NethServer Documentation

Release 6.10 Final

Nethesis

Jan 16, 2020

Contents

Official site: www.nethserver.org

CHAPTER 1

Release notes 6.10 Final

1.1 Release notes

NethServer release 6.10 Final

- Upstream release notes from CentOS 6.10 and RHEL 6.10
- CentOS 6 will receive security updates until 2020-11-30
- List of updates of 6.10
- All updates of 6.9

1.1.1 Major changes on 2018-07-23

- Default Server Manager session idle timeout is 60 minutes, session life time is 8 hours. This new policy is enforced on upgraded installations too. See *Session timeouts*.

1.1.2 Upgrade of version 6.9 to 6.10

Start the update as usual from the *Software Center* page. It is recommended to reboot the system at the end of the update procedure.

CHAPTER 2

Installation

2.1 Installation

2.1.1 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

2.1.2 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

2.1.3 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 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 be 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:

- User name: `root`
- Default password: `Nethesis,1234`
- Network: DHCP enabled on all interfaces
- Keyboard: `en`
- Time zone: `Greenwich`

- Language: English
- 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
- fspassword: enable file system encryption with given password This option can be used even in Interactive Mode

Interactive Mode

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

- Language
- Software RAID
- Network configuration

Language

Select the language in which you want to use the interactive mode. Keyboard layout and time zone are changed accordingly and can be modified just after the first login to the web interface.

System language is always set to English.

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 can change the `root` user's password inside the first configuration wizard.

A good password is:

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

Default password is `Nethesis,1234`.

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.

Warning: Following characters are not supported inside the password: `#`, = and `$`.

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. See also *Next steps*.

2.1.4 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 server (VPS), or
- an USB stick.

For example, if you wish to install NethServer 6.10, just start with a CentOS 6.10 on your system (many VPS providers offer CentOS pre-installed virtual machines), and then execute below commands to transform CentOS into NethServer.

Enable specific YUM repositories with this command:

```
yum localinstall -y http://mirror.nethserver.org/nethserver/nethserver-release-6.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
```

2.1.5 Next steps

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

2.2 Accessing the Server Manager

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.

2.2.1 Login

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

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

Warning: Change the root's password as soon as possible, by picking a secure one, composed of a random sequence of mixed-case letters, digits and symbols.

If the File server, Email server or any other module requiring Users and groups module is installed from the Software center, the `admin` user is also available to access the web interface with same privileges as the `root` user. See *Admin account* for details.

2.2.2 Session timeouts

By default (starting from NethServer 6.10), a Server Manager session terminates after **60 minutes of inactivity** (idle timeout) and **expires 8 hours after the login** (session life time).

The following shell command sets 2 hours of idle timeout, and 16 hours of maximum session life time. Time is expressed in seconds:

```
config setprop httpd-admin MaxSessionIdleTime 7200 MaxSessionLifeTime 57600
```

To disable the timeouts

```
config setprop httpd-admin MaxSessionIdleTime '' MaxSessionLifeTime ''
```

The new timeout values will affect new sessions. They do not change any active session.

CHAPTER 3

Configuration

3.1 Base system

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

3.1.1 Dashboard

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

Disk analyzer

This tool is used to visualize disk usage in a simply and nice graph in which you can interact with click and double click to navigate in the directories tree.

After installation go in *Dashboard* and then *Disk usage* tab and click *Update* to index the root directory and to display the graph. This process can take several minutes depending on occupied disk space.

Well known folders are:

- Shared folders: `/var/lib/nethserver/ibay`
- User home directories: `/var/lib/nethserver/home`
- Windows roaming profiles: `/var/lib/nethserver/profile`
- Mail: `/var/lib/nethserver/vmail`
- Faxes: `/var/lib/nethserver/fax`
- MySQL databases: `/var/lib/mysql`

3.1.2 Network

The *Network* page configures how the server is connected to the local network (LAN) or other ones (i.e. 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 has 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 is installed on a public VPS (Virtual Private Server), it should must be configured with a green interface. All critical services should be closed using *Network services* panel.

Alias IP

Use alias IP to assign more IP addresses to the same NIC.

The most common use is with a red interface: when the ISP provides a pool of public IP addresses (within the same subnet) you can add some (or all) of them to the same red interface and manage them individually (e.g. in the port forward configuration).

Alias IP section can be found in the dropdown menu of the related network interface.

Note: Alias IPs on PPPoE interface could not work properly, due to different implementations of the service made by internet providers.

Logical interfaces

In *Network* page press *New interface* button to create a logical interface. Supported logical interfaces are:

- 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 logically separated networks using a single interface
- PPPoE (Point-to-Point Protocol over Ethernet): connect to Internet through a DSL modem

Bonds allow you to aggregate bandwidth or tollerate link faults. Bonds can be configured in multiple modes.

Modes providing load balancing and fault tolerance:

- Balance Round Robin (recommended)
- Balance XOR
- 802.3ad (LACP): it requires support at driver level and a switch with IEEE 802.3ad Dynamic link aggregation mode enabled
- Balance TLB: it requires support at driver level
- Balance ALB

Modes providing fault tolerance only:

- Active backup (recommended)
- Broadcast policy

A **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 a 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.

Warning: The **PPPoE** logical interface must be assigned the red role, thus requires the gateway functionality. See *Firewall and gateway* for details.

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

3.1.3 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.

3.1.4 Trusted networks

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

For example, hosts inside trusted networks can access to:

- Server Manager
- Shared folders (SAMBA)

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

3.1.5 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.

3.1.6 Organization contacts

The *Organization contacts* page fields are used as default values for user accounts. The organization name and address are also displayed on the Server Manager login screen.

3.1.7 Server certificate

The *Server certificate* page shows the currently installed SSL certificate that is provided by all system services.

The *Generate certificate* button allows generating a new self-signed SSL certificate. When a new certificate is generated, all SSL services are restarted and network clients will be required to accept the new certificate.

Note: To avoid problems while importing the certificate in Internet Explorer, the Common Name (CN) field should match the server FQDN.

Install a custom certificate

Custom certificates should be placed inside the following standard directories:

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

Set the private key and certificate file paths:

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

You can also set a SSL certificate chain file:

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

Notify registered daemons about certificate update:

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

Custom certificate backup

Always remember to add custom certificates to configuration backup. Just add the paths inside `/etc/backup-config.d/custom.include` file.

For example, if the certificate is `/etc/pki/tls/certs/mycert.crt`, simply execute:

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

Let's Encrypt certificate

Let's Encrypt is a free, automated, and open certificate authority brought to you by the non-profit Internet Security Research Group (ISRG). It can create free valid SSL certificate for you server.

From https://letsencrypt.readthedocs.org:

> The Let's Encrypt Client is a fully-featured, extensible client for the Let's Encrypt CA (or any other CA that speaks the ACME protocol) that can automate the tasks of obtaining certificates and configuring webservers to use them.

Prerequisites

1. The server must be reachable from outside at port 80.

   Make sure your port 80 is open to the public Internet, you can check with sites like http://www.canyouseeme.org/

2. The fully qualified name (FQDN) of the server must be a public domain name associated to its own public IP.

   Make sure you have a public DNS name pointing to your server, you can check with sites like http://viewdns.info/

How it works

The system will release a single certificate for server FQDN (Fully Qualified Domain Name).

When you want to access your server, you MUST always use the FQDN, but sometimes the server has multiple aliases. Let's Encrypt can add extra valid names to the FQDN certificate, so you will be able to access the server with other names.

Example

The server FQDN is: ''server.nethserver.org" with public IP "1.2.3.4''. But you want to access the server also using this names (aliases):" mail.nethserver.org" and ''www.nethserver.org''.

The server must:

- have the port 80 open to the public internet: if you access http://1.2.3.4 from a remote site you must see NethServer landing page
- have a DNS public record for ''server.nethserver.org'', ''mail.nethserver.org" and ''www.nethserver.org''. All DNS records must point to the same server (it may have multiple public IP addresses, though)

Installation

Install the package from command line:

```
yum install nethserver-letsencrypt
```

Configuration

Let's Encrypt configuration must be done from command line using the root user. Access the server with a monitor or connect to it with SSH.

Certificate for FQDN

Enable Let's Encrypt globally, this will automatically enable the generation of a certificate for the FQDN. Execute:

```
config setprop pki LetsEncrypt enabled
signal-event nethserver-letsencrypt-update
```

Certificate for server alias (optional)

The FQDN certificate can be extended to be valid also for extra domains configured as server alias. This feature is called SubjectAltName (SAN): https://en.wikipedia.org/wiki/SubjectAltName

Create a server alias inside the DNS page, then enable Let's Encrypt on the newly created record.

Example for ''alias.mydomain.com" alias:

```
db hosts setprop alias.mydomain.com LetsEncrypt enabled
```

Options

You can customize the following options by using config command:

- `LetsEncryptMail`: if set, Let's Encrypt will send notification about your certificate to this mail address (this must be set before executing the letsencrypt-certs script for the first time!)
- `LetsEncryptRenewDays`: minimum days before expiration to automatically renew certificate (default: 30)

Example:

```
config setprop pki LetsEncryptMail admin@mydomain.com
signal-event nethserver-letsencrypt-update
```

Test certificate creation

Since you can request the certificate maximum 5 times per week, make sure the configuration is correct by requesting a fake certificate. Execute:

```
/usr/libexec/nethserver/letsencrypt-certs -v -t
```

This command will try to generate a fake certificate using Let's Encrypt server. If everything goes well, the output should be something like this:

```
INFO: Using main config file /tmp/3XhzEPg7Dt
+ Generating account key...
+ Registering account key with letsencrypt...
Processing test1.neth.eu
+ Signing domains...
+ Creating new directory /etc/letsencrypt.sh/certs/test1.neth.eu ...
+ Generating private key...
+ Generating signing request...
+ Requesting challenge for test1.neth.eu...
+ Responding to challenge for test1.neth.eu...
+ Challenge is valid!
+ Requesting certificate...
+ Checking certificate...
+ Done!
+ Creating fullchain.pem...
+ Done!
```

Verify the presented certificate has been signed by Let's Encrypt CA on all SSL-enabled services like: If something goes wrong, please make sure all prerequisites are met.

Obtaining a valid certificate

If your configuration has been validated by the testing step, you're ready to request a new valid certificate. Execute the following script against the real Let's Encrypt server:

```
/usr/libexec/nethserver/letsencrypt-certs -v
```

Access your http server and check your certificate is valid.

3.1.8 Change user password

All users can login to Server Manager using their own credentials and access the user profile.

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

3.1.9 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.

3.1.10 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

3.1.11 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.

3.1.12 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
```

3.2 Software center

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.

CHAPTER 4

Modules

4.1 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 configuration backup also saves a list of installed modules. All modules will be reinstalled during the configuration restore process. 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 (See: *USB disk configuration*)
- 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.

4.1.1 Data restore

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

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).

Graphic interface

In the *Restore Data* menu section it is possible to search, select and restore one or more directories from backup, navigating the graphical tree with all paths included in the backup.

There are two options to restore:

- Restore data in the original path, the current files in the filesystem are overwritten by the restored files from backup.
- Restore data in original path but the restored files from backup are moved on a new directory (the files are not overwritten) in this path:

```
/complete/path/of/file_YYYY-MM-DD (YYYY-MM-DD is the date of restore)
```

To use the search field, simply insert at least 3 chars and the searching starts automatically, highlighting the matched directories

It is possible to restore the directories by clicking on **Restore** button.

Note: Multiple selection can be done with Ctrl key pressed.

4.1.2 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. If the old machine was the network gateway, remember to re-install firewall module
4. Restore the configuration backup from page *Backup (configuration)* > *Restore* in Server Manager, or executing: **`restore-config`**
5. If a warning message requires it, reconfigure the network roles assignment. See *Restore network roles* below.
6. Verify the system is functional
7. Restore data backup executing: **`restore-data`**

Restore network roles

If a role configuration points to a missing network interface, the *Dashboard*, *Backup (configuration)* > *Restore* and *Network* pages pop up a warning. This happens for instance in the following cases:

- configuration backup has been restored on a new hardware
- one or more network cards have been substituted
- system disks are moved to a new machine

The warning points to a page that lists the network cards present in the system, highlighting those not having an assigned *role*. Such cards have a drop down menu where to select a role available for restoring.

For instance, if a card with the *orange* role has been replaced, the drop down menu will list an element `orange`, near the new network card.

The same applies if the old card was a component of a logical interface, such as a bridge or bond.

By picking an element from the drop down menu, the old role is transferred to the new physical interface.

Click the *Submit* button to apply the changes.

> **Warning:** Choose carefully the new interfaces assignment: doing a mistake here could lead to a system isolated from the network!

If the missing role is `green` an interactive procedure asks to fix the configuration at boot-time, to ensure a minimal network connectivity and login again on the Server Manager.

Restore installed modules

By default the process of configuration restore will also restore all previously installed modules.

To avoid the reinstallation, execute this command before the restore:

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

4.1.3 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.

4.1.4 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.

4.1.5 USB disk configuration

The best filesystem for USB backup disks is EXT3. FAT filesystem is supported but *not recommended*, while NTFS is **not supported**.

Before formatting the disk, attach it to the server and find the device name:

```
# dmesg | tail -20

Apr 15 16:20:43 mynethserver kernel: usb-storage: device found at 4
Apr 15 16:20:43 mynethserver kernel: usb-storage: waiting for device to settle before␣
↪scanning
Apr 15 16:20:48 mynethserver kernel:   Vendor: WDC WD32  Model: 00BEVT-00ZCT0     Rev:
Apr 15 16:20:48 mynethserver kernel:   Type:   Direct-Access           ANSI SCSI␣
↪revision: 02
Apr 15 16:20:49 mynethserver kernel: SCSI device sdc: 625142448 512-byte hdwr sectors␣
↪(320073 MB)
Apr 15 16:20:49 mynethserver kernel: sdc: Write Protect is off
Apr 15 16:20:49 mynethserver kernel: sdc: Mode Sense: 34 00 00 00
Apr 15 16:20:49 mynethserver kernel: sdc: assuming drive cache: write through
Apr 15 16:20:49 mynethserver kernel: SCSI device sdc: 625142448 512-byte hdwr sectors␣
↪(320073 MB)
Apr 15 16:20:49 mynethserver kernel: sdc: Write Protect is off
Apr 15 16:20:49 mynethserver kernel: sdc: Mode Sense: 34 00 00 00
Apr 15 16:20:49 mynethserver kernel: sdc: assuming drive cache: write through
Apr 15 16:20:49 mynethserver kernel:  sdc: sdc1
Apr 15 16:20:49 mynethserver kernel: sd 7:0:0:0: Attached scsi disk sdc
```

(continues on next page)

(continued from previous page)

```
Apr 15 16:20:49 mynethserver kernel: sd 7:0:0:0: Attached scsi generic sg3 type 0
Apr 15 16:20:49 mynethserver kernel: usb-storage: device scan complete
```

Another good command could be:

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

In this scenario, the disk is accessibile as *sdc* device.

- Create a Linux partition on the whole disk:

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

- Create the filesystem on *sdc1* partition with a label named *backup*:

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

- Detach and reconnect the USB disk:

  You can simulate it with the following command:

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

- Now the *backup* label will be displayed inside the *Backup (data)* page.

4.2 Users and groups

4.2.1 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: *Change user password*.

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 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.

4.2.2 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.

Tip: For delegating permissions to the Server Manager, use the groups `managers` or `administrators`.

Two special groups can be created, the users who belong in one of these groups are granted access to the panels of the Server Manager

- *administrators*: Users of this group have the same permissions as the root or admin user.
- *managers*: Users of this group are granted access to the Management section.

4.2.3 Admin account

The *Users* page has one default entry: *admin*. This account allows access to the Server Manager with the same permissions of the *root* account. It is initially *disabled* and has no access from the console.

Tip: To enable `admin` account set its password.

Where applicable, the `admin` user also is granted special privileges on some specific services, such as *joining a workstation in Samba domain*.

4.2.4 Password management

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

Password policies can be changed from web interface after installing `nethserver-password` module.

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 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.

4.2.5 Notification language

Default language for notifications is English. If you wish to change it, use the following command:

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

Example for Italian:

```
config setprop sysconfig DefaultLanguage it_IT.utf8
```

4.2.6 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 /root/users.csv
```

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

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

4.3.1 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.

[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
[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

- *Relay* messages to another mail server.

Note: If a domain is deleted, email will not be deleted; 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 notice to sent messages*. This text is called *disclaimer* and it can be used to meet some legal 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 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.

4.3.2 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
- 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 outside the organization 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.

[9] The Markdown plain text formatting syntax, http://en.wikipedia.org/wiki/Markdown

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

4.3.3 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*.

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*.

The `admin` user can impersonate another user, gaining full rights to the latter's mailbox contents and on folder permissions. The *Admin can log in as another user* option controls this empowerment, known also as *master user* in[2].

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

When *Admin can log in as another user* is enabled, the IMAP server accepts any user name with `*admin` suffix appended and admin's password.

For instance, to access as `john` with admin's password `secr3t`, use the following credentials:

- username: `john*admin`
- password: `secr3t`

4.3.4 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 used only if the server is temporarily blacklisted[12], or normal SMTP access is restricted by the ISP.

4.3.5 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

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

Block of attachments

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

- 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[14] analyzes emails by detecting and classifying *spam*[13] messages using heuristic criteria, predetermined rules and statistical evaluations on the content of messages. The rules are public and updated on a regular basis. The filter can also check if sender server is listed in one or more blacklists (DNSBL). 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` exists, only users in this group will be allowed to train the filters.

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

---

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

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 messages.

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

It's possible to create an 'Allow' or 'Block' rule even for a complete email domain, not just for a single email address : you just need to specificy the desired domain (e.g. : nethserver.org).

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

4.3.6 Block port 25

If the system is acting as the network gateway, green and blue zones will not be able to send mail to external servers through port 25 (SMTP). Blocking port 25 could prevent remotely controlled machines inside the LAN from sending SPAM.

The administrator can change this policy creating a custom firewall rule inside the *Rules* page.

4.3.7 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-update
```

4.3.8 Special SMTP access policies

The default NethServer configuration requires that all clients use the submission port (587) with encryption and authentication enabled to send mail through the SMTP server.

To ease the configuration of legacy environments, the *Email* > *SMTP access* page allows making some exceptions on the default SMTP access policy.

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

For instance, there are some devices (printers, scanners, ...) that do not support SMTP authentication, encryption or port settings. Those can be enabled to send email messages by listing their IP address in *Allow relay from IP addresses* text area.

Moreover, under *Advanced options* there are further options:

- The *Allow relay from trusted networks* option allows any client in the trusted networks to send email messages without any restriction.
- The *Enable authentication on port 25* option allows authenticated SMTP clients to send email messages also on port 25.

4.3.9 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.

4.3.10 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 work properly. See BUG#2744.

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

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

4.3.11 Outlook deleted mail

Unlike almost any IMAP client, Outlook does not move deleted messages to the trash folder, but simply marks them as "deleted".

It's possibile to automatically move messages inside the trash using following commands:

```
config setprop dovecot DeletedToTrash enabled
signal-event nethserver-mail-server-save
```

You should also change Outlook configuration to hide deleted messages from inbox folder. This configuration is available in the options menu.

4.3.12 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

4.4 Webmail

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

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

4.4.1 Plugins

Roundcube supports many plugins already bundled within the installation.

Plugins enabled by default:

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

- 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 `/usr/share/roundcubemail/plugins` directory. To get the list, just execute:

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

4.4.2 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
```

4.5 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*[1]. 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.

References

4.6 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

4.6.1 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.

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

4.7 Shared folders

A *shared folder* is a place where files can be accessed by a group of people using different methods, or *protocols*. Since NethServer is a modular system, the actual methods depends on what modules have been installed.

The available methods/protocols are:

- Web access (HTTP)
- Samba (SMB/CIFS)

4.7.1 Access privileges

A shared folder is always owned by a group of users (*Owning group*). Each member of the group is allowed to read the folder contents. Optionally the group can be entitled to modify the folder contents and the read permission can be extended to everyone accessing the system. This simple permission model is based on the traditional UNIX file system permissions.

Access privileges can be refined further with the *ACL* tab, allowing individual users and other groups to gain read and write permissions. This extended permission model is based on the POSIX ACL specification.

4.7.2 Web access

The *Web access* method allows the connection of a web browser to a shared folder using the HTTP protocol. Web resources are identified by a string, the Uniform Resource Locator, or URL.

For instance, if `docs` is the name of the shared folder, the URLs that allow the access to it could be:

```
http://192.168.1.1/docs
https://192.168.1.1/docs
http://myserver/docs
http://www.domain.com/docs
http://docs.domain.com/
```

Each URL has three components:

- protocol (`http://` or `https://`),
- host name (`192.168.1.1`, `myserver`, `www.domain.com`),
- path (`docs`).

The *Web address* radio group defines the "path" component.

- *Folder name* is the default, the same as the shared folder name, as `docs` in the example above.
- *Web site root* means no path at all. For instance `http://docs.domain.com`.
- *Custom* means an alternative name, to be detailed.

The *Virtual host* selector lists all *Server alias* defined under the *DNS* page. "Any" means the host part is not considered to map the URL to the shared folder.

The web access is anonymous and read-only. There are some options that can be tweaked to restrict the access.

- *Allow access from trusted networks only*, restricts the access by looking at the IP address of the client,
- *Protect by password*, requires an unique password to gain read access (to be specified here),
- *Require SSL encrypted connection*.

4.7.3 Configuring a web application

The *Allow .htaccess and write permissions overrides* check box activates a special Apache configuration designed to host a simple web application on a shared folder. It allows overriding the default Apache configuration and grants Apache the write permissions on specific sub-directories.

Warning: If a shared folder contains executable code, such as PHP scripts, user permissions and security implications must be evaluated carefully.

If the check box is enabled

- any file named `.htaccess` is loaded as configuration for Apache.
- a text file named `.htwritable` positioned in the root level of the shared folder may contain a list of sub-directories where Apache is granted write permission. The syntax of the file is one sub-directory for each line. Lines beginning with `#` are comments. When the content of `.htwritable` changes, the *Reset permission* button must be pressed again to propagate the file system permissions.

Note: Shared folders are a powerful tool but are not meant to be a complete web hosting solution! For advanced Apache and virtual host setups drop a `.conf` file under the `/etc/httpd/conf.d/` directory. Refer to the official Apache documentation for this.

4.7.4 Samba

SMB/CIFS is a widley adopted protocol that allows to share files across a computer network. In a way similar to Web URLs above, the shared folder name becomes the SMB "share name".

For instance, the SMB network addresses of the `docs` share could be

```
\\192.168.1.1\docs
\\MYSERVER\docs
```

Compatible SMB clients can be used to set special ACLs on a specific file or sub-directory. At any time, the *Reset permissions* button restores UNIX and POSIX permissions according to what is defined in the *General* and *ACL* pages.

If the option *Network recycle bin* is enabled, removed files are actually moved into a special "wastebasket" directory. The *Keep omonym files* keeps distinct file names inside the wastebasket directory, preventing overwrites.

If *Guest access* is enabled, any provided authentication credentials are considered valid.

If *Browseable* is enabled, the shared folder is listed publicly. This does not affect the permission to use this resource.

4.8 Windows network

Microsoft Windows™ interoperability is provided by Samba[1]. 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.

Currently the following roles are available:

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

- 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 information.

Workstation

In this role NethServer uses 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.

4.8.1 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.

4.8.2 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 information refer to Microsoft Naming conventions[2].

[2] 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[3] for more information.

4.8.3 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*.

4.9 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.

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

4.9.1 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.

4.9.2 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.

4.10 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. Via *Administration/Software centre* install the UPS package. In *Configuration* appears the new entry *UPS* where can be find the supported model by typing in *Search driver for model* field.

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.

4.10.1 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
```

4.10.2 UPS statistics

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

4.11 Fax server

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

The web interface allows you to configure:

- Area code and fax number
- Sender (TSI)
- A physical modem with phone line parameters and how to send/receive faxes
- One or more *Virtual modems*
- Email notifications for sent and received faces, with the attached document in multiple formats (PDF, PostScript, TIFF)
- Print received faxes
- Virtual Samba printer
- Daily report of sent faxes
- Sending faxes via email

4.11.1 Modem

Although HylaFAX supports a large number of brands and models, we recommend using an external serial or USB modem.

If an internal modem blocks, you must reboot the whole server, while an external modem can be turned off separately. In addition, the majority of internal modems on the market belongs to the so-called family of winmodem, "software" modems that need a driver, usually available only on Windows.

Also be aware that many external USB modem are also winmodem.

You should prefer modems in Class 1 or 1.0, especially if based on Rockwell/Conexant or Lucent/Agere chips. The system also supports modems in classes 2, 2.0 and 2.1.

4.11.2 Client

We recommend using the fax client YajHFC (http://www.yajhfc.de/) that connects directly to the server and allows:

- the use of an LDAP address book
- ability to select the modem to send
- view the status of modems

Authentication

The system supports two authentication methods for sending faxes:

- Host Based: uses the IP address of the computer sending the request
- PAM: uses username and password, users must belong to the group *faxmaster*

Also make sure to enable the *View faxes from clients* option.

4.11.3 Samba virtual printer

If SambaFax option is enabled, the server will create virtual printer called "sambafax" available to the local network.

Each client must configure the printer using the Apple LaserWriter 16/600 PS driver.

Sent documents must meet the following prerequisites:

- Must contain exactly the string "Fax Number", containing the fax number, for example:

```
Fax Number: 12345678
```

- The string may be present in any position of the document, but on a single line
- The string must be written in non-bitmap font (eg. Truetype)

Faxes will be sent using the sending user id. This information will be displayed in the fax queue.

4.11.4 Mail2Fax

All emails sent to the local network at `sendfax@<domainname>` will be transformed into a fax and sent to the recipient.

The `<domainname>` must match a local mail domain configured for local delivery.

The email must comply with this format:

- The recipient's number must be specified in the object (or subject)
- The email must be in plain text format
- It may contain attachments such as PDF or PS which will be converted and sent with your fax

Note: This service is enabled only for clients that send email from the green network.

4.11.5 Virtual modems

Virtual modems are software modems connected to a PBX (Asterisk usually) using a IAX extension.

The configuration of the virtual modems consists of two parts:

1. Creation of IAX extension within the PBX
2. Configuration of virtual modem

4.12 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

---

Note: Please make sure to have Users module installed (nethserver-directory package), if you plan to use authenticate mode.

4.12.1 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.

Note: To make the WPAD file accessible from guest network, add the address of blue network inside the *Allow hosts* field for httpd service from the *Network services* page.

4.12.2 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).

4.12.3 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

Bypass rules are also configured inside the WPAD file.

4.12.4 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*.

4.12.5 Cache

Under tab *Cache* there is a form to configure cache parameters:

- The cache can be enabled or disabled (*disabled* by default)
- **Disk cache size**: maximum value of squid cache on disk (in MB)
- **Min object size**: can be left at 0 to cache everything, but may be raised if small objects are not desired in the cache (in kB)
- **Max object size**: objects larger than this setting will not be saved on disk. If speed is more desirable than saving bandwidth, this should be set to a low value (in kB)

The button *Empty cache* also works if squid is disabled, it might be useful to clear space on disk.

Sites without cache

Sometime the proxy can't correctly handle some bad crafted sites. To exclude one or more domain from the cache, use the `NoCache` property.

Example:

```
config setprop squid NoCache www.nethserver.org,www.google.com
signal-event nethserver-squid-save
```

4.12.6 Safe ports

Safe ports are a list of ports accessible using the proxy. If a port is not inside the safe port list, the proxy will refuse to contact the server. For example, given a HTTP service running on port 1234, the server can't be accessed using the proxy.

The `SafePorts` property is a comma-separated list of ports. Listed ports will be added to the default list of safe ports.

Eg. Access extra ports 446 and 1234:

```
config setprop squid SafePorts 446,1234
signal-event nethserver-squid-save
```

4.13 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, a group of hosts, a zone or an interface role (like green, blue, etc).
- **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.

4.13.1 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`.

4.13.2 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.

4.13.3 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.

4.13.4 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

4.14 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
- Routing 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

4.14.1 Policy

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

When a network packet passes through a firewall zone, the system evaluates a list of rules to decide whether traffic should be blocked or allowed. *Policies* are the default rules to be applied when 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.

4.14.2 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 a 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 four 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 no notification is sent to the sender host
- *ROUTE*: route the traffic to the specified WAN provider. See *Multi WAN*.

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: -

4.14.3 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 cards, 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.

To determine the status of a provider, the system sends an ICMP packet (ping) at regular intervals. If the number of dropped packets exceeds a certain threshold, the provider is disabled.

The administrator can configure the sensitivity of the monitoring through the following parameters:

- Percentage of lost packets
- Number of consecutive lost packets
- Interval in seconds between sent packets

The *Firewall rules* page allows to route network packets to a given WAN provider, if some criteria are met. See *Rules*.

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 connections on Provider1; only if Provider1 becomes unavailable the connections will be redirected to Provider2.

4.14.4 Port forward

The firewall blocks requests 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

- The destination port, which can be different from the origin port
- The address of the internal host to which the traffic should be redirected
- It's possibile to specify a port range using a colon as separator in the source port field (eX: 1000:2000), in this case the field destination port must be left void

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
- Other services in the port range beetween 5000 and 6000 on Server1

If you want to make the web server 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.

In case you want to make accessible from outside the server on the whole port range beetween 5000 and 6000, you will have to create a port forward like this:

- origin port: 5000:6000
- destination port:
- host address: 192.168.1.10

All incoming traffic on firewall's red interfaces on port range beetween 5000 and 6000 will be redirected to same ports 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 only 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

4.14.5 NAT 1:1

One-to-one NAT is a way to make systems behind a firewall and configured with private IP addresses appear to have public IP addresses.

If you have a bunch of public IP addresses and if you want to associate one of these to a specific network host, NAT 1:1 is the way.

Example

In our network we have an host called `example_host` with IP `192.168.5.122`. We have also associated a public IP address `89.95.145.226` as an alias of `eth0` interface (`RED`).

We want to map our internal host (`example_host` - `192.168.5.122`) with public IP `89.95.145.226`.

In the *NAT 1:1* panel, we choose for the IP `89.95.145.226` (read-only field) the specific host (`example_host`) from the combo-box. We have configured correctly the one-to-one NAT for our host.

4.14.6 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 it is necessary to know the amount of available bandwidth in both directions and fill in the fields indicating the speed of the 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 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 bandwidth on network interfaces.

4.14.7 Firewall objects

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

There are 6 types of objects, 5 of them represent sources and destinations:

- 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

- CIDR Networks: You can express a CIDR network in order to simplify firewall rules.

  Example 1 : last 14 IP address of the network are assigned to servers (192.168.0.240/28).

  Example 2 : you have multiple green interfaces but you want to create firewall rules only for one green (192.168.2.0/24).

- *Zone*: representing networks of hosts, they must be expressed in CIDR notation. Their usage is for defining a part of a network with different firewall rules from those of the nominal interface. They are used for very specific needs.

Note: By default, all hosts belonging to a zone are not allowed to do any type of traffic. It's necessary to create all the rules on the firewall in order to obtain the desired behavior.

The last type of object is used to specify the type of traffic:

- 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.

4.14.8 IP/MAC binding

When the system is acting as DHCP server, the firewall can use the list of DHCP reservations to strictly check all traffic generated from hosts inside local networks. When IP/MAC binding is enabled, the administrator will choose what policy will be applied to hosts without a DHCP reservation. The common use is to allow traffic only from known hosts and block all other traffic. In this case, hosts without a reservation will not be able to access the firewall nor the external network.

To enable traffic only from well-known hosts, follow these steps:

1. Create a DHCP reservation for a host
2. Go to *Firewall rules* page and select from *Configure* from the button menu
3. Select *MAC validation (IP/MAC binding)*
4. Choose *Block traffic* as policy to apply to unregistered hosts

---

Note: Remember to create at least one DHCP reservation before enabling the IP/MAC binding mode, otherwise no hosts will be able to manage the server using the web interface or SSH.

4.15 Cloud content filter

The cloud content filtering allows you to profile and block the user web traffic. The system allows you to create multiple profiles based on user name (authenticated web proxy) or on the IP source (transparent or manual proxy).

4.15.1 Preliminary operations

You need to access https://register.nethesis.it, inside *Administration* section, and add the server to the *Cloud content filter* section.

4.15.2 Configuration

The configuration is composed of two parts:

- a profile associated to a group of users or a host group
- a selection of blacklists associated with the created profile

Profiles must be created through the web interface of NethServer, while the association between profiles and blacklist can be configured accessing the FlashStart remote interface. To access FlashStart remote interface, click on *Configure* inside the *Cloud content filter* page.

Manual or transparent proxy

Using manual or transparent proxy, you can profile the users only through the source IP address.

Steps:

- Create a host group
- Open the tab *IP profiles* and click on *Create new*
- Select a host group and enter a description
- To select the blacklist associated with the profile, click on *Configure* and access the FlashStart

Authenticated proxy

Using authenticated proxy, you can profile the users through the user name.

Steps:

- Create a user group
- Open the tab *User profiles* and click on *Create new*
- Select a user group and enter a description
- To select the blacklist associated with the profile, click on *Configure* and access the FlashStart

---

Note: The filter will work only if all client are using the web proxy.

4.16 Proxy pass

The proxy pass feature is useful when you want to access internal sites from the outside network.

Proxy pass configuration must be done via command line. Before proceed, make sure `nethserver-httpd` package in installed:

```
yum install -y nethserver-httpd
```

Scenario:

- NethServer is the firewall of your LAN
- You have a domain http://mydomain.com
- You would like http://mydomain.com/mysite to forward to the internal server (internal IP: 192.168.2.100)

Commands for this example:

```
db proxypass set mysite ProxyPass
db proxypass setprop mysite Target http://192.168.2.100
db proxypass setprop mysite Description "My internal server"
db proxypass setprop mysite HTTP on
db proxypass setprop mysite HTTPS on
signal-event nethserver-httpd-update
```

You can also restrict the access to a list of IPs:

```
db proxypass setprop mysite ValidFrom 88.88.00.0/24,78.22.33.44
signal-event nethserver-httpd-update
```

4.16.1 Manual configuration

If this is not enough, you can always manually create your own proxy pass by creating a new file inside `/etc/httpd/conf.d/` directory.

Example

Create `/etc/httpd/conf.d/myproxypass.conf` file with this content:

```
<VirtualHost *:443>
    SSLEngine On
    SSLProxyEngine On
    ProxyPass /owa https://myserver.exchange.org/
    ProxyPassReverse /owa https://myserver.exchange.org/
</VirtualHost>

<VirtualHost *:80>
    ServerName www.mydomain.org
    ProxyPreserveHost On
    ProxyPass / http://10.10.1.10/
    ProxyPassReverse / http://10.10.1.10/
</VirtualHost>
```

Please refer to official Apache documentation for more information: http://httpd.apache.org/docs/2.2/mod/mod_proxy.html

4.17 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.

4.18 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 increase 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.

Interfaces Interfaces on which ntopng will listen to.

4.19 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, named

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

The web interface will create a random URL accessible from the *Applications* tab inside the *Dashboard*. It's possible to share the random URL to let non-authenticated users view graphs. Access is allowed only from the zones and IP addresses of the http-admin service (see Network services).

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

4.19.1 Network latency

The ping plugin measure network latency. At regular intervals, it sends an ICMP 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
```

4.20 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 itself for name resolution.

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

4.20.1 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.

4.20.2 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.

4.21 DHCP and PXE server

The *Dynamic Host Configuration Protocol* (DHCP)[1] 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)[3] 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.

4.21.1 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`.

4.21.2 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.

4.21.3 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[2],
- 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:

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

```
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

4.22 VPN

A VPN (Virtual Private Network) allows you to establish a secure and encrypted connection between two or more systems using a public network, like the Internet.

The system supports two types of VPNs:

1. roadwarrior: connect a remote client to the internal network
2. net2net or tunnel: connect two remote networks

4.22.1 OpenVPN

OpenVPN lets you easily create VPN connections, It brings with numerous advantages including:

- Availability of clients for various operating systems: Windows, Linux, Apple, Android, iOS
- Multiple NAT traversal, you do not need a dedicated static IP on the firewall
- High stability

- Simple configuration

Roadwarrior

The OpenVPN server in roadwarrior mode allows connection of multiple clients.

Supported authentication methods are:

- System user and password
- Certificate
- System user, password and certificate

The server can operate in two modes: routed or bridged. You should choose bridged mode only if the tunnel must carry non-IP traffic.

To allow a client to establish a VPN:

1. Create a new account: it is recommended to use a dedicated VPN account with certificate, avoiding the need to create a system user.

   On the other hand, it's mandatory to choose a system account if you want to use authentication with user name and password.

2. Download the file containing the configuration and certificates.
3. Import the file into the client and start the VPN.

Tunnel (net2net)

When creating an OpenVPN net2net connection, you must choose a master between involved servers. All other servers are considered as slaves (clients).

Steps to be performed on the master server:

- Enable roadwarrior server
- Create a VPN-only account for each slave
- During the account creation remember to specify the remote network configured behind the slave

Steps to be performed on the slave:

- Create a client from the *Client* page, specifying the connection data to the master server.
- Copy and paste the content of downloaded certificates from the master configuration page.

4.22.2 IPsec

IPsec (IP Security) protocol is usually used to create tunnels with devices from other manufacturers.

Roadwarrior (L2TP)

L2TP is considered the replacement for PPTP which is insecure. Many devices include native support for this protocol but not all implementations are compatible.

Supported authentication methods are:

- System user, password and certificate

- Secret shared key (PSK)

To allow a client to establish a VPN:

1. Configure the server as PDC (Primary Domain Controller) from the *Windows Network* page.
2. Create a new system account.
3. Download the file that contains certificates.
4. Import client and CA (Certification Authority) certificates within the client.
5. Proceed with the configuration of connection data and start the VPN.

Note: Use of L2TP is recommended if and only if it is not possible to install a OpenVPN client into the device.

Tunnel (net2net)

IPsec is extremely reliable and compatible with many devices. In fact, it is an obvious choice when you need to create net2net connections between firewalls of different manufacturers.

Unlike OpenVPN configuration, in an IPsec tunnel, firewalls are considered peers.

If you are creating a tunnel between two NethServer, given the firewalls A and B:

1. Configure the server A and specify the remote address and LAN of server B. If the *Remote IP* field is set to the special value `%any`, the server waits for connections from the other endpoint.
2. Configure the second firewall B by mirroring the configuration from A inside the remote section. The special value `%any` is allowed in one side only!

If an endpoint is behind a NAT, the values for *Local identifier* and *Remote identifier* fields must be set to custom unique names prepended with `@`. Common names are the geographic locations of the servers, such as the state or city name.

4.23 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.

4.23.1 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
```

4.24 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

4.24.1 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.

4.24.2 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

4.24.3 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")

4.24.4 Trusted Domains

Trusted domains are a list of domains that users can log into. Default trusted domains are:

- domain name
- ip address

To add a new one use:

```
config setprop owncloud TrustedDomains server.domain.com
signal-event nethserver-owncloud-update
```

To add more than one, concatenate the names with a comma.

4.25 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.

4.25.1 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.

4.25.2 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__
```

4.26 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

4.26.1 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

4.27 SNMP

SNMP (Simple Network Management Protocol) protocol allows to manage and monitor devices connected to the network. The SNMP server can reply to specific queries about current system status.

The server is disabled by default.

During first configuration. you should set three main options:

- the SNMP community name
- the location name where the server is located
- the name and mail address of system administrator

4.28 WebTop 4

WebTop is a full-featured groupware which implements ActiveSync protocol.

Access to web interface is: `https://<server_name>/webtop`.

4.28.1 Authentication

Web interface

The login to the web application is always with simple user name and password, no matters how many mail domains are configured.

Example

- Server name: mymail.mightydomain.com
- Alternative mail domain: baddomain.net
- User: goofy
- Login: goofy

Active Sync

Login to Active Sync account is with <username>@<domain> where `<domain>` is the domain part of server FQDN.

Example

- Server name: mymail.mightydomain.com
- Alternative mail domain: baddomain.net
- User: goofy
- Login: goofy@mightydomain.com

When configuring an Active Sync account, make sure to specify the server address and leave the domain field empty.

Note: Active Sync protocol is supported only on Android and iOS devices. Outlook is not supported. Mail synchronization is currently not supported.

Admin user

After installation, WebTop will be accessible with an administrator user. The administrator user can change global settings and login as all other users, but it's not a system users and can't access any other services like Mail, Calendar, etc.

Default credentials are:

- User: admin
- Password: admin

Admin user password must be changed from WebTop interface.

Warning: Remember to change the admin password just after installation.

To check the mail of the system user admin use the following login: admin@<domain> where `<domain>` is the domain part of server FQDN.

Example

- Server name: mymail.mightydomain.com
- User: admin
- Login: admin@mightydomain.com

4.28.2 WebTop vs SOGo

WebTop and SOGo can be installed on the same machine.

ActiveSync is enabled by default on SOGo and WebTop, but if both packages are installed, SOGo will take precedence.

To disable ActiveSync on SOGo:

```
config setprop sogod ActiveSync disabled
signal-event nethserver-sogo-update
```

To disable ActiveSync on WebTop:

```
config setprop webtop ActiveSync disabled
signal-event nethserver-webtop4-update
```

All incoming mail filters configured within SOGo, must be manually recreated inside WebTop interface. The same apply if the user is switching from WebTop to SOGo.

4.28.3 Active Directory authentication

After performing the join to Active Directory domain, access WebTop administration page, then from tree menu on the left, select *Domain -> NethServer*.

Edit the following fields:

- Authentication Uri: select `ldapAD` mode and insert the full FQDN of the server and port 389. Example: w2k8.nethserver.org:389
- Admin LDAP: user name of AD domain administrator
- LDAP Password: user password of AD domain administrator

After saving, the page *Users* will display users from Active Directory.

4.28.4 Importing from SOGo

You can migrate some data from SOGo to WebTop using the following script:

- Calendars: `/usr/share/webtop/doc/sogo2webtop_cal.php`
- Address books: `/usr/share/webtop/doc/sogo2webtop_card.php`

Before using the scripts you need to install this package:

```
yum install php-mysql -y
```

When launching the scripts, indicate the user name you want to import from SOGo:

```
php /usr/share/webtop/doc/sogo2webtop_cal.php <user>
php /usr/share/webtop/doc/sogo2webtop_card.php <user>
```

Where `user` can be a username or `all`.

Examples

Import all address books from SOGo:

```
php /usr/share/webtop/doc/sogo2webtop_card.php all
```

Import the calendar of user "foo":

```
php /usr/share/webtop/doc/sogo2webtop_cal.php foo
```

Note: If the script is executed multiple times, both calendars and address books will be imported multiple times. Import of distribution lists and recurring events are not currently supported.

4.28.5 Importing from Outlook PST

You can import email, calendars and address books from an Outlook PST archive.

Before using followings scripts, you will need to install *libpst* package:

```
yum install libpst -y
```

Mail

Initial script to import mail messages: `/usr/share/webtop/doc/pst2webtop.sh`

To start the import, run the script specifying the PST file and the system user:

```
/usr/share/webtop/doc/pst2webtop.sh <filename.pst> <user>
```

All mail messages will be imported. Contacts and calendars will be saved inside a temporary files for later import. The script will list all created temporary files.

Contacts

Script for contacts import: `/usr/share/webtop/doc/pst2webtop_card.php`.

The script will use files generated from mail import phase:

```
/usr/share/webtop/doc/pst2webtop_card.php <user> <file_to_import> <phonebook_category>
```

Example

Let us assume that the pst2webtop.sh script has generated following output from mail import:

```
Contacts Folder found: Cartelle personali/Contatti/contacts
 Import to webtop:
./pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Cartelle personali/Contatti/contacts'
↪<foldername>
```

To import the default address book (WebTop) of *foo* user:

```
/usr/share/webtop/doc/pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Cartelle personali/
↪Contatti/contacts' WebTop
```

Calendars

Script for calendars import: `/usr/share/webtop/doc/pst2webtop_cal.php`

The script will use files generated from mail import phase:

```
/usr/share/webtop/doc/pst2webtop_cal.php <user> <file_to_import> <foldername>
```

Example

Let us assume that the pst2webtop.sh script has generated following output from mail import:

```
Events Folder found: Cartelle personali/Calendario/calendar
 Import to webtop:
./pst2webtop_cal.php foo '/tmp/tmp.0vPbWYf8Uo/Cartelle personali/Calendario/calendar'
↪<foldername>
```

To import the default calendar (WebTop) of *foo* user:

```
/usr/share/webtop/doc/pst2webtop_cal.php foo '/tmp/tmp.0vPbWYf8Uo/Cartelle personali/
↪Calendario/calendar' WebTop
```

Note: The script will import all events using the timezone selected by the user inside WebTop, if set. Otherwise system timezone will be used.

4.28.6 Google and Dropbox integration

Users can add their own Google Drive and Dropbox accounts inside WebTop. Before proceeding, the administrator must create a pair of API access credentials.

Google API

- Access https://console.developers.google.com/project and create a new project
- Create new credentials by selecting "OAuth 2.0 clientID" type and remember to compile "OAuth consent screen" section
- Insert new credentials (Client ID e Client Secret) inside WebTop configuration

  From shell, access webtop database:

```
su - postgres -c "psql webtop"
```

  Execute the queries, using the corresponding value in place of __value__ variable:

```
INSERT INTO settings (idsetting,value) VALUES ('main.googledrive.clientid', '__
↪value__');
INSERT INTO settings (idsetting,value) VALUES ('main.googledrive.clientsecret', '_
↪_value__');
```

Dropbox API

- Access https://www.dropbox.com/developers/apps and create a new app
- Insert the new credential key pair (App key e App secret) inside WebTop configuration

  From shell, access webtop database:

```
su - postgres -c "psql webtop"
```

  Execute the queries, using the corresponding value in place of __value__ variable:

```
INSERT INTO settings (idsetting,value) VALUES ('main.googledrive.clientsecret', '_
↪_value__');
INSERT INTO settings (idsetting,value) VALUES ('main.dropbox.appsecret', '__value_
↪_');
```

If you need to raise the user limit, please read the official Dropbox documentation.

Note: The Enterprise version is already integrated with Google and Dropbox.

4.29 Adagios

Adagios is a web based Nagios configuration interface built to be simple and intuitive in design, exposing less of the clutter under the hood of Nagios. Additionally Adagios has a rest interface for both status and configuration data as well a feature complete status interface that can be used as an alternative to Nagios web interface.

Key features:

- full view/edit of hosts,services, etc
- tons of pre-bundled plugins and configuration templates
- network scan
- remote installation of linux/windows agents

- modern Status view as an alternative to default nagios web interface
- backup Adagios data with NethServer backup data tool
- rest interface for status of hosts/services and for for viewing and modifying configuration
- full audit of any changes made

4.29.1 Installation

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

- enable the admin account (see *Admin account* for details)
- open the url https://your_nethserver_ip/adagios
- use `admin` credentials to access web interface

For more information, see official documentation:

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

4.30 OCS Inventory NG

OCS Inventory NG is free software that enables users to inventory IT assets. OCS Inventory NG collects information about the hardware and software of networked machines running the OCS client program (*OCS Inventory Agent*). OCS Inventory NG can visualize the inventory through a web interface and includes the capability of deploying applications on computers according to search criteria. Agent-side *IpDiscover* makes it possible to discover the entirety of networked computers and devices.

Key features:

- relevant inventory information
- powerful deployment system allowing to distribute software installation or scripts
- web administration console
- network scan
- Multiple operating systems support (Windows, Linux, BSD, Sun Solaris, IBM AIX, HP-UX, MacOSX)
- web service accessible through SOAP interface
- plugins support through API
- backup Adagios data with NethServer backup data tool

4.30.1 Installation

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

- enable the admin account (see *Admin account* for details)
- open the url https://your_nethserver_ip/ocsreports
- use `admin` credentials to access web interface

For more information, see official documentation:

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

4.31 HA (High Availability)

NethServer supports High Availability only for some specific scenarios.

The cluster is based on two nodes in active-passive mode: the master node (or primary node) runs all the service, meanwhile the slave node (or secondary node) takes over only if the master node fails. Both nodes share a DRBD storage in active-passive mode.

This configuration supports:

- Virtual IPs connected to the green network
- Clustered services storing data inside the shared storage

Example

The MySQL daemon listens on a virtual IP and stores its data inside the DRBD partition. In case of failure of the master node, the mysqld service will restart on the secondary node. All clients should connect to MySQL using the virtual IP.

4.31.1 Limitations

- The LDAP service and all services depending on it can't be clustered. We recommend using an external LDAP server.
- Only STONITH fence devices are supported

4.31.2 Hardware requirements

You must use two identical nodes. Each node must have:

- a disk, or a partition, dedicated to the DRBD (Distributed Replicated Block Device) shared storage
- two network interfaces to be bonded on a *green* role, both interfaces must be connected to LAN switches

You should also have two LAN switches, let's say SW1 and SW2. On each node, create a bond using two interfaces. Every node must be attached both to SW1 and SW2.

Fence device

Each node must be connected at least to one pre-configured fence device.

Fencing is the action which disconnects a node from the shared storage. The *fence device* is a hardware device than can be used to shutdown a node using the STONITH (Shoot The Other Node In The Head) method, thus cutting off the power to the failed node.

We recommend a switched PDU (Power Distribution Unit), but IPMI (Intelligent Platform Management Interface) devices should work with some limitations. It's also possible to use a managed switch that supports the SNMP IF-MIB protocol.

External links:

- list of supported devices: https://access.redhat.com/articles/28603
- more info about fencing: http://clusterlabs.org/doc/crm_fencing.html

4.31.3 Installation

Before install:

- connect both nodes as described before, while the secondary node is powered off. Proceed by installing NethServer on the primary node
- make sure the System Name of the master node is *ns1*. Example: ns1.mydomain.com. Also choose the domain name, which *can not* be changed later.

Primary node

The primary node will be the one running services on normal conditions. First, you must configure a logical volume reserved for DRBD shared storage.

Configuring DRBD storage

- Add a new disk (example: vdb)
- Create a new partition:

```
parted /dev/vdb mklabel gpt
parted /dev/vdb --script -- mkpart primary 0% 100%
```

- Create a physical volume:

```
pvcreate /dev/vdb1
```

- Extend the volume group:

```
vgextend VolGroup /dev/vdb1
```

- Create a logic volume for DRBD:

```
lvcreate -n lv_drbd -l 100%FREE VolGroup
```

Software

Cluster options are saved inside the `ha` configuration key. The key must have the same configuration on both nodes.

Execute the following steps to proceed with software installation and configuration.

- Configure a bond on green interfaces.
- Install cluster services:

```
yum install nethserver-ha
```

- Install extra software, like MySQL:

```
yum install nethserver-mysql
```

- Configure the virtual IP and inform the cluster about the green IPs of both nodes:

```
config setprop ha VirtualIP <GREEN_IP_HA>
config setprop ha NS1 <NS1_GREEN_IP>
config setprop ha NS2 <NS2_GREEN_IP>
```

- Apply the configuration and start services on master node:

```
signal-event nethserver-ha-save
```

When the command completes, the primary node is ready to run the services. You can check the cluster status with following command:

```
pcs status
```

Service configuration

Cluster services must be handled by the resource manager daemon (pacemaker), you should disable NethServer service handling for the clustered service:

```
service mysqld stop
chkconfig mysqld off
/sbin/e-smith/config settype mysqld clustered
```

The following commands will configure a MySQL instance bound to the virtual IP. Data is saved inside the DRBD:

```
/usr/sbin/pcs cluster cib /tmp/mycluster
/usr/sbin/pcs -f /tmp/mycluster resource create DRBDData ocf:linbit:drbd drbd_
↪resource=drbd00 op monitor interval=60s
/usr/sbin/pcs -f /tmp/mycluster resource master DRBDDataPrimary DRBDData master-max=1␣
↪master-node-max=1 clone-max=2 clone-node-max=1 is-managed="true" notify=true
/usr/sbin/pcs -f /tmp/mycluster resource create VirtualIP IPaddr2 ip=`config getprop␣
↪ha VirtualIP` cidr_netmask=`config getprop ha VirtualMask` op monitor interval=30s
/usr/sbin/pcs -f /tmp/mycluster resource create drbdFS Filesystem device="/dev/drbd/
↪by-res/drbd00" directory="/mnt/drbd" fstype="ext4"
/usr/sbin/pcs -f /tmp/mycluster resource create mysqld lsb:mysqld
/usr/sbin/pcs -f /tmp/mycluster resource create sym_var_lib_asterisk␣
↪ocf:heartbeat:symlink params target="/mnt/drbd/var/lib/mysql" link="/var/lib/mysql"␣
↪backup_suffix=.active
/usr/sbin/pcs -f /tmp/mycluster resource create sym_etc_my.pwd ocf:heartbeat:symlink␣
↪params target="/mnt/drbd/etc/my.pwd" link="/etc/my.pwd" backup_suffix=.active
/usr/sbin/pcs -f /tmp/mycluster resource create sym_root_.my.cnf␣
↪ocf:heartbeat:symlink params target="/mnt/drbd/root/.my.cnf" link="/root/.my.cnf"␣
↪backup_suffix=.active

/usr/sbin/pcs -f /tmp/mycluster constraint order promote DRBDDataPrimary then start␣
↪drbdFS
/usr/sbin/pcs -f /tmp/mycluster constraint colocation add drbdFS with DRBDDataPrimary␣
↪INFINITY with-rsc-role=Master
/usr/sbin/pcs -f /tmp/mycluster resource group add mysqlha drbdFS VirtualIP sym_var_
↪lib_mysql sym_etc_my.pwd sym_root_.my.cnf var_lib_nethserver_secrets mysqld

/usr/sbin/pcs cluster cib-push /tmp/mycluster
```

Check cluster and service status:

```
pcs status
```

Take a look at the official pacemaker documentation for more information.

Secondary node

- Install NethServer on the secondary node
- Make sure the secondary node is named *ns2* and the domain name is the same as primary node
- Configure the DRBD storage as already done for the primary node
- Install and configure software following the same steps as in the primary node
- Configure Virtual IP, NS1 and NS2 options, then apply the configuration:

```
signal-event nethserver-ha-save
```

Final steps

- Enable the STONITH (commands can be executed on any node):

```
pcs property set stonith-enabled=true
```

- Configure the fence device (commands can be executed on any node).

  Example for libvirt fence, where nodes are virtual machines hosted on the same KVM-enabled host with IP 192.168.1.1:

```
pcs  stonith create Fencing fence_virsh ipaddr=192.168.1.1 login=root␣
↪passwd=myrootpass pcmk_host_map="ns1.nethserver.org:ns1;ns2.nethserver.org:ns2"␣
↪pcmk_host_list="ns1.nethserver.org,ns2.nethserver.org"
```

- Configure an email address where notification will be sent in case of failure:

```
pcs resource create MailNotify ocf:heartbeat:MailTo params email="admin@nethserver.org
↪" subject="Cluster notification"
```

- It's strongly advised to change root password from web interface on both nodes. Root password is used to send commands to all cluster nodes.

Fencing with IPMI

Many servers have a built-in management interface often known by commercial names like ILO (HP), DRAC (Dell) or BMC (IBM). Any of these interfaces follow the IPMI standard. Since any management interface controls only the node where it resides, you must configure at least two fence devices, one for each node.

If the cluster domain is `nethserver.org`, you should use the following commands:

```
pcs stonith create ns2Stonith fence_ipmilan pcmk_host_list="ns2.nethserver.org"␣
↪ipaddr="ns2-ipmi.nethserver.org" login=ADMIN passwd=ADMIN timeout=4 power_timeout=4␣
↪power_wait=4 stonith-timeout=4 lanplus=1 op monitor interval=60s
pcs stonith create ns1Stonith fence_ipmilan pcmk_host_list="ns1.nethserver.org"␣
↪ipaddr="ns1-ipmi.nethserver.org" login=ADMIN passwd=ADMIN timeout=4 power_timeout=4␣
↪power_wait=4 stonith-timeout=4 lanplus=1 op monitor interval=60s
```

Where ns1-ipmi.nethserver.org and ns2-ipmi.nethserver.org are host names associated with IP of the management interface.

Also, you should make sure that each stonith resource is hosted by the right node:

```
pcs constraint location ns2Stonith prefers ns1.nethserver.org=INFINITY
pcs constraint location ns1Stonith prefers ns2.nethserver.org=INFINITY
```

Fencing with IF-MIB switch

It's also possible to use a managed switch that supports SNMP IF-MIB as a fence device. In this case, fenced node does not get powered off, but instead it is cut offline by the switch, with the same effect.

Verify the switch configuration using the fence agent for opening and closing ports on the switch:

```
fence_ifmib -a <SWITCH_IP> -l <USERNAME> -p <PASSWORD> -P <PASSWORD_PRIV> -b MD5 -B␣
↪DES -d <SNMP_VERSION> -c <COMMUNITY> -n<PORT> -o <off|on|status>
```

The following commands configure two switches connected in this way: Node 1 network port 1 is connected to switch 1 port 1 Node 1 network port 2 is connected to switch 2 port 1 Node 2 network port 1 is connected to switch 1 port 2 Node 2 network port 2 is connected to switch 2 port 2

```
pcs stonith create ns1sw1 fence_ifmib action=off community=<COMMUNITY>␣
↪ipaddr=<SWITCH_1_IP> login=<USERNAME> passwd=<PASSWORD> port=1 snmp_auth_
↪prot=MD5 snmp_priv_passwd=<PASSWORD_PRIV> snmp_priv_prot=DES snmp_sec_
↪level=authPriv snmp_version=3 pcmk_host_list="<HOST_1>"
pcs stonith create ns1sw2 fence_ifmib action=off community=fence ipaddr=
↪<SWITCH_2_IP> login=<USERNAME> passwd=<PASSWORD> port=1 snmp_auth_prot=MD5␣
↪snmp_priv_passwd=<PASSWORD_PRIV> snmp_priv_prot=DES snmp_sec_
↪level=authPriv snmp_version=3 pcmk_host_list="<HOST_1>"
pcs stonith create ns2sw1 fence_ifmib action=off community=fence ipaddr=
↪<SWITCH_1_IP> login=<USERNAME> passwd=<PASSWORD> port=2 snmp_auth_prot=MD5␣
↪snmp_priv_passwd=<PASSWORD_PRIV> snmp_priv_prot=DES snmp_sec_
↪level=authPriv snmp_version=3 pcmk_host_list="<HOST_2>"
pcs stonith create ns2sw2 fence_ifmib action=off community=fence ipaddr=
↪<SWITCH_2_IP> login=<USERNAME> passwd=<PASSWORD> port=2 snmp_auth_prot=MD5␣
↪snmp_priv_passwd=<PASSWORD_PRIV> snmp_priv_prot=DES snmp_sec_
↪level=authPriv snmp_version=3 pcmk_host_list="<HOST_2>"
pcs stonith level add 1 <HOST_1> ns1sw1,ns1sw2
pcs stonith level add 1 <HOST_2> ns2sw1,ns2sw2
pcs constraint location ns1sw1 prefers <HOST_2>=INFINITY
pcs constraint location ns1sw2 prefers <HOST_2>=INFINITY
pcs constraint location ns2sw1 prefers <HOST_1>=INFINITY
pcs constraint location ns2sw2 prefers <HOST_1>=INFINITY
```

4.31.4 Failure and recovery

A two-node cluster can handle only one fault at a time.

Note: If you're using IPMI fence devices, the cluster can't handle the power failure of a node, since the power is shared with its own fence device.

In this case you must manually confirm the eviction of the node by executing this command on the running node:

```
pcs stonith confirm <failed_node_name>
```

Failed nodes

When a node is not responding to cluster heartbeat, the node will be evicted. All cluster services are disabled at boot to avoid problems just in case of fencing: a fenced node probably needs a little maintenance before re-joining the cluster.

To re-join the cluster, manually start the services:

```
pcs cluster start
```

Disconnected fence devices

The cluster will periodically monitor the status of configured fence devices. If a device is not reachable, it will be put into the stopped state.

When the fence device has been fixed, you must inform the cluster about each fence device with this command:

```
crm_resource --resource <stonith_name> --cleanup --node <node_name>
```

DRBD Split Brain

When a DRBD split brain happens, data between two nodes storage is no longer synchronized. It could happen when a fence fails. Active node DRBD status (cat /proc/drbd) will be Primary/Unknown and on the inactive node Secondary/Unknown (instead of Primary/Secondary and Secondary/Primary). And with command

```
pcs status
```

DRBD state will be:

> **Master/Slave Set: DRBDDataPrimary [DRBDData]** Masters: [ns1.nethserver.org] Stopped: [ns2.nethserver.org]

instead of:

> **Master/Slave Set: DRBDDataPrimary [DRBDData]** Masters: [ns1.nethserver.org] Slaves: [ns2.nethserver.org]

Solution:

On the node with valid data launch the following command

```
drbdadm invalidate-remote drbd00
```

On the node with wrong storage data, run

```
drbdadm invalidate drbd00
```

On both nodes, launch

```
drbdadm connect drbd00
```

Check drbd synchronization with

```
cat /proc/drbd
```

Disaster recovery

If case of hardware failure, you should simply re-install the failed node and rejoin the cluster. Clustered services will be automatically recovered and data will be synced between nodes.

Just follow these steps:

1. Install NethServer on machine.
2. Restore the configuration backup of the node, if you don't have the configuration backup, reconfigure the server and make sure to install `nethserver-ha` package.
3. Execute the join cluster event:

   ```
   signal-event nethserver-ha-save
   ```

4.31.5 Backup

The backup must be configured on both nodes and must be executed on a network shared folder. Only the primary node will actually execute the backup process, the backup script will be enabled on the secondary node only if the master node has failed.

If both nodes fail, you should re-install the primary node, restore the configuration backup and start the cluster:

```
signal-event nethserver-ha-save
```

Then restore the data backup only as the last step. When the restore ends, reboot the system.

If you wish to backup the data inside the DRBD, take care to add the directories inside the `custom.include` file.

Example:

```
echo "/mnt/drbd/var/lib/mysql" >> /etc/backup-data.d/custom.include
```

4.32 Upgrade tool

The *Upgrade tool* module upgrades NethServer from version 6 to version 7 with an automated procedure that acts in three steps:

1. **preparation**: downloads all required packages from the configured software repositories
2. **upgrade**: at next reboot runs the packages upgrade transaction, the upgrade tasks, then reboots automatically
3. **post-upgrade**: completes by fully re-configuring the system

Each step is described in the sections below. The time estimations depend on the number of packages, internet connection, CPU and disks speed.

Warning: Read carefully *Upgrade risks and how to reduce them*

4.32.1 Preparation step

Estimated time: 1 hour

The (1) **preparation** step can be started from the *Upgrade tool* page of the Server Manager.

If the File server module is present and the Samba server role is *Primary Domain Controller* or *Workstation* the system has to be configured with a local Active Directory accounts provider. See *Upgrade to Active Directory*.

The Upgrade tool does not work if the Samba server role is set to *Active Directory Member*.

During the preparation step the system is still operational as usual. The package download runs in background. It requires some time, depending on the available network bandwidth.

The available disk space is checked twice, before and after the preparation step, to ensure the next steps do not run in short of disk space.

At the end of the download the web page asks to abort the procedure or continue with the system reboot to the upgrade step.

4.32.2 Upgrade step

Estimated time: 30 minutes

The (2) **upgrade** step starts at the next system reboot. The upgrade procedure boots the Linux kernel of version 7 by default. If the disk controller is not compatible with it, the procedure fails at this point.

Hint: It is possible to select the old kernel and boot the system in the previous state, actually aborting the upgrade

---

If the new kernel boots and mounts the disks correctly the system is **disconnected from the network** and the packages upgrade starts. From this point there is no way back. During the upgrade the system can be accessed from the system console.

It takes some time to upgrade all the packages, depending on the system speed and the number of the packages. At the end of the upgrade step the system is automatically rebooted.

4.32.3 Post-upgrade step

Estimated time: 15 minutes

The (3) **post-upgrade** step starts at the second reboot.

The basic system was completely upgraded by the previous step; the post-upgrade step renames the network interfaces according to the new NIC naming rules and re-configures the installed modules.

In this last step a fault can be recovered safely through the system console. At the end of the post-upgrade step SSH, Server Manager and the other services are available again.

Any daily, weekly and monthly scheduled cron job will be started again within one hour since the system boot ends.

4.32.4 Post-upgrade checklist

Warning:

1. Some modules, like ownCloud, need to be upgraded or replaced manually. Refer to the Upgrade documentation of NethServer 7
2. Once the Server Manager is accessible again remember to refresh the browser cache with `Ctrl + Shift + R` to fix display issues caused by the upgraded style sheets (CSS)

Upgrade completed check

To ensure the upgrade procedure has finished run `systemd-analyze`. The output should begin like

```
Startup finished
```

Upgrade errors check

To check if any error occurred, run

```
grep -B 5 -E '(ERROR|FAILED)' /var/log/messages
```

Installed modules check

In *Software center*, check if the previously installed modules are still marked as installed on the upgraded system. Each module is composed by some packages: as the module compositions has changed from version 6 to 7, some module may appear as not installed. To fix it, try to install it again with the *add* button.

Let's Encrypt certificate check

A Let's Encrypt certificate, if present, must be requested again from the *Server certificate* page. Then set it as the default system certificate from the same page. For more information, refer to the "Server certificate" manual page of NethServer 7.

4.32.5 Upgrade to Active Directory

If the system requires a local Active Directory (AD) accounts provider, the Upgrade tool expects some additional parameters to be issued:

- The AD *DNS domain name*
- The *NetBIOS domain name* (read only)
- A green bridge interface
- The *Domain Controller IP address*: an additional, free IP address that AD services binds to. The IP must be in the same subnet of the green bridge

If a green bridge interface is not present go to the *Network* page and create one with *Create new logical interface*.

The *NetBIOS domain name* is a read-only field. To change it, refer to the *Windows Network* page.

Warning: In virtualized systems, remember to enable **promiscuous mode** in the hypervisor settings, otherwise access to AD will be blocked from LAN clients

For more information refer also to the NethServer 7 documentation, especially:

- the "Samba Active Directory local provider installation" section, under the "Users and groups" chapter
- the "Upgrade from NethServer 6" chapter

4.32.6 Upgrade risks and how to reduce them

A major system version upgrade is a risky operation and must be planned carefully.

- Ensure the system has enough free **disk space**. The procedure checks the free disk space, but it is always a good idea to check it early, even before installing the *Upgrade tool* module.
- Prepare a complete backup or snapshot of the whole system. A **power outage** or an **hardware fault** during the upgrade step, as long as an **unknown bug** in this procedure could compromise the system
- Consider the **system downtime** and how it impacts on the end-users
- Make a list of the modules that need to be configured, replaced, **upgraded manually** after the automated procedure completes. Refer to the Upgrade documentation of NethServer 7
- During the upgrade any existing **custom template** is archived into `/root/templates-custom.upgrade/`. It is recommended to check the existing customized templates before starting the upgrade procedure and decide if and how to restore them
- The system is **disconnected from the network** during the upgrade step and until the post-upgrade step completes. If any error occurs during those steps a direct **console access** is required.

CHAPTER 5

Best practices

5.1 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
```

5.1.1 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`.

5.1.2 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*.

5.1.3 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
```

5.1.4 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 6

Appendix

6.1 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.

6.1.1 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.

6.2 Documentation license

CHAPTER 7

Indices

- General index
- Search

Index

X

Z