NethServer Documentation

Release 6.5

Nethesis

September 10, 2015

Contents

NethServer is an operating system designed for small offices and medium enterprises. It's simple, secure and flexible.

About

- **Official site**: http://www.nethserver.org
- **Bug tracker**: http://dev.nethserver.org
- **Twitter**: @NethServer
- **Source code**: http://dev.nethserver.org
- **Mailing list**: *nethserver@googlegroups.com*
- **ML archive**: Google Groups
- **IRC**: *#nethserver on freenode.net*

CHAPTER 1

Installation and configuration

1.1 Installation

1.1.1 Minimum requirements

Minimum requirements are:

- 64 bit CPU (x86_64)
- 1 GB of RAM
- 8 GB of disk space

Hint: We recommend to use at least 2 disks to setup a RAID 1. The RAID software will ensure data integrity in case of a disk failure.

Hardware compatibility

NethServer is compatible with any hardware certified by Red Hat® Enterprise Linux® (RHEL®), listed on hardware.redhat.com

1.1.2 Installation types

NethServer supports two installation modes. In short:

Installing from ISO

- Download the ISO image,
- Prepare a CD / DVD
- Follow the wizard

Installing from YUM

- Install CentOS Minimal
- Configure the network
- Install from network

1.1.3 Installing from ISO

Warning: The ISO installation will erase all existing data on hard drives!

Download the ISO file from official site www.nethserver.org. The downloaded ISO file can be used to **create a bootable media** such as CD or DVD. The creation of a bootable disk is different from writing files into CD/DVD, and it requires the use of a dedicated function (e.g. *write* or *burn ISO image*). Instructions on how to create a bootable CD/DVD from the ISO are easily available on the Internet or in the documentation of your system operating system.

Start the machine using the freshly backed media. If the machine will not start from the CD/DVD, please refer to the documentation of the motherboard BIOS. A typical problem is how boot device priority is configured. First boot device should be the CD/DVD reader.

On start a menu will display different types of installation:

NethServer interactive install

> It allows you to select the language, configure RAID support, network, and encrypted file system. It will be described in depth in the next paragraph.

Other / Unattended NethServer install

> This installation mode does not require any kind of human intervention: a set of default parameters will applied to the system.

Standard CentOS installations

> Use the standard CentOS installation procedure.

Tools

> Start the system in *rescue* (recovery) mode, execute a memory test or start the hardware detection tool.

Boot from local drive

> Attempts to boot a system that is already installed on the hard disk.

At the end of the installation process you will be asked to reboot the machine. Be sure to remove the installation media before restarting.

Unattended mode

After installation, the system will be configured as follows:

- Credentials: `root / Nethesis,1234`
- Network: DHCP enabled on all interfaces
- Keyboard: `|ks_keyboard|`
- Time zone: `|ks_timezone|`
- Language: `|ks_language|`
- Disks: if there are two or more disks, a RAID 1 will be created on first two disks

Install options

You can add extra parameters to unattended installation by pressing TAB and editing the boot loader command line.

To disable raid, just add this option to the command line:

```
raid=none
```

If you need to select installation hard drives, use:

```
disks=sdx,sdy
```

Other available options:

- lang: system language, default is en_US
- keyboard: keyboard layout, default is us
- timezone: default is UTC Greenwich
- password: enable file system encryption with given password

Interactive Mode

The interactive mode allows you to make a few simple choices on the system configuration:

1. Language
2. Keyboard layout
3. Time zone
4. Software RAID
5. System administrator password
6. Encrypted file system
7. Network interfaces
8. Network configuration

Language

Select the language in which you want to use the interactive mode. Selected language will be the default language of installed system. The system will also suggest default values for keyboard and time zone.

Keyboard layout

A keyboard can have different layout depending on the language for which it was made. Leave the suggested value or enter a custom value.

Time zone

The choice of time zone allows you to configure the date and time of the system. Leave the suggested value or enter a custom value.

Software RAID

RAID (Redundant Array of Independent Disks) allows you to combine all the disks in order to achieve fault tolerance and an increase in performance.

This screen is displayed when two or more disks were detected at start.

Available levels:

- RAID 1: it creates an exact copy (mirror) of all the data on two or more disks. Minimum number of disks: 2
- RAID 5: it uses a subdivision of the data at the block level, distributing the parity data evenly across all disks. Minimum number of disks: 3

Spare disk You can create a spare disk if disk number is greater than the minimum required by the selected level RAID, A spare disk will be added to the RAID in case a failure occurs.

System administrator password

You are strongly advised to set a custom administrator password.

A good password is:

- at least 8 characters long
- contain uppercase and lowercase letters
- contain symbols and numbers

Encrypted file system

When enabling this option, all data written to the disk will be encrypted using symmetric encryption. In case of theft, an attacker will not be able to read the data without the encryption key.

It is possible to choose a password for the encryption, otherwise the system administrator password will be used.

Note: You will need to enter the password at every system boot.

Network interfaces

Select the network interface that will be used to access the LAN. This interface is also known as *green* interface.

Network configuration

Host and Domain Name (FQDN)

Type the host name and domain in which the server will operate (e.g. `server.mycompany.com`).

Note: **Domain name can only contain letters, numbers and the** dash.

IP Address

Type a private IP address (from RFC 1918) to be assigned to the server; if you want to install it in an existing network, you must provide a unused IP address valid for that network (in general you can use the first or last host inside the network range, e.g. 192.168.7.1 or 192.168.7.254).

Netmask

Type the subnet mask of the network. You can safely leave the default value.

Gateway

Type the IP address of the gateway on which you are installing the server.

DNS

Type a valid DNS. Example: 8.8.8.8

End of installation procedure

After parameters input, the procedure will start the installation.

At the end of the installation procedure, *access the server-manager* to *install additional software*.

1.1.4 Install on CentOS

It is possible to install NethServer on a fresh CentOS installation using the **yum** command to download software packages. This is the recommended installation method if you have

- a virtual private servers (VPS), or
- an USB stick.

For example, if you wish to install NethServer 6.5, just start with a CentOS 6.5 on your system (many VPS providers offer CentOS pre-installed virtual machines), and then execute below commands to transform CentOS into NethServer.

Enable NethServer repositories with this command:

```
yum localinstall -y http://pulp.nethserver.org/nethserver/nethserver-release.rpm
```

To install the base system, run:

```
nethserver-install
```

Alternatively, to install base system *and* additional modules, pass the name of the module as a parameter to the install script. Example:

```
nethserver-install nethserver-mail nethserver-nut
```

At the end of the installation procedure, *access the server-manager* to *install additional software*.

1.2 Access to NethServer

NethServer can be configured using the *Server Manager* web interface. You need a web browser like Mozilla Firefox or Google Chrome to access the web interface using the address (URL) `https://a.b.c.d:980` or `https://server_name:980` where *a.b.c.d* and *server_name* respectively are the server IP address and name configured during installation.

If the web server module is installed, you can also access the web interface using this address `https://server_name/server-manager`.

The Server Manager uses self-signed SSL certificates. You should explicitly accept them the first time you access the server. The connection is safe and encrypted.

1.2.1 Login

The login page will gave you a trusted access to the web interface. Use following credentials:

- User name: **root**
- Password: **root_password** (chosen during installation process)

If the directory module is installed, and the admin user has been enabled, you can use it to access the web interface with same privileges as root user. See *Administrator user*.

1.3 Base system

This chapter describes all available modules at the end of installation. All modules outside this section must be installed from *Package manager*, including backup and users support.

1.3.1 Dashboard

The index:*Dashboard* page is the landing page after a successful login. The page will display the status and configurations of the system.

1.3.2 Network

Network configuration tells the system how the server is connected to local network (LAN) or public ones (Internet).

If the server has firewall and gateway functionality, it will handle extra networks with special function like DMZ (DeMilitarized Zone) and guests network.

NethServer supports an unlimited number of network interfaces. Any network managed by the system must follow these rules:

- networks must be physically separated (multiple networks can't be connected to the same switch/hub)
- networks must be logically separated: each network must have different addresses
- private networks, like LANs, must follow address's convention from RFC1918 document. See *Address for private networks (RFC1918)*

Every network interface as a specific role which determinates its behavior. Roles are identified by colors. Each role correspond to a well-known zone with special network traffic rules:

- *green*: local network. Hosts on this network can access any other configured network
- *blue*: guests network. Hosts on this network can access orange and red network, but can't access to green zone
- *orange*: DMZ network. Hosts on this network can access red networks, but can't access to blue, orange and green zones
- *red*: public network. Hosts on this network can access only the server itself

See *Policy* for more information on roles and firewall rules.

Note: The server must have at least one network interface. When the server has only one interface, this interface must have green role.

If the server i installed on a public VPS (Virtual Private Server) public, it should must be configured with a green interface. All critical services should be closed using *Network services* panel.

Logical interfaces

Supported logical interfaces are:

- alias: associate more than one IP address to an existing network interface. The alias has the same role of its associated physical interface
- bond: arrange two or more network interfaces, provides load balancing and fault tolerance
- bridge: connect two different networks, it's often used for bridged VPN and virtual machine
- vlan (Virtual Local Area Network): create two or more physically separated networks using a single interface

Aliases are used to configure multiple IPs on a single NIC. For example, if you want to have more public IP on a red interface.

Bonds allow you to aggregate bandwidth between two or more network interfaces. The system will use all network interfaces at the same time, balancing traffic among all active interfaces. If an error occurs, the faulty card is automatically excluded from the bond.

Bridge has the function to connect different network segments, for example by allowing virtual machines, or client connected using a VPN, to access to the local network (green).

When it is not possible to physically separate two different networks, you can use tagged vlan. The traffic of the two networks can be transmitted on the same cable, but it will be handled as if it were sent and received on separate network cards. The use of VLAN, requires properly configured switches.

Address for private networks (RFC1918)

TCP/IP private networks not directly connected to Internet should use special addresses selected by Internet Assigned Numbers Authority (IANA).

Private network	Subnet mask	IP addresses interval
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

Reset network configuration

In case of misconfiguration, it's possible to reset network configuration by following these steps.

1. Delete all logical and physical interfaces from the db

   Display current configuration:

```
db networks show
```

   Delete all interfaces:

```
db network delete eth0
```

   Repeat the operation for all interfaces including bridges, bonds and vlans.

2. Disable interfaces

   Physical interfaces:

```
ifconfig eth0 down
```

   In case of a bridge:

```
ifconfig br0 down
brctl delbr br0
```

In case of a bond (eth0 is enslaved to bond0):

```
ifenslave -d bond0 eth0
rmmod bonding
```

3. Remove configuration files

   Network configuration files are inside the `/etc/sysconfig/network-scripts/` directory in the form: `/etc/sysconfig/network-scripts/ifcfg-<devicename>`. Where *devicename* is the name of the interface like *eth0*, *br0*, *bond0*.

   Delete the files:

```
rm -f /etc/sysconfig/network-scripts/ifcfg-eth0
```

   Repeat the operation for all interfaces including bridges, bonds and vlans.

4. Restart the network

   After restarting the network you should see only the loopback interface:

```
service network restart
```

   Use **`ifconfig`** command to check the network status.

5. Manually reconfigure the network

   Choose an IP to assign to an interface, for example *192.168.1.100*:

```
ifconfig eth0 192.168.1.100
```

   Then reconfigure the system:

```
signal-event system-init
```

   The interface will have the chosen IP address.

6. Open the web interface and reconfigure accordingly to your needs

1.3.3 Network services

A network service is a service running on the firewall itself.

These services are always available to hosts on green network (local network). Access policies can be modified from *Network services* page.

Available policies are:

- Access only from green networks (private): all hosts from green networks and from VPNs
- Access from green and red networks (public): any host from green networks, VPNs and external networks. But not guests (blue) and DMZ (orange) networks
- Access only from the server itself (none): no host can connect to selected service

Custom access

If selected policy is private or public, it's possible to add hosts and networks which are always allowed (or blocked) using *Allow hosts* and *Deny hosts*. This rule also apply for blue and orange networks.

Example

Given the following configuration:

- Orange network: 192.168.2.0/24
- Access for NTP server set to private

If hosts from DMZ must access NTP server, add 192.168.2.0/24 network inside the *Allow hosts* field.

1.3.4 Remote access

Server Manager

It's possible to grant Server Manager's access to selected networks. For example, if the server is inside a customer network, you should allow connections from remote management networks.

SSH

The SSH (Secure Shell) should be always available. SSH is a protocol to open remote shells over secure connections.

Default configuration allows authentication using password and public/private keys.

1.3.5 Trusted networks

Trusted networks are special networks (local or remote) allowed to access special server's services.

For example, hosts inside trusted networks can access to:

- Server Manager
- Shared folders (SAMBA)

If users connected from VPNs must access system's services, add VPN networks to this page.

If the remote network is reachable using a router, remember to add a static route inside *Static routes* page.

1.3.6 Static routes

This page allow to create special static routes which will use the specified gateway. These routes are usually used to connect private network.

Remember to add the network to *Trusted networks*, if you wish to allow remote hosts to access local services.

1.3.7 Organization contacts

Fields in this section are used to generate self-signed SSL certificates and for user creation.

Note: Any modification to these data will regenerate all SSL certificates. Most clients will must be reconfigured.

1.3.8 User's profile

All users can login to Server Manager using their own credentials.

After login, a user can change the password and information about the account, like:

- Name and surname
- External mail address

The user can also overwrite fields set by the administrator:

- Company
- Office
- Address
- City

1.3.9 Shutdown

The machine where NethServer is installed can be rebooted or halted from the *Shutdown* page. Choose an option (reboot or halt) then click on submit button.

Always use this module to avoid bad shutdown which can cause data damages.

1.3.10 Log viewer

All services will save operations inside files called *logs*. The log analysis is the main tool to find and resolve problems. To analyze log files click in *Log viewer*.

This module allows to:

- start search on all server's logs
- display a single log
- follow the content of a log in real time

1.3.11 Date and time

After installation, make sure the server is configured with the correct timezone. The machine clock can be configured manually or automatically using public NTP servers (preferred).

The machine clock is very important in many protocols. To avoid problems, all hosts in LAN can be configured to use the server as NTP server.

1.4 Package manager

NethServer is highly modular: at the end of the installation only base system will be ready to be used. Base system includes modules like network configuration and log viewer. The administrator can install additional modules like *Email*, *DHCP and PXE server* and *Firewall and gateway*.

The main page shows all available and installed (checked) modules. The view can be filtered by category.

To install a module, check the corresponding box and click on *Apply*. To remove a module, uncheck the corresponding box and click on *Apply*. Next page will resume all modifications and display all optional packages.

Note: Optional packages can be added to the system *after* installation of the main component. Just click again on *Apply* and select optional packages from confirmation page.

The section *Installed software* displays all packages already installed into the system.

1.4.1 Inline help

All packages inside the Server Manager contain an inline help. The inline help explains how the module works and all available options.

These help pages are available in all Server Manager's languages.

A list of all available inline help pages can be found at the address:

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

Example

If the server has address `192.168.1.2`, and you want to see all English help pages, use this address:

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

CHAPTER 2

Modules

2.1 Backup

Backup is the only way to restore a machine when disasters occur. The system handles two kinds of backup:

- configuration backup
- data backup

Configuration backup contains only system configuration files. It's scheduled to be executed every night and it will create a new archive, `/var/lib/nethserver/backup/backup-config.tar.xz`, only if any file is changed in the last 24 hours. The purpose of this kind of backup is to quickly restore a machine in case of disaster recovery. When the machine is functional, a full data restore can be done even if the machine is already in production.

Data backup is enabled installing "backup" module and contains all data like user's home directories and mails. It runs every night and can be full or incremental on a weekly basis. This backup also contains the archive of the configuration backup.

Data backup can be saved on three different destinations:

- USB: disk connected to a local USB port
- CIFS: Windows shared folder, it's available on all NAS (Network Attached Storage)
- NFS: Linux shared folder, it's available on all NAS, usually faster than CIFS

The backup status can be notified to the system administrator or to an external mail address.

Note: The destination directory is based on the server host name: in case of FQDN change, the administrator should take care to copy backup data from the old directory to the new one.

2.1.1 Data restore

Make sure that backup destination is reachable (for example, USB disk must be connected).

Note: The current version supports restore only from command line.

Listing files

It's possible to list all files inside the last backup using this command:

```
backup-data-list
```

The command can take some times depending on the backup size.

File and directory

All relevant files are saved under `/var/lib/nethserver/` directory:

- Mails: `/var/lib/nethserver/vmail/<user>`
- Shared folders: `/var/lib/nethserver/ibay/<name>`
- User's home: `/var/lib/nethserver/home/<user>`

To restore a file/directory, use the command:

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

Example, restore *test* mail account to `/tmp` directory:

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

Example, restore *test* mail account to original position:

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

The system can restore a previous version of directory (or file).

Example, restore the version of a file from 15 days ago:

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

The `-t` option allows to specify the number of days (15 in this scenario).

2.1.2 Disaster recovery

The system is restored in two phases: configuration first, then data. Right after configuration restore, the system is ready to be used if proper packages are installed. You can install additional packages before or after restore. For example, if mail-server is installed, the system can send and receive mail.

Other restored configurations:

- Users and groups
- SSL certificates

Note: The root/admin password is not restored.

Steps to be executed:

1. Install the new machine with the same host name as the old one
2. Configure a data backup, so the system can retrieve saved data and configuration
3. Install additional packages (optional)
4. Restore configuration backup executing: **`restore-config`** or using the web interface
5. If the old machine was the network gateway, remember to reinstall firewall module
6. Reconfigure network from web interface

7. Verify the system is functional
8. Restore data backup executing: **`restore-data`**

2.1.3 Data backup customization

If additional software is installed, the administrator can edit the list of files and directories included (or excluded).

Inclusion

If you wish to add a file or directory to data backup, add a line to the file `/etc/backup-data.d/custom.include`.

For example, to backup a software installed inside `/opt` directory, add this line:

```
/opt/mysoftware
```

Exclusion

If you wish to exclude a file or directory from data backup, add a line to the file `/etc/backup-data.d/custom.exclude`.

For example, to exclude all directories called *Download*, add this line:

```
**Download**
```

To exclude a mail directory called *test*, add this line:

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

Same syntax applies to configuration backup. Modification should be done inside the file `/etc/backup-config.d/custom.exclude`.

Note: Make sure not to leave empty lines inside edited files.

2.1.4 Configuration backup customization

In most cases it is not necessary to change the configuration backup. But it can be useful, for example, if you have installed a custom SSL certificate. In this case you can add the file that contains the certificate to the list of files to backup.

Inclusion

If you wish to add a file or directory to configuration backup, add a line to the file `/etc/backup-config.d/custom.include`.

For example, to backup `/etc/pki/mycert.pem` file , add this line:

```
/etc/pki/mycert.pem
```

Do not add big directories or files to configuration backup.

Exclusion

If you wish to exclude a file or directory from configuration backup, add a line to the file `/etc/backup-config.d/custom.exclude`.

Note: Make sure not to leave empty lines inside edited files. The syntax of the configuration backup supports only simple file and directory paths.

2.2 Users and groups

2.2.1 Users

A system user is required to access many services provided by NethServer (email, shared folders, etc..).

Each user is characterized by a pair of credentials (user and password). A newly created user account remains locked until it has set a password. A blocked user can not use the services of servers that require authentication.

When creating a user, following fields are mandatory:

- Username
- Name
- Surname

Optional fields:

- Company
- Office
- Address
- City
- Phone

Just after creation, the user is disabled. To enable the user, set a password using the *Change password* button. When a user is enabled, the user can access to the Server Manager and change his/her own password: *User's profile*.

A user can be added to one or more group from the *Users* page or from the *Groups* one.

Sometimes you need to block user's access to service without deleting the the account. This behavior can be achieved using the *Lock* and *Unlock* buttons.

Note: When a user is deleted, all user data will be also deleted.

Access to services

After creation a user can be enabled only to some (or all) services. This configuration can be done using the *Services* tab page.

2.2.2 Groups

A group of user can be used to assign special permissions to some users or to create email distribution lists.

As for the users, a group can be enabled to some (or all) services.

2.2.3 Administrator user

The *Users* module creates the user *admin* that allows access to the web interface with the same password for the *root* user. The admin user does not have access to the system from the command line. Despite being two separate users, the password of both coincide and can be changed from the web interface.

On some occasions, it may be useful to differentiate the admin and root password, for example, to allow an inexperienced user to use the web interface to perform common tasks and inhibiting access to the command line.

Avoid root and admin password synchronization by run the following command

```
config setprop AdminIsNotRoot enabled
```

Then change the admin password from the panel *Users*. Without password synchronization, admin will have the new password, and root will keep keep the old one.

If you want to change the root password, it should be done from the command line using **passwd**.

2.2.4 Password management

The system provides the ability to set constraints on password *complexity* and *expiration*.

Complexity

The password complexity is a set of minimum conditions that password must match to be accepted by the system: You can choose between two different management policies about password complexity:

- *none*: there is no specific control over the password entered, but minimum length is 7 characters
- *strong*

The strong policy requires that the password must comply with the following rules:

- Minimum length of 7 characters
- Contain at least 1 number
- Contain at least 1 uppercase character
- Contain at least 1 lowercase character
- Contain at least 1 special character
- At least 5 different characters
- Must be not present in the dictionaries of common words
- Must be different from the username
- Can not have repetitions of patterns formed by 3 or more characters (for example the password As1.$ AS1. $ is invalid)

The default policy is *strong*.

Warning: Changing the default policies is highly discouraged. The use of weak passwords often lead to compromised servers by external attackers.

To change the setting to none

```
config setprop passwordstrength Users none
```

To change the setting to strong

```
config setprop passwordstrength Users strong
```

Check the policy currently in use on the server

```
config getprop passwordstrength Users
```

Expiration

The password expiration is enabled by default to 6 months from the time when the password is set. The system will send an e-mail to inform the users when their password is about to expire.

Note: The system will refer to the date of the last password change, whichever is the earlier more than 6 months, the server will send an email to indicate that password has expired. In this case you need to change the user password. For example, if the last password change was made in January, and the activation of the deadline in October, the system will assume the password changed in January is expired, and notify the user.

If you wish to bypass the password expiration globally (also allow access for users with expired password)

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

To disable password expiration for a single user (replace username with the user)

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

Below are the commands to view enabled policies.

Maximum number of days for which you can keep the same password (default: 180)

```
config getprop passwordstrength MaxPassAge
```

Minimum number of days for which you are forced to keep the same password (default 0)

```
config getprop passwordstrength MinPassAge
```

Number of days on which the warning is sent by email (default: 7)

```
config getprop passwordstrength PassWarning
```

To change the parameters replace the **getprop** command with **setprop**, then add the desired value at end of the line. Finally apply new configurations:

```
signal-event password-policy-update
```

For example, to change to 5 “Number of days on which the warning is sent by email”

```
config setprop passwordstrength PassWarning 5
signal-event password-policy-update
```

Effects of expired password

After password expiration, the user will be able to read and send mails but can no longer access the shared folders and printers (Samba) or or other computer if the machine is part of the domain.

Domain password

If the system is configured as a domain controller,users can change their password using the Windows tools.

In the latter case you can not set passwords shorter than 6 *characters* regardless of the server policies. Windows performs preliminary checks and sends the password to the server where they are then evaluated with enabled policies.

2.2.5 Import users

The system can import a list of users from a CSV file. The file must contain a line per user, each line must have TAB-separated fields and must respect following format:

```
username    firstName    lastName    email    password
```

Example:

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

Make sure the mail server is installed, then execute:

```
/usr/share/doc/nethserver-directory-<ver>/import_users <youfilename>
```

For example, if the user's file is `/root/users.csv`, execute following command:

```
/usr/share/doc/nethserver-directory-`rpm --query --qf "%{VERSION}" nethserver-directory`/import_users
```

The command can be executed multiple times: already existing users will be skipped.

Note: The command will fail if mail server module is not installed

2.3 Email

The Email module is split in three main parts:

- SMTP server for sending and receiving [1]
- IMAP and POP3 server to read email [2], and Sieve language to organize it [3]
- Anti-spam filter, anti-virus and attachments blocker [4]

Benefits are

- complete autonomy in the mail management
- avoid problems due to the Internet Service Provider
- ability to track the route of messages in order to detect errors
- optimized anti-virus and anti-spam scan

See also the following related topics:

- How electronic mail works [5]

[1] Postfix mail server http://www.postfix.org/
[2] Dovecot Secure IMAP server http://www.dovecot.org/
[3] Sieve mail filtering language http://en.wikipedia.org/wiki/Sieve_(mail_filtering_language)
[4] MTA/content-checker interface http://www.ijs.si/software/amavisd/
[5] Email, http://en.wikipedia.org/wiki/Email

- MX DNS record [6]
- Simple Mail Transfer Protocol (SMTP) [7]

2.3.1 Domains

NethServer can handle an unlimited number of mail domains, configurable from the *Email* > *Domains* page. For each domain there are two alternatives:

- *Deliver* messages to local mailboxes, according to the Maildir [8] format.
- *Relay* messages to another mail server.

Note: If a domain is deleted, email will not be deleted, too; any message already received is preserved.

NethServer allows storing an *hidden copy* of all messages directed to a particular domain: they will be delivered to the final recipient *and also* to a local user (or group). The hidden copy is enabled by the *Always send a copy (Bcc)* check box.

Warning: On some countries, enabling the *Always send a copy (Bcc)* can be against privacy laws.

NethServer can automatically *append a legal note to sent messages*. This text is called *disclaimer* and it can be used to meet some law's requirements. Please note *signature* and disclaimer are very different concepts.

The signature should be inserted inside the message text only by the mail client (MUA): Outlook, Thunderbird, etc. Usually it is a user-defined text containing information such as sender addresses and phone numbers.

Signature example:

```
John Smith
President | My Mighty Company | Middle Earth
555-555-5555 | john@mydomain.com | http://www.mydomain.com
```

The "disclaimer" is a fixed text and can only be *attached* (not added) to messages by the mail server.

This technique allows maintaining the integrity of the message in case of using digital signature.

Disclaimer example:

```
This email and any files transmitted with it are confidential and
intended solely for the use of the individual or entity to whom they
are addressed.  If you have received this email in error please
notify the system manager.  This message contains confidential
information and is intended only for the individual named.
```

The disclaimer text can contain Markdown [9] code to format the text.

2.3.2 Email addresses

The system enables the creation of an unlimited number of *email addresses* also known as *pseudonyms*, from the *Email addresses* page. Each address is associated with a system user or group owning a *mailbox* (see *User and group mailboxes*). It can be enabled on all configured domains or only on specific domains. For example:

- First domain: mydomain.net

[6] The MX DNS record, http://en.wikipedia.org/wiki/MX_record
[7] SMTP, http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
[8] The Maildir format, http://en.wikipedia.org/wiki/Maildir
[9] The Markdown plain text formatting syntax, http://en.wikipedia.org/wiki/Markdown

- Second domain: example.com
- Email address *info* valid for both domains: info@mydomain.net, info@example.com
- Email address *goofy* valid only for one domain: goofy@example.com

Sometimes a company forbids communications from the external world using personal email addresses. The *Local network only* option blocks the possibility of an address to receive email from the outside. Still the "local network only" address can be used to exchange messages with other accounts of the system.

When creating a new account from the *Users* or *Groups* page, the system suggests a default email address for each configured mail domain.

For instance, creating a new account for user *Donald Duck*:

- User name: donald.duck
- Domains: ducks.net, ducks.com
- Suggested addresses: donald.duck@ducks.net, donald.duck@ducks.com

2.3.3 User and group mailboxes

Email messages delivered to a user or group account, as configured from the *Email addresses* page, are written to a disk location known as *mailbox*.

When the Email module is installed, existing user and group accounts do not have a mailbox. It must be explicitly enabled from the *Users* > *Services* or *Groups* > *Services* tab. Instead, newly created accounts have this option enabled by default.

From the same *Services* page under *Users* or *Groups* it can be defined an external email address where to *Forward messages*. Optionally, a copy of the message can be stored on the server.

When an address is associated with a group, the server can be configured to deliver mail in two ways, from the *Groups* > *Services* tab:

- send a copy to each member of the group
- store the message in a *shared folder*. This option is recommended for large groups receiving big messages.

Warning: Deleting a user or group account erases the associated mailbox!

The *Email* > *Mailboxes* page controls what protocols are available to access a user or group mailbox:

- IMAP [10] (recommended)
- POP3 [11] (obsolete)

For security reasons, all protocols require STARTTLS encryption by default. The *Allow unencrypted connections*, disables this important requirement, and allows passing clear-text passwords and mail contents on the network.

Warning: Do not allow unencrypted connections on production environments!

From the same page, the *disk space* of a mailbox can be limited to a *quota*. If the mailbox quota is enabled, the *Dashboard* > *Mail quota* page summarizes the quota usage for each user. The quota can be customized for a specific user in *Users* > *Edit* > *Services* > *Custom mailbox quota*.

[10] IMAP http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol
[11] POP3 http://en.wikipedia.org/wiki/Post_Office_Protocol

Messages marked as **spam** (see *Filter*) can be automatically moved into the *junkmail* folder by enabling the option *Move to "junkmail" folder"*. Spam messages are expunged automatically after the *Hold for* period has elapsed. The spam retention period can be customized for a specific user in *Users* > *Edit* > *Services* > *Customize spam message retention*.

2.3.4 Messages

From the *Email* > *Messages* page, the *Queue message max size* slider sets the maximum size of messages traversing the system. If this limit is exceeded, a message cannot enter the system at all, and is rejected.

Once a message enters NethServer, it is persisted to a *queue*, waiting for final delivery or relay. When NethServer relays a message to a remote server, errors may occur. For instance,

- the network connection fails, or
- the other server is down or is overloaded.

Those and other errors are *temporary*: in such cases, NethServer attempts to reconnect the remote host at regular intervals until a limit is reached. The *Queue message lifetime* slider changes this limit. By default it is set to *4 days*.

While messages are in the queue, the administrator can request an immediate message relay attempt, by pressing the button *Attempt to send* from the *Email* > *Queue management* page. Otherwise the administrator can selectively delete queued messages or empty the queue with *Delete all* button.

To keep an hidden copy of any message traversing the mail server, enable the *Always send a copy (Bcc)* check box. This feature is different from the same check box under *Email* > *Domain* as it does not differentiate between mail domains and catches also any outgoing message.

Warning: On some countries, enabling the *Always send a copy (Bcc)* can be against privacy laws.

The *Send using a smarthost* option, forces all outgoing messages to be directed through a special SMTP server, technically named *smarthost*. A smarthost accepts to relay messages under some restrictions. It could check:

- the client IP address,
- the client SMTP AUTH credentials.

Note: Sending through a *smarthost* is generally not recommended. It might be accepted only if the server is temporarily blacklisted [12], or normal SMTP access is restricted by the ISP.

2.3.5 Filter

All transiting email messages are subjected to a list of checks that can be selectively enabled in *Email* > *Filter* page:

- Block of attachments
- Anti-virus
- Anti-spam

Block of attachments

The system can inspect mail attachments, denying access to messages carrying forbidden file formats. The server can check following attachment classes:

[12] DNSBL http://en.wikipedia.org/wiki/DNSBL

- executables (eg. exe, msi)
- archives (eg. zip, tar.gz, docx)
- custom file format list

The system recognizes file types by looking at their contents, regardless of the file attachment name. Therefore it is possible that MS Word file (docx) and OpenOffice (odt) are blocked because they actually are also zip archives.

Anti-virus

The anti-virus component finds email messages containing viruses. Infected messages are discarded. The virus signature database is updated periodically.

Anti-spam

The anti-spam component [13] analyzes emails by detecting and classifying *spam* [14] messages using heuristic criteria, predetermined rules and statistical evaluations on the content of messages. The rules are public and updated on a regular basis. A score is associated to each rule.

Total spam score collected at the end of the analysis allows the server to decide whether to *reject* the message or *mark* it as spam and deliver it anyway. The score thresholds are controlled by *Spam threshold* and *Deny message spam threshold* sliders in *Email* > *Filter* page.

Messages marked as spam have a special header `X-Spam-Flag: YES`. The *Add a prefix to spam messages subject* option makes the spam flag visible on the subject of the message, by prepending the given string to the `Subject` header.

Statistical filters, called Bayesian [15], are special rules that evolve and quickly adapt analyzing messages marked as **spam** or **ham**.

The statistical filters can then be trained with any IMAP client by simply moving a message in and out of the *junkmail folder*. As prerequisite, the junkmail folder must be enabled from *Email* > *Mailboxes* page by checking *Move to "junkmail" folder"* option.

- By *putting a message into the junkmail folder*, the filters learn it is spam and will assign an higher score to similar messages.
- On the contrary, by *getting a message out of junkmail*, the filters learn it is ham: next time a lower score will be assigned.

By default, all users can train the filters using this technique. If a group called `spamtrainers` exits, only users in this group will be allowed to train the filters.

Note: It is a good habit to constantly check the junkmail folder in order to not losing email wrongly marked as spam.

If the system fails to recognize spam properly even after training, the *whitelists* and *blacklists* can help. Those are lists of email addresses or domains respectively always allowed and always blocked to send or receive a message.

The section *Rules by mail address* allows creating three types of rules:

- *Block From*: any message from specified sender is blocked
- *Allow From*: any message from specified sender is accepted
- *Allow To*: any message to the specified recipient is accepted

[13] Spamassassin home page http://wiki.apache.org/spamassassin/Spam
[14] SPAM http://en.wikipedia.org/wiki/Spamming
[15] Bayesian filtering http://en.wikipedia.org/wiki/Naive_Bayes_spam_filtering

Note: Antivirus checks are enforced despite *whitelist* settings.

2.3.6 Client configuration

The server supports standard-compliant email clients using the following IANA ports:

- imap/143
- pop3/110
- smtp/587
- sieve/4190

Authentication requires the STARTTLS command and supports the following variants:

- LOGIN
- PLAIN

Also the following SSL-enabled ports are available for legacy software that still does not support STARTTLS:

- imaps/993
- pop3s/995
- smtps/465

Warning: The standard SMTP port 25 is reserved for mail transfers between MTA servers. On clients use only submission ports.

If NethServer acts also as DNS server on the LAN, it registers its name as MX record along with the following aliases:

- `smtp.<domain>`
- `imap.<domain>`
- `pop.<domain>`
- `pop3.<domain>`

For example:

- Domain: `mysite.com`
- Hostname: `mail.mysite.com`
- MX record: `mail.mysite.com`
- Available aliases: `smtp.mysite.com`, `imap.mysite.com`, `pop.mysite.com`, `pop3.mysite.com`.

Note: Some email clients (e.g. Mozilla Thunderbird) are able to use DNS aliases and MX record to automatically configure email accounts by simply typing the email address.

To disable local MX and aliases, access the root's console and type:

```
config setprop postfix MxRecordStatus disabled
signal-event nethserver-hosts-save
```

2.3.7 Special SMTP access policies

By default, all clients must use the submission port 587 with encryption and authentication enabled to send mail through the SMTP server.

The server also implements special access policies to ease the configuration of legacy environments.

Warning: Do not change the default policy on new environments!

Use these commands to enable sending on port 25 with TLS and authentication:

```
config setprop postfix AccessPolicies smtpauth
signal-event nethserver-mail-common-save
```

Use these commands to enable sending on port 25 without authentication from any client from trusted networks:

```
config setprop postfix AccessPolicies trustednetworks
signal-event nethserver-mail-common-save
```

Policies can be used together, by separating with a comma `,`:

```
config setprop postfix AccessPolicies trustednetworks,smtpauth
signal-event nethserver-mail-common-save
```

However, there are some devices (printers, scanners, ...) that do not support SMTP authentication, encryption or port settings. They can be enabled to send messages by looking at their IP address in Postfix `access` table:

```
mkdir -p /etc/e-smith/templates-custom/etc/postfix/access
echo "192.168.1.22 OK" >> /etc/e-smith/templates-custom/etc/postfix/access/20clients
signal-event nethserver-mail-common-save
```

2.3.8 Custom HELO

The first step of an SMTP session is the exchange of *HELO* command (or *EHLO*). This command takes a valid server name as required parameter (RFC 1123).

NethServer and other mail servers try to reduce spam by not accepting HELO domains that are not registered on a public DNS.

When talking to another mail server, NethServer uses its full host name (FQDN) as the value for the HELO command. If the FQDN is not registered in public DNS, the HELO can be fixed by setting a special *prop*. For instance, assuming `myhelo.example.com` is the publicly registered DNS record, type the following commands:

```
config setprop postfix HeloHost myhelo.example.com
signal-event nethserver-mail-common-save
```

This configuration is also valuable if the mail server is using a free dynamic DNS service.

2.3.9 Email in Active Directory

The Email module integrates with an Active Directory (AD) environment, if *Active Directory member* role is enabled in *Windows Network* page.

Make sure *LDAP accounts branch* in *Windows Network* page is actually set to the LDAP branch where email users and groups are placed.

This is an example of an user entry in AD LDAP (some attributes omitted):

```
dn: CN=John Smith,OU=Sviluppo,OU=Nethesis,DC=adnethesis,DC=it
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: John Smith
sn: Smith
givenName: John
distinguishedName: CN=John Smith,OU=Sviluppo,OU=Nethesis,DC=adnethesis,DC
 =it
instanceType: 4
displayName: John Smith
memberOf: CN=sviluppo,OU=Nethesis,DC=adnethesis,DC=it
memberOf: CN=secgroup,OU=Nethesis,DC=adnethesis,DC=it
memberOf: CN=tecnici,OU=Nethesis,DC=adnethesis,DC=it
name: John Smith
primaryGroupID: 513
sAMAccountName: john.smith
sAMAccountType: 805306368
userAccountControl: 66048
userPrincipalName: john.smith@adnethesis.it
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=adnethesis,DC=it
mail: john@adnethesis.it
otherMailbox: smtp:js@adnethesis.it
proxyAddresses: smtp:j.smith@adnethesis.it
```

To make NethServer work with the external LDAP database provided by Active Directory, the following rules applies:

1. Only enabled accounts are considered (`userAccountControl` attribute).
2. IMAP and SMTP login name is the value of `sAMAccountName` attribute.
3. Email addresses associated with an user are the values of `mail`, `otherMailbox` and `proxyAddresses` attributes. The last two attributes expect a `smtp:` prefix before the actual value. Also `userPrincipalName` is considered an email address, by default; this can be disabled (see *commands below*).
4. A group email address is the value of its `mail` attribute. By default any group is treated as a *distribution list*: a copy of the email is delivered to its members.
5. The domain part of email addresses specified by the above attributes must match a *configured domain*, otherwise it is ignored.

To configure security groups as *shared folders* globally, type the following commands at root's console:

```
config setprop postfix AdsGroupsDeliveryType shared
signal-event nethserver-samba-save
```

Warning: Avoid AD group names containing uppercase letters with shared folder: IMAP ACLs does not to work properly. See BUG#2744.

To avoid the `userPrincipalName` attribute is considered a valid email address, type the following commands at root's console:

```
config setprop postfix AdsMapUserPrincipalStatus disabled
signal-event nethserver-samba-save
```

2.3.10 Log

Every mail server operation is saved in the following log files:

- `/var/log/maillog` registers all mail transactions
- `/var/log/imap` contains users' login and logout operations

A transaction recorded in the `maillog` file usually involves different components of the mail server. Each line contains respectively

- the timestamp,
- the host name,
- the component name, and the process-id of the component instance
- a text message detailing the operation

Here follows a brief description of the component names and the typical actions performed.

`transfer/smtpd`

This is the public-facing SMTP daemon, listening on port 25. A log line from this component identifies an activity involving another Mail Transfer Agent (MTA).

`submission/smtpd`

This is the SMTP daemon listening on submission port 587 and smtps port 465. A log line from this component identifies a Mail User Agent (MUA) that sends an email message.

`amavis`

The Amavis SMTP daemon enforces all mail filtering rules. It decides what is accepted or not. Log lines from this component detail the filter decisions.

`queue/smtpd`

This is an internal SMTP daemon, accessible only from the local system. It receives and queues good messages from Amavis.

`relay/smtp`

This is the SMTP client talking to a remote server: it picks a message from the queue and relays it to the remote server, as specified by the mail domain configuration.

`delivery/lmtp`

Messages directed to local accounts are picked up from the queue and transferred to the local Dovecot instance.

`dovecot`

The Dovecot daemon delivers messages into users' mailboxes, possibly applying Sieve filters.

A picture of the whole system is available from *workaround.org* [16].

References

2.4 Webmail

The default webmail client is Roundcube. Roundcube main features are:

- Simple and fast
- Built-in address book integrated with internal LDAP

[16] The wondrous Ways of an Email https://workaround.org/ispmail/lenny/bigpicture

- Support for HTML messages
- Shared folders support
- Plugins

The webmail is available at the following URLs:

- http://_server_/webmail
- http://_server_/roundcubemail

For example, given a server with IP address *192.168.1.1* and name *mail.mydomain.com*, valid addresses are:

- http://192.168.1.1/webmail
- http://192.168.1.1/roundcubemail
- http://mail.mydomain.com/webmail
- http://mail.mydomain.com/roundcubemail

2.4.1 Plugins

Roundcube supports many plugins already bundled within the installation.

Plugins enabled by default:

- Manage sieve: manage filters for incoming mail
- Mark as junk: mark the selected messages as Junk and move them to the configured Junk folder

Other recommended plugins:

- New mail notifier
- Emoticons
- VCard support

Plugins can be added or removed by editing the comma-separated list inside the `Plugins` property. For example, to enable "mail notification", "mark as junk" and "manage sieve plugins", execute from command line:

```
config setprop roundcubemail PluginsList managesieve,markasjunk,newmail_notifier
signal-event nethserver-roundcubemail-update
```

A list of bundled plugins can be found inside file:`/usr/share/roundcubemail/plugins` directory. To get the list, just execute:

```
ls /usr/share/roundcubemail/plugins
```

2.4.2 Access

With default configuration webmail is accessible using HTTPS from any network.

If you want to restrict the access only from green and trusted networks, execute:

```
config setprop roundcubemail access private
signal-event nethserver-roundcubemail-update
```

If you want to open the access from any network:

```
config setprop roundcubemail access public
signal-event nethserver-roundcubemail-update
```

2.5 POP3 connector

The *POP3 connector* page allows configuring a list of mail accounts that will be checked regularly. Messages from these remote accounts will be delivered to local users or groups.

It is not recommended to use the POP3 connector as the primary method for managing email. Mail delivery can be affected by space and connectivity problems of the provider's server. Also the spam filter is less effective, because the original email envelope information are lost.

POP3/IMAP accounts are configured from *POP3 connector* > *Accounts* page. For each account can be specified:

- the email address (as unique account identifier),
- the protocol (IMAP/POP3),
- the remote server address,
- the account credentials,
- the local user or group account where to deliver messages,
- if SSL should be disabled (not recommended),
- if a message has to be deleted from the remote server after delivery.

Note: It is allowed to associate more external accounts to a local one. Deleting an account will *not* delete already delivered messages.

After the account configuration has been completed, the POP3 connector module must be activated explicitly from the *POP3 connector* > *General* page. On the same page the remote server polling interval can be set from *Check accounts every* menu.

The underneath implementation is based on *Fetchmail* [17]. After fetching mail messages from the POP3/IMAP provider, Fetchmail delivers them locally by connecting directly to the local mail-filter server. All messages are filtered accordingly to the *configured rules*.

All operations are logged to the following files:

- `/var/log/fetchmail.log`
- `/var/log/maillog`

Warning: If an *Active Directory* account was selected for delivery and has been subsequently deleted, the configuration becomes inconsistent! The existing account configuration in *POP3 connector* page must be disabled or deleted.

[17] Fetchmail is a remote-mail retrieval and forwarding utility http://www.fetchmail.info/

References

2.6 POP3 proxy

A user on the LAN can configure an email client in order to connect to an external POP3 server and download mail messages. However, fetched mail could contain viruses that may infect computer on the network.

The POP3 proxy intercepts connection to external servers on port 110, then it scans all incoming email, in order to block viruses and tag spam. The process is absolutely transparent to mail clients: the user believes to connect directly to the provider's POP3 server, but the proxy will intercept all traffic and handle the connection to the server.

It's possible to selectively activate following controls:

- antivirus: messages containing virus are rejected and a notification email is sent to the user
- spam: messages will be marked with the appropriate anti-spam scores

2.6.1 POP3s

The proxy can also intercept POP3s connections on port 995. The proxy will establish a secure connection to the external server, but data exchange with LAN client will be in the clear text.

Note: Mail clients must be configured to connect to port 995 but will have to turn off encryption.

2.7 Shared folders

A shared folder is a resource on the system which can be accessed according to services installed on the system and permissions set by this module.

2.7.1 Create new / edit

Depending on the services installed on your system you will see several tabs.

General

Name The name of the shared folder. It can only contain lower case letters, numbers, dots, dashes and underscores. The maximum length of the name is 12 characters.

Description Optional field for a brief description of the shared folder.

Group owner The owning group of the shared folder, only members of the group can access the folder.

Allow writing to the group owner Allow write access to members of the owning group.

Allow read access to all Read access to anyone who connects to the system, as well as public networks.

ACL

The Access Control List allows specifing access permissions to the shared folder for each users or groups, in addition to those of the group owner.

Read Allow or deny read access to the user or group selected.

Write Allow or deny the access in writing to the user or group selected.

2.7.2 Delete

Removes the folder and all its contents. *The action is not reversible!* The only way to recover the contents of a folder shared that as been removed is to restore a backup.

2.7.3 Reset permissions

Set the group owner and ACLs configured using this module on all files in the folder. The operation will be performed recursively on all files and subfolders in the shared folder.

Web access

Enables access to the shared folder from the web.

Virtual Host Allows you to choose which host name is available on the shared folder. The list comes from the card "Server Alias" in the module "DNS and DHCP."

Web address (URL) Defines the web address on which the resource is available.

Allow access only from local networks If only enabled, restricts access to the resource only to local networks.

Require a password The access to the resource from the web requires no authentication. Enable this option to require a password: specify it in the field below.

Samba

Samba provides file and printer sharing to client SMB/CIFS (Windows File and Printer Sharing).

Enable Samba Enables access as a "shared folder" of Windows.

Network Recycle Bin Collects files deleted by this shared folder, so similar to the Windows Recycle Bin.

Keep files of the same name If two files of the same name, they remain distinct in trash. By disabling this option, the last one overwrites the previous year.

Guest Access A *guest user* is a user whose identification is failed because it did not provide credentials or has provided incorrect. For users or devices that act in this mode, you can grant the following permissions:

- None
- Read-only
- Read and write

2.8 Windows network

Microsoft Windows™ interoperability is provided by Samba [18]. To install it, select the *File Server* module, or any other module that requires it.

NethServer configures Samba to act in a Windows network according to its *role*. You can choose the role from the Server Manager, in the *Windows network* page.

[18] Samba official website http://www.samba.org/

Currently the following roles are available:

- Workstation
- Primary Domain Controller
- Active Directory Member

The differences between these roles concern *where* user database is stored and *which hosts* can access it. The user database contains the list of users of the system, their passwords, group membership and other informations.

Workstation

> In this role NethServer use only its own local user database. Only local users can access its resources, by providing the correct user name and password credentials. This is the behaviour of a Windows standalone workstation.

Primary Domain Controller

> When acting as *Primary Domain Controller* (PDC), NethServer emulates a Windows 2000/NT domain controller, by providing access to the local user database only from trusted workstations. People can log on any trusted workstation by typing their domain credentials, then have access to shared files and printers.

Active Directory member

> In this role NethServer becomes a trusted server of an existing Active Directory domain. When accessing a resource from a domain workstation, user credentials are checked against a domain controller, and the access to the resource is granted.

2.8.1 Workstation

When acting as a workstation, NethServer registers itself as member of the *Windows workgroup* specified by the *Workgroup name* field. The default value is `WORKGROUP`.

From the other hosts of the Windows network, NethServer will be listed in *Network resources*, under the node named after the *Workgroup name* field value.

As stated before, to access the server resources, clients must provide the authentication credentials of a valid local account.

2.8.2 Primary domain controller

The Primary Domain Controller (PDC) is a centralized place where users and hosts accounts are stored. To setup a Windows network where NethServer acts in PDC role follow these steps.

1. From the Server Manager, *Windows Network* page, select *Primary Domain Controller*, then *SUBMIT* the change.

   The Domain name by default is assumed to be the second domain part of the host name in capital letters (e.g. if the FQDN server host name is `server.example.com` the default domain name will be `EXAMPLE`. If the default does not fit your needs, choose a simple name respecting the rules:

   - length between 1 and 15 characters;
   - begin with a letter, then only letters, numbers, or the minus – char;
   - only capital letters.

   For more informations refer to Microsoft Naming conventions [19].

[19] Naming conventions in Active Directory for computers, domains, sites, and OUs http://support.microsoft.com/kb/909264

2. For each workstation of the Windows network, join the new domain. This step requires privileged credentials. In NethServer, members of the `domadmins` group can join workstations to the domain. Moreover, `domadmins` members are granted administrative privileges on domain workstations. By default, only the `admin` user is member of the `domadmins` group.

   Some versions of Windows may require applying a system registry patch to join the domain. From the Server Manager, follow *Client registry settings* link to download the appropriate `.reg` file. Refer to the official Samba documentation [20] for more informations.

2.8.3 Active Directory member

The Active Directory member role (ADS) configures NethServer as an Active Directory domain member, delegating authentication to domain controllers. When operating in ADS mode, Samba is configured to map domain accounts into NethServer, thus files and directories access can be shared across the whole domain.

Joining an Active Directory domain has some pre-requisites:

1. In *DNS and DHCP* page, set the domain controller as DNS. If a second DC exists, it can be set as secondary DNS.
2. In *Date and time* page, set the DC as NTP time source; the Kerberos protocol requires the difference between systems clocks is less than 5 minutes.

After pre-requisites are set, proceed in *Windows network* page, by selecting the *Active Directory member* role:

- Fill *Realm* and *Domain* fields with proper values. Defaults come from FQDN host name: maybe they do not fit your environment so **make sure Realm and Domain fields are set correctly**.
- *LDAP accounts branch* must be set to the LDAP branch containing your domain accounts if you plan to install the *Email* module. It is not actually required by Samba.
- *SUBMIT* changes. You will be prompted for an user name and password: provide AD `administrator` or any other account credentials with permissions to join the machine to the domain.

Note: For Email integration with AD, refer also to *Email in Active Directory*.

2.9 Chat

The chat service uses the standard protocol Jabber/XMPP and support TLS on standard ports (5222 or 5223).

The main features are:

- Messages between users of the system
- Possibility to divide the users into groups, according to the company or department / office
- Chat server's administrators
- Broadcast messages
- Group chat
- Offline messages
- Transfer files over LAN

All system users can access the chat using their own credentials.

[20] Registry changes for NT4-style domains https://wiki.samba.org/index.php/Registry_changes_for_NT4-style_domains

2.9.1 Client

Jabber clients are available for all desktop and mobile platforms.

Some widespread clients:

- Pidgin is available for Windows and Linux
- Adium for Mac OS X
- BeejibelIM for Android and iOS, Xabber only for Android

When you configure the client, make sure TLS (or SSL) is enabled. Enter the user name and the domain of the machine.

If NethServer is also the DNS server of the network, the client should automatically find the server's address through special pre-configured DNS records. Otherwise, specify the server address in the advanced options.

2.9.2 Administrators

All users within the group `jabberadmins` are considered administrators of the chat server.

Administrators can:

- Send broadcast messages
- Check the status of connected users

The group `jabberadmins` is configurable from *Groups* page.

2.10 UPS

NethServer supports the management of UPS (Uninterruptible Power Supply) connected to the system.

The server can be configured in two ways:

- *master*: UPS is directly connected to the server, the server accepts connections from slaves
- *slave*: UPS is connected to another server accessible over the network

---

Note: You should consult the list of supported models before buying, by trying to put the model into the search field of the web interface

---

In master mode, the UPS can be connected to the server:

- on a serial port
- on a USB port
- with a USB to serial adapter

In slave mode, you will need to provide the IP address of the master server.

The default configuration provides a controlled shutdown in the event of the absence of power.

2.10.1 Custom device

If the UPS is connected to a port that is not listed in the web interface, you can configure a custom device with the following commands:

```
config setprop ups Device <your_device>
signal-event nethserver-nut-save
```

2.10.2 UPS statistics

If the statistics module (collectd) is installed and running, the module will automatically collect statistic data about UPS status.

2.11 Fax Server

The fax server allows you to send and receive faxes via a modem connected directly to a server port (COM or USB) or through a virtual IAX modem.

The modem must support sending and receiving faxes preferably in class 1 or 1.0 (2, 2.0 and 2.1 classes are also supported).

2.11.1 General

Country code The international prefix to be prepended to your fax number.

Prefix Area code.

Fax Number Fax number of the sender.

Sender (TSI) The TSI is printed in the header of the recipient fax, usually in the top row. It's possible to enter the fax number or name of a total length of up to 20 characters (recommended your company name). Only alphanumeric characters are allowed.

2.11.2 Modem

Modem The physical port (COM or USB) to which the modem is attached or virtual fax modem

- Device Standard: allows you to select the device from a list of common ports
- Custom Device: allows you to specify a custom device to be used as a fax modem. * Must be the name of a device in the system.*

Mode Specifies the operating mode of the selected device. The available modes are:

- Send and receive: the modem will be used to send and receive faxes
- Receive only: the modem will be used only for receiving faxes
- Send only: the modem will only be used for sending faxes

PBX Prefix If the fax modem is connected to a PABX, you may need to enter an access code to "get an outside line." If the modem is directly connected to a line, or the PBX requires no code, leave the field empty. If you are behind a PBX, enter the prefix to be dialed.

Wait for dial tone Some modems are not capable of recognizing a dial tone (especially if connected to a PBX) and do not dial the number signalling the absence of tone (error "No Dial Tone").

To configure the modem to ignore the absence of line and immediately dial the number select Disabled. The recommended setting is "Enabled", you may want to disable * Wait for dial tone * only in case of problems.

2.11.3 Email notifications

Received faxes format By default, the fax server forwards the received faxes as emails with an attachment. Specify the email address where faxes will be delivered, and one or more formats for the attachment. To not receive the fax as attachment, but only a notification of reception, deselect all formats.

Forward received faxes to

- **Group "faxmaster"** By default, the received faxes are sent to *faxmaster*: if a user needs to receive incoming faxes should be added to this group.
- **External email** Input an external email address in case you want to send received faxes to an email address not on this server.

Sent faxes format If requested by the client, the server sends an email notification with an attachment. Choose the format in which you prefer to receive the fax. Deselect all options if you do not want to receive the fax attached.

Add delivery notification If selected, adds a delivery notification report in the sent fax email.

2.11.4 Additional functions

View faxes sent by the client The fax clients also allow you to view all incoming faxes. If, for reasons of confidentiality, you want to filter out faxes received, disable this option.

Automatically print received faxes Automatically print all received faxes on a PCL5 compatible printer configured on NethServer. The printer should be selected using the appropriate drop down menu.

SambaFax By selecting this option, the fax server can make available to the local area network a virtual printer named "sambafax" that will be configured on the client, by selecting the Apple LaserWriter driver 16/600 PS. Documents printed on the network printer sambafax must contain the exact phrase "Fax Number:" followed by the fax number of the recipient.

Send daily report Send a daily report to the administrator

2.12 IAX Modem

This page allows you to configure IAX modems.

An IAX modem is a software modem that uses an IAX channel (usually provided by an Asterisk PBX) instead of a traditional telephone line.

2.12.1 Create / Modify

Name Name the new IAX modem that you are creating.

Server IP IP address of the server on which the IAX modem registers (eg IP address of the Asterisk server).

Extension IAX extension on which you want to receive faxes.

Password IAX extension password defined previously.

Caller ID Caller ID (number) shown in the outgoing faxes.

Caller Name Caller name shown in the outgoing faxes.

2.13 Web proxy

The web proxy is a server that sits between the LAN PCs and Internet sites. Clients make requests to the proxy which communicates with external sites, then send the response back to the client.

The advantages of a web proxy are:

- ability to filter content
- reduce bandwidth usage by caching the pages you visit

The proxy can be enabled only on green and blue zones. Supported modes are:

- Manual: all clients must be configured manually
- Authenticated users must enter a user name and password in order to navigate
- Transparent: all clients are automatically forced to use the proxy for HTTP connections
- Transparent SSL: all clients are automatically forced to use the proxy for HTTP and HTTPS connections

2.13.1 Client configuration

The proxy is always listening on port **3128**. When using manual or authenticated modes, all clients must be explicitly configured to use the proxy. The configuration panel is accessible from the browser settings. By the way, most clients will be automatically configured using WPAD protocol. In this case it is useful to enable *Block HTTP and HTTPS ports* option to avoid proxy bypass.

If the proxy is installed in transparent mode, all web traffic coming from clients is diverted through the proxy. No configuration is required on individual clients.

Certificate file is saved inside `/etc/pki/tls/certs/NSRV.crt` file, it can be downloaded from client at `http://<ip_server>/proxy.crt` address.

2.13.2 SSL Proxy

> **Warning:** Decrypting HTTPS connection without user consent is illegal in many countries.

In transparent SSL mode, server is able to also filter encrypted HTTPS traffic. The proxy establishes the SSL connection with remote sites, it checks the validity of certificates and it decrypts the traffic. Finally, it generates a new certificate signed by the Certification Authority (CA) server itself.

The traffic between client and proxy is always encrypted, but you will need to install on every client (browser) the CA certificate of the server.

The server certificate is located in `/etc/pki/tls/certs/NSRV.crt`. It is advisable to transfer the file using an SSH client (eg FileZilla).

2.13.3 Bypass

In some cases it may be necessary to ensure that traffic originating from specific IP or destined to some sites it's not routed through the HTTP/HTTPS proxy.

The proxy allows you to create:

- bypass by source, configurable from *Hosts without proxy* section
- bypass by destination, configurable from *Sites without proxy* section

2.13.4 Report

Install `nethserver-lightsquid` package to generate web navigation reports.

LightSquid is a lite and fast log analyzer for Squid proxy, it parses logs and generates new HTML report every day, summarizing browsing habits of the proxy's users. Link to web interface can be found at the *Applications* tab inside the *Dashboard*.

2.14 Web content filter

The content filter analyzes all web traffic and blocks selected websites or sites containing viruses. Forbidden sites are selected from a list of categories, which in turn must be downloaded from external sources and stored on the system.

The system allows to create an infinite number of profiles. A profile is composed by three parts:

- **Who**: the client associated with the profile. Can be a user, a group of users, a host or a group of hosts.
- **What**: which sites can be browsed by the profiled client. It's a filter created inside the *Filters* section.
- **When**: the filter can always be enabled or valid only during certain period of times. Time frames can be created inside the *Times* section.

This is the recommended order for content filter configuration:

1. Select a list of categories from *Blacklists* page and start the download
2. Create one or more time conditions (optional)
3. Create custom categories (optional)
4. Create a new filter or modify the default one
5. Create a new profile associated to a user or host, then select a filter and a time frame (if enabled)

If no profile matches, the system provides a default profile that is applied to all clients.

2.14.1 Filters

A filter can:

- block access to categories of sites
- block access to sites accessed using IP address (recommended)
- filter URLs with regular expressions
- block files with specific extensions
- enable global blacklist and whitelist

A filter can operate in two different modes:

- Allow all: allow access to all sites, except those explicitly blocked
- Block all: blocks access to all sites, except those explicitly permitted

Note: The category list will be displayed only after the download of list selected from :guilabel‘Blacklist‘ page.

Blocking Google Translate

Online translation services, like Google Translate, can be used to bypass the content filter because pages visited trough the translator always refer to a Google's domain despite having content from external servers.

It's possible to block all requests to Google translate, creating a blocked URL inside the *General* page. The content of the blocked URL must be: `translate.google`.

2.14.2 Users from Active Directory

If the server is joined to an Active Directory domain (*Active Directory member*), you can create profiles connected to the users from the domain.

Note: Groups from Active Directory are not supported.

2.14.3 Antivirus

It is recommended to always enable virus scanning on the web page content. If the proxy is configured in SSL transparent mode (*SSL Proxy*), virus scanning will work even on contents downloaded via HTTPS.

2.14.4 Troubleshooting

If a bad page is not blocked, please verify:

- the client is surfing using the proxy
- the client doesn't have a configured bypass inside *Hosts without proxy* section
- the client is not browsing a site with a configured bypass inside *Sites without proxy* section
- the client is really associated with a profile not allowed to visit the page
- the client is surfing within a time frame when the filter is permissive

2.15 Firewall and gateway

NethServer can act as firewall and gateway inside the network where is installed. All traffic between computers on the local network and the Internet passes through the server that decides how to route packets and what rules to apply.

Main features:

- Advanced network configuration (bridge, bonds, alias, etc)
- Multi WAN support (up to 15)
- Firewall rules management

- Traffic shaping (QoS)
- Port forwarding
- Routeing rules to divert traffic on a specific WAN
- Intrusion Prevention System (IPS)

Firewall and gateway modes are enabled only if:

- the *nethserver-firewall-base* package is installed
- at least there is one network interface configured with red role

2.15.1 Policy

Each interface is identified with a color indicating its role within the system. See *Network*.

When a packet network passed through a firewall zone, the system evaluates a list of rules to decide whether traffic should be blocked or allowed. *Policies* are the default which rules are applied if the network traffic does not match any existing criteria.

The firewall implements two default policies editable from the page *Firewall rules -> Configure*:

- *Allowed*: all traffic from green to red is allowed
- *Blocked*: all traffic from green to red network is blocked. Specific traffic must be allowed with custom rules.

Firewall policies allow inter-zone traffic accordingly to this schema:

```
GREEN -> BLUE -> ORANGE -> RED
```

Traffic is allowed from left to right, blocked from right to left.

You can create rules between zones to change default policies from *Firewall rules* page.

Note: Traffic from local network to the server on SSH port (default 22) and Server Manager port (default 980) is **always** permitted.

2.15.2 Rules

Rules apply to all traffic passing through the firewall. When a network packet moves from one zone to another, the system looks among configured rules. If the packet match rule, the rule is applied.

Note: Rule's order is very important. The system always applies the first rule that matches.

A rule consists of three main parts:

- Action: action to take when the rule applies
- Source:
- Destination:
- Service:

Available actions are:

- *ACCEPT*: accept the network traffic
- *REJECT*: block the traffic and notify the sender host

- *DROP*: block the traffic, packets are dropped and not notification is sent to the sender host

Note: The firewall will not generate rules for blue and orange zones, if at least a red interface is configured.

REJECT vs DROP

As a general rule, you should use REJECT when you want to inform the source host that the port to which it is trying to access is closed. Usually the rules on the LAN side can use REJECT.

For connections from the Internet, it is recommended to use DROP, in order to minimize the information disclosure to any attackers.

Log

When a rule matches the ongoing traffic, it's possible to register the event on a log file by checking the option from the web interface. Firewall log is saved in `/var/log/firewall.log` file.

Examples

Below there are some examples of rules.

Block all DNS traffic from the LAN to the Internet:

- Action: REJECT
- Source: green
- Destination: red
- Service: DNS (UDP port 53)

Allow guest's network to access all the services listening on Server1:

- Action: ACCEPT
- Source: blue
- Destination: Server1
- Service: -

2.15.3 Multi WAN

The term *WAN* (Wide Area Network) refers to a public network outside the server, usually connected to the Internet. A *provider* is the company who actually manage the WAN link.

The system supports up to 15 WAN connections. If the server has two or more configured red card, it is required to proceed with provider configuration from *Multi WAN* page.

Each provider represents a WAN connection and is associated with a network adapter. Each provider defines a *weight*: higher the weight, higher the priority of the network card associated with the provider.

The system can use WAN connections in two modes (button *Configure* on page *Multi WAN*):

- *Balance*: all providers are used simultaneously according to their weight
- *Active backup*: providers are used one at a fly from the one with the highest weight. If the provider you are using loses its connection, all traffic will be diverted to the next provider.

Example

Given two configured providers:

- Provider1: network interface eth1, weight 100
- Provider2: network interface eth0, weight 50

If balanced mode is selected, the server will route a double number of connections on Provider1 over Provider2.

If active backup mode is selected, the server will route all connection on Provider1; only if Provider1 become unavailable connections will be redirected to Provider2.

2.15.4 Port forward

The firewall blocks request from public networks to private ones. For example, if web server is running inside the LAN, only computers on the local network can access the service on the green zone. Any request made by a user outside the local network is blocked.

To allow any external user access to the web server you must create a *port forward*. A port forward is a rule that allows limited access to resources from outside of the LAN.

When you configure the server, you must choose the listening ports. The traffic from red interfaces will be redirected to selected ports. In the case of a web server, listening ports are usually port 80 (HTTP) and 443 (HTTPS).

When you create a port forward, you must specify at least the following parameters:

- The source port, can be a number or a range in the format XX:YY (eg: 1000:1100 for begin port and end port 1100)
- The destination port, which can be different from the origin port
- The address of the internal host to which the traffic should be redirected

Example

Given the following scenario:

- Internal server with IP 192.168.1.10, named Server1
- Web server listening on port 80 on Server1
- SSH server listening on port 22 on Server1

If you want to make the server web available directly from public networks, you must create a rule like this:

- origin port: 80
- destination port: 80
- host address: 192.168.1.10

All incoming traffic on firewall's red interfaces on port 80, will be redirected to port 80 on Server1.

In case you want to make accessible from outside the SSH server on port 2222, you will have to create a port forward like this:

- origin port: 2222
- destination port: 22
- host address: 192.168.1.10

All incoming traffic on firewall's red interfaces on port 2222, will be redirected to port 22 on Server1.

Limiting access

You can restrict access to port forward only from some IP address or networks using the field *Allow only from*.

This configuration is useful when services should be available on from trusted IP or networks. Some possible values:

- `10.2.10.4`: enable port forward for traffic coming from 10.2.10.4 IP
- `10.2.10.4,10.2.10.5`: enable port forward for traffic coming from 10.2.10.4 and 10.2.10.5 IPs
- `10.2.10.0/24`: enable port forward only for traffic coming from 10.2.10.0/24 network
- `!10.2.10.4`: enable port forward for all IPs except 10.2.10.4
- `192.168.1.0/24!192.168.1.3,192.168.1.9`: enable port forward for 192.168.1.0/24 network, except for hosts 192.168.1.3 and 192.168.1.9

2.15.5 Traffic shaping

Traffic shaping allows to apply priority rules on network traffic through the firewall. In this way it is possible to optimize the transmission, check the latency and tune the available bandwidth.

To enable traffic shaping is necessary to know the amount of available bandwidth in both directions and fill in the fields indicating the speed Internet link. Be aware that in case of congestion by the provider there is nothing to do in order to improve performance.

Traffic shaping can be configured inside from the page *Traffic shaping -> Interface rules*.

The system provides three levels of priority, high, medium and low: as default all traffic has medium priority. It is possible to assign high or low priority to certain services based on the port used (eg low traffic peer to peer).

The system works even without specifying services to high or low priority, because, by default, the interactive traffic is automatically run at high priority (which means, for example, it is not necessary to specify ports for VoIP traffic or SSH). Even the traffic type PING is guaranteed high priority.

Note: Be sure to specify an accurate estimate of the band on network interfaces.

2.15.6 Firewall objects

Firewall objects are representations of network components and are useful to simplify the creation of rules.

There are 4 types of objects:

- Host: representing local and remote computers. Example: web_server, pc_boss
- Groups of hosts: representing homogeneous groups of computers. Hosts in a host group should always be reachable using the same interface. Example: servers, pc_segreteria
- Zone: representing networks of hosts. Although similar in concept to a group of hosts, you can express networks using CIDR notation
- Services: a service listening on a host with at least one port and protocol. Example: ssh, https

When creating rules, you can use the records defined in *DNS* and *DHCP and PXE server* like host objects. In addition, each network interface with an associated role is automatically listed among the available zones.

2.16 IPS (Snort)

Snort is a *IPS* (Intrusion Prevention System), a system for the network intrusion analysis. The software analyzes all traffic through the firewall searching for known attacks and anomalies.

When an attack or anomaly is detected, the system can decide whether to block traffic or simply save the event on a log n (`/var/log/snort/alert`).

A special widget inside the dashboard summarizes all detected attacks.

Snort can be configured accordingly to following policies. Each policy consists of several rules:

- Connectivity: check a large number of vulnerabilities, do not impact on non-realtime applications (eg VoIP)
- Balanced: suitable for most scenarios, it is a good compromise between security and usability (recommended)
- Security: safe mode but very invasive, may impact on chat and peer-to-peer applications
- Expert: the administrator must manually select the rules from the command line

---

Note: The use of an IPS impacts on all traffic passing through the firewall. Make sure you fully understand all the implications before enabling it.

2.17 Bandwidth monitor (ntopng)

ntopng is a powerful tool that allows you to analyze real-time network traffic. It allows you to evaluate the bandwidth used by individual hosts and to identify the most commonly used network protocols.

Enable ntopng Enabling ntopng, all traffic passing through the network interfaces will be analyzed. It can cause a slowdown of the network and an increased in system load.

Port The port where to view the ntopng web interface.

Password for 'admin' user Admin user password. This password is not related to the NethServer admin password.

2.18 Statistics (collectd)

Collectd is a daemon which collects system performance statistics periodically and stores them in RRD files. Statistics will be displayed inside a web interface.

The administrator can choose between two web interfaces:

- Collectd web, package *nethserver-collectd-web*
- Collectd Graph Panel (CGP), package *nethserver-cgp*

Both web interfaces will create a random URL accessible from *Applications* tab inside the *Dashboard*.

After installation, the system will gather following statistics:

- CPU usage
- system load
- number of processes
- RAM memory usage
- virtual memory (swap) usage

- system uptime
- disk space usage
- disk read and write operations
- network interfaces
- network latency

For each check, the web interface will display a graph containing last collected value and also minimum, maximum and average values.

2.18.1 Network latency

The ping plugin measure the network latency. At regular intervals, it sends a ping to the configured upstream DNS. If the multi WAN module is configured, any enabled provider is also checked.

Additional hosts could be monitored (i.e. a web server) using a comma separated list of hosts inside the `PingHosts` property.

Example:

```
config setprop collectd PingHosts www.google.com,www.nethserver.org
signal-event nethserver-collectd-update
```

2.19 DNS

NethServer can be configured as *DNS* (Domain Name System) server inside the network. A DNS server is responsible for the resolution of domain names (eg. *www.example.com*) to their corresponding numeric addresses (eg. 10.11.12.13) and vice versa.

The server performs DNS name resolution requests on behalf of local clients, and it is accessible only from the LAN network (green) and the guest's network (blue).

During a name lookup the server will:

- search for the name between hosts configured locally
- perform a query on external dns: requests are stored in cache to speed up subsequent queries

If NethServer is also the DHCP server on the network, all the machines will be configured to use the server istelf for name resolution.

Note: You must specify at least one external DNS inside the *DNS server* page.

2.19.1 Hosts

The *Hosts* page allows you to map host names to IP addresses, whether they are local or remote.

For example, if you have an internal web server, you can associate the name *www.mysite.com* with the IP of the web server. Then all clients can reach the website by typing the chosen name.

Locally configured names always take precedence over DNS records from external servers. In fact, if the provider inserts *www.mydomain.com* with an IP address corresponding to the official web server, but inside NethServer the IP of *www.mydomain.com* is configured with another address, hosts inside the LAN will not be able to see the site.

2.19.2 Alias

An *alias* is an alternative name used to reach the local server. For example, if the server is called *mail.example.com*, you can create a DNS alias *myname.example.com*. The server will then be accessible from clients on the LAN even using the name you just defined.

Aliases are only valid for the internal LAN. If you want the server is reachable from the outside with the same name you need to ask the provider to associate the public address of the server to the desired name.

2.20 DHCP and PXE server

The *Dynamic Host Configuration Protocol* (DHCP) [21] server centralizes the management of the local network configuration for any device connected to it. When a computer (or a device such as a printer, smartphone, etc.) connects to the local network, it can ask the network configuration parameters by means of the DHCP protocol. The DHCP server replies, providing the IP, DNS, and other relevant network parameters.

Note: In most cases, the devices are already configured to use DHCP protocol on start up.

The *Preboot eXecution Environment* (PXE) [22] specification allows a network device to retrieve the operating system from a centralized network location while starting up, through the DHCP and TFTP protocols. See *Boot from network configuration* for an example about configuring a such case.

2.20.1 DHCP configuration

The DHCP server can be enabled on all *green* and *blue* interfaces (see *Network*). NethServer will assign a free IP address within the configured *DHCP range* in *DHCP > DHCP server* page.

The DHCP range must be defined within the network of the associated interface. For instance, if the green interface has IP/netmask `192.168.1.1/255.255.255.0` the range must be `192.168.1.2 - 192.168.1.254`.

2.20.2 Host IP reservation

The DHCP server leases an IP address to a device for a limited period of time. If a device requires to always have the same IP address, it can be granted an *IP reservation* associated to its MAC address.

The page *DHCP > IP reservation* lists the currently assigned IP addresses:

- a line with *IP reservation* button identifies an host with a temporary lease (gray color);
- a line with *Edit* button identifies an host with a reserved IP (black color). A small two arrows icon near the host name says the DHCP lease is expired: this is a normal condition for hosts with static IP configuration, as they never contact the DHCP server.

2.20.3 Boot from network configuration

To allow clients to boot from network, the following components are required:

- the *DHCP* server, as we have seen in the previous sections,
- the *TFTP* server [23],

[21] Dynamic Host Configuration Protocol (DHCP) http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
[22] Preboot eXecution Environment http://en.wikipedia.org/wiki/Preboot_Execution_Environment
[23] Trivial File Transfer Protocol https://en.wikipedia.org/wiki/Tftp

- the software for the client, served through TFTP.

TFTP is a very simple file transfer protocol and usually it is used for automated transfer of configuration and boot files.

In NethServer the TFTP implementation comes with the DHCP module and is enabled by default. To allow accessing a file through TFTP, simply put it in `/var/lib/tftpboot` directory.

Note: To disable TFTP type the following commands in a root's console:

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

For instance, we now configure a client to boot CentOS from the network. In NethServer, type at root's console:

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

Then create the file `/var/lib/tftpboot/pxelinux.cfg/default` with the following content:

```
default menu.c32
prompt 0
timeout 300

MENU TITLE PXE Menu

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

Create a CentOS directory:

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

Copy inside the directory `vmlinuz` and `initrd.img` files. These files are public, and can be found in the ISO image, in `/images/pxeboot` directory or downloaded from a CentOS mirror.

Finally, power on the client host, selecting PXE boot (or boot from network) from the start up screen.

References

2.21 VPN

VPN supported configurations:

1. Connecting a remote terminal to the internal network (Roadwarrior), based on L2TP/IPsec or OpenVPN.
2. Connecting two remote networks (net2net), based on OpenVPN.

2.21.1 Account

The account tab allows to manage users used for VPN connections to the local server. Users can be normal system users or dedicated exclusively to the VPN service (without standard services like email).

Create new

Allow the creation of a new user. For each user, the system creates a x509 certificate.

VPN only The name used for VPN access. It can contain only lowercase letters, numbers, hyphens, underscores (_) and must begin with a lowercase letter. For example "luisa", "Jsmith" and "liu-jo" is a valid user name, while "4Friends" "Franco Blacks" and "aldo / mistake" are not.

System User Enable VPN access for a user already existing in the system. The user can be selected from the drop-down list.

Remote network Enter this information only when you want to create a nt2net VPN. These fields are used by the local server to correctly create routes to the remote network.

- Network Address: the network address of the remote network. Eg: 10.0.0.0
- Netmask: Netmask of the remote network. Eg: 255.255.255.0

2.21.2 Client

The VPN client allows you to connect the server to another VPN server in order to create a net2net VPN. Currently only OpenVPN net2net are supported.

2.22 FTP

Note: The FTP protocol is insecure: password are sent in clear text.

The FTP server allows to transfer files between client and server.

A FTP user can be *virtual* or a system users. Virtual users can access only the FTP server. This is the recommended configuration. The web interface allows the configuration only of virtual users.

When accessing the FTP server, a user can explore the entire filesystem accordingly to its own privileges. To avoid information disclosure, the FTP user can be configured in a jail using the *chroot* option: the user will not be able to exit the jail directory.

This behavior can be useful in case a shared folder is used as part of a simple web hosting. Insert the shared folder path inside the custom field. For example, given a shared folder called *mywebsite*, fill the field with:

```
/var/lib/nethserver/ibay/mywebsite
```

The FTP virtual user will be able to access only the specified directory.

2.22.1 System users

Warning: This configuration is highly discouraged

After enabling system users, all virtual users will be disabled. All configuration must be done using the command line.

Enable system users:

```
config setprop vsftpd UserType system
signal-event nethserver-vsftpd-save
```

Given a user name *goofy*, first make sure the user has Remote shell access. See *Access to services*. Then, enable the FTP access:

```
db accounts setprop goofy FTPAccess enabled
signal-event user-modify goofy
signal-event nethserver-vsftpd-save
```

To disable an already enabled user:

```
db accounts setprop goofy FTPAccess disabled
signal-event nethserver-vsftpd-save
```

If not explicitly disabled, all system users are chrooted. To disable a chroot for a system user:

```
db accounts setprop goofy FTPChroot disabled
signal-event nethserver-vsftpd-save
```

2.23 ownCloud

ownCloud provides universal access to your files via the web, your computer or your mobile devices wherever you are. It also provides a platform to easily view and synchronize your contacts, calendars and bookmarks across all your devices and enables basic editing right on the web.

Key features:

- preconfigure ownCloud with mysql and default access credential
- preconfigure httpd
- integration with NethServer system users and groups
- documentation
- backup ownCloud data with nethserver-backup-data tool

2.23.1 Installation

The installation can be done through the NethServer web interface. After the installation:

- open the url https://your_nethserver_ip/owncloud
- use **admin/Nethesis,1234** as default credentials
- change the default password

LDAP access authentication is enabled by default, so each user can login with its system credentials. After the installation a new application widget is added to the NethServer web interface dashboard.

2.23.2 Update

Updates are automatic. Do not do the manual update.

2.23.3 Update from ownCloud 5

To update:

```
yum update nethserver-owncloud
```

Note: The update does not change the current configuration.

2.23.4 LDAP Configuration

Note: New installations do not need the LDAP configuration because it is done automatically.

1. Copy the LDAP password using the following command:

```
cat /var/lib/nethserver/secrets/owncloud
```

2. Login to ownCloud as administrator
3. Search LDAP user and group backend: *Applications -> LDAP user and group backend*
4. Enable "LDAP user and group backend"
5. Configure server parameters: *Admin -> Admin -> Server tab*
6. Fill "Server" tab with these parameters:

```
Host: localhost:389
Port: 389
DN user: cn=owncloud,dc=directory,dc=nh
Password: "you can use copied password"
DN base: dc=directory,dc=nh
```

7. Fill "User filter" tab with:

```
Modify coarse filter: (&(objectClass=person)(givenName=*))
```

8. Fill "Access filter" tab with:

```
Modify coarse filter: uid=%uid
```

9. Fill "Group filter" tab with:

```
Modify coarse filter: (&(objectClass=posixGroup)(memberUid=*))
```

10. Configure "Advanced" tab with:

```
Directory settings
    Display username: cn
    User structure base: dc=directory,dc=nh
    Display group name: cn
    Group structure base: dc=directory,dc=nh
    Group-member association -> memberUid

Special Attributes
    Email field: email
```

11. Configure "Expert" tab with:

```
Internal username Attribute: uid
Click on "Clear Username-LDAP user mapping"
```

12. Click the "Save" button

2.23.5 LDAP Note

User list

After ownCloud LDAP configuration, the user list can show some usernames containing random numbers. This is because ownCloud ensures that there are no duplicate internal usernames as reported in section Internal Username.

If two administrator users are present, they are of ownCloud and LDAP. So you can remove that of ownCloud after have assigned the LDAP one to the administrator group. So, as a result, you can use only the LDAP administrator user. You can do this by the following steps:

1. login to ownCloud as administrator
2. open the user list: *admin -> Users*
3. change the group of "admin_xxx" user, checking "admin"
4. change the password of ownCloud admin user
5. logout and login with LDAP admin user
6. delete ownCloud admin user (named "admin")

Domain or IP change

When you change the domain name or IP address of NethServer, you have to adapt the `trusted_domains` key into the file:

```
/var/www/html/owncloud/config/config.php
```

Modify the old values with the new ones. For example if the domain name and IP address were *oldname.server.it 192.168.5.250* and the new ones are *newname.server.it 192.168.5.251*, the old file was:

```
...
'trusted_domains' =>
array (
    0 => '192.168.5.250',
    1 => 'oldname.server.it',
),
...
```

and must be changed as:

```
...
'trusted_domains' =>
array (
    0 => '192.168.5.251',
    1 => 'newname.server.it',
),
...
```

2.24 Phone Home

This tool is used to track all NethServer's installations around the world. Each time a new NethServer is installed, this tool sends some installation information through comfortable APIs. The information are stored in database and used to display nice markers in a Google Map view with number of installation grouped by country and release.

2.24.1 Overview

The tool is *disabled* by default.

To enable it simply run: `config set phone-home configuration status enabled`

If the tool is *enabled* the information sent are:

- UUID: stored in `/var/lib/yum/uuid`
- RELEASE: get by `/sbin/e-smith/config getprop sysconfig Version`

All the infos are used to populate the map.

2.24.2 Configuration

If you use a proxy edit the correct placeholders in file `phone-home` stored in `/etc/sysconfig/` :

```
SERVER_IP=__serverip__
PROXY_SERVER=__proxyserver__
PROXY_USER=__proxyuser__
PROXY_PASS=__proxypass__
PROXY_PORT=__proxyport__
```

2.25 WebVirtMgr

This tool is used to manage virtual machine through a simple web interface:

- Create and destroy new machines (KVM)
- Create custom template of virtual machines
- Easy shell remote access
- Amazing UI

2.25.1 Configuration

The web application listen on port **8000** of your host machine, for example: `http://HOST_IP:8000/`.

The service is disabled by default.

From the *Virtual machines* page you can:

- enable the virtual machines manager
- enable the virtual machines console access from web browser

To access the web interface you must login with credentials that can be found on the same page:

- *User:* admin
- *Password*: random alphanumeric (editable)

Warning: Do not create network bridges using WebVirtManager interface. Just create the bridge inside *Network* page and use it under WebVirtManager.

For more information, see official documentation:

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

CHAPTER 3

Best practices

3.1 Third-party software

You can install any CentOS/RHEL certified third-party software on NethServer.

If the software is 32-bit only, you should install compatibility libraries before installing the software. Relevant libraries should be:

- glibc
- glib
- libstdc++
- zlib

For example, to install the above mentioned packages:

```
yum install glibc.i686 libgcc.i686 glib2.i686 libstdc++.i686 zlib.i686
```

3.1.1 Installation

If the software is an RPM package, please use **yum** to install it: the system will take care to resolve all needed dependencies.

In case a yum installation is not possible, the best target directory for additional software is under `/opt`. For example, given a software named *mysoftware*, install it on `/opt/mysoftware`.

3.1.2 Backup

Directory containing relevant data should be included inside the backup by adding a line to `/etc/backup-data.d/custom.include`. See *Data backup customization*.

3.1.3 Firewall

If the software needs some open ports on the firewall, create a new service named `fw_<softwarename>`.

For example, given the software *mysoftware* which needs ports 3344 and 5566 on LAN, use the following commands:

```
config set fw_mysoftware service status enabled TCPPorts 3344,5566 access private
signal-event firewall-adjust
signal-event runlevel-adjust
```

3.1.4 Starting and stopping

NethServer uses the standard runlevel 3.

Software installed with yum should already be configured to start at boot on runlevel 3. To check the configuration, execute the **chkconfig** command. The command will display a list of services with their own status.

To enable a service on boot:

```
chkconfig mysoftware on
```

To disable a service on boot:

```
chkconfig mysoftware off
```

CHAPTER 4

Upgrades

4.1 Migration from NethService/SME Server

Migration is the process to convert a SME Server/NethService machine (*source*) into a NethServer (*destination*).

1. In the source host, create a full backup archive and move it to the destination host.
2. In the destination host, install all packages that cover the same features of the source.
3. Explode the full backup archive into some directory; for instance, create the directory `/var/lib/migration`.
4. In NethServer, signal the event `migration-import`:

```
signal-event migration-import /var/lib/migration
```

   This step will require some time.

5. Check for any error message in `/var/log/messages`:

```
grep -E '(FAIL|ERROR)' /var/log/messages
```

Note: No custom template is migrated during the migration process. Check the new template files before copying any custom fragment from the old backup.

4.1.1 Email

Before running NethServer in production, some considerations about the network and existing mail client configurations are required: what ports are in use, if SMTPAUTH and TLS are enabled. Refer to *Client configuration* and *Special SMTP access policies* sections for more informations.

In a mail server migration, the source mail server could be on production even after the backup has been done, and email messages continue to be delivered until it is taken down permanently.

An helper `rsync` script is provided by package `nethserver-mail-server`, to re-synchronize destination mailboxes with the source host: `/usr/share/doc/nethserver-mail-server-<VERSION>/sync_maildirs.sh`. It runs on the destination host:

```
Usage:
  ./sync_maildirs.sh [-h] [-n] [-p] -s IPADDR
      -h          help message
      -n          dry run
```

```
    -p PORT     ssh port on source host (default 22)
    -s IPADDR   rsync from source host IPADDR
```

The source host at `IPADDR` must be accessible by the `root` user, through `ssh` with public key authentication.

CHAPTER 5

Appendix

5.1 License

CHAPTER 6

Indices

- genindex
- search

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X