt Shell-in-a-box aber allemal.

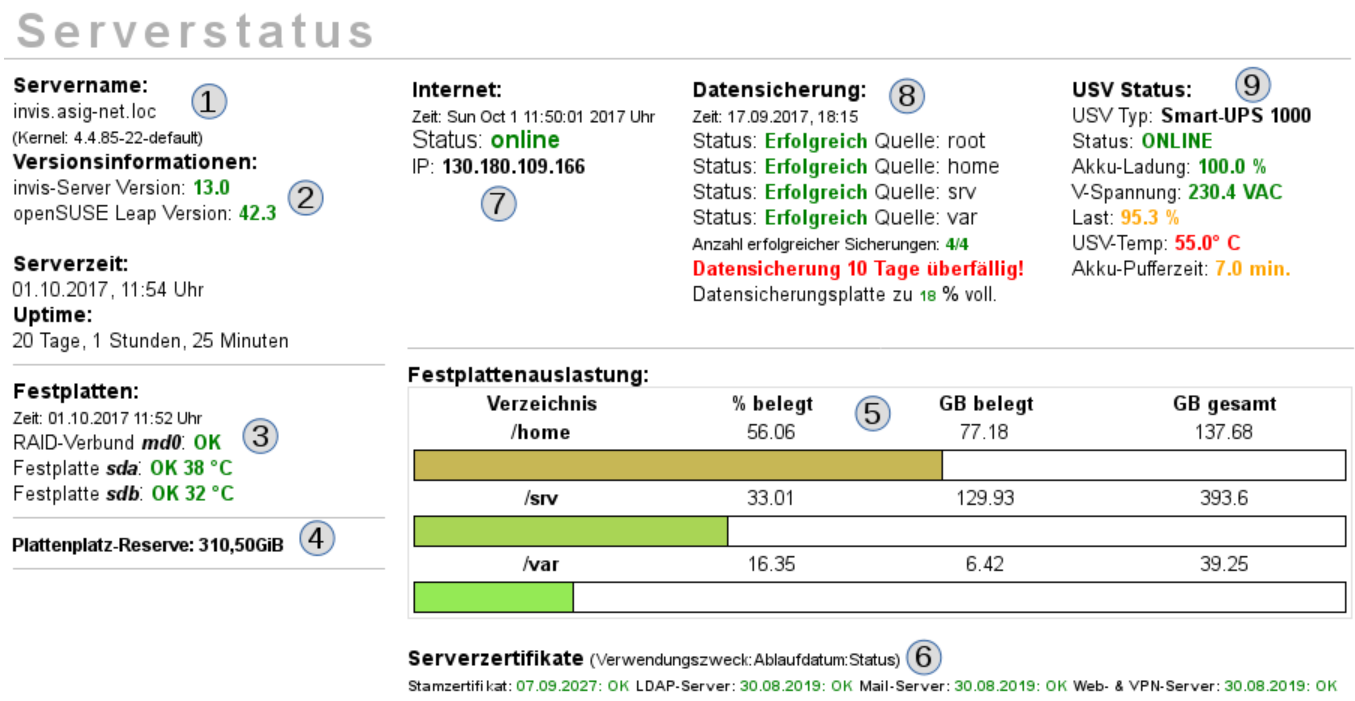
- **Druckerverwaltung:** Ihr invis-Server ist in der Lage im Netzwerk vorhandene Drucker zentral zu verwalten und freizugeben. Hierüber erhalten Sie Zugriff auf die Administrationsseiten des zugehörigen Dienstes CUPS.
- **Netzwerkanalyse:** Das Programm ntop dient der Analyse des Datenverkehrs in Ihrem Netzwerk, nützlich etwa bei der Suche nach Fehlern. ntop ist im Normalbetrieb Ihres invis-Servers deaktiviert, da es diesen ansonsten unnötig belastet.
- **Firewall-Test:** Dieser Link führt Sie auf die Internetseite von hackerswatch.org. Sie haben von dort umfangreiche Möglichkeiten die Firewall Ihres invis-Servers von außen zu testen.
- **Virtualbox:** Dahinter verbirgt sich die Software phpVirtualBox, ein Webfrontend zur Verwaltung virtueller Maschinen, die der klassischen VirtualBox-Management GUI zum verwechseln ähnlich sieht und über nahezu den gleichen Funktionsumfang verfügt. (Nur sichtbar, wenn VirtualBox installiert ist.)

Eine weitere Funktion des Portals ist die Verwaltung externer Mailkonten von denen der invis-Server die Emails der Benutzer abruft. Diese Funktion verlangt allerdings keine administrativen Rechte, sondern kann von jedem Benutzer selbst genutzt werden. Sie wird weiter unten auf dieser Seite gesondert beschrieben.

Status-Informationen

Nicht dem Administrator vorbehalten, sondern öffentlich für alle Benutzer einsehbar, ist die Status-Seite des invis-Servers. Sie enthält wichtige Informationen über den aktuellen Zustand des Server.

Hinweis: *Um die Status-Seite via Internet sehen zu können ist eine Anmeldung am Portal erforderlich.*



Erläuterungen:

1. **Systemdaten:** Servername, Uhrzeit des Servers und die Uptime. Diese Informationen können keine kritischen Werte annehmen. Sollte aber die Uhrzeit des Servers um mehr als 5 Minuten von der Uhrzeit Ihres Computers abweichen führt dies zu Problemen. Bitten Informieren Sie darüber Ihren Administrator.
2. **Versionsinformationen:** Hier wird die Aktualität Ihrer invis-Server Installation und des darunter liegenden Linux Betriebssystems angezeigt. Solange die angezeigten Versionsnummern in grün oder orange angezeigt werden, müssen Sie sich keine Sorgen machen. Handlungsbedarf besteht wenn sich die Zahlen rot färben. Rechnen Sie alle 1 bis2 Jahre mit einem umfangreicheren Upgrade um Ihren Server wieder auf Stand zu bringen.
3. **Festplatten und RAID-Verbünde:** Festplatten sind die Speicherorte für Ihre Daten, sie sind nicht für die Ewigkeit gebaut, sondern müssen als Verschleißteile angesehen werden. Damit es möglichst nicht zu überraschenden Ausfällen kommt, überwachen Festplatten sich selbst. Diese Überwachungsdaten werden von Ihrem Server abgerufen und hier angezeigt. Fehler werden hier in „rot“ angezeigt und sind sofort Ihrem Administrator zu melden. RAID-Verbünde sind der doppelte Boden, sie schützen vor Datenverlust bei einem Festplatten-Ausfall. Dies geschieht, in dem alle gespeicherten Daten mehrfach vorgehalten werden. Fällt eine Festplatte aus, gilt ein RAID-Verbund als beschädigt. Auch dies muss Ihr Administrator unmittelbar erfahren. Ab invis-Server 14.1 wird auch die bisherige Gesamtlaufzeit der Festplatten angezeigt und mit der durch den Hersteller garantierten Laufzeit ins Verhältnis gesetzt. Hilfreich, um rechtzeitige Erneuerung der Festplatten zu planen.
4. **Plattenplatz-Reserve:** In aller Regel wird bei der Installation eines invis-Servers nicht der gesamte zur Verfügung Festplattenplatz verwendet. Statt dessen kann eine Reserve dazu genutzt werden, sie je nach Bedarf auf genutzte Laufwerke zu verteilen.
5. **Festplattenauslastung:** Der zur Verfügung stehende Festplattenplatz wird während der Serverinstallation bedarfsorientiert auf sogenannte „Volumes“ verteilt. In diesen Volumes speichern Sie Ihre Nutzdaten. Wichtig sind dabei die Volumes „home“ (persönliche Benutzerverzeichnisse), „var“ (Datenbanken und Emails) sowie „srv“ (Arbeitsverzeichnisse). Für diese Volumes zeigt hier jeweils ein farbiger Balken den jeweiligen Füllstand. Die Balken verfärben sich je nach Belegung von grün nach rot. Sind alle Volumes im „roten Bereich“ und es steht keine Plattenplatz-Reserve mehr zur Verfügung muss der Server mit größeren oder weiteren Festplatten ausgerüstet werden. Versteht sich, dass Sie auch das Ihrem Administrator mitteilen müssen.
6. **Serverzertifikate:** Serverzertifikate werden zur Verschlüsselung von Datenübertragungen genutzt. Beispielsweise werden Emails verschlüsselt übertragen, auch die Anmeldung am System läuft verschlüsselt ab. Serverzertifikate werden üblicherweise auf Zeit ausgestellt und werden nach Ablauf dieser Lebenszeit ungültig. Ungültige Serverzertifikate beeinträchtigen die Funktion eines invis-Servers massiv. Es kommt zu vielen Fehlern, deren Ursachen nicht unmittelbar erkennbar sind. Verfärbt sich die Schriftfarbe hier nach „orange“ bedeutet dies, dass ein Zertifikat in Kürze abläuft, rot hingegen, dass es bereits abgelaufen ist. Informieren Sie Ihren Administrator bitte rechtzeitig darüber. Die voreingestellt Lebensdauer von Serverzertifikaten eines invis-Servers beträgt 2 Jahre, die des Stammzertifikats 10 Jahre.
7. **Internet:** Ihr invis-Server übernimmt in Ihrem Netzwerk die Funktion eines Routers und verbindet Ihr lokales Netzwerk mit dem Internet. Er überprüft die Verbindung zum Internet zyklisch alle 10 Minuten. Das Ergebnis der Überprüfung kann 4 verschiedene Zustände, die natürlich farblich unterschiedlich dargestellt werden, annehmen: „online“ → Verbindung steht und funktioniert, „Verbindung schlecht“ → Die Verbindung steht zwar, es kommt aber zu Datenverlusten, in diesem Fall sollten Sie eine Störung beim Provider melden, „DNS Problem“ → Verbindung steht aber die Namensauflösung funktioniert nicht. Melden Sie dies Ihrem

Administrator und „offline“ → keine Verbindung. In diesem Fall sollten Sie sich zuerst bei Ihrem Administrator und anschließend ggf. bei Ihrem Provider melden.
8. **Datensicherung:** Diese Anzeige ist optional und nur dann sinnvoll, wenn das invis-Server eigene Datensicherungssystem genutzt wird. Es informiert über Erfolg bzw. Misserfolg der letzten Datensicherung und zeigt (wenn möglich) den Füllstand des Sicherungsmediums an. Wenn alles korrekt läuft, werden 4 einzelne Sicherungsaufgaben mit einem grünen „Erfolgreich“ gemeldet. Werden Informationen in rot angezeigt oder sind weniger bzw. keine Sicherungsergebnisse sichtbar, melden Sie dies umgehend Ihrem Administrator.
9. **USV Status:** Auch diese Anzeige ist optional. Sie funktioniert nur, wenn Ihr Server über eine „Unterbrechungsfreie Stromversorgung“ (USV) des Herstellers APC gegen Stromausfälle abgesichert ist. Geräte anderer Hersteller können leider nicht unterstützt werden. Auch hier verändert sich die farbliche Darstellung der Anzeige. In orange oder gar rot dargestellte Werte sind umgehend Ihrem Administrator zu melden.

Anpassung des Portals

Hinweis: *Um Anpassungen am invis-Portal vornehmen zu können ist Kommandozeilen-Zugriff auf den invis-Server erforderlich. Dazu finden Sie etwas weiter unten auf dieser Seite entsprechende Anleitungen.*

Für die Konfiguration des invis-Portals sind zwei Dinge von Bedeutung:

1. Die Datei **/etc/invis/portal/config.php** (siehe unten)
2. Der Knoten **ou=informationen,ou=iportal** im LDAP-Verzeichnis des Classic-Servers
3. Der Knoten **cn=informationen,cn=iportal,cn=invis-server** im LDAP-Verzeichnis des AD-Servers

Die genannte Konfigurationsdatei dient der grundsätzlichen Anpassung des Portals an die lokale Umgebung. Hier muss im laufenden Betrieb in der Regel nichts geändert werden, außer evtl.:

- Die Passworteinstellungen der Benutzer und
- ob die invis-eigene Datensicherung mit invisrdbu oder USVs des Herstellers APC überwacht werden sollen.

Das Portal warnt dann, wenn die Datensicherung überfällig ist. Die Konfigurationsdatei ist gut dokumentiert und weitestgehend selbsterklärend.

Interessant sind die Möglichkeiten das Portal via LDAP zu steuern. Für nahezu jeden Link (bzw. jede Schaltfläche) im Portal existiert ein eigener Knoten im LDAP. Über diese Knoten können die Links aktiviert bzw. deaktiviert werden:

- iPortEntryActive – [TRUE/FALSE]

Es lassen sich alle Links anpassen oder neue hinzufügen. Die Attribute im Einzelnen:

- iPortEntryButton – Beschriftung des Links bzw. der Schaltfläche.
- iPortEntryDescription – zugehöriger Beschreibungstext.
- iPortEntryName – Name des Eintrag, kennzeichnendes Attribut des LDAP-Knotens (RDN).
- iPortEntryPosition – Position des Links bzw. der Scaltfläche. [Lokal/Internet/Dokumentation/Administration]
- iPortEntryPriv – Entscheidet, welche Benutzerrechte für die Sichtbarkeit des Eintrages

Voraussetzung sind. [admin/user/guest]
    - admin – Setzt die Mitgliedschaft eines Benutzers in der Gruppe „Domain Users“ voraus.
    - user – Setzt eine erfolgreiche Anmeldung am Portal voraus.
    - guest – Wird jedem gezeigt, vorausgesetzt er greift aus dem lokalen Netz heraus auf das Portal zu
- iPortEntrySSL – Legt fest, ob der Link TLS-Verschlüsselung erfordert.
- iPortEntryURL – Legt die Zieladresse des Links fest. Dabei müssen externe Ziele vollständig aber ohne vorangestelltes „http:“ *oder „https:*“ angegeben werden. Interne Ziele werden wie folgt angegeben: [servername]/phpldapadmin.

Beispiel für eine LDIF Datei

```
# Groupware Tine 2.0
dn: cn=Tine-2.0,cn=invis-Portal,cn=Informationen,cn=invis-server,dc=invis-
net,dc=loc
objectClass: top
objectClass: iPortEntry
cn: Tine-2.0
iPortEntryName: Tine-2.0
iPortEntrySSL: FALSE
iPortEntryURL: [servername]/tine20
iPortEntryDescription: Die Groupware "Tine 2.0" bietet unter anderem Zugriff
auf Terminkalender, Kontakt- & Projektverwaltung, E-Mails, CRM und
Zeiterfassung.
iPortEntryActive: FALSE
iPortEntryPosition: Lokal
iPortEntryButton: Groupware
iPortEntryPriv: user
```

Um Einträge im Portal über die Kommandozeile zu aktivieren oder deaktivieren bringen invis-Server das Script ***swpestat*** mit:

```
linux:~ # swpestat entryname [TRUE|FALSE]
```

Um die Namen der Einträge zu ermitteln bietet das Script eine Statusabfrage an:

```
linux:~ # swpestat status
....
```

Achten Sie bei der Verwendung des Scripts auf die Korrekte Schreibweise der Eintragsnamen.

Benutzer- und Gruppenveraltung

Die Verwaltung von Benutzern und Gruppen eines invis-Servers wird grundsätzlich über das invis-Portal vorgenommen. Eine weitere Möglichkeit stellen die Microsoft'schen Remote Server Administration Tools dar. Letztere sind allerdings nicht für den invis-Server optimiert. Die Verwaltung über das invis-Portal ist also vorzuziehen.

Für das Verwalten von Benutzern und Gruppen via invis-Portal, müssen Sie sich als Administrator am Portal anmelden.

Sie können mit dem Portal Benutzer und Gruppen anlegen, löschen und bearbeiten. Zum Bearbeiten von Benutzern gehört auch das Ändern von Kennwörtern.

invis-Server verfügen über eine automatische Archivierungsfunktion. Wenn Sie Benutzer oder Gruppen löschen werden deren Verzeichnisse automatisch archiviert. Die Archivierung findet immer nachts statt. Die archivierten Verzeichnisse sind anschließend in der Freigabe „archiv“ zu finden den Unterverzeichnissen „\user“ und „\gruppen“. Da speziell die Benutzer-Archive auch persönliche Daten enthalten können ist der Zugriff auf die Freigabe „archiv“ recht restriktiv gehalten.

Hinweis: *Achten Sie also auch aus rechtlichen Gründen darauf, wem Sie Zugriff auf die Freigabe „archiv“ geben. Der Zugriff auf solche Daten sollte im Idealfall über eine entsprechende Betriebsvereinbarung rechtlich abgesichert sein.*

Hinweis: *Wenn Sie viele Gruppen auf einmal anlegen möchten, sollten Sie sich das Toolbox-Script* ***groupadd2ad*** *anschauen.*

Gruppen

Die Möglichkeit Benutzer eines Computersystems zu Benutzergruppen zusammenzufassen ist beinahe so alt wie Computer überhaupt. Vor allem in Hinblick auf die Vergabe von Zugriffsrechten, beispielsweise auf Dateien oder Verzeichnisse hat das Vorteile, da es dies deutlich vereinfacht. Orientieren Sie sich bei der Rechtevergabe ausschließlich an Gruppen, müssen Sie einerseits bei der Rechtevergabe nicht alle Benutzer einzeln berücksichtigen. Es müssen also wesentlich weniger Regel vergeben werden.

Scheidet ein Mitarbeiter aus dem Unternehmen aus, müssen Sie nicht alles irgendwie und irgendwo gesetzten Zugriffsrechte überarbeiten, sondern Sie nehmen den Mitarbeiter einfach aus den entsprechenden Gruppen heraus. In aller Regel klappt letzteres auch automatisch, wenn ein Benutzerkonto gelöscht wird. Auf irgendwie und irgendwo gesetzte Zugriffsregeln trifft das nicht zu.

Auf invis-Servern entscheidet vielfach auch die Mitgliedschaft in bestimmten Gruppen darüber ob ein Benutzer eine auf dem Server installierte Software oder bestimmte Funktionen verwenden kann oder nicht. Für diese Zwecke existieren auf dem invis-Server folgende Gruppen:

1. **owncloud:** Mitglieder dürfen ownCloud verwenden.
2. **zeiterfassung:** Mitglieder dürfen die Zeiterfassungssoftware „Kimai“ verwenden.
3. **mobilusers:** Mitglieder dürfen sich via Internet am invis-Portal anmelden.
4. **verwaltung:** Mitglieder dürfen auf die Netzwerkfreigabe „verwaltung“ zugreifen.
5. **archiv:** Mitglieder dürfen auf auf die Netzwerkfreigabe „archiv“ zugreifen.
6. **diradmins:** Mitglieder dürfen Gruppen-Verzeichnisvorlagen erstellen und bearbeiten.
7. **wiki-nutzer:** Mitglieder haben Leserecht im Wiki.
8. **wiki-redakteure:** Mitglieder dürfen im Wiki schreiben.
9. **wiki-chefredakteure:** Dürfen im Wiki schreiben und auch Beiträge löschen.

Die Gruppenverwaltung finden Sie im invis-Portal unter „administration“; erforderlich ist natürlich, dass sie am invis-Portal als Administrator angemeldet sind. Sie können dort neue Gruppen anlegen, sowie bestehende Gruppen bearbeiten. D.h. Benutzer hinzufügen oder entfernen.

Wenn Sie eine neue Gruppe anlegen möchten, können Sie dabei von vorne herein ein paar Entscheidungen fällen. Sie können zunächst festlegen von welchem Typ die anzulegende Gruppe ist. Unterschieden wird zwischen drei Typen:

- **Team:** Ist eine einfache Benutzergruppe, um diese zur Vergabe von Zugriffsrechten zu verwenden.
- **Team+Gruppenmail:** Auch diese Gruppe kann zur Vergabe von Zugriffsrechten verwendet werden. Darüber hinaus ist sie auch für die Groupware Kopano zur Vergabe von Rechten innerhalb der Groupware verfügbar. Weiterhin können innerhalb der Groupware Mails an diese Gruppe gesendet werden. D.h. alle Mitglieder empfangen diese Mails.
- **Mail-Verteiler:** Dient nicht der Rechtevergabe, sondern kann mit Email-Adressen gefüllt werden um später als Email-Verteilerliste zu dienen.

Benutzer

Das Anlegen von Benutzern über die Administrationsseite des invis-Portal ist weitestgehend selbsterklärend. Ungewöhnlich ist lediglich, dass es nicht möglich ist mit der Tabualtor-Taste zwischen den Eingabefeldern zu springen. (Gerade für Tastatur-Junkies wie mich ist das immer wieder ein Ärgernis, lässt sich aber leider nicht ohne weiteres beheben.)

Wichtig für das Verständnis beim Anlegen von Benutzern ist allerdings die Unterschiede zwischen den verschiedenen Benutzertypen zu kennen:

1. **Gast** – Gäste sind einfache „Windows-Benutzer“, die lediglich der Gruppe „Domain Guests“ angehören. Das berechtigt Sie zum Zugriff auf die Transfer-Freigabe. Sie können sich nicht an Linux-Computern oder auch an der Kommandozeile des Servers anmelden. Auch steht für Sie kein Mailkonto zur Verfügung.
2. **Mailkonto** – Benutzer dieses Typs verfügen über Windows und Unix Attribute, können sich aber dennoch nicht an der Linux-Kommandozeile des Servers anmelden. Sie sind Mitglied der Gruppe „maildummies“ und können das Mailsystem nutzen. Wird Kopano (ehemals Zarafa) als Groupware genutzt, werden Benutzer dieses Typs mit den Attributen „zarafaAccount“ und „zarafaSharedStoreOnly“ versehen. Dadurch können Sie Emails empfangen, sich aber nicht an Kopano anmelden. Gedacht ist dies für Email-Funktionskonten wie z.B. „info@…“ usw. Diese Konten können in Kopano freigegen werden. Um in deren Namen Mails zu versenden müssen zugelassene Absender als „SendAs Benutzer“ im Benutzerkonto des Mailusers eingetragen werden. Dies ist entweder über phpLDAPAdmin oder die Microsoft Remote Server Administration Tools möglich.
3. **Windows+UNIX** – Reiner Windows-Benutzer und Linux-Benutzer, ohne Zugang zum Mailsystem. Sie sind Mitglied der Gruppe „Domain Users“ haben also das Recht verschiedene Verzeichnisfreigaben des Servers zu nutzen.
4. **Windows+UNIX+Groupware** – Wie oben nur ergänzt um die Möglichkeit die Groupware und das Mailsystem zu nutzen.
5. **WinAdmin+UNIX** – Wie „Windows+UNIX“, allerdings Mitglied der Gruppe „Domain Admins“. Sie verfügen also auf allen Windows-PCs der Domäne über administrative Rechte.
6. **WinAdmin+UNIX+Groupware** – Wie „Windows+UNIX+Groupware“ und Mitglied der Gruppe „Domain Admins“. Zusätzlich werden Benutzer dieses Typs wenn Kopano als Groupware eingesetzt wird auch als kopano Admins geführt. Sie haben also das Recht jedes Postfach zu öffnen.

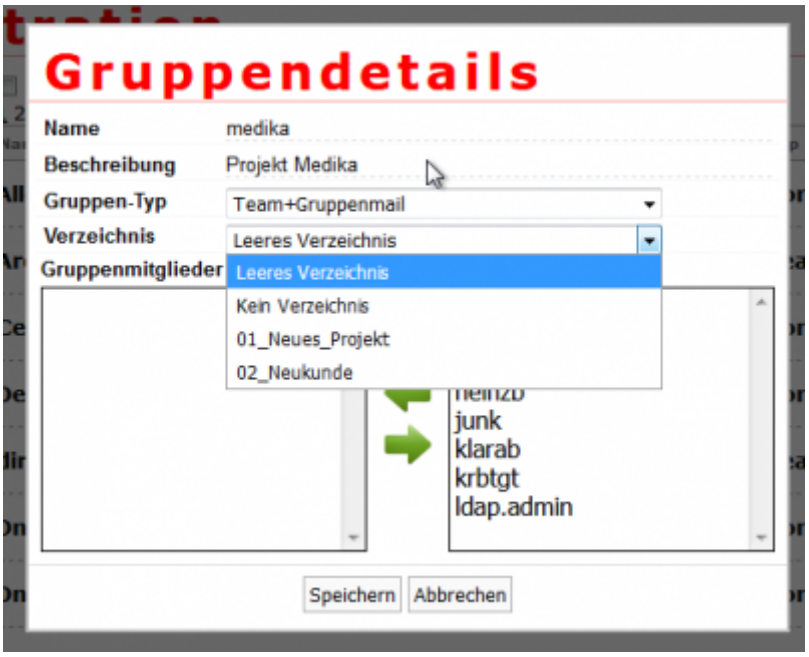
Hinweis: *Damit sich Benutzer via Internet am invis-Portal anmelden können um von dort aus auf installierte Applikationen wie etwa das Wiki oder die Zeiterfassung zugreifen zu können, müssen Sie Mitglied in der Gruppe* ***mobilusers*** *sein. Davon ausgenommen sind Zugriffe auf ActiveSync (Smartphone-Synchronisation), die Kopano-Webapp und ownCloud. Zugriffe auf diese Applikationen ist ohne „Umweg“ über das invis-Portal möglich, d.h. die Mitgliedschaft in* ***mobilusers*** *ist dafür nicht erforderlich.*

Beim Anlegen eines Benutzers sind nur wenige Pflichtangaben zu machen. Dazu gehören der Anmeldename (Login), Vor- und Zuname, Passwort und der Benutzertyp zu wählen. Dabei gelten für Login-Name und Passwort ein paar Spielregeln:

1. **Login:** Der Login-Name darf weder Leer- noch Sonderzeichen enthalten, ausgenommen Binde- und Unterstrich. Sie sollten beim Loginnamen ausschließlich Kleinbuchstaben verwenden.
2. **Passwort:** Es gelten hier die Passwortregeln des ActiveDirectory. Diese können mit Hilfe des Tools ***pwsettings*** auf der Kommandozeile des invis-Servers definiert werden. Werden Veränderungen hinsichtlich der Passwortregeln vorgenommen müssen diese in der Konfigurationsdatei des invis-Portals (siehe oben) übernommen werden.

Verzeichnisvorlagen

Neben dem Gruppentyp, können Sie ab invis-Server Version 14.0 entscheiden, ob der Gruppe eine Arbeitsverzeichnis zur Verfügung gestellt wird oder nicht. Wenn Sie ein Gruppenverzeichnis wünschen, können Sie überdies entscheiden ob ein leeres Verzeichnis oder ein Verzeichnis auf Basis einer Verzeichnisvorlage, also inklusive Unterverzeichnissen erstellt wird.



Die Verzeichnisvorlagen werden in der Netzwerkfreigabe „media“ im Unterverzeichnis

```
\portal\verzeichnisvorlagen
```

gepflegt. Mitglieder der Gruppe „diradmins“ dürfen dort Verzeichnisstrukturen anlegen. Das invis-Portal schaut dort selbsttätig nach und zeigt diese dann zur Auswahl an.

Es empfiehlt sich die Verzeichnisvorlagen nach dem Schema „01_Vorlagenname“ durchnummeriert zu benennen. Das invis-Portal zeigt die Vorlagen genau in der nummerierten Reihenfolge an.

Exit Strategie

Scheidet ein Mitarbeiter aus einem Unternehmen aus, ist das aus Sicht der IT-Verwaltung ein komplexer Vorgang. Je nach dem welche Berechtigungen und Möglichkeiten der Benutzer hatte, muss sichergestellt werden, dass er nach dem Ausscheiden nicht mehr auf den Datenbestand des Unternehmens zugreifen bzw. diesen verändern kann. Verfügt er über ein eigenes Mailkonto, muss auch hier festgelegt werden wie damit verfahren wird.

Entscheidend für die Vorgehensweise sind überdies datenschutzrechtliche Bestimmungen, bzw. die Beachtung von Regelungen aus Betriebsvereinbarungen.

Je nach Berechtigungen des ausscheidenden Mitarbeiters sind unterschiedliche Schritte nach seinem Ausscheiden erforderlich. Gehen wir davon aus, dass der Mitarbeiter neben lokalen Verzeichnisbereichtigungen über ein Mailkonto inklusive Groupwarezugang, das Recht von Ferne auf das invis-Portal zuzugreifen sowie einen VPN-Zugang hat.

Folgende Schritte sind in diesem Fall durchzuführen:

1. **Passwort ändern** - Die Änderung des Passworts eines ausgeschiedenen Mitarbeiters sollte unmittelbar nach dessen Ausscheiden erfolgen. Damit kann er sich weder lokal am System, noch am invis-Portal anmelden. Diesen Schritt kann der Administrator im invis-Portal vornehmen. (Administration → Benutzer → Löschen)
2. **VPN-Schlüssel zurück ziehen** - Dieser Schritt verhindert, dass der Mitarbeiter weiterhin VPN-Verbindungen zum Unternehmensnetz aufbauen kann. Dieser Schritt erfordert eine Anmeldung an der Kommandozeile des Servers. Zurückgezogen wird der VPN-Schlüssel unter Verwendung des Scripts **`inviscerts`**.

Um ein VPN-Client-Zertifikat zurückzuziehen geben Sie folgendes Kommando ein:

```
invis:~ # inviscerts vpn
```

Das Script fragt Sie nach dem Namen für den das Zertifikat ausgestellt wurde. Sie müssen diesen Namen hier exakt eingeben, da ansonsten davon ausgegangen wird, dass ein neues Zertifikat ausgestellt werden soll.

Achten Sie bitte genau auf die Abfragen des Scripts. Sie benötigen in dessen Verlauf das Passwort der CA.

Alle folgenden Schritte können dann in Ruhe geplant werden. Es geht jetzt vor allem darum, wie mit dem Datenbestand des ehemaligen Mitarbeiters verfahren wird. Dabei ist zu prüfen, ob dem Mitarbeiter das Recht auf private Email-Nutzung und die Ablage privater Daten auf dem Unternehmensserver gewährt wurde. Ist dies der Fall, darf auch nach dem Ausscheiden **niemand** auf das Postfach bzw. das persönliche Verzeichnis dieses Mitarbeiters zugreifen. Die Daten müssen entweder gelöscht oder sicher und vor Zugriffen geschützt archiviert werden. Löschen, ist dabei ein relativ schwieriges Unterfangen, da sich seine Daten auch in diversen Datensicherungen befinden dürften.

Gehen wir für die nächsten Schritte davon aus, dass eine rechtsgültige Betriebsvereinbarung existiert, die den Umgang mit Mitarbeiterdaten regelt.

„Private“ Datenbestände eines Benutzers befinden sich in dessen:

- **persönlichem Verzeichnis auf dem Server**
- **ownCloud Konto**
- **Email-Konto**
- **ggf. auf seinem Arbeitsplatz-Computer**

Besondere Überlegungen müssen bezüglich des Email-Kontos des Mitarbeiters angestellt werden. Dabei ist zunächst zu überlegen, ob der Mailbestand des Mitarbeiters für die weitere Arbeit des Unternehmens von Bedeutung sind. Ist das der Fall, muss der Mailbestand des Ausscheidenden einem anderen Mitarbeiter (seinem Nachfolger) oder seiner Abteilung zugänglich gemacht werden.

Wird Kopano als Groupware eingesetzt, bietet sich die Möglichkeit das Konto des Benutzers in einen Kopano „Shared Store“ umzuwandeln und daruf Zugriffsberechtigungen zu setzen, die andere zum Zugriff berechtigt. Wird diese Vorgehensweise gewählt, darf das Benutzerkonto des Mitarbeiters nicht gelöscht werden. Dies sollte maximal eine Maßnahme für begrentzte Zeit sein. Der Mailbestand sollte gesichtet und ggf. in ein anderes Konto oder in entsprechende öffentliche Ordner überführt werden.

Hinweis: *Wird im Unternehmen (wie vom Gesetzgeber gefordert) ein revisionssicheres Email-Archiv betrieben, kann der Zugriff auf den Mailbestand des Mitarbeiters darüber erfolgen.*

Ist der Umgang mit dem Mailbestand geregelt bzw. abgeschlossen, kann das Benutzerkonto des ausgeschiedenen Mitarbeiters gelöscht werden. Dieser Schritt wird im invis-Portal durchgeführt. Dabei wird das persönliche Verzeichnis des Benutzers automatisch archiviert. Zu finden sind die Daten anschließend in der Freigabe „Archiv“ des invis-Servers. Zugriffsberechtigt sind lediglich Mitglieder der Gruppe „Archiv“. Dies sollten maximal Mitglieder der Unternehmensleitung sein.

Nach dem Löschen des Benutzerkontos bleibt der Mailbestand des Benutzers, im Falle von Kopano, als sogenannter „orphand Store“ erhalten. Dieser aund andere „Datenleichen“ können unter Verwendung des Scripts **`inhume`** endgültig beseitigt werden.

```
invis:~ # inhume username
```

Inspizieren Sie abschließend noch den PC des Mitarbeiters auf relvenanten Daten und sichern Sie diese soweit vorhanden auf den Server.

Damit sind alle erforderlichen Schritte getan.

Mailkonten verwalten

Die Verwaltung von E-Mailkonten setzt sich aus mehreren Schritten zusammen und spielt sich entsprechend auf mehreren Ebenen ab.

1. **Provider:** Zunächst muss ein Mailkonto bei einem Provider existieren oder eben angelegt werden. Für den weiteren Ablauf benötigen Sie dann die „reale“ Email-Adresse, den Postausgangsserver des Providers und die zugehörigen Zugangsdaten zum Mailkonto. In vielen Fällen ist die Email-Adresse auch gleich der Benutzername zum Postfach.

2. **Benutzerverwaltung des invis-Servers:** Hier muss, soweit nicht bereits geschehen, ein lokales Benutzerkonto angelegt werden, dem die externe Email-Adresse zugeordnet wird. invis-Server unterscheiden verschiedene Benutzerkonten-Typen die auch Email-berechtigt sind. Darunter ist der Typ „Mailkonto“ nicht für reale Benutzer gedacht sondern zur Nutzung nicht personenbezogene Mail-Adressen, wie etwa „info@….“
3. **Mailkontenverwaltung des invis-Servers:** Hier wird das externe Mailkonto dem lokalen Benutzer zugeordnet. Diese Zuordnung wird nachfolgend beschrieben.

Hinweis: *Ab invis-Server Version 14.3 können Mailkonten auch vollständig administrativ auf der Kommandozeile verwaltet werden. Die Grund-Idee bei der Entwicklung des invis-Servers war eigentlich, dass wir die Kontenverwaltung, so einfach gestalten, dass Anwender sich selbst darum kümmern können. Leider wird dieses Angebot nicht angenommen. Meine persönliche Meinung ist, dass die meisten Anwender, trotz einfacher Gestaltung dazu nicht mehr in der Lage sind, da sie die Hintergründe nicht „mehr“ verstehen.*

Achtung: *Auf invis-Servern vor Version 14.0 erfolgte die Anmeldung an CorNAz gegen den auf dem invis-Server installierten IMAP-Dienst. Verfügt der Benutzer nicht über ein lokales Postfach (dies ist abhängig vom Benutzertyp) schlägt die Anmeldung fehl. Das war gewünschtes Verhalten, da es keinen Sinn macht Emails von einem externen Server abzuholen, wenn diese nicht in einem lokalen Konto abgelegt werden können. Aus technischen Gründen ist das auf neueren Systemen nicht mehr so. Passen Sie also auf, dass der lokale Benutzer beispielsweise auch die Berechtigung hat etwa die Groupware Kopano zu verwenden. Ohne diese Berechtigungen könnten eingehende Mails nicht lokal zugestellt werden.*

Mailkontenverwaltung via invis-Portal

Mailkonten "zuordnen"

Noch aus den Anfangstagen des invis-Servers stammt das Programm „CorNAz“ zur Verwaltung von Email-Konten. Zu finden ist es in der Rubrik „local“ des Portals hinter der Schaltfläche „Mailkonten“. CorNAz steht jedem Benutzer des Servers zur Verfügung, es benötigt also keinen administrativen Zugang zum invis-Portal. Ziel dahinter ist, dass Benutzer in der Lage sein sollen Ihre Mailkonten selbst zu verwalten. Dabei können jedem lokalen Benutzer beliebig viele externe Mailkonten zugeordnet werden.

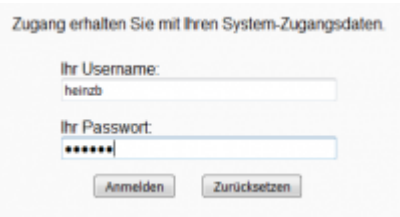
Hinweis: *Ab invis-Version 13.5 ist CorNAz voll ins invis-Portal integriert. Sie finden es unter dem Reiter „mail“*

Funktionen

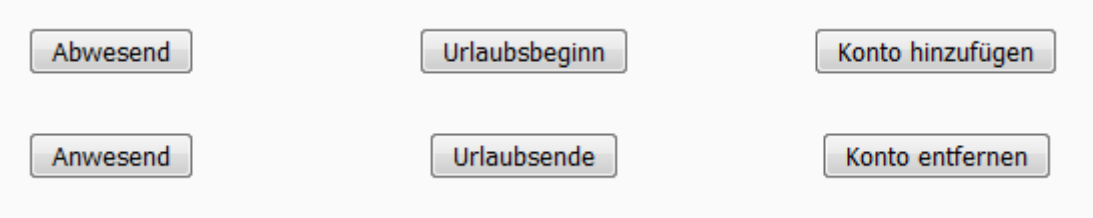
- externe Mailkonten einrichten oder löschen

- Benutzer auf an- oder abwesend setzen.
- Urlaubsbenachrichtigung einrichten oder abschalten
- Auswahl des Mailkontos über welches die Emails eines Benutzers versendet werden sollen.

CorNAz verlangt eine gesonderte Anmeldung desjenigen lokalen Benutzers, dessen externe Mailkonten verwaltet werden sollen. Benötigt werden die Zugangsdaten des Benutzers die er auch zur Anmeldung am PC benötigt.

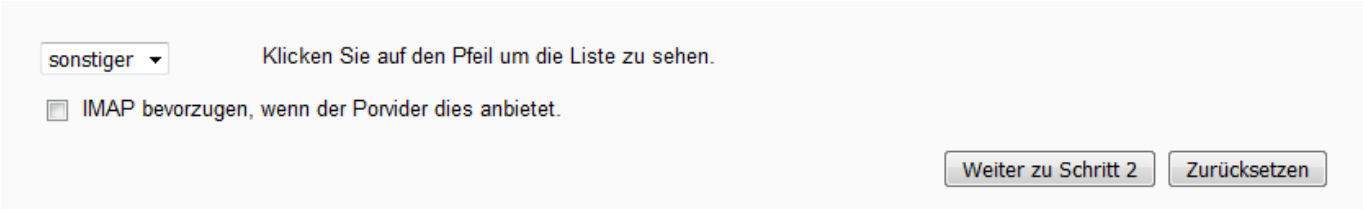


Nach der Anmeldung stehen die verschiedenen Funktionen über entsprechende Schaltflächen zur Verfügung.



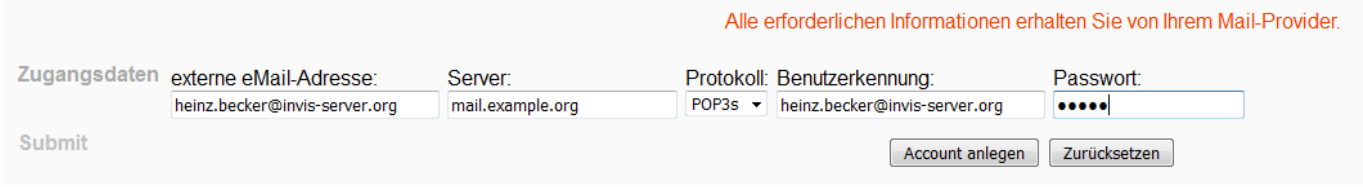
Mailkonto anlegen

Klicken Sie auf die Schaltfläche „Konto hinzufügen“. Das Anlegen erfolgt in zwei Schritten. Im ersten Schritt können (müssen aber nicht) Sie einen Mailprovider aus einer Liste bekannter Provider auswählen und wenn gewünscht IMAP als Protokoll für den Mailabruf bevorzugen. Beides ist nicht notwendig, es kann im nächsten Schritt alles manuell angepasst werden.



Hinweis: *Die Verwendung von IMAP macht hier weniger Sinn. IMAP belässt abgerufene Emails auf dem externen Server beim Provider. Da diese Konten meist in ihrer Größe begrenzt sind, besteht die Gefahr, dass ein solches Postfach irgendwann unbemerkt voll läuft. Nützlich ist dies lediglich um unabhängig vom invis-Server von „Überall“ auf eingehende Emails zugreifen zu können. Da Ihr invis-Server aber ebenfalls von „Überall“ erreichbar ist, spielt dies keine Rolle.*

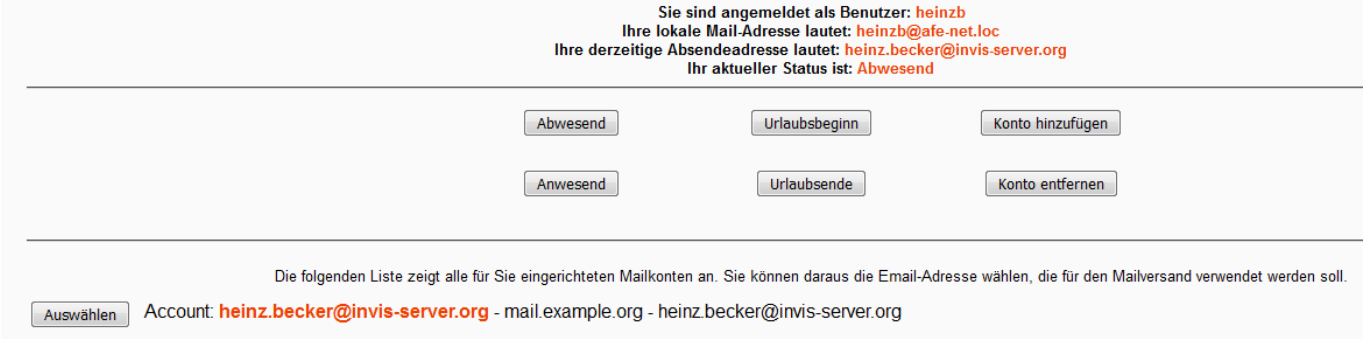
Klicken Sie auf Schaltfläche „Weiter zu Schritt 2“. Hier können Sie die Zugangsdaten zu Ihrem externen Postfach eingeben. Die Zuordnung zum lokalen Benutzer erfolgt automatisch, da Sie ja mit dem gewünschten Benutzer an CorNAz angemeldet sind.



Sie benötigen für diesen Schritt die Zugangsdaten zum externen Postfach. Als Protokoll für den Mail-Abruf ist die Auswahl „POP3s“ zu bevorzugen. D.h. Alle Mails werden über eine verschlüsselte Verbindung vom Provider abgerufen und nach Erhalt beim Provider gelöscht. Nach Bestätigung der Zugangsdaten zeigt CorNAz alle eingegebenen Daten inklusive Passwort zur Überprüfung noch einmal an. Achten Sie also darauf, wer Ihnen über die Schulter schaut.

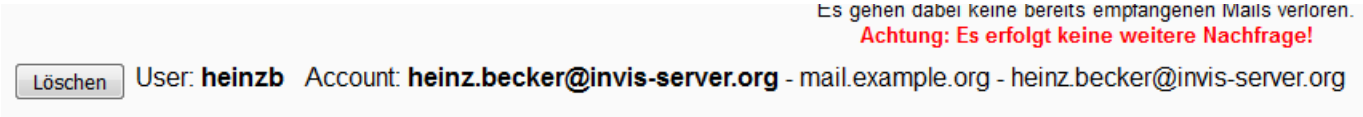
Über die Verknüpfung „Hauptmenü“ gelangen Sie wieder zurück zur Funktionsübersicht.

Abschließend müssen Sie zumindest beim Erstanlegen eines externen Kontos den Benutzer als „Anwesend“ führen. Dazu einfach auf die Schaltfläche Anwesend klicken.



Mailkonto löschen

Zum Löschen eines externen Kontos müssen Sie einfach auf die Schaltfläche „Konto löschen“ klicken und dann aus der Liste der Konten des Benutzers das zu löschende Auswählen. Klicken Sie zum Löschen einfach auf die Schaltfläche „Löschen“ links neben dem zu entfernenden Konto.



Der im Screenshot gezeigte Warntext ist ernst gemeint. Es erfolgt beim Löschen keine Sicherheitsabfrage, es wird unmittelbar gelöscht.

weitere Funktionen

Grundsätzlich sind alle weiteren Funktionen von CorNAz in Ihrer Anwendung weitgehend selbsterklärend.

Hauptadresse auswählen

Verfügt ein invis-Benutzer über mehrere externe Email-Konten, muss dem invis-Server mitgeteilt werden, welche Adresse für den Versand von genutzt werden soll. Sie wählen die jeweilige Adresse einfach im Hauptmenü über die Schaltfläche „“ links neben dem gewünschten Konto aus. Diese Auswahl kann jederzeit geändert werden. Sollen statt dessen mehrere Konten gleichberechtigt genutzt werden, sollten dafür jeweils eigene invis-Server Benutzer angelegt werden. Hierfür eignet sich der Benutzertyp „Maildummy“ bzw. „Mailkonto“.

Abwesend / Anwesend

Diese Funktion schaltet den Abruf von Emails aus externen Konten eines Benutzers je nach Wunsch ein oder aus. Nützlich ist dies bei längerer Abwesenheit, wenn der invis-Server nicht via Internet erreicht werden kann. In diesem Fall können während der Abwesenheit neue Emails direkt beim Provider, so dieser eine Webmail-Anbindung anbietet eingesehen werden. Im Normalfall sollte hier also immer **Anwesend** aktiviert sein.

Urlaubsbeginn / Urlaubsende

Diese Funktion generiert nach Wunsch Abwesenheitsbenachrichtigungen. Sie wurde von uns in letzter Zeit allerdings etwas stiefmütterlich behandelt, da Kopano, andere Groupwaresysteme und auch Roundcubemail eine solche Funktion selbst anbieten.

Administrative Mailkontenverwaltung auf der Kommandozeile

Insgesamt zählen (bisher / V. 14.3) 3 einzelne Scripts zur Mailkontenverwaltung:

- ***addmailaccount*** - Dient dem zuordnen externer Mailkonten zu einem lokalen Benutzerkonto. Es hinterlegt die Zugangsdaten dieses Mailkontos im ActiveDirectory.
- ***changemacstate*** - Damit läßt sich der Status eines Benutzers zwischen an- und abwesend ändern. D.h. Emails werden beim Provider abgerufen, oder eben nicht. Das hat nichts mit eine Abwesenheitsbenachrichtigung zu tun. Neue Mails verbleiben einfach beim Provider.
- ***refreshfrc*** - Wurden beispielsweise via phpLDAPAdmin Änderungen an den Zugangsdaten eines Email-Postfachs vorgenommen, müssen diese Daten in die aktive fetchmailrc-Datei übernommen werden um wirksam zu sein. Das Script generiert die fetchmailrc-Datei einfach neu auf Basis der bestehenden. D.h. ist ein Benutzer als „abwesend“ geführt ändert das Script daran nichts.

Die Scripts sind dazu gedacht, es dem Administrator einfach zu machen Mailkonten der Anwender zu verwalten. Via Portal benötigt er das Passwort des jeweiligen Benutzers, nicht schön. Kümmern sich die Benutzer (was leider quasi immer der Fall ist) nicht um ihre eigenen Mailkonten ist es für den Admin via Portal umständlich Mailkonten zu verwalten. Mit den Scripts ändert sich das. Das Anlegen eines neuen Mailkontos inkl. der Zuordnung zum lokalen Benutzer wird wie folgt eingeleitet:

```
invis:~ # addmailaccount username
```

Es öffnet sich ein „Dialog-Formular“, in dem alle Daten eingetragen werden können. Das Script schreibt diese Informationen dann ins ActiveDirectory.

Um dann den Mailabruf einzuschalten genügt folgendes Kommando:

```
invis:~ # changemacstate username a
```

Der Buchstabe „d“ anstelle von „a“ würde den Mailabruf wieder deaktivieren.

Physische Geräte und Computer ins Netzwerk integrieren

Bei der Integration eines neuen Gerätes, wie beispielsweise einen PC oder einen Netzwerkdrucker, in Ihr Netzwerk sorgen Sie dafür, dass dieses Gerät immer unter der gleichen IP-Adresse mit dem

Netzwerk verbunden ist und es über einen von Ihnen festzulegenden Namen ansprechbar ist. Dahinter stehen die Dienste DNS (Namensauflösung) und DHCP (IP-Adressvergabe).

Um ein neues Gerät ins Netzwerk zu integrieren müssen Sie es im invis-Portal Ihres Servers registrieren. Dabei wird eine sogenannte DHCP-Reservierung erzeugt, d.h. dafür Sorge getragen, dass das Gerät zuverlässig immer die selbe IP-Adresse vom DHCP-Dienst erhält. Weiterhin wird diese IP-Adresse im DNS-Dienst fest dem von Ihnen erdachten Namen verbunden.

Damit dies funktioniert benötigen Sie als Erkennungsmerkmal für den DHCP-Dienst die sogenannte Hardware- oder auch MAC-Adresse des Gerätes. In vielen Fällen ist diese irgendwo am Gerät aufgedruckt. Netzwerkdrucker sind meist in der Lage eine Statusseite auszudrucken, die diese Information enthält.

MAC-Adressen haben folgendes Format: **28:d2:44:2d:21:a5**
Sie bestehen aus 6 Zeichenpaaren (Hexadezimalzahlen) bestehend aus den Ziffern **0-9** und den Buchstaben **a-f**.

Weiterhin muss das Gerät bzw. der Computer **zwingend** für den automatischen Adressbezug (DHCP-Client) konfiguriert sein! In vielen Fällen entspricht das der Vorkonfiguration, ist dies nicht der Fall entnehmen Sie bitte dem Handbuch des Gerätes wie Sie dessen Konfiguration entsprechend ändern können.

Achtung: *Von der Vergabe fester IP-Adressen am Gerät oder PC selbst, raten wir* ***dringend*** *ab. Derartiges Vorgehen birgt die Gefahr doppelter Adressvergabe im Netz und somit massiver Netzwerkprobleme.*

Hinweis: *Wenn Sie viele neue Geräte auf einmal registrieren möchten, sollten Sie sich das Toolbox-Script* ***hostadd2ad*** *anschauen.*

MAC-Adresse ermitteln

Es gibt eine Reihe von Möglichkeiten die MAC-Adresse eines Gerätes oder Computers zu ermitteln. Wir werden hier lediglich erläutern, wie Sie dies mit Hilfe des invis-Servers selbst tun können. Mit den Netzwerkverwaltungswerkzeugen gängiger Betriebsysteme wie Linux, Windows oder MAC OS können Sie sich die MAC-Adresse des Computers auch am Gerät selbst anzeigen lassen.

Melden Sie sich bevor Sie das neue Gerät mit dem Netzwerk verbinden als Benutzer „root“ an der Konsole Ihres Servers an (siehe oben) und geben Sie folgendes Kommando ein:

```
invis:~ # journalctl -fu dhcpd.service
...
```

Verbinden sie jetzt das neue Gerät mit dem Netzwerk, schalten es ein und beobachten dabei die Konsole. Nach kurzer Zeit wird sich die Konsole mit Zeilen wie nachfolgend gezeigt füllen:

```
...
Dez 19 08:56:51 invis dhcpd[5367]: DHCPREQUEST for 172.20.200.3 from
7c:2f:80:1e:4b:c9 (DX600A-ISDN) via intern
Dez 19 08:56:51 invis dhcpd[5367]: DHCPACK on 172.20.200.3 to
```

```
7c:2f:80:1e:4b:c9 (DX600A-ISDN) via intern
...
```

Sie sehen dort die MAC Adresse des Gerätes, im Beispiel eines Netzwerk-fähigen ISDN-Telefons der Telekom. Es besteht bei dieser Methode die Gefahr, dass sich während Sie auf Ihr neues Gerät warten bereits im Netzwerk registrierte Geräte beim DHCP-Dienst melden. Um zu verhindern, dass Sie sich die falsche MAC-Adresse notieren, gehen Sie sicher, dass die dem Gerät zugewiesene Adresse aus dem freien Adress-Pool des DHCP-Servers stammt (Erläuterungen, siehe **hier**.

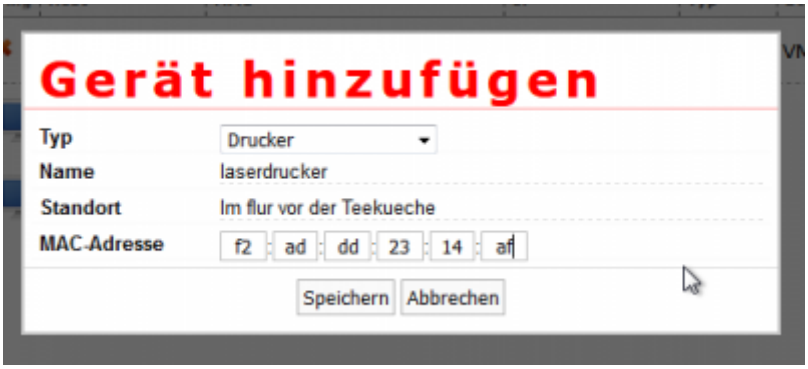
Im gezeigten Beispiel ist es eine Adresse aus dem freien Pool, zu erkennen an der Zahl „200“ an der dritten Stelle der vergebenen IP-Adresse.

Um ganz sicher zu gehen, können Sie den Vorgang mehrfach wiederholen.

Haben Sie die MAC-Adresse identifiziert und notiert, stoppen Sie das gestartete Kommando mit der Tastenkombination **`Strg+C`** und schalten das Gerät wieder ab, bzw. trennen es vom Netzwerk. (Am besten beides.)

Gerät registrieren

Zur Registrierung melden Sie sich als Administrator am invis-Portal Ihres Servers an und wechseln nach „administration“ → „Netzwerk“. Klicken Sie im Hauptfenster jetzt auf „Gerät hinzufügen“. Im sich öffnenden Eingabefenster wählen Sie zunächst den Gerätetyp aus, vergeben einen Namen, tragen den Standort und die MAC-Adresse ein.



Dabei ist folgendes zu beachten:

1. **Gerätetyp:** Diese Unterscheidung dient lediglich der Ordnung im Netz. Halten Sie sich daran, können Sie schon anhand der IP-Adresse zwischen PC und Drucker unterscheiden.
2. **Name:** Hier muss ein gültiger DNS-Hostname (ohne Domäne) vergeben werden. D.h.: Keine Leer- und Sonderzeichen außer Bindestrichen, keine Umlaute und idealerweise nur Kleinbuchstaben. Neuere Versionen des invis-Portals verweigern Falscheingaben, ältere leider nicht.
3. **Standort:** Freitext, der keine Umlaute enthalten darf.
4. **MAC-Adresse:** MAC-Adressen sind weltweit einmalig und dienen als eindeutiges Erkennungsmerkmal, entsprechend dürfen Sie niemals zwei Einträge mit gleicher MAC-Adresse anlegen. Neuere Versionen des invis-Portals verhindern dies, ältere leider nicht.

Bestätigen Sie Ihre Eingabe mit der Schaltfläche „Speichern“.

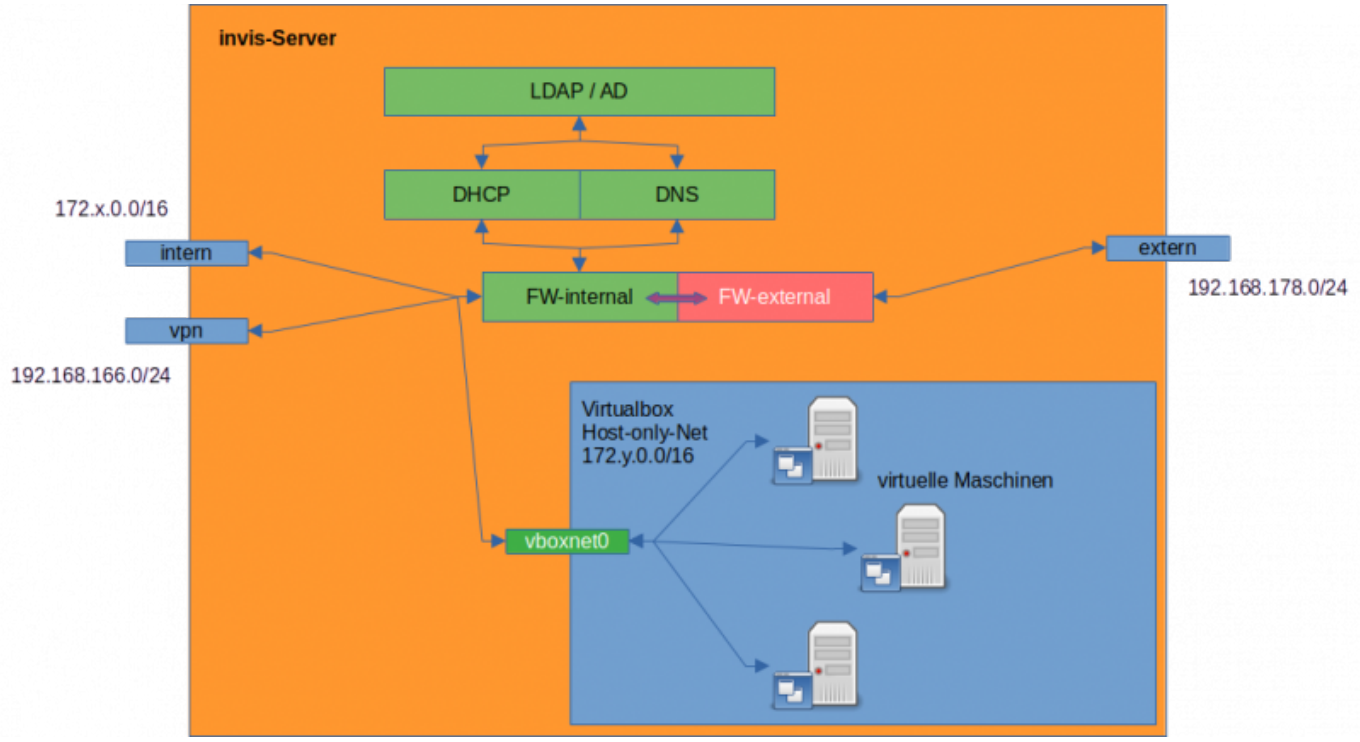
Verbinden Sie Ihr Gerät jetzt wieder mit dem Netzwerk bzw. starten es neu. Wenn Sie sich nicht bei

der MAC-Adresse vertippt haben, sollte es jetzt eine fest reservierte IP-Adresse erhalten. Sie können dies auf die gleiche Weise überprüfen, wie Sie evtl. bei der oben beschriebenen Methode zur Ermittlung der MAC-Adresse vorgegangen sind.

Handelt es sich bei Ihrem Gerät um Netzwerkhardware (Acce-Point, Switch usw.) oder einen Netzwerkdrucker, verfügt dieses/dieser garantiert über eine Webapplikation zur Konfiguration. Geben Sie einfach die IP-Adresse oder den vollen Namen des Gerätes mit vorangestelltem **`http`** in einem Browser ein. Wenn Sie auf dem Gerät landen, hat alles funktioniert.

Virtuelle Maschinen ins Netz integrieren

Ab invis-Server 15.0 werden virtuelle Maschinen nicht mehr per Netzwerkbrücke mit dem internen (lokalen) Netz des invis-Servers verbunden. Diese Art der Anbindung bremst sowohl die VMs selbst, als auch den Zugriff darauf. Virtuelle Maschinen werden in ein eigenes Subnetz integriert und dies geschieht nicht über das invis-Portal sondern über neue Scripts. Die nachfolgende Abbildung verdeutlicht die neue Umgebung.



Durch die Integration der VMs in ein eigenes Subnetz, welches aus Sicht von Virtualbox als „Host-only-Subnetz“ sichtbar ist, teilen sich nicht mehr der invis-Server selbst und alle VMs die physische interne Netzwerkschnittstelle, wie es mit Netzwerkbrücken der Fall ist. Dadurch werden „Hänger“ beim Zugriff auf die VMs vermieden und sie reagieren deutlich schneller auf Anfragen.

Die Subnetze werden dennoch vom lokalen DHCP-Dienst des invis-Servers mit IP-Adressen und Netzwerkinformationen versorgt. Sie sind der selben Firewall-Zone zugehörig wie das interne Netz und sind von dort aus ungehindert erreichbar.

Zunächst muss dafür ein Subnetz eingerichtet werden. Dieses muss zum einen Virtualbox als Host-only-Subnetz bekannt gemacht werden. Dem lokalen DHCP-Dienst und der internen Zone der Firewall

muss die dafür am invis-Server endende virtuelle Netzwerkschnittstelle des Subnetzes zugeordnet werden. Das alles wird mit dem Toolbox-Script ***addvbsubnet*** in einem Schritt erledigt (Anwendung, siehe Toolbox hier im Wiki).

Danach können VMs aus diesem Netz mit dem Script ***addvm2subnet*** mit einer festen DHCP-Lease und DNS-Einträgen versorgt werden (Anwendung, siehe Toolbox hier im Wiki).

Hinweis: *Bei vorhandenen per Netzwerkbrücke verbundenen VMs, müssen die bestehenden DHCP- und DNS Einträge zunächst per invis-Portal gelöscht werden, bevor sie dem neuen Subnetz zugeordnet werden können.*

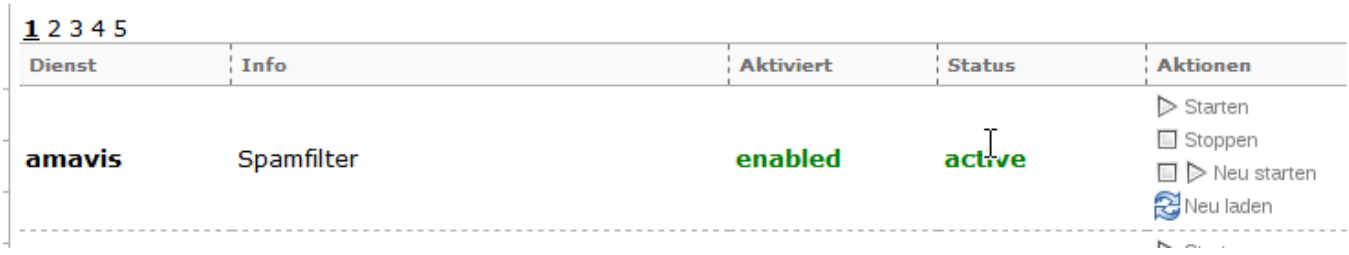
Dienste

invis-Server verfügen über eine Reihe von Funktionen, viele dieser Funktionen werden durch auf dem Server permanent laufende Programme, Dienste oder auch Dämonen genannt, repräsentiert. Es kann jederzeit vorkommen, dass ein solcher Dienst aufgrund eines Fehlers seine Arbeit verweigert. Der Anwender bemerkt das natürlich daran, dass gewisse Dinge nicht mehr funktionieren, beispielsweise kann er keine Emails mehr versenden.

Im einfachsten Fall genügt es einen gestörten Dienst neu zu starten um seine Funktion wieder herzustellen. Diese Möglichkeit bietet das invis-Portal.

Achtung: *Die Verwaltung von Diensten ist kein Spaß. Einfach mal einen Dienst, den man nicht genau zuordnen kann zu stoppen, kann empfindliche Störungen der Betriebsabläufe Ihres Unternehmens nach sich ziehen. Wenn Sie sich hierbei nicht sicher sind kontaktieren Sie Ihren IT-Dienstleister.*

Klicken Sie im invis-Portal auf „administration“ → „Dienste“. Es kann jetzt eine ganze Weile dauern (30 Sekunden und mehr sind schon vorgekommen), bis sich im Hauptfenster des Portals eine mehrseitige Tabelle aufbaut. Jede Tabellenzeile entspricht dabei einem Dienst:



Das Beispiel zeigt den Eintrag des Dienstes „amavis“, der sich um das herausfiltern Viren-verseuchter, bzw. markieren Spam-verseuchter Mails Ihres Servers kümmert.

Jede Spalte der Zeile hat natürlich eine eigene Bedeutung:

1. Name des Dienstes
2. Funktion des Dienstes
3. Wird der Dienst beim Start Ihres Servers automatisch gestartet (enabled = ja)
4. Läuft der Dienst im Moment (active = ja)
5. In der letzten Spalte können Sie den Dienst steuern

Sie haben die Optionen **Starten**, **Stoppen**, **Neu starten** und **Neu laden**. Dabei bedeutet „Neu

laden“ einen Dienst dazu zubringen eine veränderte Konfiguration neu einzulesen, ohne den Dienst zu stoppen. Diese Aufgabe wird allerdings in aller Regel direkt auf der Kommandozeile des Server erledigt, da auch dort Konfigurationsänderungen vorgenommen werden.

Beherzigen Sie hier bitte folgende Tipps:

1. Nur weil ein Dienst **nicht** läuft ist dies kein Grund ihn einfach so zu starten. Möglicherweise ist dessen Inaktivität ja beabsichtigt. Aufmerksam sollten Sie allerdings bei der Kombination aus „enabled“ und „inactive“ werden, dies ist in der Regel keine gewünschte Kombination.
2. Nutzen Sie diese Funktionen nur aus gegebenem Anlass mit klarem Kontext. Also nur dann, wenn etwas nicht funktioniert.
3. Sind Sie sich nicht sicher, halten Sie Rücksprache mit Ihrem IT-Dienstleister.
4. Sie handeln hier auf eigene Gefahr, dessen sollten Sie sich bewusst sein!

Sonderfunktionen im invis-Portal (Ab invis-Server Version 14.1)

Die administrative-Seite „Funktionen“ im invis-Portal bildet eine Schnittstelle zur Ausführung administrativer Shell-Scripts auf am Server auszuführen, ohne sich an dessen Konsole anzumelden.

Derzeit vorhandene Funktionen:

- **Maschinenkonten erweitern** - Gedacht um Maschinen-Konten mit UNIX-Attributen zu erweitern. Notwendig ist das um beispielsweise Maschinen-Konten Zugriff auf Fileserver-Freigaben zu gewähren, etwa wenn Software via GPOs ausgerollt wird.
- **Fix Groupshare ACLs** - Damit können „verkorkste“ Zugriffs-ACLs für die Gruppen-Arbeitsverzeichnisse in der Gruppen-Freigabe auf die Anfangswerte zurück gesetzt werden. Gleichzeitig werden Verzeichnisse, die manuell auf der obersten Ebene der Gruppen-Freigabe angelegt wurden umbenannt, indem die Endung „-bitte_Support_anrufen“ an die Verzeichnisnamen anhängt wird. **Achten** Sie bei Nutzung dieser Funktion unbedingt darauf, dass Sie über eine aktuelle Datensicherung verfügen. Das zugrunde liegende Script „könnte“ über merkwürdige Datei- und Verzeichnisnamen stolpern. Mit „merkwürdig“ ist die Verwendung von Sonderzeichen in Dateinamen gemeint. Wir haben versucht das Script so gut es geht, dagegen zu immunisieren, 100 prozentige Sicherheit gibt es aber nicht. Die unangenehme Folge wären zerstörte Dateien.
- **Software-Versionen prüfen** - Gibt die Versionsnummern wichtiger auf dem Server installierter Software aus.
- **Benutzerdaten bereinigen** - (Ab Version 14.3) Wird ein Benutzerkonto gelöscht, verbleiben dessen Kopano- und ownCloud-Daten im jeweiligen System. Sie können über diese Funktion unter Angabe des Benutzernamens **endgültig** gelöscht werden.
- **Steuerdatei Mailabruf auffrischen** - (Ab Version 14.3) Wurde beispielsweise per „phpLDAPAdmin“ manuell eine Veränderung an irgendwelchen Zugangsdaten für den Abruf von Mails aus externen Postfächern geändert, kann hierüber die „fetchmailrc“ Datei neu geschrieben werden.

Die Integration weiterer Scripts ist in Planung.

Konsolenzugriff

Für einige Administrative Tätigkeiten am invis-Server ist Zugriff auf dessen Kommandozeile mit root-Rechten unabdingbar.

Achtung: *Wenn Sie sich auf der Kommandozeile eines Linux-Servers bewegen, sollten Sie wissen, was Sie tun! „Ich bin **root** ich darf das.“ ist ein schöner und sehr zutreffender Spruch, der einem schnell auf die Füße fallen kann.*

Eine der wichtigsten Voraussetzungen für die Administration eines Linux-Servers ist Erfahrung im Umgang mit einem Konsolen-Editor. Selbstverständlich bringen invis-Server die üblichen Verdächtigen wie ***vi*** oder ***joe*** mit. Auch der Kommandozeilen-Dateimanager Midnight-Commander (***mc***) mit seinem Editor ***mcedit*** ist auf jedem invis-Server vorinstalliert.

Je nach Ausgangssituation oder Umgebung gibt es verschiedene Wege sich mit der Kommandozeile des invis-Servers zu verbinden. Verwendet wird in jedem Fall das SSH-Protokoll.

- **von einem Linux System:** Jedes Linux System verfügt von Haus aus über einen SSH-Client auf der Kommandozeile, aber das werden Sie als Linux Nutzer natürlich wissen.
- **von einem Windows System:** Hier empfiehlt sich die Verwendung des SSH-Clients ***putty***
- **Mal eben von irgendwo:** Teil der administrativen Werkzeuge, die das invis-Portal im Gepäck hat, ist die Software „Shell-in-a-box“, die Sie im Browser verwenden können.

Verbindungen aus dem lokalen Netz heraus können Sie unter Verwendung des SSH-Standard-Ports „22“ vornehmen:

```
linux-pc:~ # ssh root@invis.invis-net.loc
```

Verbinden Sie sich via Internet benötigen Sie den „verschobenen“ SSH-Port des Servers sowie des Namens unter dem der invis-Server im Internet erreichbar ist:

```
linux:-pc:~ ssh -p 53482 root@ddns.ihredomain.de
```

Das der im Beispiel genannte Port nicht allgemeingültig ist sollte klar sein. Jeder invis-Server erhält während des Setups seinen eigenen per Zufallsgenerator ausgewürfelten SSH-Port. Wenn Sie den Server nicht selbst aufgesetzt haben, erfragen Sie diesen Port bei Ihrem IT-Dienstleister. Gleiches gilt natürlich für den Hostnamen.

Gleiches gilt natürlich bei der Verwendung von ***putty***.

Bei Verwendung von „Shell In A Box“, zu finden im invis-Portal unter „administration“ → „Server Administration“, müssen Sie wissen, dass ein direkter Login als Benutzer „root“ aus Sicherheitsgründen nicht möglich ist. Sie müssen sich zunächst als „normaler Benutzer“ anmelden und dann mit:

```
invis:~ # su -
```

die Identität von „root“ annehmen.

Die Konfigurationsdateien

Das Bearbeiten der Konfigurationsdateien setzt einen Kommandozeilenzugriff auf den Server mit „root-Rechten“ voraus.

/etc/invis/invis.conf

Dies ist die zentrale Konfigurationsdatei des invis-Servers. Sie hat derzeit noch einen recht überschaubaren Umfang. Aus Ihr beziehen die Tools der invis Toolbox ihre Vorgaben.

Sie wird während des Setups angelegt und an die Umgebung des invis Servers angepasst. Spätere Anpassungen sind kein Problem.

Alle Einträge sind in der Datei gut dokumentiert.

Bei manuellen Veränderungen an der Datei ist auf die Dateisyntax zu achten.

Beispiel:

```
# Wo liegt das Quarantäne-Verzeichnis?
quarDir:/var/spool/infected
```

Jede Zeile beginnt mit dem Namen der Konfigurationsoption gefolgt von zugehörigen Parameter. Option und Parameter sind durch einen Doppelpunkt getrennt. Vor und nach dem Doppelpunkt darf sich **kein** Leerzeichen befinden.

Hier noch ein paar Beispiele zu besonderen invis-Server Funktionen, die über die Konfigurationsdatei gesteuert werden können.

Bereinigung der Tranfer-Freigabe

Die Transfer-Freigabe ist eine File-Server Freigabe die vor allem dem Datenaustausch zwischen Benutzern und Gruppen ohne Veränderung von Zugriffs- und Besitzrechten dient. Es ist die „jeder darf alles“ Freigabe, und somit prädestiniert zur **Betriebsmüllhalde** zu mutieren.

Um dem zu begegnen können invis-Server dieses Verzeichnis selbsttätig bereinigen. Es werden alle Dateien die älter als X Tage sind gelöscht. Resultieren daraus leere Verzeichnisse, werden auch diese gelöscht. In der Freigabe wird immer eine „Liesmich-Datei“ angelegt, die auf diesen Umstand hinweist.

Über die invis-Konfigurationsdatei kann das maximale Alter von Dateien eingestellt und die Funktion im Ganzen aktiviert oder deaktiviert werden:

```
# Clean Transfer Directory
# Soll das Transferverzeichnis des Fileservers regelmässig von alten Dateien
befreit werden?
# [j/n]
```

```
cleanTrOn:j

# Maximales Alter der Dateien und Verzeichnisse im Transferordner
trMaxDays:42

# Pfad zum Transferordner
trDir:/srv/shares/transfer
```

Bereinigung der Netzwerk-Papierkörbe

In wichtigen Freigaben pflegen invis-Server einen recht nützlichen „Netzwerk-Papierkorb“. Damit auch diese nicht ins unermessliche anwachsen, gibt es für die Papierkörbe eine entsprechende Funktion wie für die Bereinigung der Tranfer-Freigabe.

Auch hier können die Zeiten über die invis-Konfigurationsdatei geteuert werden:

```
# Clean Recycle Directories
# Sollen die Samba-Recycle-Verzeichnisse des Fileservers regelmässig von
alten Dateien befreit werden?
# [j/n]
cleanRecOn:j

# Maximales Alter der Dateien und Verzeichnisse im Transferordner
RecMaxDays:30
```

Interne Datensicherungen

invis-Server führen regelmäßig interne Datensicherungen des Active-Directories, der lokalen Datenbanken und des Dokuwiki Datenbestandes durch. Die Sicherungen werden jeweils als Vollsicherungen in der Archiv-Freigabe abgelegt. Dabei sammeln sich mit der Zeit nicht unwesentliche Datenmengen an. Um dem entgegen zu wirken kann der invis-Server regelmäßig alte Sicherungen im Sicherungsverzeichnis löschen. Es lassen sich über die invis-Konfigurationsdatei sowohl die Zielpfade, als auch die Aufbewahrungsdauer einstellen.

```
# Datensicherungen
DasiDir:/srv/shares/archiv/sicherungen
DBTarget:datenbanksicherungen
DWTarget:dokuwikisicherungen

# Soll aeltere Sicherungen automatisch aus dem Sicherungsverzeichnis
geloescht werden
cleanDasi:j
# Maximales Alter
dasiMaxDays:21
```

Achtung: *Die interne Datensicherungsfunktion entbindet Sie* ***NICHT*** *von der Pflicht regelmäßige Datensicherungen Ihres Servers durchzuführen. Vor dem Gesetzt gilt eine Datensicherung nur dann als Datensicherung wenn gesicherte Daten „räumlich getrennt“ von den Originaldaten aufbewahrt*

werden. Dabei meint „räumlich getrennt“ mindestens einen anderen Brandabschnitt!

DDNS Funktion

DDNS oder „dynamic DNS“ ist eine Funktion mit der ein Client selbsttätig Daten eines DNS-Servers aktualisieren kann. invis-Server werden meist hinter einfachen DSL-Anschlüssen ohne feste-IP Adresse betrieben. Um einen invis-Server zuverlässig auch aus dem Internet heraus erreichen zu können, braucht er daher einen festen Namen dem automatisch die jeweils gültige IP-Adresse zugeordnet werden. DDNS ist Teil des DNS-Netzwerk-Protokolls. invis-Server können als DDNS-Client arbeiten.

***Hinweis:** DDNS hat in diesem Fall zwar die gleiche Funktion wie das was beispielsweise das Unternehmen „dynDNS.org“ anbietet, ist aber nicht das Gleiche. Im Falle von dynDNS.org oder deren Mitbewerber setzt der Client keinen DDNS-Call ab, sondern übermittelt die zu aktualisierenden Daten per HTTP.*

Um die DDNS-Client-Funktion zu nutzen müssen Sie Zugriff auf den Primary-DNS-Server verfügen, der für die Domain verantwortlich ist, in der Sie für Ihren invis-Server einen Namen eintragen möchten.

Die DDNS-Funktion des invis-Servers setzt voraus, dass die Ziel-Domain auf dem DNS-Server für DDNS vorbereitet ist und Sie über einen DNSsec Key zur Authorisation eines DNS-Updates verfügen. Der DNSsec-Key besteht aus zwei Schlüsseldateien (public und private Key), die letztlich aber den gleichen Inhalt haben. DDNS arbeitet mit synchroner Verschlüsselung, daher beinhalten beide Dateien den gleichen Schlüssel. Diese Dateien müssen Ihnen vorliegen. Betreiben Sie selbst den DNS Server müssen Sie sie selbst generieren.

Kopieren Sie auf dem invis-Server einfach beide Schlüsseldateien nach:

```
/etc/invis/ddns
```

Jetzt können Sie die Funktion in der invis-Konfigurationsdatei aktivieren. Weiterhin müssen Sie den im Internet gültigen Namen des invis-Servers, den anzusprechenden DNS-Server und die 5-stellige Nummer des DNSsec Keys eintragen:

```
# DDNS-Update
# Verwenden Sie anstelle von z.B. DynDNS.org einen eigenen DNS-Server, den
Sie per DDNS aktualisieren?
# [j/n]
ddnsOn:n

# Adresse des Nameservers
nameServer:ns.fspisp.de

# Hostname (FQDN) Ihres Servers im Internet
fqdn:clt.invis-server.org

# Schlüsselnummer Ihres DDNS-Keys
keyNumber:00000
```

Der DDNS-Abgleich wird jetzt zyklisch vom Script ***inetcheck*** durchgeführt.

Hinweis: *Möchten Sie statt dessen die Dienste von dynDNS.org oder deren Mitbewerber nutzen, empfehlen wir die Nutzung der entsprechenden Funktionen Ihres Routers oder die Installation des Programms „ddclient“ auf Ihrem invis-Server.*

/etc/invis/invis-pws.conf

In dieser Datei werden Passwörter für den Zugriff auf das LDAP-Verzeichnis sowie die Datenbank-Systeme gespeichert. Notwendig ist dies, damit die verschiedenen Tools der invis-Toolbox ihre Arbeit erledigen können. Die Datei wird während des Setups angelegt und muss in der Regel im laufenden Betrieb nicht mehr angefasst werden. Zugriff darauf hat lediglich **root**.

Hinweis: *Diese Datei ist nicht mit der Passwortdatei zu verwechseln, die* ***sine2*** *ab invis-Server Version 14.0 während des Setups anlegt.*

/etc/cron.d/invis.cron

Über diese Datei werden alle für den invis Server relevanten Cronjobs gesteuert. Die Datei wird während des Setups automatisch angeleget und braucht in der Regel nicht verändert werden.

Sind Veränderungen notwendig, finden sich in der Datei zu jedem Eintrag Kommentare, die den Sinn und Zweck des jeweiligen Jobs erläutern.

/etc/invis/portal/config.php

Dies ist die zentrale Konfigurationsdatei des invis-Portals. Sie wird während des Setups automatisch an die Installationsumgebung angepasst.

Im Falle eines invis-Server Upgrades, bei dem auch das Portal neue Funktionen erhält, kann es vorkommen, dass die Konfigurationsdatei nach dem Update manuell um neue Konfigurationsoptionen erweitert werden muss. Nach einem solchen Upgrade finden Sie eine neue inaktive Konfigurationsdatei unter

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

. Vergleichen Sie beide Dateien und übernehmen Sie neue Konfigurationsoptionen aus der Vorlage in die aktive Datei und passen Sie sie ggf. an Ihre Bedürfnisse an.

Datensicherung

Wird eine Datensicherung per ***udevsync*** oder ***udevrdbu*** durchgeführt, kann das Portal an die fällige Datensicherung erinnern und über Erfolg bzw. Misserfolg informieren. Diese Funktion kann in der Datei config.php freigeschaltet und konfiguriert werden.

Dazu ist einfach die Zeile:

```
//$STATUS_BACKUP_TIMER = 3;
```

von den beiden führenden Slashes zu befreien. Die Zahl am Ende der Zeile legt das gewünschte Datensicherungsintervall in Tagen fest. Dies ist allerdings nur eine Erinnerungsfunktion, die Datensicherung müssen Sie schon selbst durchführen.

USV Überwachung

Seit invis-Server AD 10.3 können invis-Server auch mit USVs des Herstellers APC kommunizieren und wichtige Zustandsdaten im Portal anzeigen. Voraussetzung dafür ist, dass die USV „modbus“ unterstützt und „modbus“ auch aktiviert ist.

Um einen invis-Server entsprechend einzurichten muss der standardmäßig installierte **apcupsd** laufen und für „modbus“ konfiguriert sein. Bearbeiten Sie für diesen Zweck die Datei

```
/etc/apcupsd/apcupsd.conf
```

wie folgt:

```
...
UPSCABLE usb
...
UPSTYPE modbus
...
```

Danach können Sie in der Portal-Konfiguration die folgende Zeile von „false“ auf „true“ setzen:

```
// Aktivieren der APCUPS Daemon Abfrage
$STATUS_APCUPSD = true;
```

Nach wenigen Minuten sollten auf der Statusseite des Portals Zustandsdaten Ihrer USV angezeigt werden.

Achtung: *Evtl. müssen Sie „modbus“ auch noch an der USV selbst aktivieren. Entsprechende Hinweise entnehmen Sie dem Handbuch der USV.*

IP-Adressbereiche

Auf invis-Servern werden verschiedenen IP-Geräte Gattungen verschiedene IP-Adressbereiche innerhalb eines IP-Netzes zugewiesen. Dies hilft Geräte, wie etwa Drucker schon anhand Ihrer IP-Adresse zu erkennen. invis-Server unterscheiden folgende Geräteklassen:

- Server
- Drucker
- Client PCs
- IP Geräte

Die Bereiche werden ebenfalls in der Konfiguration des Portals vorgenommen. Ein Beispiel für ein privates Klasse A Netz:

```
// DHCP
$IP_NETBASE_ADDRESS = '192.186.42.0';
$DHCP_IP_MASK = '24';
$DHCP_IP_BASE = '192.168.42';
$DHCP_IP_REV = '42.168.192';
$DHCP_RANGE_SERVER = array(11, 19);
$DHCP_RANGE_PRINTER = array(20, 50);
$DHCP_RANGE_IPDEV = array(60, 90);
$DHCP_RANGE_CLIENT = array(120, 199);
```

Der DHCP-Server hält hier einen freien Adresspool im Bereich 192.168.42.200 bis 192.168.42.220 vor.

Seit invis-Server 11.0 können invis-Server auch mit privaten Klasse B Netzen (172.16.0.0/16 bis 172.31.0.0/16) umgehen. In diesem Fall sieht die Aufteilung der Adressbereiche wie folgt aus:

```
// DHCP
$IP_NETBASE_ADDRESS = '172.19.0.0';
$DHCP_IP_MASK = '16';
$DHCP_IP_BASE = '172.19';
$DHCP_IP_REV = '19.172';
$DHCP_RANGE_SERVER = array(0.11, 0.253);
$DHCP_RANGE_PRINTER = array(1.1, 1.254);
$DHCP_RANGE_IPDEV = array(2.1, 3.254);
$DHCP_RANGE_CLIENT = array(4.1, 4.254);
```

Der DHCP-Server hält hier einen freien Adresspool im Bereich 172.19.200.0 bis 172.19.200.254 vor.

Dienste

Seit invis-Server AD 10.2 ist es möglich auf dem Server laufende Dienste über die Administrationsseite des invis-Portals zu steuern. Die Dienste die dort aufgeführt werden sollen müssen in der Portal-Konfiguration aufgeführt werden:

```
$SERVER_SERVICES = array(
        array('amavis', 'Spamfilter'),
        array('clamd', 'Virenscanner'),
        array('cups', 'Druckserver'),
        array('dhcpd','IP Adressvergabe'),
        array('fetchmail','Emails abholen'),
        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', 'Active Directory'),
        array('kopano-dagent', 'Kopano Empfang'),
        array('kopano-gateway', 'Kopano Postfach'),
        array('kopano-ical', 'Kopano Kalender'),
        array('kopano-monitor', 'Kopano Monitor'),
        array('kopano-search', 'Kopano Suche'),
        array('kopano-server', 'Kopano Server'),
        array('kopano-spooler', 'Kopano Versand'),
        array('kopano-precense', 'Kopano Anwesenheit'),
        );
```

Dabei muss in der ersten Spalte der genaue Name des Dienstes und in der zweiten Spalte ein „Menschen-verständlicher“ Name eingetragen werden.

Hinweis: *Es ist beabsichtigt, dass der Apache-Webserver-Dienst hier* ***nicht*** *aufgeführt ist. Ihn aus einer Webanwendung heraus neuzustarten oder gar zu beenden ist gewiss keine gute Idee.*

Passwortsicherheit

Es ist möglich Anforderungen an die Komplexität der Benutzerpasswörter zu konfigurieren. Leider sind die derzeit noch im Portal eingebauten Anforderungen nicht kompatibel mit den Einstellungen des Microsoft Active Directory.

Gültig sind die Einstellungen nur für Passworteingaben oder Passwortänderungen die über das Portal getätigt werden.

Hier die entsprechenden Konfigurationszeilen:

```
$USER_PW_MIN_LENGTH = '8';
$USER_PW_COMPLEX = 'off';
```

Wir haben die Einstellungen inzwischen mit den Einstellungen des ActiveDirectory harmonisiert. Daher kann keine stufenlose Passwortkomplexität mehr eingestellt werden, sondern nur noch „on“ oder „off“. Dabei bedeutet „on“, dass ein Passwort mindestens 3 der der 4 möglichen Merkmale:

1. Groß- und Kleinschreibung
2. Buchstaben
3. Zahlen
4. Sonderzeichen

aufweisen muss.

Die Vorgaben des ActiveDirectories können Sie auf der Kommandozeile des invis-Servers mit dem Tool ***pwsettings*** aus der invis-Toolbox vorgegeben werden. Das Tool wird einfach ohne Aufrufparameter gestartet und ist dann selbsterklärend. Die für das invis-Portal getroffenen Einstellungen müssen mit den Vorgaben des AD übereinstimmen.

Wartungsarbeiten

Online Updates

Sorgen Sie dafür, dass Ihr invis Server über den Maintenance-Zeitraum der zugrunde liegenden openSUSE Version immer mit den aktuellen Sicherheits-Updates versorgt wird.

Dabei ist zwischen dem Aktualisieren aller installierten Pakete und dem exklusiven Installieren von Sicherheitsupdates der Distribution. Ersteres ist nicht ganz frei von Gefahren. Beim Aktualisieren aller Pakete könnte beispielsweise auch das invis-Server Setup-Paket installiert werden. Das ist solange ungefährlich, wie dieses Paket keine strukturellen Änderungen am Server vornimmt. Ist dies doch der Fall kann die Funktionsweise des Servers erheblich gestört werden. Lesen Sie dafür hier im Wiki die Beschreibungen im Abschnitt Server Upgrade.

Wenn Sie wissen, was Sie tun läuft eine vollständige Aktualisierung wie folgt ab:

```
invis:~ # zypper refresh
invis:~ # zypper up
invis:~ # afterup
```

Hinweis: *Es ist weder notwendig noch ratsam ein „Distribution Upgrade“ mit* ***zypper dup*** *durchzuführen!*

Möchten Sie lediglich die Sicherheitspatches der Distribution installieren können Sie dies mit „YaST Online Update“ (kurz: you) erledigen:

```
invis:~ # you
```

Dabei werden definitiv nur Patches installiert, die keine strukturellen Veränderungen am Setup mitbringen.

SMTP-Relay / SMTP-Auth für Postfix einrichten

invis Server sind meist via DSL mit dem Internet verbunden, verfügen also nicht über eine dauerhafte Internet-Anbindung. Das macht sie aus Sicht vieler Internet-Mailserver **zurecht** nicht vertrauenswürdig. Um aus dieser Situation heraus zuverlässig Emails versenden zu können, wird für den Mailversand eine Relais-Station (Relay-Server) benötigt, die uns vertraut. Dabei handelt es sich eigentlich um nichts anderes als die Konfiguration eines Postausgangsservers, so wie das auch in Mail-Clients gemacht wird.

Üblicherweise kann, von wenigen Ausnahmen abgesehen, der Postausgangsserver des eigenen Providers genutzt werden. Für die Postfix-Konfiguration werden dessen Name (FQDN), sowie Benutzernam und Passwort für die Anmeldung via SMTP-Auth benötigt.

Hinweis: *Wenn T-Online der Provider ist, kann auf keinen Fall „securesmtp.t-online.de“, „smtpmail.t-online.de“ oder der alte „mailto.t-online.de“ verwendet werden, wenn mit einer eigenen Domain gearbeitet wird. Die beiden genannten Mailserver haben die Angewohnheit beim relayen die Absender-Adressen umzuschreiben. Da wird aus „absender@eigenedomain.tld“ dann einfach „T-*

Online-Nr@t-online.de“. Das wäre in vielen Fällen mehr als peinlich. Mit „smtprelay.t-online.de“ bietet T-Online einen weiteren Mailserver an, der diese miese Angewohnheit nicht hat. Wie nicht anders zu erwarten kostet dessen Nutzung allerdings Geld.

***Achtung:** Die folgenden Konfigurationsschritte müssen nur dann vorgenommen werden, wenn Sie Ihrem invis-Server nicht bereits während der Installation mit den entsprechenden Daten versorgt haben. Das invis-Setup-Script **sine2** fragt nach den entsprechenden Daten und nimmt die Konfiguration automatisch vor.*

Zunächst muss in der Datei „/etc/postfix/main.cf“ der zu verwendende Relay-Server nebst zu verwendetem Protokoll (SMTP: Port 25 oder Submission: Port 587) eingetragen werden. Diese Einstellung ist bereits vorbereitet. Suchen Sie in der Datei einfach nach „*relayhost*“:

```
#relayhost = $mydomain
#relayhost = [gateway.my.domain]
relayhost = [mail.example.de]:587
#relayhost = uucphost
#relayhost = [an.ip.add.ress]
```

Tragen Sie an dieser Stelle einfach den vollen Namen des für Sie zuständigen Postausgangsserver ein. Ist der Postausgangsserver bekannt gemacht, muss Postfix noch Zugangsdaten bekommen um sich an diesem als berechtigter Nutzer anmelden zu können. Tragen Sie dazu in der Datei „/etc/postfix/sasl_passwd“ die Zugangsdaten in folgender Form ein:

```
[mail.example.de]:587             benutzername:passwort
```

Als Zugangsdaten werden einfach Benutzername und Passwort eines beim Provider angelegten Mail-Kontos verwendet.

Sind alle Einträge vorgenommen, müssen Sie zunächst die SASL-Passwort-Datei in eine für Postfix lesbare Form umwandeln. Dabei hilft das Kommando ***postmap***:

```
Kommandozeile: postmap /etc/postfix/sasl_passwd
```

Abschließend müssen wir Postfix noch dazu bewegen seine Konfiguration neu einzulesen:

```
Kommandozeile: postfix reload
```

Danach steht dem Mailversand über Ihren invis-Server nichts mehr im Wege. Aus Sicht Ihrer Clients ist der invis-Server der zu verwendende Postausgangsserver. Konfigurieren Sie Ihre Mailclients entsprechend. Im lokalen Netzwerk verlangt der invis-Server derzeit beim Mailversand weder Verschlüsselung noch die Authentifizierung mit Benutzernamen und Passwort.

openVPN Starten/Stoppen/Neustarten

Mit Einführung des Systemd lässt sich openVPN nicht mehr pauschal mittels „***rcopenvpn***“ starten/stoppen/neustarten. Statt dessen müssen jetzt mittels ***systemctl*** alle vorhandenen openVPN Konfigurationen einzeln verwaltet werden. Für die mittels ***sine2*** vorbereite openVPN Verbindung sieht

dies wie folgt aus:

```
linux:~ # systemctl {start|stop|restart} openvpn@invis-server.service
```

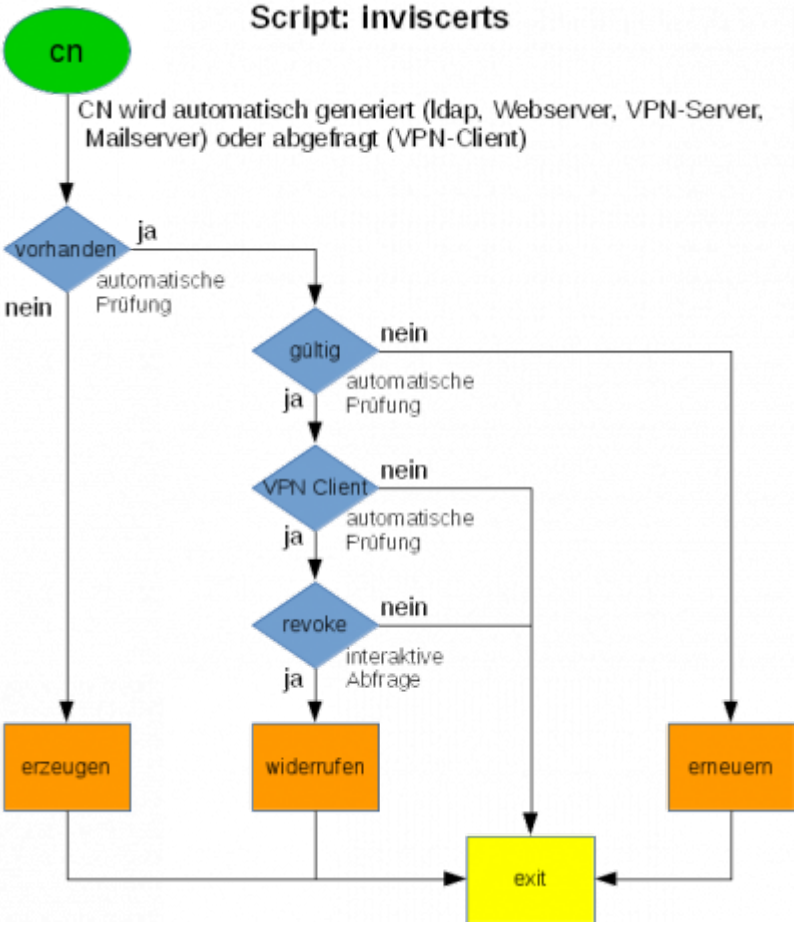
Verwaltung von Schlüsseln und Zertifikaten

Einige Dienste Ihres Servers sind aus Sicherheitsgründen auch oder ausschließlich verschlüsselt erreichbar. Darunter der LDAP-Dienst des Active-Directory, die Mailserver-Funktionen sowie die Webserver-vHosts für Portal, z-Push oder ownCloud, so diese via Internet angesprochen werden.

invis-Server verfügen dafür über eine eigene Zertifizierungsstelle (Certification Authority / CA). Mit dieser CA werden alle Zertifikate des Servers signiert. Ab invis-Server 12.1 besteht die Möglichkeit, das für den externen Zugriff auf den invis-Server notwendige Zertifikat auch via Let's Encrypt zu beziehen.

interne Zertifikatsverwaltung

Ab invisAD Version 11.0 werden alle Server- und Client-Zertifikate mittels der Software **easy-rsa** mit einer einzigen CA verwaltet. Damit unterscheidet sich Version 11.0 von Ihren Vorgängern, in denen zwei CAs, eine für das System selbst und eine für den VPN-Dienst vorhanden waren.



Physikalisch liegt die CA im Verzeichnis

```
/etc/easy-rsa/interne-domain.tld
```

. Zur Verwaltung aller Schlüssel und Zertifikate verfügen invis-Server über das Script ***inviscerts***.

inviscerts verfügt über folgende Funktionen:

- Erzeugen und Verlängern des LDAP-Server Zertifikats.
- Erzeugen und Verlängern des Zertifikats für externen Zugriff. Für den Fall, dass für externe Zugriffe nicht mit Let's Encrypt Zertifikaten gearbeitet wird, wird das so erzeugte „Extern-Zertifikat“ sowohl vom Apache-Webserver für Portal-Zugriff, z-Push und ownCloud, sowie dem openCPN-Server genutzt.
- Erzeugen und Verlängern des Mailserver-Zertifikates.
- Erzeugen, Sperren und Verlängern von VPN-Client-Zertifikaten.
- Aktualisieren der Certificate Revocation List (CRL)

Nebenstehend erläutert ein Ablaufdiagramm die Funktionsweise des Scripts.

Die voreingestellten Lebensdauern der Server- und Client-Zertifikate beträgt 730 Tage, also 2 Jahre. Die Lebensdauer der CA selbst liegt bei 10 Jahren. Ändern lässt sich dies in:

```
/etc/easy-rsa/vars
```

Notwendig ist das aber nicht.

Die Anwendung des Scripts ist denkbar einfach:

```
linux:~ # inviscerts [ms|intern|extern|vpn|crl]
```

Sie benötigen in jedem Fall das Passwort der Zertifizierungsstelle.

Die Optionen im Einzelnen:

- **ms** - Internes Mailserver-Zertifikat, wird ausgestellt auf den Namen mail.ihre-domain.tld
- **intern** - Zertifikat für den verschlüsselten Zugriff auf das invis-Portal und lokale Webapplikationen. Wird auf den lokalen Hostnamen des invis-Servers ausgestellt.
- **extern** - Zertifikat für den Zugriff via Internet, gilt sowohl für das invis-Portal, ActiveSync, Kopano-Webapp, ownCloud und OpenVPN. Wird auf den im Internet gültigen DDNS Namen des invis-Servers ausgestellt.
- **vpn** - Erstellt OpenVPN Client-Zertifikate. Hier wird als „Common Name“ des Zertifikats der Hostname des Client-Computers erstellt. Alternativ ist auch „vorname.zuname“ des Anwenders möglich.
- **crl** - Aktualisiert die „Certificate Revocation List“. Dies ist wichtig, damit speziell OpenVPN keine zurückgezogenen Zertifikate mehr akzeptiert.

Ohne Option aufgerufen gibt ***inviscerts*** einfach nur eine kurze Hilfe für dessen Verwendung aus.

Werden mit ***inviscerts*** VPN-Client-Zertifikate erzeugt, so werden Zertifikat und privater Schlüssel in einer Passwort-geschützten PKCS-12 Datei verpackt. ***inviscerts*** fordert Sie zur Eingabe eines solchen Passwortes auf. Bedenken Sie dass eine solche Datei ungehinderten Zugang zu Ihrem Server ermöglicht, nutzen Sie also bitte sichere Passwörter.

Selbstsignierte Zertifikate, auch wenn die Signatur über eine eigene CA erfolgte, erzeugen auf Client-Seite (zunächst) immer eine Sicherheitswarnung. Diese Warnungen, etwa wenn sie in einem Browser

auftauchen, verunsichern Anwender erfahrungsgemäß. Um Sie zu verhindern muss das Stammzertifikat der Zertifizierungsstelle in den Client integriert werden. Für diesen Zweck halten invis-Server das Zertifikat zum Download im invis-Portal (unten rechts) vor.

Unter Windows muss ein solches Stammzertifikat mit dem Zertifikatsmanager importiert werden, damit steht es allen Microsoft-Produkten zur Verfügung, nicht aber Software von Drittherstellern wie etwa Mozilla Firefox. Dieser und andere Produkte verfügen über eine eigene Zertifikatsverwaltung in die das Stammzertifikat importiert werden muss.

Weiterhin gibt das invis-Portal auf der Status-Seite auch Auskunft darüber, wie lange die vom Server genutzten Zertifikate noch gültig sind. Nichts ist ärgerlicher als **überraschend** abgelaufene Zertifikate, da man in einem solchen Fall Gefahr läuft viel Zeit in die Suche von Fehlern zu investieren, die gar nicht existieren.

Weitere Informationen zum Umgang mit easyRSA sind im deutschsprachigen Wiki von OpenVPN zu finden: OpenVPN Wiki

Individuelle Zertifikate

Werden weitere individuelle Server- oder Client-Zertifikate, so ist dies direkt mit dem Kommando `easy-rsa` möglich.

Hinweis: *Dabei ist zu beachten, dass Googles Chrome-Browser inzwischen verlangt, dass Server-Zertifikate das Attribut SubjectAltNames enthalten. Ohne dieses Attribut erfolgt immer eine Zertifikatswarnung.*

Ein Beispiel für ein Server-Zertifikat:

```
invis:~ # easyrsa --subject-alt-name="DNS:host.example.loc" build-server-full host.example.loc nopass
```

Die Option „nopass“ am Ende des Kommandos sorgt dafür, dass der private Schlüssel seinerseits nicht mit einem Passwort verschlüsselt wird. Im Falle von Server-Zertifikaten erleichtert das den Umgang damit, da dem Server-Dienst ansonsten immer das Passwort mitgegeben werden müsste. Bei vielen Diensten ist dies gar nicht möglich.

Beispiel für ein Client-Zertifikat:

```
invis:~ # easyrsa --subject-alt-name="DNS:host.pe.loc" build-client-full host.pe.loc nopass
```

Zum Erstellen von Zertifikaten wird immer das Passwort des privaten CA-Schlüssels benötigt.

Neue Zertifikate werden in:

```
/etc/easy-rsa/example.loc/issued
```

und die zugehörigen privaten Schlüssel in:

```
/etc/easy-rsa/example.loc/private
```

abgelegt.

PKCS#12

Werden Schlüsselpaare in PKCS12-Containerformat benötigt, können diese nach Erstellung der Schlüsselpaare als solche exportiert werden:

```
invis:~ # easyrsa export-p12 host.example.loc
```

Dabei fragt das Kommando nach einem Export-Passwort. Soll die p12-Datei nicht Passwort-verschlüsselt werden, kann die Passworteingabe durch einfaches Drücken der Enter-Taste quittiert werden.

Zu finden sind die erstellten p12-Dateien in:

```
/etc/easy-rsa/example.loc/private
```

Öffentlichen Schlüssel extrahieren

```
server14:~ # openssl x509 -in hostname.crt -noout -pubkey > hostname-public.pem
```

Zertifikate von Let's Encrypt (ab invis Version 12.1)

Wir unterscheiden hier generell zwischen Zertifikaten die nur innerhalb des vom invis-Server verwalteten Netzes eine Rolle spielen und solchen die beim Server Zugriff via Internet relevant sind. Lediglich für letzteres besteht die Möglichkeit mit einem Zertifikat von **Let's Encrypt** zu arbeiten. Für die internen Zwecke müssten Zertifikate für eine im Internet nicht gültige Fantasie-Domain generiert werden, was die Let's Encrypt Verfahrensweise schlicht nicht zulässt. Dafür ist es einfach nicht gedacht.

Hintergrund: *Sinn und Zweck der Nutzung von Let's Encrypt Zertifikaten ist es natürlich beim Server-Zugriff via Internet nicht mit verunsichernden Sicherheitswarnungen bezüglich ungültiger Zertifikate belästigt zu werden. Sicherlich ist es bei einem überschaubaren Nutzerkreis möglich auf allen beteiligten Geräten zunächst das Stammzertifikat des invis-Servers zu installieren um solche Warnungen zu umgehen. Schwieriger ist das schon, wenn Links für per ownCloud geteilte Dateien an externe Dritte versendet werden. Den Empfängern solcher Links deren Unbedenklichkeit glaubhaft zu vermitteln liegt irgendwo zwischen „nicht einfach“ und „unmöglich“.*

Für folgende Dienste des Servers sind die Let's Encrypt Zertifikate gedacht:

- Zugriff auf das invis-Portal
- Zugriff auf ownCloud
- Nutzung von ActiveSync

Da alle drei Funktionen ausschließlich HTTPs nutzen, spielt sich die wesentliche Konfiguration im Apache Webserver ab und wird bereits beim Setup des invis-Servers vorbereitet.

In den vHost-Konfigurationen aller drei Funktionen befindet eine wie folgt aussehende Passage:

```
<IfDefine LETSENCRYPT>
```

```
#   You can use per vhost certificates if SNI is supported.
    SSLCertificateFile /etc/dehydrated/certs/your.ddns-name.de/cert.pem
    SSLCertificateKeyFile /etc/dehydrated/certs/your.ddns-
name.de/privkey.pem
    SSLCertificateChainFile /etc/dehydrated/certs/your.ddns-
name.de/chain.pem
</IfDefine>

<IfDefine OWNCERTS>
    SSLCertificateFile /etc/apache2/ssl.crt/invis-server.crt
    SSLCertificateKeyFile /etc/apache2/ssl.key/invis-server.key
</IfDefine>
```

Dabei handelt es sich um zwei konkurrierende Konfigurationen die jeweils über ein Apache Server Flag aktiviert werden können **(ja ich weiss, man müsste das Setup noch davor schützen, dass jemand versucht beide Flags gleichzeitig zu setzen, aber wer das macht ist selbst schuld!)**.

Die Pfade zu den Let's Encrypt Dateien sind natürlich individuell, abhängig vom Namen des Servers, Sie werden aber automatisch angepasst.

Die Umschaltung zwischen beiden Setup funktioniert wie folgt:

```
invis:~ # ae2nflag -d OWNCERTS
invis:~ # a2enflag LETSENCRYPT
invis:~ # systemctl restart apache2.service
```

Achtung: *Beim Aktivieren oder deaktivieren von Apache Server-Flags muss ein Neustart erfolgen, ein Reload genügt nicht!*

Weiterhin wurde ein zusätzlicher vHost eingerichtet, der das Let's Encrypt Challenge-Verzeichnis beherbergt. Dieses Verzeichnis wird verwendet, damit sich der eigene Server als berechtigter Empfänger der Let's Encrypt Zertifikate verifiziert und umgekehrt sich der Zet's Encrypt Server sich gegenüber dem invis-Server authentifiziert.

Dieser vHost ist nach dem Setup des invis Servers bereits aktiv und so konfiguriert, dass er Anfragen auf Port 80, allerdings lediglich auf der externen Netzwerkschnittstelle entgegen nimmt. Damit die Zertifikats Übertragung und das Challenge Verfahren funktionieren **muss** dieser vHost unter dem gültigen DDNS-Namen des Servers via Internet erreichbar sein. Steht der invis-Server hinter einem Router, was der Standard sein dürfte ist am Router ein Portforwarding für Port 80 auf den invis-Server einzurichten.

Nach der Installation des invis-Servers ist das Flag „OWNCERTS“ aktiviert und es werden die von der eigenen CA signierten Zertifikate verwendet.

Um auf Zertifikate von Let's Encrypt umzuschalten bringt der invis-Server mit ***actdehydrated*** ein eigenes Script mit. Es schaltet automatisch mittels der zuvor genannten Server Flags die vHosts von „invis-Portal“, „ownCloud“ und „ActiveSync“ Apache auf das Let's Encrypt Setup um, legt für den DDNS-Namen einen Let's Encrypt Account an und generiert die gewünschten Zertifikate.

Das Script wird **einmalig** (es sei den, es geht etwas schief) ohne weitere Optionen aufgerufen:

```
invis:~ # actdehydrated
```

Danach sollte es beim externen Zugriff auf den invis-Server keine Sicherheitswarnung bezüglich ungültiger Zertifikate mehr geben.

Alles weitere wird dann per Cron-Job erledigt. Let's Encrypt Zertifikate haben nur eine Lebenszeit von 90 Tagen, der eingerichtete Cron-Job erneuert das eigene Zertifikat automatisch.

Achtung: *bei der bis invis-Server Versionen 13.x eingesetzten Version des Let's Encrypt Clients* ***dehydrated*** *funktioniert das automatische Neuladen des abhängigen Dienstes Apache-Webserver nicht. Das resultiert in Zertifikatswarnungen, trotz korrekt aktualisierter Zertifikate. In einem solchen Fall ist einfach der Apache Webserver manuell neu zu laden:*

```
invis:~ # systemctl reload apache2.service
```

DNS Forwarder anpassen

invis-Server arbeiten als DNS-Server für die eigene lokale Domäne und als Forward-Nameserver für die Namensauflösung im Internet. Für letzteren Zweck nutzt der auf einem invis-Serverlaufende DNS-Dienst ***bind*** seinerseits wieder Forward-Nameserver. Oft werden hierfür beispielsweise die DNS-Server des Internet-Providers oder der vorgeschaltete Router genutzt. Es kann vorkommen, beispielsweise bei einem Provider-Wechsel, dass auf andere DNS-Forwarders umgestellt werden muss.

Hinweis: *Die genutzten DNS-Forwarder werden bereits beim Setup des invis-Servers abgefragt. Ändern müssen Sie daran lediglich etwas, wenn einer der ursprünglich gwählten Server seinen Dienst einstellt.*

Die Einstellungen werden in der Datei

```
/etc/named.conf
```

vorgenommen. Hier können in der folgenden Zeile bis zu drei Nameserver eingetragen werden:

```
...
forwarders { 9.9.9.9; 1.1.1.1; 194.129.25.2; };
...
```

Achten Sie darauf, dass hinter jeder IP-Adresse wie auch am Ende der Zeile ein Semikolon stehen muss. Es können bis zu 3 Adressen angegeben werden.

Danach, genügt es den Nameserver zum auffrischen seiner Konfiguration zu bringen:

Mit systemd

```
linux:~ # systemctl reload named.service
```

Alt

```
linux:~ # /etc/init.d/named reload
```

Hinweis: *Sie sollten sich allerdings Gedanken über die Wahl Ihrer DNS-Forwarder machen. Nehmen wir beispielsweise die DNS-Server von Google (8.8.8.8 & 8.8.4.4), sicher sie sind schnell und mit Ihnen lassen sich DNS-basierte Websperren des eigenen Providers umgehen, allerdings bietet Google solche Dienste sicherlich nicht aus reiner Nächstenliebe an. Mehr zum Thema* ***hier****.*
Es geht auch anders. Die Initiative „Quad9“ (9.9.9.9) stellt ebenfalls schnelle DNS Server kostenfrei zur Verfügung, bei deren Nutzung bleibt die Privatsphäre auf jeden Fall gewahrt. Mehr zum Thema ***hier***
Auch die Fa. Cloudflare bietet unter der Adresse „1.1.1.1“ einen DNS-Resolver an bei dem der Datenschutz priorisiert wird.
Selbstverständlich können sie auch einfach die DNS-Server Ihres Internet-Providers nutzen. ***Es ist Ihre Entscheidung.***

Volumes vergrößern

Wird an irgendeiner Stelle des Servers der Plattenplatz knapp, kann dieser – die Nutzung von LVM vorausgesetzt – zur Laufzeit des Servers erweitert werden.

Schauen Sie immer zunächst nach, wie viel ungenutzer Platz zur Verfügung steht:

```
invis:~ # pvscan
  PV /dev/md0   VG system          lvm2 [21,83 TiB / 10,49 TiB free]
  Total: 1 [21,83 TiB] / in use: 1 [21,83 TiB] / in no VG: 0 [0   ]
```

Im gezeigten Beispiel sind es knapp 10,5TB. Dieser Platz kann nach Bedarf portionsweise auf die verschiedenen Volumes „root“, „home“, „var“ und „srv“ verteilt werden.

Das vergrößern eines Volumes geht wie folgt:

```
invis:~ # lvresize -L +1TB /dev/system/srv
```

Damit wird lediglich das Volume selbst vergrößert, nicht aber das Dateisystem. Dies zu vergrößern ist ein eigener Arbeitsschritt. Dieser ist vom verwendeten Dateisystem ab:

ext4, xfs

```
invis:~ # reseize2fs /dev/system/srv
```

btrfs

Hier wird nicht das Dateisystem angegeben, sondern der Mount-Point. Da wir üblicherweise nur das Root-Dateisystem mit btrfs formatieren, hier der zugehörige Befehl zum Vergrößern:

```
invis:~ # btrfs filesystem resize max /
```

In beiden Fällen, wird automatisch der gesamte zur Verfügung stehende Platz genutzt.

System allgemein

In diesem Abschnitt werden Themen der Server-Administration beschrieben, die nicht direkt die invis-Server Funktionen, sondern das System allgemein betreffen und aus unserer Sicht für den Umgang mit dem invis-Server von Bedeutung sein könnten.

System-Protokolle

Mit der Einführung des *systemd* unter openSUSE Linux wurde auch dessen System-Protokolldienst ***journald*** eingeführt. Seit openSUSE 42.1 ersetzt dieser den alten Syslog-Dienst vollständig. Neben einigen praktischen Eigenschaften verfügt Journald aber auch über ein paar echte Ärgernisse.

Eines davon, ist seine Langsamkeit beim Umgang mit dem Systemprotokoll. Seitens openSUSE wurde die maximale Größe des Protokolls auf 4GB beschränkt. Aber auch 4GB verlangen dem Admin einiges an Geduld ab, wenn er beispielsweise vom Anfang des Protokolls direkt ans Ende springen möchte. Auch die Ausgabe der Status-Abfragen bei System-Diensten mit ***systemctl*** werden mit einem 4GB großen Protokoll unangenehm langsam.

Wir empfehlen daher das Protokoll auf einen kleineren Wert zu beschränken.

Dazu ist in der Datei

```
/etc/systemd/journald.conf
```

der folgende Wert auf eine vernünftige Größe zu ändern:

```
...
SystemMaxUse=1000M
...
```

In der Vorgabe ist diese Option auskommentiert. Auch mit einem auf 1GB reduzierten Journal wird aus dem Journald kein Rennpferd, die Wartezeiten verkürzen sich jedoch deutlich. (Schade eigentlich, von einem binären Datenformat hätte ich mehr erwartet.…)

Nachdem der Wert gesetzt wurde muss der Journal-Daemon noch neu gestartet werden.

```
invis:~ # systemctl restart systemd-journald.service
```

Jeder Admin muss für sich selbst entscheiden, wie weit seine Protokolle zurückreichen sollen. Die voreingestellten 4G decken auf unserem Server einen Zeitraum von ca. 2 bis 3 Monaten ab. Das mag im einzelnen unterschiedlich sein, mehr als ein bis 2 Monate sollten aber eigentlich zur Fehlersuche nicht notwendig sein. Auch in Sachen Datenschutz macht es Sinn das Protokoll zu reduzieren, schließlich können Systemprotokolle auch Daten aus denen sich ein Personenbezug herstellen lässt enthalten. Solche Daten dürfen ohnehin nicht bzw. nur zur Fehlersuche gespeichert werden. Auch bei personenbezogenen Daten die zur Fehlersuche gespeichert wurden besteht eine Löschpflicht, ist doch schön, wenn unser Server dem selbständig nachkommt.

Das Protokoll lässt sich auch manuell verkleinern:

```
invis:~ # journalctl --vacuum-size=1000M
```

...und mit folgendem Befehl lässt sich abfragen wie viel Platz das Systemprotokoll aktuell belegt:

```
invis:~ # journalctl --disk-usage
```

VirtualBox Erweiterungspack

VirtualBox wird auf invis-Servern automatisch mit einem Open-Source Erweiterungspack installiert. Teil der Funktionen dieses Erweiterungspacks ist der Zugriff auf virtuelle Maschinen via VNC. VNC läuft leider nicht immer frei von Problemen. Um statt dessen das offizielle Erweiterungspaket von Oracle nutzen möchte muss dieses zunächst installiert werden. ***Beachten Sie dabei bitte dessen Lizenzbedingungen***.

Laden Sie es zunächst passend zur installierten VirtualBox Version von http://download.virtualbox.org/virtualbox/ herunter. Die Installation erfolgt auf der Kommandozeile des Servers:

```
invis:~ # VBoxManage extpack install --replace
Oracle_VM_VirtualBox_Extension_Pack-7.0.18.vbox-extpack
```

Danach muss die Fernsteuerung der Maschinen auf das in diesem Erweiterungspack integrierten RDP-Server umgeschaltet werden:

```
invis:~ # VBoxManage setproperty vrdeextpack "Oracle VM VirtualBox Extension
Pack"
```

Jetzt können Sie in phpVirtualBox die Fernsteuerung der virtuellen Maschinen via RDP konfigurieren.

Router Tausch

Wird der Router für den Internetzugangs getauscht, hat das auch Auswirkungen auf den invis-Server. Klar sollte sein, dass beim neuen Router wieder die für den invis-Server erforderlichen Portweiterleitungen eingerichtet werden (80/TCP, 443/TCP, 1194/UDP sowie die verschobenen Ports für HTTPs Zugriff aufs invis-Portal und den SSH-Zugriff (beides TCP)). Die beiden verschobenen Ports können Sie den Dateien

```
/etc/ssh/sshd_conf
```

und

```
/etc/apache2/listen.conf
```

entnehmen.

So Ihr invis-Server seine externe IP-Adresse per DHCP vom Router erhält sorgen Sie dafür, dass er für seine IP-Adresse im Router eine feste Reservierung erhält.

Für den nicht unwahrscheinlichen Fall, dass Ihr invis-Server nach dem Router-Tausch eine neue IP-Adresse erhält, müssen Sie diese in die Apache-Konfiguration für die Erneuerung der Let's Encrypt Zertifikate eintragen.

Zu finden ist die anzupassende Stelle der Konfiguration in:

```
/etc/apache2/vhosts.d/vh-dehydrated.conf
```

Tragen Sie dort im VirtualHost-Tag die neue IP-Adresse ein und starten Sie den Webserver neu.

```
# Alias definition for dehytrated wellknown output directory for challenge-
hooks
# Stefan Schaefer - stefan@invis-server.org

<Virtualhost 192.168.178.21:80>
    ServerName dhxxx.example.de
    DocumentRoot /srv/www/htdocs/dehydrated
...
```

```
invis:~ # systemctl restart apache2.service
```