NethServer Documentation

Release 6.7

Nethesis

19.09.2022

Inhaltsverzeichnis

1 Release notes 6.7 **3**

2 Installation **5**
2.1 Zugriff auf die Management-Oberfläche 5

3 Configuration **7**
3.1 Basis System 7

4 Modules **13**
4.1 Backup 13
4.2 Benutzer und Gruppen 18
4.3 Chat 22
4.4 Fax server 23
4.5 Web Inhaltsfilter 25
4.6 Firewall und Gateway 27
4.7 Bandbreiten Überwachung (ntopng) 33
4.8 DNS 33
4.9 DHCP und PXE Server 34
4.10 WebVirtMgr 36
4.11 Adagios 37
4.12 OCS Inventory NG 37

5 Best practices **39**

6 Appendix **41**

7 Indices **43**

Stichwortverzeichnis **45**

Official site: www.nethserver.org

KAPITEL 1

Release notes 6.7

KAPITEL 2

Installation

2.1 Zugriff auf die Management-Oberfläche

NethServer kann mit Hilfe der *Server Manager* Weboberfläche konfiguriert werden. Man benötigt einen Browser, wie den Mozilla Firefox oder Google Chrome um auf die Weboberfläche zugreifen zu können. Die Adresse (URL) lautet: `https://a.b.c.d:980` oder `https://server_name:980` wobei *a.b.c.d* und *server_name* die IP-Adresse bzw. der Name des Servers sind, die bei der Installation vergeben wurden.

Falls das Webserver-Modul installiert ist, kann auch über die Adresse `https://server_name/server-manager` auf die Weboberfläche zugegriffen werden.

Die Konfigurationsoberfläche verwendet ein selbst-signiertes SSL-Zertifikat. Es muss bei der ersten Benutzung explizit akzeptiert werden. Die Verbindung ist dann verschlüsselt und damit sicher.

2.1.1 Anmeldung (Login)

Nach dem Ausfüllen des Anmeldedialogs kann der Zugriff auf die Konfigurationsoberfläche erfolgen. Die erste Anmeldung ist mit folgenden Benutzerdaten möglich:

- Default Benutzer name: **root**
- Default password: **Nethesis,1234**

2.1.2 Warnung

Das Kennwort des Benutzers root sollte so bald wie möglich geändert werden. Für ein möglichst sicheres Kennwort ist eine zufällige Zeichenkette sinnvoll, die aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen

besteht.

Falls der Dateiserver, Mailserver oder ein anderes Modul installiert wurde, das auf dem Benutzer- und Gruppenmodul basiert, so kann der `admin` Benutzer mit dem gleichen Kennwort und den gleichen Rechten auf die Konfigurationsoberfläche zugreifen wie `root` (siehe *Admin Benutzer* für Details).

KAPITEL 3

Configuration

3.1 Basis System

Dieses Kapitel enthält eine Beschreibung aller Module, die am Ende der Installation verfügbar sind. Alle weiteren, hier nicht genannten Module Müssen über das Paket-Management package_manager-section installiert werden (einschließlich backup und Benutzerunterstützung).

3.1.1 Übersicht

Die Übersicht Seite ist die Startseite nach einer erfolgreichen Anmeldung.. Hier ist der Status status und die Konfiguration des Systems ersichtlich.

Festplattennutzung

Das Werkzeug Festplattennutzung macht die Belegung der Festplatte optisch erkennbar . Ein einfach bedienbares Diagramm ermöglicht durch Klick und Doppelklick eine Navigation in der Ordnerstruktur.

Nach dem Ende der Installation kann man im Bereich *Fetplattennutzung* der *Übersicht* den Punkt *Update* auswählen um eine Katalogisierung des Verzeichnisbaums auszulösen und im Anschluss das Diagramm anzeigen zu lassen. Je nach Datenmenge kann dies mehrere Minuten dauern.

Bekannte Verzeichnisse sind:

- Freigegebene Verzeichnisse: `/var/lib/nethserver/ibay`
- Benutzerhomes: `/var/lib/nethserver/home`
- Windows roaming profiles: `/var/lib/nethserver/profile`
- Mail: `/var/lib/nethserver/vmail`
- Faxes: `/var/lib/nethserver/fax`
- MySQL Datenbanken: `/var/lib/mysql`

3.1.2 Netzwerk

Die Seite *Netzwerk* legt fest, wie der Server mit dem lokalen Netzwerk (LAN) und anderen Netzen (z.B. Internet) verbunden ist.

Falls der Server als Firewall und Gateway arbeitet, so wird er spezielle Netze verwalten, wie zum Beispiel eine DMZ (Entmilitarisierte Zone) und ein Gästenetz.

NethServer unterstützt eine belibige Anzahl von Netzwerkkarten. Jedes Netzwerk muss folgenden Anforderungen genügen:

- Netzwerke müssen physikalisch getrennt sein (keine verbindung mit dem gleichen Switch/Hub)
- Netzwerke müssen logisch getrennt sein (unterschiedliche Adressbereiche)
- Private Netzwerke (wie LANs) müssen den Adresskonventionen nach RFC1918 folgen. Siehe *Addressen für private Netzwerke (RFC1918)*

Jede Netzwerkkarte hat eine bestimmte *Rolle* (Funktion), die ihr Verhalten festlegt. Die Rolle wird durch eine Farbkodierung beschrieben, die einer Zone mit bestimmten Regeln gehört:

- *grün*: Lokales Netzwerk. Rechner in diesem Netz können auf alle anderen Netze zugreifen.
- *blau*: Gast Netzwerk. Rechner in diesem Netz können auf das rote und orange Netz zugreifen. Das grüne Netz ist nicht erreichbar.
- *orange*: DMZ Netzwerk. Rechner in diesem Netz können auf das rote Netzwerk zugreifen. Blau, Grün und Orange sind nicht erreichbar.
- *rot*: Öffentliches Netzwerk. Rechner in diesem Netz können nur auf den Server zugreifen.

Siehe *Richtlinien* für weitere INformationen zu Rollen und Firewallregeln.

Bemerkung: Der Server benötigt immer mindestens eine Netzwerkkarte. Wenn nur eine Netzwerkkarte vorhanden ist, muss diese im grünen Netz sein.

Falls der Server auf einem öffentlichen Server (Virtual Private Server) installiert wird, so muss er mit einem grünen Netz konfiguriert werden. Alle kritischen Dienste sollten über die Konfigurationsoberfläche *Netzwerk Dienste* deaktiviert werden.

Alias IPs

Mit Hilfe von Alias IPs können einer Netzwerkkarte mehrere IP-Adressen zugeordnet werden.

Beim typischsten Szenario werden einer roten Netzwerkkarte mehrere Adressen zugeordnet. Dies kann sinnvoll sein, wenn der ISP mehrere Adressen aus dem gleichen Subnet anbietet. Von diesen können dann mehrere (oder alle) an diese Netzwerkkarte gebunden werden. Auf diese Weise kann man individuelle Konfigurationen erstellen (z.B. im Bereich Port-Forwarding).

Der Menüpunkt zum Erstellen eine Alias IP befindet sich im Dropdown Menü der entsprechenden Netzwerkkarte (Erstelle IP Alias).

Logische Metzwerkkarten

Im Bereich *Netzwerk* den Knopf *Neue Schnittstelle* anklicken, um eine logische Netzwerkkarte zu erstellen.

Mögliche logische Netzwerkkarten sind:

- Bond: Zusammenfassen von zwei oder mehr Netzwerkkarten, um Lastausgleich und Fehrertoleranz zu ermöglichen.
- Bridge: Zwei verschiedene Netzwerke verbinden. Wird oft für bridged VPN und virtuelle Maschinen verwendet.
- VLAN (Virtual Local Area Network): Erstellen von zwei oder mehr logisch getrennten Netzwerken auf einer Netzwerkkarte.
- PPPoE (Point-to-Point Protocol over Ethernet): Internetverbindung über ein DSL-Modem

Bonds erlauben die Zusammenfassung von Bandbreite von zwei oder mehr Netzwerkkarten. Das System verwendet alle Netzwerkkarten gleichzeitig und verteilt den Verkehr auf die einzelnen Karten. Beim Auftreten von Fehlern wird die defekte Karte automatisch aus dem **bond** entfernt.

Eine **bridge** dient zur Verbindung zweier verschiedener Netzwerksegmente, zum Beispiel um virtuelle Maschinen zu verbinden oder einem Client via VPN eine Verbindung ins grüne Netz zu ermöglichen.

Wenn eine physikalische Trennung zweier Netze nicht möglich ist, kann ein **tagged VLAN** verwendet werden. Der Datenverkehr der beiden Netze läuft über das gleiche Kabel, wird aber behandelt, als käme er von getennten Netzwerkkarten. Die Verwendung von VLANs erfordert sauber konfigurierte Switche.

Warnung: Die logische **PPPoE** Netzwerkkarte muss dem roten Netz zugeordnet werden, da dies für die Funktion als Gateway benötigt wird. Siehe *Firewall und Gateway* für Details.

Addressen für private Netzwerke (RFC1918)

Private TCP/IP Netzwerke, die nicht direkt mit dem Internet verbunden werden, sollten spezielle Adressbereiche verwenden, die von der IANA (Internet Assigned Numbers Authority) dafür reserviert wurden:

Privates Netzwerk	Subnetmaske	IP Adressbereich
10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 - 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

3.1.3 Netzwerk Dienste

Ein Netzwerkdienst ist ein Dienst, der direkt auf der Firewall läuft.

Diese Dienste sind für alle Rechner im grünen Netz (LAN) erreichbar. Zugriffsrichtlinien können über den Bereich *Netzwerkdienste* geändert werden.

Mögliche Richtlinien sind:

- Zugriff nur aus dem grünen Netz (private): Alle Rechner aus dem grünen Netz und VPN-Clients.
- Zugriff aus grün und rot (public): Jeder Rechner aus grün, VPN-Clients und externe Netzwerke. Zugriffe aus blau (Gäste) und orange (DMZ) sind nicht erlaubt.
- Zugriff nur vom Server (lokal): Kein Rechner kann den Dienst verwenden.

Benutzerdefinierter Zugriff

Wenn die gewählte Richtlinie *private* oder *public* ist, so kann man Rechner oder Netzwerke hinzufügen, denen der Zugriff immer erlaubt (verboten) ist, indem man *Erlaubte hosts* oder *Deny hosts* wählt. Diese Regeln gelten auch für das blaue und orange Netz.

Beispiel

Gegeben ist folgende Konfiguration:

- Oranges Netz: 192.168.2.0/24
- Zugriff auf NTP Dienst ist *privat*

Wenn Rechner aus der DMZ auf den NTP Dienst zugreifen müssen, so fügt man das 192.168.2.0/24 Netz im Bereich *Erlaubte Hosts* hinzu.

3.1.4 Vertrauenswürdige Netzwerke

Vertrauenswürdige Netzwerke sind spezielle Netze (local, VPNs oder auch entfernt) denen der Zugriff auf spezielle Dienste des Servers erlaubt wird.

Zum Beispiel können Rechner in vertrauenswürdigen Netzen auf folgende Dienste zugreifen:

- Server Manager
- Freigegebene Verzeichnisse (SAMBA)

Wenn das entfernte Netzwerk über einen Router erreicht wird, so muss in *Statische Route* eine statische Route eingetragen werden.

3.1.5 Statische Route

Auf dieser Seite werden statische Routen erstellt Statische Route, die ein bestimmtes Gateway verwenden. Derartige Routen werden üblicherweise verwendet, um Verbindungen zu privaten Netzen aufzubauen.

Es ist wichtig, dass das Netzwerk in *Vertrauenswürdige Netzwerke* als vertrauenswürdiges Netz eingetragen wird.

3.1.6 Firmenkontaktdaten

Die Felder der *Organisation* Seite liefert die Voreinstellungen für Benutzeraccounts. Der Name der Firme sowie die Adresse werden auch auf der Login-Seite angezeigt.

3.1.7 Server Zertifikate

Die *Server Zertifikate* Seite zeigt das aktuell installierte SSL-Zertifikat, das für alle Systemdienste gültig ist.

Der Knopf *Neues zertifikat* erlaubt die Erstellung eines neuen selbstsignierten SSL-Zertifikat. Wird ein neues Zertifikat erstellt, so werden alle Dienste neu gestartet. Alle Clients müssen dieses Zertifikat dann noch akzeptieren.

Bemerkung: Um Probleme beim Import des Zertifikates in den Internet Explorer zu vermeiden, sollte der *Common Name* (CN) dem FQDN des Servers entsprechen.

Installation eines Benutzerzertifikates

Benutzerzertifikate sollten in den den folgenden (üblichen) Verzeichnissen abgespeichert werden:

- `/etc/pki/tls/certs`: public key

- `/etc/pki/tls/private`: private key

Einstellen der Pfade für den privaten Schlüssel und das Zertifikat

```
db configuration setprop pki CrtFile '/path/to/cert/pem-formatted.crt'
db configuration setprop pki KeyFile '/path/to/private/pem-formatted.key'
```

Man kann auch ein *SSL certificate chain file* verwenden:

```
db configuration setprop pki ChainFile '/path/to/cert/pem-formatted-chain.crt'
```

Informieren der Dienste über das neue Zertifikat:

```
signal-event certificate-update
```

Sicherung eines Benutzerzertifikates

Benutzerzertifikate müssen explizit in das Konfigurationsbackup aufgenommen werden. Dafür müssen die Pfade in `/etc/backup-config.d/custom.include` eingetragen werden.

Wenn das Zertifikat beispielsweise hier zu finden ist `/etc/pki/tls/certs/mycert.crt`, so genügt die Ausführung von

```
echo "/etc/pki/tls/certs/mycert.crt" >> /etc/backup-config.d/custom.include
```

3.1.8 Benutzerkennwort ändern

Alle Benutzer können sich an der Konfigurationsoberfläche anmelden und auf ihr Benutzerprofil zugreifen.

Nach der Anmeldung kann ein Benutzer eine Kennwortädnerung vornehmen und folgende Informationen ändern:

- Name und Vorname
- External Mail-Addresse

Der Benutzer kann auch die vom Administrator voreingestellten Felder ändern:

- Firme
- Bereich
- Addresse
- Stadt

3.1.9 Herunterfahren

der Rechner, auf dem NethServer installiert ist kann von *Herunterfahren* ausgeschaltet oder neu gestartet werden. Man wählt die gewünschte Aktion an und klickt auf den Knopf mit der Aufschrift **Das System herunterfahren**.

Man sollte stets diesen Weg wählen, um den Computer herunterzufahren. Andere Methoden können zu inkonsistenten Daten führen.

3.1.10 Protokoll Betrachter (LogViwer)

Alle Dienste schreiben ihr Protokoll (Log) in die Dateien (*logs*).

Die Protokoll Analyse ist das Hauptwerkzeug um Probleme zu finden und zu lösen. Das Werkzeug findet man unter *Log viewer*.

Dieses Modul erlaubt:

- Alle Logs durchsuchen
- Eine einzelne Datei durchsuchen
- Die Einträge in eine Logdatei in Echtzeit verfolgen

3.1.11 Datum und Zeit

Nach der Installation ist es wichtig, dass sich der Server in der richtigen Zeitzone befindet. Die Uhrzeit des Rechners kann manuell oder automatisch via NTP (bevorzugt) eingestellt werden.

Die Uhrzeit des Rechners ist für viele Protokolleinträge wichtig. Um Probleme zu vermeiden, sollten alle Rechner im LAN den Server als NTP-Server verwenden.

3.1.12 Inline Hilfe

Alle Programme im Server Manager enthalten eine inline help. Sie erklärt wie das Modul arbeitet und welche Optionen es besitzt.

Diese Hilfeseiten sind in allen Sprachen des Server Managers verfügbar.

Eine Liste aller verfügbaren Hilfeseitenfindet man unter

```
https://<server>:980/<language>/Help
```

Beispiel

Wenn der Server die Adresse `192.168.1.2` besitzt, so erhält man alle englischen Hilfeseiten durch

```
https://192.168.1.2:980/en/Help
```

KAPITEL 4

Modules

4.1 Backup

Backup ist der einzige Weg NethServer im Fehlerfall wiederherzustellen. NethServer kennt zwei Arten von :index:‘Sicherung‘en:

- Konfigurationssicherung
- Datensicherung

Die Konfigurationssicherung sichert nur die Konfigurationsdaten von NethServer. Diese Art der Sicherung wird jede Nacht ausgeführt und erstellt ein neues Archiv, `/var/lib/nethserver/backup/backup-config.tar.xz`, falls sich die Konfiguration in den letzten 24 Stunden geändert hat. Die Konfigurationssicherung sichert außerdem eine Liste der installierten Module. Alle Module werden bei einer Rücksicherung wieder installiert. Dieses Backupverfahren wird genutzt um im Falle des Fehlerfalls NethServer schnellstmögoich wiederhergestellt werden kann. Nachdem die Konfiguration aus dem Backup zurückgesichert wurde, kann die Datenrücksicherung durchgeführt werden, auch wenn NethServer bereits in Betrieb ist.

Die Datensicherung wird aktiviert, indem das „Backup“-Mdoul installiert wird. Die Datensicherung enthält alle Daten wie die Home-Ordner der Benutzer sowie deren E-Mails. Die Datensicherung wird jede Nacht ausgeführt und kann inkrementell oder vollständig in einem wöchentlichen Intervall durchgeführt werden. Die Datensicherung enthält ebenfalls die Daten aus der Konfigurationssicherung.

Das Backup kann an drei verschiedene Orte gesichert werden:

- USB: Eine USB-Laufwerk, dass an einem USB-Port von NethServer angeschlossen ist (Siehe: *USB-Laufwerk konfigurieren*)
- CIFS: Windows Netzwerkfreigaben (z.B. durch einen Server, PC oder NAS)
- NFS: Linux Netzwerkfreigaben, (z.B. durch einen Server, PC oder NAS; in der Regel schneller als CIFS)

Das Ergebniss einer Sicherung kann an den Administrator oder an eine E-Mail-Adresse gesendet werden.

Hinweis: Das Zielverzeichniss basiert auf dem Zielservernamen: Sollte der FQDN des Zielservers sich ändern, muss

dieser auch im Backup angepasst werden.

4.1.1 Rücksicherung

Zunächst muss sichergestellt sein, dass das Sicherungsmedium angeschlossen oder erreichbar ist.

Befehlszeile

Dateien anzeigen

Mit diesem Befehl lassen sich alle Dateien anzeigen, die in einem Backup enthalten sind:

```
backup-data-list
```

Die Ausführung des Befehls kann, abhängig von der Backupgröße, einige Zeit in Anspruch nehmen.

Dateien und Ordner

Alle relevanten Dateien sind im Verzeichniss `/var/lib/nethserver/` zu finden:

- E-Mails: `/var/lib/nethserver/vmail/<user>`
- Netzwerkfreigaben: `/var/lib/nethserver/ibay/<name>`
- Home-Verzeichnisse: `/var/lib/nethserver/home/<user>`

Zum Wiederherstellen einer Datei oder eines Ordners ist folgender Befehl zu verwenden:

```
restore-file <position> <file>
```

Beispiel: Den E-Mail-Account „franz“ nach `/tmp` wiederherstellen:

```
restore-file /tmp /var/lib/nethserver/vmail/franz
```

Beispiel: Den E-Mail-Account „franz“ im Original wiederherstellen:

```
restore-file / /var/lib/nethserver/vmail/franz
```

NethServer kann auch alte Versionen von Ordnern und Dateien wiederherstellen.

Beispiel: Eine Version der Datei „myfile“ von vor 15 Tagen nach /tmp wiederherstellen:

```
restore-file -t 15D /tmp "/var/lib/nethserver/ibay/test/myfile"
```

Der Parameter `-t` gibt die Anzahl an Tagen an, die seit dem Backup vergangen sein sollen.

Grafische Oberfläche

Unter dem Menüpunkt *Wiederherstellen* kann nach Backups gesucht werden. Eine Wiederherstellung von Daten aus einem Backup kann über die Oberfläche durchgeführt werden

Es gibt zwei Möglichkeiten der Wiederherstellung:

- Wiederherstellen der Daten in den ursprünglichen Pfad. Vorhandene Daten werden mit den Daten aus dem Backup überschrieben.
- Wiederherstellen der Daten in den ursprünglichen Pfad. Wiederhergestellte Daten werden jedoch in einen neuen Ordner zurückgesichert. Dieser lautet:

```
/complete/path/of/file_YYYY-MM-DD (YYYY-MM-DD ist das Datum der Wiederherstellung)
```

Um das Suchfeld zu nutzen, mpssen mindestens 3 Zeichen eingegeben werden. Die Suche startet dann automatisch und markiert die übereinstimmenden Daten.

Über die Schaltfläche **Wiederherstellen** können die Daten wiederhergestellt werden.

Hinweis: Mehrere Daten können mittels drücken der Strg-Taste ausgewählt werden.

4.1.2 Rücksicherung im Fehlerfall

NethServer wird in zwei Phasen wiederhergestellt: Zuerst die Konfiguration, anschließend den Daten. Direkt nach der Wiederherstellung der Konfigration ist NethServer wieder verwendbar, sofern alle Module vollständig wieder installiert wurden. Zusätzliche Module können vor oder nach der Wiederherstellung installiert werden. Beispiel: Wenn der E-mail-Server installiert ist, kann NethServer wieder E-Mails senden und empfangen.

Weitere wiederhergestellte Konfigurationen:

- Benutzer und Gruppen
- SSL Zertifikate

Hinweis: Das root- und admin-Passwort wedern nicht wiederhergestellt.

Vorgehensweise zur Wiederherstellung:

1. Installiere eine neue NethServer-Installation mit dem gleichen Hostname wie dem alten
2. Konfiguriere ein Datenbackup, sodass NethServer auf die gesicherten Daten zugreifen kann
3. Wenn die alte (defekte) NethServer-Installation das Netzwerk-Gateway war, nicht vergessen das Firewall-Modul zu installieren.
4. Stelle die Konfiguration aus dem Backup wieder her. *Backup (configuration)* > *Restore* im Servermanager oder führe folgenden Befehl aus: **`restore-config`**
5. Sofern eine Warnung es verlangt, konfiguriere die Zuordnung der Netzwerkrollen erneut. Siehe *Netzwerkrollen wiederherstellen*.
6. Prüfe, ob alle korrekt funktioniert (soweit möglich ohne Daten)
7. Stelle die Datensicherung wieder her. Führe dazu folgenden Befehl aus: **`restore-data`**

Netzwerkrollen wiederherstellen

Wenn eine Konfiguration auf einen fehlenden Netzwerkadapter verweist, erscheint unter *Dashboard*, *Backup (configuration)* > *Restore* und *Network* eine Warnung. Dies passiert zum Beispiel in folgenden Fällen:

- Die Konfiguration wurde auf neuer Hardware wiederhergestellt
- Eine oder mehrere Netzwerkkarten wurde ersetzt

- Die Festplatten wurden in einem neuen System wieder eingebaut

Durch das Anklicken der Warnung erfolgt eine Weiterleitung zur Liste der vorhandenen Netzwerkadapter. Dort sind die Adapter markiert, welche keine Zugewiesene *role* haben. Diese Adapter haben ein Dropdown-Menü, in dem eine Rolle für die Wiederherstellung ausgewählt werden kann.

Beispiel: Wenn die Karte mit der Rolle *orange* ersetzt wurde, so zeigt das Dropdown-Menü eine Liste mit dem Eintrag `orange` bei dem Netzwerkadapter an.

Das gleiche geschieht, wenn der alte Netzwerkadapter ein Teil eines logischen Adapters war (z.B. Bridge oder Bond).

Beim Auswählen eines Eintrags aus dem Dropdown-Menü wird die alte Rolle auf den neuen Adapter übertragen.

Zum Übernehmen muss auf die Schaltfläche *Übernehmen* geklickt werden.

Achtung: Die Neuzuordnung muss vor dem Übernehmen gründlich geprüft werden! Ein Fehler kann dazu führen, dass der NethServer nicht mehr erreichbar sein wird und vom Netzwerk isoliert ist!

Wenn die fehlende Rolle `GRÜN` ist, so fragt beim Starten von NethServer eine interaktive Prozedur danach, ob das Problem gelöst werden soll. Dies ist nötig um wieder eine Verbindung zum NethServer herstellen zu können und die weitere Verwaltung über den Servermanager zu tätigen.

Installierte Module wiederherstellen

Standardmäßig werden beim Wiederherstellen der Konfigurationsdaten auch die vorher installierten Module installiert.

Um dieses Verhalten zu unterbinden, muss dieser Befehl vor der Wiederherstellung ausgeführt werden:

```
config setprop backup-config reinstall disabled
```

4.1.3 Datensicherung anpassen

Wenn weitere Software installiert wurde, kann ein Administrator die Liste der Dateien und Ordner anpassen, die ein- oder ausgeschlossen werden sollen.

Einschließen

Wenn eine Datei oder ein Verzeichniss aus dem Datenbackup ausgeschlossen werden soll, muss eine Zeile in diese Datei eingefügt werden: `/etc/backup-data.d/custom.include`.

Beispiel: Um eine installierte Software zu sichern, die unter `/opt/mysoftware` installiert wurde, muss diese Zeile hinzugefügt werden:

```
/opt/mysoftware
```

Ausschließen

Wenn eine Datei oder ein Verzeichniss aus der Sicherung ausgeschlossen werden soll, dann muss eine Zeile in diese Datei eingefügt werden: `/etc/backup-data.d/custom.exclude`.

Beispiel: Um alle Verzeichnisse, die „Download“ heißen, auzuschließen, muss diese Zeile hinzugefügt werden:

```
**Download**
```

Um das E-Mail-Postfach „test“ aus der Datensicherung auszuschließen, füge diese Zeile hinzu:

```
/var/lib/nethserver/vmail/test/
```

Der gleiche Syntax trifft auch auf die Konfigurationssicherung zu. Änderung müssen jedoch in der Datei `/etc/backup-config.d/custom.exclude` durchgefürht werden.

Hinweis: Stelle sicher, dass keine leeren Zeilen in den editierten Dateien vorhanden sind (auch nicht am Ende!)

4.1.4 Konfigurationssicherung anpassen

In der Regel ist es nicht notwendig, dass an der Konfigurationssicherung anpassung vorgenommen werden müssen. Es kann jedoch in Einzelfällen nützlich sein - zum Beispiel bei eigenen SSL-Zertifikaten. In diesem Fall sollten die Dateien, die die Zertifikate enthalten, in die Liste der zu sichernden Dateien aufgenommen werden.

Einschließen

Wenn eine Datei oder ein Verzeichniss aus dem Datenbackup ausgeschlossen werden soll, muss eine Zeile in diese Datei eingefügt werden: `/etc/backup-config.d/custom.include`.

Beispiel: Um die Datei `/etc/pki/mycert.pem` zu sichern, füge folgende Zeile hinzu:

    /etc/pki/mycert.pem

In die Konfigurationssicherung gehören keine großen Datenmengen! Die Konfigurationssicherung enthält ausschließlich Daten, die zur Neukonfiguration von NethServer notwendig sind! Daten (z.B. Freigaben und E-Mails-Postfächer) gehören in die Datensicherung!

Ausschließen

Wenn eine Datei oder ein Verzeichniss aus der Sicherung ausgeschlossen werden soll, dann muss eine Zeile in diese Datei eingefügt werden: `/etc/backup-config.d/custom.exclude`.

Hinweis: Stelle sicher, dass keine leeren Zeilen in den editierten Dateien vorhanden sind (auch nicht am Ende!) Der Syntax der Konfigurationsssicherung erlaubt nur einfache Datei- und Ordnernamen.

4.1.5 USB-Laufwerk konfigurieren

Das geeignetste Dateisystem für USB-Laufwerke ist EXT3. FAT-Dateisysteme sind möglich aber nicht empfohlen. NTFS-Dateisysteme sind nicht unterstützt.

Vor dem Formatieren des USB-Laufwerks muss dieses an den Server angeschlossen werden. Anschließend muss der Gerätename ermittelt werden:

```
# dmesg | tail -20

Apr 15 16:20:43 mynethserver kernel: usb-storage: device found at 4
Apr 15 16:20:43 mynethserver kernel: usb-storage: waiting for device to settle before␣
↪scanning
Apr 15 16:20:48 mynethserver kernel:   Vendor: WDC WD32  Model: 00BEVT-00ZCT0     Rev:
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
Apr 15 16:20:48 mynethserver kernel:   Type:   Direct-Access           ANSI SCSI␣
↪revision: 02
Apr 15 16:20:49 mynethserver kernel: SCSI device sdc: 625142448 512-byte hdwr sectors␣
↪(320073 MB)
Apr 15 16:20:49 mynethserver kernel: sdc: Write Protect is off
Apr 15 16:20:49 mynethserver kernel: sdc: Mode Sense: 34 00 00 00
Apr 15 16:20:49 mynethserver kernel: sdc: assuming drive cache: write through
Apr 15 16:20:49 mynethserver kernel: SCSI device sdc: 625142448 512-byte hdwr sectors␣
↪(320073 MB)
Apr 15 16:20:49 mynethserver kernel: sdc: Write Protect is off
Apr 15 16:20:49 mynethserver kernel: sdc: Mode Sense: 34 00 00 00
Apr 15 16:20:49 mynethserver kernel: sdc: assuming drive cache: write through
Apr 15 16:20:49 mynethserver kernel:  sdc: sdc1
Apr 15 16:20:49 mynethserver kernel: sd 7:0:0:0: Attached scsi disk sdc
Apr 15 16:20:49 mynethserver kernel: sd 7:0:0:0: Attached scsi generic sg3 type 0
Apr 15 16:20:49 mynethserver kernel: usb-storage: device scan complete
```

Ein anderer hilfreicher Befehl ist:

```
lsblk -io KNAME,TYPE,SIZE,MODEL
```

In diesem Beispiel ist das USB-Laufwerk als *sdc* aufgeführt.

- Erstelle eine Linux-Partition auf dem USB-Laufwerk:

  ```
  echo "0," | sfdisk /dev/sdc
  ```

- Erstelle das Dateisystem auf der *sdc1*-Partition mit den Namen „backup“:

  ```
  mke2fs -v -T largefile4 -j /dev/sdc1 -L backup
  ```

- Entferne das USB-Laufwerk und verbinde es anschließend erneut:

  Dies kann mit folgendem Befehl simuliert werden:

  ```
  blockdev --rereadpt /dev/sdc
  ```

- Nun wird auf der Seite *Sicherung (Daten)* ein Laufwerk „Backup“ angezeigt.

4.2 Benutzer und Gruppen

4.2.1 Benutzer

Ein Systennutzer wird benötigt, um auf viele Dienste zuzugreifen. z.B. NethServer (email, shared folders, etc..).

Jeder Benutzer wird durch seine Anmeldedaten identifiziert (Benutzer und Kennwort). Ein neuer Benutzer ist solange gesperrt, bis ein Kennwort für diesen festgelegt wurde. Ein gesperrter Benutzer kann keine Dienste nutzen, die eine Authentifizierung benötigen.

Wenn ein neuer Benutzer erstellt wird, sind folgende Felder Pflichtfelder:

- Benutzername
- Vorname
- Nachname

Optionale Felder:

- Firma
- Büro/Abteilung
- Adresse
- Stadt
- Telefon

Nach dem Erstellen ist ein Benutzer zunächst deaktiviert. Um diesen zu aktivieren muss ein Kennwort gesetzt werden, indem die Schaltfläche *Change password* genutzt wird. Nachdem der Benutzer aktiviert wurde, kann dieser sich am Servermanager anmelden und sein Kennwort ändern: *Benutzerkennwort ändern*.

Ein Benutzer kann zu einer oder mehreren Gruppen hinzugefügt werden. Dies geschieht über die Seite *Benutzer* oder über *Gruppen*.

Gelegentlich muss ein Benutzer gesperrt werden ohne seinen Account zu löschen. Dies kann erreicht werden, indem die Schaltflächen *Sperren* und *Entsperren* genutzt werden.

Hinweis: Wenn ein Benutzer gelöscht wird, werden auch seine Benutzerdaten gelöscht.

Zugriff auf Dienste

Nachdem ein Benutzer erstellt wurde, kann ein Benutzer für einzelne (oder alle) Dienste aktiviert werden. Dies kann auf der Seite *Dienste* durchgeführt werden.

4.2.2 Gruppen

Eine Gruppe von Benutzern kann benutzt werden um Berechtigungen für eine Gruppe von Benutzern zu vergeben oder um E-Mail-Verteiler zu erstellen.

Wie für Benutzer können auch Gruppen für einige (oder alle) Dienste genutzt werden.

Tipp: Zum Zuweisen von Berechtigungen für den Servermanager sollten die Gruppen `managers` oder `administrators` genutzt werden.

Zwei spezielle Gruppen können erstellt werden. Deren Benutzer bekommen mit Ihrer Mitgliedschaft Zugriff auf die Seiten des Servermanagers.

- *administrators*: Benutzer dieser Gruppe haben die gleichen Berechtigungen wie die Benutzer root oder admin.
- *managers*: Benutzer dieser Gruppe haben Zgruff auf den Management-Bereich.

4.2.3 Admin Benutzer

Die Seite *Benutzer* hat einen Standardeintrag: *admin*. Dieser Benutzer ermöglicht mit den gleichen Berechtigungen wie mit dem Benutzer *root* Zugriff auf den Servermanager . Standardmäßig ist dieser Benutzer deaktiviert und hat keinen Zgurff auf die Konsole.

Tipp: Um den Benutzer `admin` zu aktiviert, muss nur der Kennwort gesetzt werden.

Bei einigen Diensten hat der Benutzer `admin` spezielle Rechte. z.B. joining a workstation in Samba domain.

4.2.4 Passwortverwaltung

NethServer kann Richtlinien für Kennwörter wie *complexity* und *expiration* konfigurieren.

Die Kennwortrichtlinien können im Webinterface geändert werden. Dafür ist das Modul `nethserver-password` erforderlich.

Komplexität

Die Passwort-Komplexität sichert ein minimum an Sicherheit für das System und die genutzten Kennwörter. Dabei kann zwischen zwei verschienenden Richtlinien gewählt werden:

- *none*: Keine Komplexität. Dennoch existiert eine Mindestlänge von 7 Zeichen.
- *strong*

Die strong-Richtlinie setzt voraus, dass das Kennwort bestimmten Regeln entspricht:

- Mindestens 7 Zeichen
- Mindestens 1 Zahl
- Mindestens 1 Großbuchstaben
- Mindestens 1 Kleinbuchstaben
- Mindestens 1 Sonderzeichen
- Mindestens 5 unterschiedliche Zeichen
- Darf nicht im Wörterbuch vorkommen
- Darf nicht der Benutzername sein
- Darf nicht aus Wiederholungen von 3 oder mehr Zeichen bestehen (z.B. As1.$As1.$ ist unzulässig)

Die Standardrichtlinie ist *strong*.

Achtung: Vom Ändern der Kennwortrichtlinie ist dringend abzuraten. Die Nutzung von schwachen Kennwörtern führen häufig zu kompromitierten Servern durch externe Angreifer.

Um den Wert auf none zu setzen, muss folgender Befehl ausgeführt werden

```
config setprop passwordstrength Users none
```

Um den Wert auf strong zu setzen, muss folgender Befehl ausgeführt werden

```
config setprop passwordstrength Users strong
```

Um zu prüfen, welche Regel derzeit angewendet wird, muss folgender Befehl ausgeführt werden

```
config getprop passwordstrength Users
```

Ablauf

Das Kennwort läuft ab ist standardmäßig aktiviert. Das maximale Kennwortalter beträgt 6 Monate vom Zeitpunkt des setzens des Kennworts. NethServer versendet eine E-Mail an den Benutzerm wenn das Kennwort abläuft.

Hinweis: NethServer verweist auf das Datum des letzten Kennwortwechsels. Ist dies älter als 6 Monate sendet der Server eine E-Mail an den Benutzer mit dem Hinweis, dass das Kennwort abgelaufen ist. Der Benutzer muss das Kennwort nun ändern.

Zum Beispiel: Der letzte Kennwortwechsel war im Januar und es wird eine Anmeldung im Oktober durchgeführt. NethServer geht nun davon aus, dass das Kennwort abgelaufen ist und benachrichtig den Benutzer.

Wenn die Kennwörter für alle Benutzer nicht ablaufen sollen oder auch abgelaufene Kennwörter weiterhin gültig sein sollen, müssen folgende Befehle ausgeführt werden

```
config setprop passwordstrength PassExpires no
signal-event password-policy-update
```

Um das Ablaufen des Kennworts für einzelne Benutzer zu deaktivieren, müssen folgende Befehle ausgeführt werden (<Benutzer> durch den Benutzernamen ersetzen):

db accounts setprop <Benutzer> PassExpires no signal event password-policy-update

Einige Befehle um die derzeitige Richtlinie abzufragen:

Das maximale Kennwortalter abfragen (Standard: 180)

```
config getprop passwordstrength MaxPassAge
```

Das minimale Kennwortalter abfragen (verhindert das mehrfache ändern des Kennworts innerhalb eines Zeitraums) (Standard: 0)

```
config getprop passwordstrength MinPassAge
```

Anzahl an Tagen, an denen eine E-Mail an den Benutzer gesendet wird, bevor das Kennwort abläuft (Standard: 7)

```
config getprop passwordstrength PassWarning
```

Um diese Einstellungen zu ändern, ersetze den **`getprop`** durch **`setprop`** und füge den gewünschten Wert an das Ende des Befehls hinzu. Um die Information über das Ablaufen des Kennworts bereits 14 Tage vor Ablauf zu versenden, ist der Befehl

```
config setprop passwortstrength PassWarning 14
```

Abschließend müssen die geänderten Einstellungen übernommen werden:

signal-event password-policy-update

Verhalten von abgelaufenen Kennwörtern

Nachdem das Kennwort abgelaufen ist, ist der Benutzer weiterhin in der Lage E-Mails zu senden und zu empfangen. Der Benutzer kann aber nicht mehr auf Netzwerkfreigaben und Drucker (Samba) zugreifen oder auf Computer, falls der Computer in der Domäne des |productls ist.

Domänenkennwort

Falls NethServer als Domänencontroller konfiguriert ist, können Benuter in Kennwort über Windows ändern.

Wenn das Kennwort über Windows geändert wird, kann das Kennwort nicht kürzer als 6 Zeichen sein - unabhängig von den in NethServer konfigurierten Kennwortrichtlinien. Windows prüft zuerst das Kennwort und sendet dies anschließend an NethServer wo es dann anhand der konfigurierten Kennwortrichtlinien geprüft wird.

4.2.5 Sprache der Benachrichtigungen

Die Standardsprache für Benachrichtigungen ist Englisch. Wenn diese geändert werden soll, muss folgender Befehl ausgeführt werden:

```
config setprop sysconfig DefaultLanguage <lang>
```

Beispiel für Deutsch:

```
config setprop sysconfig DefaultLanguage de_DE.utf8
```

4.2.6 Benutzer importieren

NethServer kann Benutzer anhand einer CSV-Datei importieren. Diese Datei muss einen Benutzer pro Zeile enthalten. Die Werte der Zeile sind mittels TAB separiert und müssen dem folgenden Format entsprechen:

```
Benutzername    Vorname    Nachname    E-Mail    Kennwort
```

Beispiel:

```
mario   Mario   Rossi   mario@example.org       112233
```

Zunächst muss sichergestellt werden, dass der E-Mail-Server installiert ist. Anschließend muss die CSV-Datei auf den Server hochgeladen werden und folgender Befehl ausgeführt werden:

```
/usr/share/doc/nethserver-directory-<Version>/import_users <Dateiname>
```

Zum Beispiel: Der Pfad zur CSV-Datei ist `/root/users.csv`. Dann lautet der Befehl:

```
/usr/share/doc/nethserver-directory-`rpm --query --qf "%{VERSION}" nethserver-
↪directory`/import_users /root/users.csv
```

Der Befehl kann mehrfach ausgeführt werden. Bereits existierende Benutzer werden dabei übersprungen.

Hinweis: Der Befehl schlägt fehl, wenn das E-Mail-Servermodul nicht installiert ist.

4.3 Chat

Der chat-Dienst nutzt das Standardprotokoll Jabber/XMPP und unterstützt TLS auf den Standardports (5222 oder 5223).

Die Hauptfunktionen sind:

- Nachrichten zwischen Benutzern von NethServer senden

- Möglichkeit die Benutzer in Gruppen zu organisieren, basierend auf der Firma oder der Abteilung/Büro.
- Chatserver-Administratoren
- Rundnachrichten versenden
- Gruppenchat
- Offlinenachrichten
- Dateien versenden

Alle Benutzer haben Zugriff auf den Chat, indem sie sich mit ihren Anmeldedaten authentifizieren.

4.3.1 Client

Jabber Clients sind verfügbar für alle Desktopsysteme und Mobile Plattformen.

Einige verbreitete Clients:

- Pidgin für Windows und Linux
- Adium für Mac OS X
- BeejibelIM für Android und iOS, Xabber nur für Android
- JABBIM für Windows Phone

Wenn ein Client konfiguriert wird, muss sichergestellt sein, dass TLS (oder SSL) aktiviert ist. Zur Authentifizierung den Benutzernamen und den Domainnamen des Systems angeben.

Wenn NethServer ebenfalls als DNS-Server im Netzwerk betrieben wird, findet der Client über vorkonfiguriert DNS-Records den Chatserver automatisch. Ansonsten muss die Serveradresse in den erweiterten Optionen angegeben werden.

4.3.2 Administratoren

Alle Benuzter in der Gruppe `jabberadmins` sind Administratoren des Chatservers.

Administratoren können:

- Rundnachrichten versenden
- Den Status von verbundenen Benutzern prüfen

Die Gruppe `jabberadmins` ist konfigurierbar auf der Seite *Gruppen*.

4.4 Fax server

Der fax‘server macht es möglich Faxe über ein Modem, dass direkt an den Server angeschlossen ist, oder über ein :index:‘virutelles Modem zu senden.

Über das Webinterface sind folgende Konfigurationen möglich:

- Vorwahl und Faxnummer
- Absender (TSI)
- Ein physisches Modem mit Leitungsdaten und wie Faxes gesendet/empfangen werden sollen
- Ein oder mehrere :ref:‘iax-modem‘s

- E-Mail Benachrichtigungen für gesendete und empfangene Faxe mit einem Fax als Anhang (PDF, PostScript, TIFF)
- Empfangene Faxe drucken
- Virtual Samba Printer
- Täglicher Bericht über gesendete Faxe
- Versenden von Faxen via E-Mail

4.4.1 Modem

Trotz das die genutzte HylaFAX-Implementierung eine Reihe von Herstellern und Modellen unterstützt, empfehlen wir die Nutzung eines externen serial- oder USB-Modems.

Der Grund für diese Empfehlung ist: Wenn ein internes Modem ein Problem erzeugt, muss der Server neugestartet werden. Extere Modems können separat neugestartet werden (Stecker raus, Stecker rein). Viele erhältliche interne Modems sind sogenannte Winmodems. Dies sind „Software“-Modems, welche einen Treiber benötigen, der in der Regel nur für Windows erhältlich ist.

Achtung: Auch viele externe USB-Modems sind Winmodems!

Die Wahl sollte auf ein Modem der Klasse 1 oder 1.0 fallen, besondern wenn diese auf Rockwell-/Conexant- oder Lucent-/Agere- Chips basieren. NethServer unterstützt auch Modems der Klassen 2, 2.0 und 2.1.

4.4.2 Client

Wir empfehlen den Fax-Client YajHFC (http://www.yajhfc.de/). Dieser verbindet direkt zum Server und erlaubt folgende Funktionen:

- Nutzung eine LDAP-Adressbuchs
- Auswahl des Modems, über das gesendet werden soll
- Ansicht des Status des Modems

Authentifizierung

NethServer unterstützt zwei Möglichkeiten zur Authentifizierung beim Senden von Faxen:

- Systembasieren: Anhand der IP-Adresse wird die Berechtigung zum Senden von Faxen geprüft
- PAM: Nutzt Benutzernamen und Passwort. Der Benutzer muss der Gruppe „faxmaster“ angehören.

Außerdem sollte sichergestellt sein, dass *Faxe vom Client ansehen* aktiviert ist.

4.4.3 Samba Virtual Printer

Wenn die Option SambaFax aktiviert ist, stellt der Server einen virtuellen Drucker mit dem Namen „sambafax“ im Netzwerk zur Verfügung.

Jeder Client muss diesen Drucker mit den Apple LaserWriter 16/600 PS-Treibern einrichten.

Zu sendende Dokumente müsse folgende Voraussetzungen erfüllen:

- Sie müssen die Wörter „Fax Number“ enthalten, gefolgt von der Faxnummer. Beispiel:

```
Fax Number: 12345678
```

- Die Zeichenfolge kann überall im Dokument stehen, aber muss in einer Zeile enthalten sein
- Die Zeichenfolge muss in einer nicht-Bitmap-Schriftart geschrieben sein (z.B. Truetype)

Die Faxe werden gesendet, indem die Benutzerdaten des absendenden Benutzers genutzt werden. Diese Information wird auch in der Fax-Warteschlange angezeigt.

4.4.4 Mail2Fax

Alle E-Mails, die an `sendfax@<domainname>` gesendet werden, werden als Fax an den Empfänger gesendet.

`<domainname>` muss einer Domäne entsprechen, die auf dem E-Mail-Server verarbeitet wird.

Die E-Mail muss wie folgt formatiert sein:

- Die Empfängernummer muss im Betreff angegeben sein
- Die E-Mail muss eine Nur-Text-E-Mail sein (kein HTML oder RichText!)
- Die E-Mail kann anhänge wie PDFs enthalten, welche zusammen mit dem Fax versendet werden

---

Hinweis: Diese Funktion steht nur für Clients zur Verfügung, welche aus einem grünen Netzwerk versenden

---

4.4.5 Virtual Modems

Virtual Modems sind Softwaremodems, welche an eine PBX (Asterisk usually) mit einer IAX Erweiterung angeschlossen sind.

Die Konfiguration von virtuellen Modems enthält zwei Teile:

1. Erstellen der IAX-Eweiterung mit der PBX
2. Konfiguration des Virtuellen Modems

4.5 Web Inhaltsfilter

Der content filter analysiert allen Webverkehr und blockiert definierte Seiten oder Seiten die Viren enthalten. Verbotene Seiten können anhand einer Liste von Kategorien ausgewählt werden, welche von einer externen Quelle heruntergeladen werden können und auf dem NethServer gespeichert werden müssen.

NethServer erlaubt es unbegrenzt viele Profile zu erstellen. Ein Profil besteht aus drei Teilen:

- **Wer**: Welcher Client ist diesem Profil zugewiesen? Dies kann ein Benutzer, eine Benutzergruppe, ein Host, eine Hostgruppe, eine Zone oder ein Netzwerkadapterrolle (grün, blau usw.) sein.
- **Was**: Welche Seiten können von den Clients aufgerufen werden? Dies ist ein Filter, der unter *Filter* definiert wird.
- **Wann**: Der Filter kann immer gelten oder nur zu einem bestimmten Zeitpunkt. Zeitfenster können unter *Zeiten* festgelegt werden.

Dies ist die empfohlene Reihenfolge für die Inhaltsfilter-Konfiguration:

1. Wähle eine Liste von Kategorien unter *Blacklists* und lade diese herunter

2. Erstelle eine oder mehrere Zeitfenster (optional)
3. Erstelle eigene Kategorien (optional)
4. Erstelle einen neuen Filter oder bearbeite den Standardfilter
5. Erstelle ein neues Profil, das eine Benutzer oder Host zugewiesen ist und wähle den Filter und das Zeitfenster (wenn aktiviert)

Wenn kein Profil den Filtern entspricht, wird das Standardprofil angewendet.

4.5.1 Filter

Ein Filter kann:

- den Zugang zu Seiten sperren, die einer Kategorien entsprechen
- den Zugang zu Seiten sperren, die über IP-Adressen aufgerufen werden (empfohlen)
- URL durch Regular Expressions filtern
- Das Herunterladen von Dateien mit bestimmten Endungen verbieten
- Eine globale Blacklist und Whitelist aktivieren

Ein Filter kann in zwei unterschiedlichen Modi ausgeführt werden:

- Alles erlauben: Alle Seiten erlauben, außer die Seiten, die explizit gesperrt sind
- Alles blockieren: Alle Seiten verieben, außer die Seiten, die explizit erlaubt sind

---

Bemerkung: Die Kategorien-Liste wird erst angezeigt, wenn die Liste unter :guilabel‘Blacklist‘ heruntergeladen wurde.

Blockieren von Google Translate

Online-Übersetzungsdienste wie Google Translate, können missbraucht werden um den Inhaltsfilter zu umgehen. Dies ist der Fall, weil die URL bei Nutzung der Übersetzung immer auf eine Google-Domain zeigt und dennoch Inhalt eines externen Servers enthält.

Es ist möglich alle Anfragen an Google translate zu blockieren, indem eine blockierte URL unter *General* erstellt wird. Der Inhalt muss dann `translate.google` lauten.

4.5.2 Benutzer aus der Active Directory

Wenn NethServer einer Active Directory (samba_ads) beigetreten ist, können Profile auch Domänen-Benutzern zugewiesen werden.

Bemerkung: Gruppen aus der Active Directory werden nicht unterstützt.

4.5.3 Antivirus

Es wird empfohlen den Virusscanner im Inhaltsfilter immer zu aktivieren. Wenn der Proxy im SSL-Transparenzmodus (proxy_ssl-section) konfiguriert ist, wird der Virusscanner auch für HTTPS-Seiten verwendet.

4.5.4 Fehlerbehebung

Wenn eine „böse Seite“ nicht blockiert wird, prüfe folgendes:

- Der Client nutzt den Proxyserver
- Der Client hat keinen Proxy-Bypass für die Seite/IP konfiguriert
- Der Client ist eine Profil zugewiesen, dass den Besuch der Website verbietet
- Der Client surft in einem Zeitraum, in dem der Filter aktiv ist

4.6 Firewall und Gateway

NethServer kann als firewall und als gateway genutzt werden. Der gesamte Netzwerkverkehr zwischen Computer im lokalen Netzwerk und dem Internet, der durch NethServer geleitet wird, wird anhand von Regeln entsprechend weiterverarbeitet.

Hauptfunktionen:

- Erweiterte Netzwerkkonfiguration (Bridge („Netzwerkbrücke“), Bonds, Alias usw.)
- Multi-WAN Unterstützung (bis zu 15)
- Regelbasierte Firewall
- Traffic Shaping (QoS)
- Port Weiterleitung
- Routen von Netzwerkverkehr zu unterschiedlichen WAN-Verbindungen
- Intrusion Prevention System (IPS)

Firewall und Gateway sind nur aktiv, wenn:

- Das Modul *nethserver-firewall-base* installiert ist
- Mindestens ein Netzwerkadapter ein rotes Webinterface ist

4.6.1 Richtlinien

Jeder Netzwerkadapter wird durch eine Farbe gekennzeichnet, die dessen Rolle im System angibt. See *Netzwerk*.

Wenn ein Netzwerkpaket die Firewall passiert, prüft NethServer, ob das Paket erlaubt ist oder ob es blockiert wird. *Richtlinien* sind die Regeln, die angewendet werden, wenn ein Paket keiner existierenden Regel zuzuordnen ist.

Die Firewall implementiert zwei Standardrichtlinien, welche über *Firewall Regeln -> Konfigurieren* bearbeitet werden können:

- *Erlaubt*: Der gesamte Netzwerkverkehr von grün nach rot ist erlaubt.
- *Blockiert*: Der gesamte Netzwerkverkehr von grün nach rot ist blockiert. Nur explizit durch Firewall Regeln erlaubter Traffic darf die Firewall passieren.

Firewall Richtlinien erlauben zonenübergreifenden Verkehr nach folgendem Schema:

```
GRÜN -> BLAU -> ORANGE -> ROT
```

Netzwerkverkehr wird erlaubt von links nach rechts. Netzwerkverkehr von rechts nach links wird blockiert.

Das Standardverhalten kann unter *Firewall Regeln* angepasst werden.

Hinweis: Netzwerkverkehr vom lokalen Netzwerk zum Server auf dem SSH-Port (Standard: 22) und auf den Servermanager-Port (Standard: 980) ist IMMER erlaubt.

4.6.2 Regeln

Regeln betreffen allen Netzwerkverkehr, welcher durch die Firewall geleitet wird. Wenn ein Netzwerkpaket von einer Zone zu einer anderen Zone möchte, prüft NethServer die konfigurierten Regeln. Wenn das Netzwerkpaket einer Regel entspricht, so wird diese Regel angewendet.

Hinweis: Die Reihenfolge der Regeln ist sehr wichtig! NethServer wendet immer die erste Regel an, welche auf das Netzwerkpaket zutrifft.

Eine Regel besteht aus vier wesentlichen Bestandteilen:

- Aktion: Was soll gemacht werden, wenn die Regel auf ein Netzwerkpaket zutrifft?
- Quelle: Woher soll das Paket kommen, damit diese Regel ggf. angewendet wird?
- Ziel: An welche Adresse/Host ist das Paket gerichtet, damit diese Regel ggf. angewendet wird?
- Dienst: Auf welche Dienste (Ports) trifft diese Regel zu?

Verfügbare Aktionen sind:

- *ACCEPT*: Erlaubt den Netzwerkverkehr
- *REJECT*: Verweigert den Netzwerkverkehr und informiert den absendenden Host auf Netzwerkebene
- *DROP*: Verweigert den Netzwerkverkehr und informiert den absendenden Host NICHT
- *ROUTE*: Route den Netzwerkverkehr zu einem definierten WAN-Anschluss. Siehe *Multi WAN*.

Hinweis: Die Firewall generiert keine Regeln für die blaue oder die orangene Zone, wenn nicht mindestens ein roter Netzwerkadapter konfiguriert wurde.

REJECT vs DROP

Generell sollte REJECT gewählt werden, wenn der Quellhost informiert werden soll, dass die Verbindung die er geöffnet hat geschlossen wurde. Normalerweise wird von Regeln für das lokale Netzwerk REJECT genutzt.

Für Verbindungen aus dem Internet wird empfohlen DROP zu nutzen um potentiellen Angreifern keinerlei Antwort zu liefern.

Log

Es ist möglich beim Zutreffen einer Regel ein Log-Eintrag zu schreiben, wenn die Option im Webinterface aktiviert wurde. Das Firewall Log wird unter `/var/log/firewall.log` gespeichert.

Beispiele

Im Folgenden einige Beispiele für Regeln.

Allen DNS-Verkehr vom LAN in das Internet blockieren:

- Aktion: REJECT
- Quelle: GRÜN
- Ziel: ROT
- Dienst: DNS (UDP port 53)

Allen Gästenetzwerken den Zugriff auf Server1 erlauben:

- Aktion: ACCEPT
- Quelle: BLAU
- Ziel: Server1
- Dienst: -

4.6.3 Multi WAN

Der Begriff *WAN* (Wide Area Network) bedeutet das öffentliche Netzwerk außerhalb der Server - im Normalfall das Internet. Ein *Provider* ist das Unternehmen, welches den Zugang zum internet, den WAN-Link, bereitstellt.

NethServer unterstützt bis zu 15 WAN-Anschlüsse. Wenn der Server zwei oder mehr konfigurierte rote Netzwerkadapter hat, ist es nötig eine Providerkonfiguration auf der Seite *Multi WAN* durchzuführen.

Jeder Provider stellt eine WAN-Verbindung, welche an einen Netzwerkadapter gekoppelt ist. Jeder Provider definiert eine *Gewichtung*: je höhere die Gewichtung, desto höher die Priorität des Netzwerkadapter, der mit dem Provider assoziiert ist.

NethServer kann die WAN-Verbindungen in zwei Modi betreiben (Schaltfläche *Konfigurieren* auf der Seite *Multi WAN*):

- *Balance*: Alle Provider werden gleichzeitig unter Beachtung ihrer Gewichtung genutzt.
- *Aktiv Backup*: Es wird der Provider mit der höchsten Gewichtung genutzt. Wenn dieser Provider die Verbindung verliert, wird der Netzwerkverkehr über den nächsthöheren Provider geleitet.

Um den Status eines Providers zu erfahren, sendet NethServer ein ICMP Paket („ping“) in regelmäßigen Intervallen. Wenn die Anzahl der verlorenen Pakete einen Grenzwert überschreitet, wird der Provider als nicht erreichbar angesehen.

Die Sensivität der Überwachung kann über die folgenden Parameter festgelegt werden:

- Prozent der verlorenen Pakete
- Anzahl der verlorenen Pakete
- Intervall in Sekunden zwischen gesendeten Paketen

Die *Firewall Regeln*-Seite erlaubt es Netzwerkpakete zu den vorhandenen WAN-Providern zu routen, wenn bestimmte Kriterien erfüllt werden. Siehe *Regeln*.

Beispiel:

Es gibt zwei konfigurierte Provider:

- Provider1: Netzwerkadapter eth1, Gewichtung 100
- Provider2: Netzwerkadpater eth0, Gewichtung 50

Wenn der Modus Balance gewählt ist, wird der Server über Provider 1 doppelt so viele Verbindungen aufbauen wie über Provider 2.

Wenn der Modus Aktiv Backup gewählt ist, wird der Server alles an Verkehr über Provider 1 leiten. Wenn Provider 1 nicht mehr verfügbar ist, wird auf Provider 2 ausgewichen.

4.6.4 Portweiterleitung

Die Firewall blockert Anfragen aus öffentlichen Netzwerken zu den privaten Netzwerken. Beispiel: Wenn ein Webserver im LAN betrieben wird, können nur Computer aus dem lokalen Netzwerk die Webseite(n) in der grünen Zone nutzen. Jede Anfrage von einem Benutzer außerhalb des lokalen Netzwerks wird blockiert.

Um den Zugriff von Außen auf den Webserver zu erlauben, muss eine *Portweiterleitung* eingerichtet werden. Eine Portweiterleitung erlaubt begrenzten Zugriff auf die Resourcen aus öffentlichen Netzwerken.

Wenn der Zugriff konfiguriert wird, muss der genutzte Port angegeben werden. Der Netzwerkverkehr von roten Netzwerkadaptern wird dann auf für die gewählten Ports weitergeleitet. Am Beispiel von Webservern ist dies normalerweise der port 80 (HTTP) und Port 443 (HTTPS).

Wenn eine Portweiterleitung eingerichtet wird, müssen mindestens die folgenden Parameter angegeben werden:

- Der Quellport
- Der Zielport, der sich vom Quellport unterscheiden kann
- Die Adresse des Servers, an den der Verkehr weitergeleitet werden soll

---

Hinweis: Es ist möglich einen Portbereich anzugeben. Dazu werden beim Quellport der erste und der letzte Port, getrennt von einem Doppelpunkt, angegeben. Z.B. „1000:2000“. Der Zielport muss dann leer bleiben.

Beispiel

Gegeben ist folgendes Szenario:

- Der interne Server hat die IP 192.168.1.10 mit dem Namen Server1
- Der Server betreibt einen Webserver auf Port 80
- Der Server hat einen Zugang via SSH auf Port 22
- Der Server hat weitere Dienste, die auf den Ports 5000 bis 6000 erreichbar sind.

Um den Zugang auf den Webserver von außerhalb freizugeben, muss folgende Regel eingerichtet werden:

- Quellport: 80
- Zielport: 80
- Host Adresse: 192.168.1.10

Jeder eingehende Netzwerkverkehr auf einem roten Netzwerkadapter der Firewall auf port 80 wird so zu Server1 weitergeleitet.

Wenn SSH von außerhalb auf Port 2222 erreichbar sein soll, so muss folgende Regel eingerichtet werden:

- Quellport: 2222
- Zielport: 22
- Host Adresse: 192.168.1.10

Jeder eingehende Netzwerkverkehr auf dem roten Netzwerkadapter der Firewall auf port 2222 wird so zu Server 1 auf Port 22 weitergeleitet.

Wenn Dienste auf den Ports 5000 bis 6000 von außerhalb freigegeben werden werden sollen und an Server 1 weitergeleitet werden sollen, so muss folgende Regel eingerichtet werden:

- Quellport: 5000:6000
- Zielport:
- Host Adresse: 192.168.1.10

Jeder eingehende Netzwerkverkehr auf dem roten Netzwerkadapter der Firewall auf den Ports 5000 bis 6000 wird auf dem gleichen Port an Server1 weitergeleitet.

Beschränkter Zugriff

Die Portweiterleitung kann eingeschränkt werden, sodass diesen nur noch bei Zugriff von bestimmten IP-Adressen oder Netzwerken durchgeführt wird. Dazu wird das Feld *Nur erlauben von* genutzt.

Diese Konfiguration ist hilfreich, wenn Dienste nur von vertrauenswürdigen Quellen erreichbar sein sollen. Eine mögliche Werte:

- `10.2.10.4`: Portweiterleitung nur durchführen, wenn von der IP 10.2.10.4 zugegriffen wird.
- `10.2.10.4,10.2.10.5`: Portweiterleitung nur durchführen, wenn von der IP 10.2.10.4 oder 10.2.10.5 zugegriffen wird.
- `10.2.10.0/24`: Portweiterleitung nur durchführen, wenn aus dem Netzwerk 10.2.10.0/24 zugegriffen wird (Alle IPs von 10.2.10.0 bis 10.2.10.255)
- `!10.2.10.4`: Portweiterleitung für alle durchführen, nur nicht für die IP 10.2.10.4
- `192.168.1.0/24!192.168.1.3,192.168.1.9`: Portweiterleitung für das Netzwerk 192.168.1.0/24 durchführen, nicht aber für die IPs 192.168.1.3 und 192.168.1.9

4.6.5 NAT 1:1

Eins-zu-Eins NAT ist eine Möglichkeit Systeme hinter einer Firewall mit einer privaten IP so erscheinen zu lassen, als hätten sie eine öffentliche IP.

Sofern mehrere öffentliche IP-Adressen zur Verfügung stehen und eine IP einem definierten Host zugeordnet werden soll, dann ist NAT 1:1 die Lösung.

Beispiel

In einem Netzwerk gibt es den Server `BeispielServer` mit der IP `192.168.5.122`. außerdem haben wir die öffentliche IP-Adresse `89.95.145.226` als alias auf dem `eth0` Netzwerkadapter (`rot`).

Wir möchten den `BeispielServer` die IP-Adresse `89.95.145.226` zuweisen.

Unter *NAT 1:1* wählen wir für die IP `89.95.145.226` (read-only Feld) den Host (`BeispielServer`) aus der Auswahlbox. Somit wurde ein Eins-zu-Eins NAT konfiguriert.

4.6.6 Traffic Shaping

Traffic Shaping erlaubt es Netzwerkverkehr durch die Firewall zu priorisieren (QoS). So ist es möglich die Verbindungen von wichtigem Netzwerkverkehr zu priorisieren und die Latenz zu verringern indem die verfügbare Bandbreite optimal ausgenutzt wird.

Um Traffic Shaping zu aktivieren ist es notwendig zu wissen wie viel Bandbreite in beide Richtungen einer Verbindung zur Verfügung steht. Dies ist in der Regel die Up- und Downloadgeschwindigkeit des Internetanschlusses. Im Falle eines Problems beim Internetprovider kann an dieser Stelle keine vollständige Abhilfe geschaffen werden um die Geschwindigkeit zu erhöhen.

Traffic Shaping kann unter *Traffic Shaping -> Adapterregeln* konfiguriert werden.

NethServer bietet drei Stufen von Prioritäten: Hoch, Mittel und Niedrig. Standardmäßig ist aller Netzwerkverkehr Mittel priorisiert. Es ist möglich basierend auf den genutzten Ports eines Dienstes die Priorität auf Hoch oder Niedrig zu setzen (z.B. für niedrig priorisierten Peer-To-Peer traffic).

NethServer hat für interaktiven Netzwerkverkehr bereits eine hoche Priorität vorkonfiguriert. Das Bedeutet, dass VoIP, SSH und PING bereits mit hoher Priorität verarbeitet werden.

Hinweis: Stelle sicher, dass die tatsächlich vorhandene Bandbreite des Anschlusses angegeben ist!

4.6.7 Firewall Objekte

Firewall Objekte repräsentieren Netzwerkkomponente und sind hilfreich um das Erstellen von Regeln zu erleichtern.

Es gibt 6 Typen von Objekte. 5 davon repräsentieren Quellen und Ziele:

- Host: Stellen einen lokalen oder entfernten Computer dar. z.B. Webserver oder PCs.
- Gruppen von Hosts: Stellen eine Gruppe von Computern da. Hosts in einer Hostgruppe sollten immer über den gleichen Netzwerkadapter erreichbar sein. z.B.: Server, Buchhaltung-PCs
- CIDR Netzwerke: Es ist möglich CIDR-Netzwerke anzugeben um die Firewall Regeln zu vereinfachen.

  Beispiel 1: Die letzten 14 IP-Adressen eines Netzwerks sind Servern zugewiesen (192.168.0.240/28).

  Beispiel 2: Es sind zwei grüne Netzwerkadapter vorhanden, aber es soll nur eine Regel für einen Adapter erstellt werden (192.168.2.0/24).
- Zone: Stellt ein Netzwerk mit Hosts dar. Dirse müssen zuvor in einer CIDR-Gruppe angelegt worden sein. Die Zonen sind dazu gedacht, dass einzelne Teile eines Netzwerks verschiedenen Firewallregeln unterliegen obwohl das gesamte Netzwerk auf einem Netzwerkadapter anliegt.

Hinweis: Standardmäßig dürfen alle Hosts einer Zone die Firewall nicht passieren. Es ist erforderlich, dass zum Passieren der Firewall Regeln erstellt werden.

Der letzte Objekttyp wird benutzt um den Typ (/Port) des Netzwerkverkehrs zu definieren:

- Dienste: Ein Dienst nutzt mindestens einen Port und ein Protokoll. Beispiel: ssh, https

Wenn Regeln erstellt werden, können die Einträge, die unter *DNS* und *DHCP und PXE Server* angelegt wurden, wie andere Host-Objekte genutzt werden. Außerdem wird jeder Netzwerkadapter mit seiner zugewiesenen Rolle automatisch bei den verfügbaren Zonen aufgelistet.

4.6.8 IP/MAC Bindung

Wenn NethServer als DHCP-Server fungiert, kann die Firewall die DHCP-Reservierungen nutzen um allen Netzwerkverkehr innerhalb des lokalen Netzwerks zu prüfen. Wenn IP/MAC Bindung aktiviert ist, kann der Administrator auswählen welche Richtlinie auf Hosts ohne DHCP-Reservierung angewendet werden soll. Ein häufiger Anwendungsfall ist, wenn nur bekannte Hosts kommunizieren dürfen und alle anderen Hosts blockiert werden. In diesem Fall würden Hosts ohne Reservierung nicht in der Lage sein die Firewall zu passieren und auf andere Netzwerke zuzugreifen.

Um Netzwerkverkehr nur von bekannten Hosts zu erlauben, müssen folgende Schritte ausgeführt werden:

1. Erstelle eine DHCP-Reservierung für einen Host
2. Gehe zu *Firewall Regeln* und wähle *Konfigurieren* aus dem Schaltflächenmenü
3. Wähle *MAC Überprüfung (IP/MAC Bindung)*
4. Wähle *Blockiere Netzwerkverkehr* als Richtlinie, die auf unregistrierte Hosts angewendet werden soll

---

Hinweis: Erstelle mindestens eine DHCP-Reservierung bevor IP/MAC-Bindung aktiviert wird. Ansonsten hat kein System mehr zugriff auf das Webinterface oder SSH von NethServer!

4.7 Bandbreiten Überwachung (ntopng)

ntopng ist ein mächtiges Tool, mit dem in Echtzeit Netzwerkverkehr analysiert werden kann. Es macht es möglich herauszufinden welcher Host wie viel Bandbreite nutzt und welche Protokolle am häufigsten genutzt werden.

ntopng aktivieren Wenn ntopng aktiviert wird, wird der gesamte Netzwerkverkehr über die Netzwerkadapter analysiert. Dies kann zu einem Geschwindkeitsverlust im Netzwerk führen sowie zu einer Erhöhten Systemauslastung des lproductls

Port Der Port, an dem das Webinterface von ntopng erreichbar ist

Passwort für den Benutzer ‚admin' Das Passwort füf den Benutzer „admin". Dieses Passwort ist nicht das gleiche Kennwort wie das NethServer admin-Kennwort.

Netzwerkadapter Die Netzwerkadapter, die ntopng analysieren wird

4.8 DNS

NethServer kann als *DNS* (Domain Name System) Server konfiguriert werden. Ein DNS Server ist dafür verantwortlich die Namensauflösung im Netzwerk zu betreiben und den DNS-Namen (z.B. www.beispiel.de) in die IP-Adresse (z.B. 11.112.231.3) aufzulösen und anders herum.

Der DNS-Server führt auf Anfrage der Clients die Namensauflösung aus. Der DNS-Server ist nur aus dem grünen und blauen Netzwerk erreichbar.

Bei einer Namensauflösung, wird der Server:

- den Namen im lokalen Netzwerk suchen

- eine Anfrage an den externen DNS-Server stellen und die Antwort zwischenspeichern um künftige Anfragen zu beschleunigen

Wenn NethServer ebenfalls als DHCP-Server konfiguriert ist, werden alle Maschinen automatisch den NethServer für die Namensauflösung nutzen.

Bemerkung: Es muss mindestes ein externer DNS-Server unter *DNS Server* angegeben werden.

4.8.1 Hosts

Die *Hosts*-Seite erlaubt es Hostnamen IP-Adressen zuzuweisen. Dabei können die IP-Adressen local oder remote oder auch dummy-IP-Adressen sein.

Zum Beispiel: Wenn ein interner Webserver betrieben wird, kann der Hostname *www.meine-seite.de* mit der IP des internen Webservers verknüpft werden. Alle Clients im lokalen Netzwerk können dann die Seite bei der Eingabe dieser Adresse um Browser aufrufen.

Lokal konfigurierte Hosts werden immer zuerst verwendet bevor ein DNS-Eintrag eines externen Servers verwendet wird. Dies bedeutet, dass der externe DNS-Server *www.meine-seite.de* mit der externen IP-Adresse der offiziellen Webseite auflöst. Da jedoch innerhalb von NethServer ein Hosteintrag für *www.meine-seite.de* vorhanden ist, werden alle Geräte im lokalen Netzwerk, die den NethServer als DNS-Server werden, die interne IP-Adresse auflösen.

4.8.2 Alias

Ein *alias* ist ein alternativer Name um den NethServer zu erreichen. Zum beispiel wenn der Server *mail.meine-seite.de* heißt, kann ein DNS alias *myname.meine-seite.de* erstellt werden. Der Server wird dann auch von dem Alias erreichbar sein.

Aliase sind nur im LAN gültig. Soll der Alias auch aus dem Internet erreichbar sein, muss dieser Alias beim DNS-Provider eingetragen werden.

4.9 DHCP und PXE Server

Der *Dynamic Host Configuration Protocol* (DHCP)[1] Server zentralisiert die Verwaltung des Netzwerks für alle Geräte, die zum Netzwerk verbunden sind und DHCP nutzen. Wenn ein Computer (oder ein Gerät wie Drucker, Smartphone usw.) sich mit dem Netzwerk verbinden, kann es vom DHCP Server unter der Verwendung des DHCP Protokolls die Netzwerkkonfiguration anfragen. Der DHCP Server stellt dann die Netzwerkparameter wie IP-Adresse, Subnetmask, Gateway, DNS-Server und weitere relevate Netzwerkparameter bereit.

Bemerkung: Meist sind Netzwerk-Geräte so konfiguriert, dass diese standardmäßig DHCP nutzen.

Die *Preboot eXecution Environment* (PXE)[3] Spezifikation erlaubt es einen Netzwerkgerät beim Starten das Betriebssystem von einem Netzwerkpfad anstelle der lokalen Installation zu laden. Dies geschieht über das DHCP- und TFTP-Protokoll. Unter *Starten aus einer Netzwerkkonfiguration (PXE-Boot)* ist ein Beispiel aufgeführt, das diese Konfiguration zeigt.

[1] Dynamic Host Configuration Protocol (DHCP) http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
[3] Preboot eXecution Environment http://en.wikipedia.org/wiki/Preboot_Execution_Environment

4.9.1 DHCP Konfiguration

Der DHCP-Server kann auf allen *grünen* und *blauen* Netzwerkadaptern aktiviert werden (siehe *Netzwerk*). NethServer wird eine freie IP-Adresse innerhalb der konfigurierten *DHCP range* zuweisen. Diese kann unter *DHCP* > *DHCP Server* konfiguriert werden.

Der DHCP-Bereich muss innerhalb des Netzwerks definiert werden, das von einem Netzwerkadapter bereitgestellt wird. Zum Beispiel wenn der grüne Netzwerkadapter die IP/Netzwerkmaske `192.168.1.1/255.255.255.0` hat, muss der IP-Bereich z.B. in folgendem Bereich liegen `192.168.1.2-192.168.1.254`.

4.9.2 Host IP Reservierung

Der DHCP-Server teilt einem Netzwerkgerät eine IP-Adresse nur für einen Zeitraum zu („Lease time“). Nach einer gewissen Zeit wird die IP-Adresse wieder für neue Netzwerkgeräte freigegeben, wenn das Gerät, das einer IP-Adresse zugewiesen ist, sich nicht beim DHCP-Server gemeldet hat (d.h. lange nicht eingeschaltet wurde). Wenn ein Gerät immer die selbe IP-Adresse benötigt, kann eine *IP Reservierung* für die MAC-Adresse dieses Gerätes vorgenommen werden. Auf diese Weise erhält das Gerät bei jeder Anforderung, auch nach langer Zeit, immer die selbe IP-Adresse.

Unter *DHCP* > *IP Reservierungen* können die aktuellen Reservierungen eingesehen werden.

- eine Zeile mit der Schaltfläche *IP Reservierung* zeigt einen Eintrag mit einer zeitweisen IP-Zuweisung (grau);
- eine Zeile mit der Schaltfläche *Bearbeiten* zeigt einen Eintrag, der eine IP-Reservierung erhalten hat (schwarz). Ein kleines Icon mit zwei schwarzen Pfeilen beim Hostnamen zeigt, dass eine DHCP lease abgelaufen ist. Dies ist normal, sofern der Host eine statische IP-Adresse hat und die Reservierung auf dem DHCP-Server durchgeführt wurde, damit diese IP nicht vom DHCP-Server vergeben wird.

4.9.3 Starten aus einer Netzwerkkonfiguration (PXE-Boot)

Um es Systemen zu ermöglichen aus dem Netzwerk zu starten, müssen folgende Bedingungen erfüllt sein:

- Der *DHCP* Server muss installiert und konfiguriert sein. (Siehe vorherige Abschnitte)
- Der *TFTP* Server[2] muss konfiguriert sein
- Der Softwareclient, bereitgestellt via TFTP.

TFTP ist ein sehr einfaches Dateiübertragungsprotokoll und wird normalerweise genutzt um automatisch Konfigurations- und Bootdateien zu übertragen.

In NethServer wird TFTP zusammen mit dem DHCP-Modul installiert und ist standardmäßig aktiviert. Um den Zugriff auf den TFTP-Server zu ermöglichen, muss eine Datei nur in den Ordner `/var/lib/tftpboot` abgelegt werden.

Bemerkung: Um TFP zu deaktivieren, muss folgender Befehl in der Konsole als Root ausgeführt werden:

config setprop dhcp tftp-status disabled signal-event nethserver-dnsmasq-save

---

Als Beispiel wird nun eine Konfiguration durchgeführt, die ein CentOS aus dem Netzwerk startet. Dazu in NethServer in der Konsole folgende Befehle ausführen:

```
yum install syslinux
cp /usr/share/syslinux/{pxelinux.0,menu.c32,memdisk,mboot.c32,chain.c32} /var/lib/
↪tftpboot/
config setprop dnsmasq dhcp-boot pxelinux.0
```

(Fortsetzung auf der nächsten Seite)

[2] Trivial File Transfer Protocol https://en.wikipedia.org/wiki/Tftp

(Fortsetzung der vorherigen Seite)

```
signal-event nethserver-dnsmasq-save
mkdir /var/lib/tftpboot/pxelinux.cfg
```

Anschließend die Datei `/var/lib/tftpboot/pxelinux.cfg/default` erstellen und folgenden Inhalt einfügen:

```
default menu.c32
prompt 0
timeout 300

MENU TITLE PXE Menu

LABEL CentOS
  kernel CentOS/vmlinuz
  append initrd=CentOS/initrd.img
```

Anschließend ein CentOS-Verzeichniss erstellen:

```
mkdir /var/lib/tftpboot/CentOS
```

In dieses Verzeichniss die Dateien `vmlinuz` und `initrd.img` kopieren. Diese Dateien sind öffentlich und können im ISO-Image gefunden werden, in dem Verzeichniss `/images/pxeboot` oder vom CentOS-Mirror heruntergeladen werden.

Als letzten Schritt den Client starten und PXE-Boot auswählen (oder „Boot from Network“) direkt nach dem Einschalten des PCs.

Referenzen

4.10 WebVirtMgr

Mit diesem Tool verwaltet man virtual machine über eine einfache Weboberfläche:

- Erstellen und Löschen von virtuellen Systemen (KVM)
- Erstellen eigener Vorlagen für virtuelle Systeme
- Einfache Konsole für entfernten Zugriff
- Tolle Benutzeroberfläche

4.10.1 Konfiguration

Die Webanwendung ist auf dem Port **8000** aktiv, zum Beispiel: `http://SYSTEM_IP:8000/`.

Der Dienst ist standardmäßig deaktiviert.

Unter der Schaltfläche *Virtual machines* kann man folgende Einstellungen vornehmen:

- Aktivieren der Verwaltungskonsole für virtuelle Systeme
- Aktivieren des Konsolenzugriffs auf das virtuelle System per Web Browser

Um auf die Weboberfläche zugreifen zu können muss man sich mit den unten stehenden Anmeldedaten anmelden:

- *Benutzer:* admin
- *Passwort*: random alphanumeric (editable)

Warnung: Keine Netzwerkbrücken(Network bridges) innerhalb der WebVirtManager Oberfläche erstellen. Hierfür eine Brücke(bridge) unter *Network* erstellen und im WebVirtManager dann entsprechend nutzen.

Weiterführende Informationen findet man unter:

- http://wiki.qemu.org/Manual
- http://www.linux-kvm.org/page/Documents

4.11 Adagios

Adagios ist eine webbasierte Oberfläche für Nagios. Adagios wurde entwickelt um eine einfache und intitive Oberfläche for Nagios bereit zu stellen. Zudem hat Adagios eine REST-Schnittstelle für Status- und Konfigurationsdaten sowie ein Dashboard, dass als Alternative zum Nagios Webinterface genutzt werden kann.

Hauptfunktionen:

- Vollständiges bearbeiten von Hosts, Diensten usw.
- Viele vorinstallierte Plugins und Konfigurationsvorlagen
- Netzwerkscanner
- Remoteinstallation von Linux-/Windows-Agenten
- Moderne Statusansicht als Alternative zu Nagios Standardwebinterface
- Backup der Adagios-Daten mit |productls Backup-Funktion
- REST-Schnittstelle für den Status von Hosts und Diensten und zur Ansicht und Bearbeitung der Konfiguration
- Vollständige Prüfung aller vorgenommenen Änderungen

4.11.1 Installation

Die installation kann über das Softwarecenter von NethServer durchgeführt werden. Hier muss das Modul „Monitoring and Inventarisation“ installiert werden. Nach der Installation:

- Aktiviere den Admin-Account (siehe *Admin Benutzer*)
- Öffne die URL https://your_nethserver_ip/adagios
- Nutze die `admin`-Anmeldung um auf das Webinterface zuzugreifen

Für weitere Informationen steht die offizielle Dokumentation bereit:

- http://adagios.org/
- https://github.com/opinkerfi/adagios/wiki

4.12 OCS Inventory NG

OCS Inventory NG ist freie Software, die es den Benutzern erlaubt, ihren IT-Bestand zu inventarisieren. OCS Inventory NG sammelt Informationen über die Hardware und Software auf den Maschinen im Netz, auf denen die OCS-Client-Software läuft (*OCS Inventory Agent*). OCS Inventory NG kann den Bestand über ein Web-Interface anschaulich darstellen und besitzt die Fähigkeit, Anwendungen auf Rechner zu verteilen, die bestimmten Suchkriterien entsprechen. Die „Agent-side *IpDiscover*“ erlaubt das Auffinden von netzwerkbasierenden Computern und Geräten.

Schlüssel-Eigenschaften:

- wichtige Bestands-Informationen
- mächtiges Werkzeug zum Verteilen von Software oder Scripts
- Web-Interface
- Netzwerk-Scan
- Unterstütz viele Systeme (Windows, Linux, BSD, Sun Solaris, IBM AIX, HP-UX, MacOSX)
- Zugriff auf Webdiesnte via SOAP interface
- Unterstützung von plugins durch API
- Backup Adagios data mit NethServer „backup data tool“

4.12.1 Installation

Die Installation kann über das Webinterface von NethServer erfolgen. Nach der installation:

- Aktivieren des Admin-Kontos (siehe *Admin Benutzer* für dDtails)
- Öffnen der Url https://your_nethserver_ip/ocsreports
- Anmeldung mit `admin` Daten, um Zugriff auf das Webinterface zu erhalten.

Weitergehende Informationen befinden sich in der Original-Dokumentation

- http://www.ocsinventory-ng.org/en/
- http://wiki.ocsinventory-ng.org/index.php/Documentation:Main
- http://www.ocsinventory-ng.org/en/download/download-agent.html

KAPITEL 5

Best practices

KAPITEL 6

Appendix

KAPITEL 7

Indices

- genindex
- search

Stichwortverzeichnis

Sonderzeichen

Übersicht, 7

A

Adagios, 37
alias: DHCP, 34
alias: PXE, 34
alias: Trivial File Transfer Protocol TFTP, 35

B

Backup, 13
Benutzerprofil, 11
Benutzerzertifikate, 10
Bond, 9
Bridge, 9

C

chat, 22
content filter, 25

D

Datensicherung, 13
Default Benutzer, 5
Default password, 5
DHCP, 34
DNS, 33
DNS alias, 34
DROP, 28
Dynamic Host Configuration Protocol, 34

F

fax'server macht es möglich Faxe über ein Modem, dass direkt an den Server angeschlossen ist, oder über ein :index:'virutelles Modem, 23
Festplattennutzung, 7
firewall, 27
Firewall Log, 28
Firewall Objekte, 32

G

gateway, 27
Gewichtung, 29
Google Translate, 26

I

inline help, 12
IP/MAC Bindung, 33

J

Jabber, 22

K

Kennwort läuft ab, 21
Kennwortädnerung, 11
Konfigurationssicherung, 13
KVM, 36

N

Nagios, 37
NAT 1:1, 31
Netzwerk, 7
Netzwerkdienst, 9
Netzwerkkarte
    Rolle, 7

O

OCS Inventory NG, 37

P

Passwort, 20
PPPoE, 9
Preboot eXecution Environment, 34
Protokoll, 12
PXE, 34

Q

QoS, 32

R

Regeln, 28
REJECT, 28
Richtlinien, 27
Rolle, 8
    Netzwerkkarte, 7

S

Server Manager, 5
SSL
    Zertifikate, 10
Statische Route, 10
status, 7
strong, 20

T

TFTP, 35
Traffic Shaping, 32

V

Vertrauenswürdige Netzwerke, 10
virtual machine, 36
VLAN, 9

W

WAN, 29
web interface, 5

X

XMPP, 22

Z

Zertifikate
    SSL, 10
Zone, 8, 32