NethServer Documentation

Release 7 Final

Nethesis

Oct 10, 2018

Contents

See also

- Web site
- Community
- Wiki
- Developer manual

CHAPTER 1

Release notes 7

1.1 Release notes 7

NethServer release 7

- ISO release 7.5.1804 “final” - 2018-06-11
- This release is based on CentOS 7 (1804)
- CentOS 7 will receive security updates until 2024-06-30
- *List of NethServer 7 ISO releases*
- List of changes
- List of known bugs
- Discussions around possible bugs
- Project board

1.1.1 Major changes on 2018-06-11

- ISO release 7.5.1804 “final” replaces any previous ISO 7.5.1804 “rc” and “beta”
- The *Email* module is now based on Rspamd
- MX DNS record override for LAN hosts has been removed. Removed `postfix/MxRecordStatus` prop
- Host name aliases are converted into `hosts` DB records. See *Additional host name aliases*
- `/etc/fstab` is no longer an expanded template. See *Requirements* and *User home directories* for details
- Default permissions for *Shared folders* is *Grant full control to the creator*
- Default *TLS policy* is `2018-03-30`
- Default Server Manager *session idle timeout* is 60 minutes, session life time is 8 hours

- Quality of Service (QoS) implementation now uses FireQOS, current configuration is automatically migrated. See *Traffic shaping*
- The menu entry *Automatic updates* in Server Manager was removed. Automatic updates are now configured from *Software center* > *Configure*. From the same panel it is possible to select the *Software updates origin*. See *Software updates*
- The *NethServer subscription* module is available by default in new installations. Run the following command to update the base module set on existing installations: `yum update @nethserver-iso`
- The WebVirtMgr project is no longer maintained and the corresponding module has been removed along with nethserver-libvirt package. See *Virtual machines* chapter for details on how to use virtualization

1.1.2 Major changes on 2017-10-26

- ISO release 7.4.1708 "final" replaces the old ISOs 7.4.1708 "beta1" and 7.3.1611 "update 1"
- The local AD account provider applies updates to the Samba DC instance automatically (#5356) Latest Samba DC version is 4.6.8
- The Software center page warns when a new upstream release is available (#5355)
- Added FreePBX 14 module
- Squid has been patched for a smoother web navigation experience when using SSL transparent proxy
- Ntopng 3 replaces Bandwidthd, the Server Manager has a new "top talkers" page which tracks hosts network usage
- Suricata can be configured with multiple categories rules
- EveBox can report traffic anomalies detected by Suricata
- Nextcloud 12.0.3
- Web antivirus based on ICAP instead of ECAP
- Web filters: ufdbGuard updated to 1.33.4, small UI improvements on web
- Diagtools: added speedtest
- ufdbGuard updated to release 1.33.4
- WebTop4 has been removed

1.1.3 Major changes on 2017-07-31

- ISO release 7.3.1611 "update 1" replaces the previous ISO 7.3.1611 "Final"
- Configuration backup page enhancement
- Accounts provider page enhancement
- Migration from sme8 and upgrade from ns6 procedures
- OpenvPN: improve net2net tunnels
- WebTop 5.0.7
- Backup data: basic WebDAV support for backups and storage stats
- UI tweaks for IPSec tunnels
- Web proxy: support divert and priority rules

- NextCloud 12
- Network diagnostic tools page

1.1.4 Major changes on 2017-01-30

- ISO release 7.3.1611 "Final" replaces the previous ISO 7.3.1611 "RC4"
- Installer: added new manual installation method
- Account providers: "administrators" group has been replaced by "domain admins" group (*Server Manager access*)
- Mail server: fix pseudonym expansion for groups
- Mail server: enable user shared mailbox by default (*User shared mailbox*)
- Mail server: specific per-domain pseudonym now override generic ones
- OpenVPN: start VPN clients on boot
- Web filter: fix group-based profiles
- Firewall: fix selection of time conditions
- IPS: update configuration for latest pulledpork release

1.1.5 Upgrading NethServer 6 to NethServer 7

It is possible to upgrade the previous major release of NethServer to 7, with a backup/restore strategy. See the *Upgrade from NethServer 6* for details.

Server Manager access

If you want to grant *Server Manager access to other users than root*, please add the users to the "domain admins" group and execute:

```
config delete admins
/etc/e-smith/events/actions/initialize-default-databases
```

User shared mailbox

If you want to enable user shared mailbox, execute:

```
config setprop dovecot SharedMailboxesStatus enabled
signal-event nethserver-mail-server-update
```

Discontinued packages

The following packages were available in the previous 6 release and have been removed in 7:

- nethserver-collectd-web: replaced by nethserver-cgp
- nethserver-password: integrated inside nethserver-sssd
- nethserver-faxweb2: see the discussion faxweb2 vs avantfax.

- nethserver-fetchmail: replaced by getmail
- nethserver-ocsinventory, nethserver-adagios: due to compatibility problems with Nagios, these modules will be mantained only on NethServer 6 release
- nethserver-ipsec: IPSec tunnels are now implemented in nethserver-ipsec-tunnels, L2TP function has been dropped
- nethserver-webvirtmgr

CHAPTER 2

Installation

2.1 Installation

2.1.1 Minimum requirements

Minimum requirements are:

- 64 bit CPU (x86_64)
- 1 GB of RAM
- 10 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 DVD or USB stick
- 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!

Media creation

Download the ISO file from official site www.nethserver.org. The downloaded ISO file can be used to **create a bootable media** such as DVD or USB stick.

USB stick

On a Linux machine, open the shell and execute:

```
dd if=NethServer.iso of=/dev/sdc
```

Where *NethServer.iso* is the file name of the downloaded ISO and */dev/sdc* is the destination device corresponding to the USB key and not a partition (such as /dev/sdc1).

On a Windows machine, make sure to format the USB drive then unmount it. Use one of the following tools to write the USB stick:

- Etcher
- Win32 Disk Imager
- Rawrite32
- dd for Windows

DVD

The creation of a bootable DVD is different from writing files into USB stick, and it requires the use of a dedicated function (e.g. *write* or *burn ISO image*). Instructions on how to create a bootable DVD from the ISO are easily available on the Internet or in the documentation of your operating system.

Install modes

Start the machine using the freshly backed media. If the machine will not start from the DVD or USB stick, 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 DVD reader or USB stick.

On start a menu will display different types of installation:

NethServer *interactive installation*

Requires only keyboard and time zone settings. By default, tries to configure the network interfaces with DHCP and the first two available disks with RAID-1.

Other NethServer installation methods

- *Unattended installation* – A set of default parameters is applied to the system with no human intervention.
- *Manual installation* – This is the opposite of *unattended*. No defaults are applied: network, storage, time zone, keyboard... all settings must be provided explicitly.

Standard CentOS installation

Use the standard CentOS installation procedure. You can then configure NethServer by following the *Install on CentOS* section.

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.

Optional boot parameters

At the boot menu, you can add extra parameters by pressing `TAB` and editing the kernel command line. This can be useful in *unattended* mode.

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
```

To enable *file system encryption*, use:

```
fspassword=s3cr3t
```

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.

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

Other available options (*unattended* mode only):

- `keyboard`, keyboard layout, default is `keyboard=us`
- `timezone`, default is `timezone=UTC`

Fallback IP configuration

If no IP is assigned by DHCP or by other means, during the first system boot the following IP configuration is applied to the **first** network interface

- IP 192.168.1.1
- netmask 255.255.255.0

System administrator password

You are strongly advised to choose a secure password for the `root` user. A good password:

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

The default password in *unattended* mode is `Nethesis,1234`.

System language

The system language of NethServer installations is *English (United States)*. Additional languages can be installed later. See *Next steps*.

Interactive and Manual modes

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

Required choices are:

- Language
- Keyboard layout
- Root password

All other options are set to a reasonable default accordingly to current hardware (see the *Unattended mode* section for details), but you are free to edit any install configuration available.

On the other hand, the **manual** mode starts the installer with no default settings at all. Also the network and storage sections must be configured.

Warning: Under the *Network* > *General* section, only the interfaces marked as *Automatically connect to this network when it is available* are enabled at boot in the installed system. For more info, refer to RHEL 7 installation guide.

Known issues

- When installing on machines with UEFI firmware, Anaconda could fail on automatic partitioning. To work around the problem, switch to *Manual installation*, or *Standard CentOS installation* then follow *Install on CentOS*. In case of installation with software RAID, make sure to manually create UEFI partitions on all boot disks.

Unattended mode

The *unattended* mode requires no human intervention. After installation, the system is rebooted and the following configuration is applied:

- Keyboard layout: `us`
- Time zone: `UTC`
- Default `root` password: `Nethesis,1234`
- DHCP enabled on all network interfaces; if no DHCP lease is received the *fallback IP configuration* is applied
- if there are two or more disks, a RAID 1 will be created on first two disks and LVM volumes are created on it
- *swap* and *root* partitions are allocated automatically; 1GB is assigned to *boot*

2.1.4 Install on CentOS

It is possible to install NethServer on a fresh CentOS minimal installation using a couple of commands to download the additional software packages. This installation method is designed for virtual private servers (VPS) where CentOS comes already installed by the VPS provider.

Enable NethServer software repositories with this command:

```
yum install -y http://mirror.nethserver.org/nethserver/nethserver-release-7.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-nextcloud
```

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 allows selecting an alternative language among those already installed on the system. After logging in, go to the *Software center* page to install additional languages.

The login page will give you a trusted access to the web interface. Log in as **root** and type the password chosen during NethServer installation.

Note: The *unattended* install procedure sets the root password to the default `Nethesis,1234`.

2.2.2 First configuration wizard

The first time **root** logs in, the *First configuration wizard* procedure is displayed.

If the root password is still at the default value, a password change is required.

It is possible to restore a **configuration backup**. Refer to *Disaster recovery* for more information.

Otherwise the wizard procedure helps on setting up:

- Host name
- *Date and time zone*
- SSH port
- *Smarthost configuration*
- *Usage statistics*

2.2.3 Change the current password

You can change the root password from the web interface by going to the *root@host.domain.com* label on the upper right corner of the screen and clicking on *Profile*.

2.2.4 Logout

Terminate the current Server Manager session by going to the *root@host.domain.com* label on the upper right corner of the screen and by clicking on *Logout*.

2.2.5 Session timeouts

By default (starting from NethServer 7.5.1804), 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.

2.3 NethServer subscription

A NethServer installation can be registered to a public or private Dartagnan[1] instance, getting access to monitoring portal and stable update repositories.

Hint: The NethServer Subscription by Nethesis[2] enables access to a public ready-to-use Dartagnan instance, along with immediate professional support services for your NethServer deployments. Detailed info available at https://my.nethserver.com

---

Activating a subscription will enable the stable YUM repositories, but will disable any other repositories you may have added. You can re-enable any other repositories by creating a "template-custom" for `/etc/nethserver/eorepo.conf`.

The subscription provider may not accept support requests for the contents of custom repositories.

2.3.1 Registering the system

1. Access *Subscription* page from the Server Manager
2. Click on *Subscribe*
3. Login or register to https://my.nethserver.com to obtain a registration code
4. Copy and paste the code inside the *Registration token* field
5. Click on *Register now* button

At the end, the subscription plan name and validity are reported inside the page. Monitoring and access to stable repositories are automatically enabled.

2.3.2 Removing a subscription

When the subscription expires, or at the end of a trial period, use the following command to revert any modification to repositories and access the community ones:

```
config setprop subscription Secret '' SystemId ''
signal-event software-repos-save
```

Refer to *Software updates* for more information about the community updates origin.

[1] Dartagnan documentation: https://nethesis.github.io/dartagnan/
[2] Nethesis official site: http://www.nethesis.it

CHAPTER 3

Configuration

3.1 Software center

NethServer is highly modular: at the end of the installation a bare minimum set of features like *network configuration* and *log viewer* is installed. The *Software center* page allows the administrator to select and **install** additional *modules*, and also list and **update** the already installed software *packages*.

A *module* is usually constituted by multiple *packages*. It extends the system functionality. For instance a module can transform NethServer into an Email server, or a Web proxy.

A software *package* is an atomic unit of software. It is published by a public software repository. NethServer packages are files in the RPM[1] file format. Thus within this context the terms *package* and *RPM* can be used as synonyms.

3.1.1 Software updates

A NethServer 7 system receives updates from different software projects:

- the NethServer project itself[2]
- the CentOS project[3]
- the EPEL repository[4]

Each project releases software updates according to its specific rules and development cycle, but all of them prefer software stability over bleeding edge features.

Refer to the Community forum[5] and *Release notes 7* for more information about NethServer updates.

Updates released by the CentOS project are immediately available on NethServer directly from the CentOS mirrors. More info about CentOS updates:

[1] RPM Package Manager – http://rpm.org
[2] NethServer – http://www.nethserver.org
[3] CentOS – Community ENTerprise Operating System https://www.centos.org/
[4] EPEL – Extra Packages for Enterprise Linux https://fedoraproject.org/wiki/EPEL
[5] NethServer community forum – http://community.nethserver.org

- https://wiki.centos.org/FAQ/General
- https://access.redhat.com/support/policy/updates/errata/
- https://access.redhat.com/security/updates/backporting
- https://access.redhat.com/security/

Updates released by EPEL are available only if the **unlocked** software updates origin is selected, as explained below.

Hint: Even if the above projects strive for software stability, care is necessary to check if the updates fit well together. Every time the system is going to be updated, **create a backup of the data and review the updates changelog** to understand what is going to happen. If possible, test the updates in a non-production system. For any doubt ask the NethServer community forum![5]

Every day an **automated scheduled task** checks if a new distribution release of CentOS is available; when this happens it sends an email notification message to the system administrator and changes the *Software updates origin*. The system administrator can temporarily change the software updates origin from *Software center* > *Configure*. The available choices are:

Unlocked (default)

> The Software center considers updates from all available software repositories. It ensures every installed package is at its latest version.
>
> The "unlocked" origin is automatically selected by the *system upgrade* procedure that can be started only by the system administrator.

Locked

> The Software center prevents to install the updates coming from a CentOS release different than the current system version. For example, it prevents to install updates from CentOS 7.6 if NethServer version is 7.5. Packages from other repositories which are generically compatible with "7" (like EPEL) are considered only when new modules are installed; once they have been installed they are never updated.
>
> The "locked" origin is automatically selected when a new CentOS distribution release is available. When also the NethServer project releases a new version, the Software center asks to start the *system upgrade*. The upgrade procedure switches to the "unlocked" origin at the end.

> **Warning:** When `yum` is run from the command line and the software origin is "locked", EPEL and other repositories which are generically compatible with "7" are **enabled**

Manual update procedure

When updates are available, a warning message appears in the *Software center* page.

Updates for the installed software are listed under the *Updates* tab. Further details about them are available under *Updates CHANGELOG*.

To start the system update click the *Download and install* button.

Hint: Regularly update the installed software to fix bugs, security issues and receive new features

---

Automatic update procedure

It is possible to perform some automatic actions when new software updates are available.

- Download and (optionally) install the updates
- Send an email to the system administrator (root) and to an additional list of recipients

The updates availability is checked by a task that runs at a random time overnight.

Hint: If the notification email is not delivered or is marked as spam, it is possible to configure a *smarthost*

3.1.2 Modules installation

The *Available* tab lists all of the modules that can be installed. This list can be filtered by category. See also *Additional languages*.

To **install a module**, check the corresponding box and click on *Add*. Some modules suggest optional packages that can be installed also at a later time.

Once a module has been installed, it is listed under the *Installed* tab.

To **install optional packages** at a later time, select *Installed* tab and push the *Edit* button on a listed entry.

To **remove a module**, go to the *Installed* tab and push the corresponding *Remove* button.

> **Warning:** When removing a module other modules could be removed, too! Read carefully the list of affected packages to avoid removing required features.

List of installed packages

The complete list of installed RPM packages is available under *Installed* > *Packages*.

The section *Installed software* displays all packages already installed into the system with the full package version.

Additional languages

The Server Manager allows selecting the interface language at the login screen. Only installed languages are listed.

In *Available* tab, select the *Languages* category and install the desired languages.

References

3.2 Base system

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

3.2.1 Dashboard

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

Disk analyzer

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

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

Well known folders are:

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

3.2.2 Network

The *Network* page configures how the server is connected to the local network (LAN) and/or other networks (i.e. Internet).

If the server has firewall and gateway functionality, it will handle extra networks with special functions 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 determines its behavior. All roles are identified by colors. Each role corresponds to a well-known *zone* with special network traffic rules:

- *green*: local network (green role/zone). Hosts on this network can access any other configured network
- *blue*: guests network (blue role/zone). Hosts on this network can access orange and red networks, but can't access the green network
- *orange*: DMZ network (orange role/zone). Hosts on this network can access red network, but can't access to blue and green networks
- *red*: public network (red role/zone). 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 the *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 tolerate 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

3.2.3 Network services

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

Each service has a list of "open" ports on which it answers to connections. Connections can be accepted from selected zones. Finer grained control of access to network services can be configured from the Firewall rules page.

3.2.4 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.

3.2.5 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.

3.2.6 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.

3.2.7 Server certificate

The *Server certificate* page shows the currently installed X.509 certificates, and the default one provided by system services for TLS/SSL encrypted communications.

NethServer checks the certificates validity and sends an email to the root user if a certificate is near to expire.

The *Set as default* button allows choosing the default certificate. When a new certificate is chosen, all services using TLS/SSL are restarted and network clients will be required to accept the new certificate.

When NethServer is installed a default RSA self-signed certificate is generated. It should be edited by inserting proper values before configuring the network clients to use it. When the self-signed certificate is due to expire a new one is automatically generated from the same RSA key and with the same attributes.

The *Server certificate* page also allows:

- uploading an existing certificate and private RSA/ECC key. Optionally a certificate chain file can be specified, too. All files must be PEM-encoded.
- requesting a new *Let's Encrypt*[1] certificate. This is possible if the following requirements are met:
  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[2]);
  2. The domains that you want the certificate for must be public domain names associated to server own public IP. Make sure you have public DNS name pointing to your server (you can check with sites like[3]).

     Wildcard certificates (i.e. `*.nethserver.org`) are not supported.

  The *Notification email* will be used by Let's Encrypt to send notifications about the certificate.

  The Let's Encrypt certificate is automatically renewd 30 days before expiration date.

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

Disable Let's Encrypt

Let's Encrypt certificate can be disabled following these steps:

1. Access the *Server certificate* page, set as default the self-signed certificate or an uploaded one
2. Open the shell and execute the following commands:

```
rm -rf /etc/letsencrypt/*
config setprop pki LetsEncryptDomains ''
```

3.2.8 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.

3.2.9 Log viewer

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

This module allows to:

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

[1] Let's Encrypt website https://letsencrypt.org/
[2] Website http://www.canyouseeme.org/
[3] Website http://viewdns.info/

3.2.10 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.

3.2.11 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
```

3.3 Users and groups

3.3.1 Account providers

NethServer supports authentication and authorization against either a **local** or **remote** account provider.

Supported provider types are:

- Local OpenLDAP running on NethServer itself
- Remote LDAP server with RFC2307 schema
- Local Samba 4 Active Directory Domain Controller
- Remote Active Directory (both Microsoft and Samba)

The root user can configure any type of accounts provider from the *Accounts provider* page.

Be aware of the following rule about account providers:

> Once NethServer has been bound to an account provider the FQDN cannot be changed any more

Remote providers After NethServer has been bound to a remote account provider the *User and groups* page shows the domain accounts in *read-only* mode.

Local providers After installing a local provider (either Samba 4 or OpenLDAP), the administrator can create, modify and delete the users and groups.

> **Warning:** Please choose wisely your account provider because **the choice could not be reversible**. Also the system will forbid any change to the FQDN after the account provider has been configured.

Choosing the right account provider

Beside choosing to bind a remote provider or install a local one, the administrator has to decide which backend type suits his needs.

The *File server* module of NethServer, which enables the *Shared folders* page, can authenticate SMB/CIFS clients only if NethServer is bound to an Active Directory domain. The LDAP providers allow access to *Shared folders* only in *guest mode*. See *Shared folders*.

On the other hand, the local OpenLDAP provider is more easy to install and configure.

In the end, if the SMB file sharing protocol support is not required, an LDAP provider is the best choice.

OpenLDAP local provider installation

To install and configure an OpenLDAP local accounts provider, go to page *Accounts provider* > *LDAP* > *Install locally*. The system needs a working internet connection to download additional packages.

At the end of the installation the package is automatically configured and the administrator will be able to manage users and groups from the *User and groups* page.

See *Admin account* section for more details about default administrative user and group.

Samba Active Directory local provider installation

When installing Samba Active Directory as local account provider, the system needs an **additional IP address** and a **working internet connection**.

The additional IP is assigned to a Linux Container that runs the Active Directory Domain Controller roles and must be accessible from the LAN (green network).

Therefore the additional IP address must satisfy three conditions:

1. the IP address has to be **free**; it must not be used by any other machine
2. the IP address has to be in the same subnet range of a green network
3. the green network has to be bound to a bridge interface where the Linux Container can attach its virtual interface; the installation procedure can create the bridge interface automatically, if it is missing

To install a local Active Directory accounts provider, go to page *Accounts provider* > *Active Directory* > *Create a new domain*.

The *DNS domain name* defines the DNS suffix of the new domain. NethServer acts as an authoritative DNS server for that domain. See also *DNS and AD domain*.

The *NetBIOS domain name* (also known as “domain short name”, “NT domain name”) is the alternative Active Directory domain identifier, compatible with older clients. See also *Network access*.

The *Domain Controller IP address* field must be filled with the **additional IP address** explained above.

When all fields are filled, press the *Create domain* button.

> **Warning:** The Active Directory *DNS domain name* and *NetBIOS domain name* values cannot be changed once that the domain has been created

The Active Directory configuration procedure might require some time to run. It creates the Linux Container chroot, by downloading additional packages.

At the end of the Active Directory configuration procedure, the NethServer host machine is automatically configured to join the Active Directory domain. Go to the page *User and groups* to see the default accounts.

The previously assigned IP address can be changed from *Accounts provider* > *Change IP*.

Warning: Changing the Domain Controller IP address can cause problems to Active Directory clients. If they use an external DNS server, update it to use the new IP address.

After installing Samba Active Directory, the *Users and groups* page has two default entries; both are disabled: *administrator* and *admin*. "Administrator" is the default Active Directory privileged account and is not required by NethServer; it is safe to keep it disabled. "admin" is defined by NethServer as the default system administrative account. It is member of the AD "domain admins" group. See *Admin account* section for more details.

DNS and AD domain

An Active Directory domain requires a reserved DNS domain to work. It is a good choice to allocate a subdomain of the public DNS domain for it. The AD subdomain can be accessible only from LAN (green) networks.

Example:

- public (*external*) domain: `nethserver.org`
- server FQDN: `mail.nethserver.org`
- Active Directory (*internal* LAN only) domain: `ad.nethserver.org`
- domain controller FQDN (assigned by default): `nsdc-mail.ad.nethserver.org`

Tip: When choosing a domain for Active Directory use an *internal* domain which is a subdomain of the *external* domain[1]

Installing on a virtual machine

Samba Active Directory runs inside a Linux Container which uses a virtual network interface bridged to the network interface of the system. The virtual network interface has to be visible inside the physical network, but often virtualization solutions block ARP traffic. As a result, the Samba Active Directory container is not visible from LAN hosts.

When installing on virtual environment, make sure the virtualization solution allows traffic in *promiscuous mode*.

VirtualBox

To setup the promiscuous mode policy, select "Allow all" from the drop down list located in the network settings section.

VMWare

Enter the networking configuration section of the virtualization mode and set the virtual switch in promiscuous mode.

[1] https://social.technet.microsoft.com/wiki/contents/articles/34981.active-directory-best-practices-for-internal-domain-and-network-names.aspx#Recommendation

KVM

Make sure the virtual machine is bridged to a real bridge (like br0) and the bridge is put in promiscuous mode.

It is possible to force a bridge (i.e. `br0`) in promiscuous mode using this command:

```
ifconfig br0 promisc
```

Hyper-V

Configure MAC Address Spoofing for Virtual Network Adapters[2]

Local accounts provider uninstallation

Both LDAP and AD local accounts provider can be uninstalled from the *Accounts provider* > *Uninstall* page.

When the local accounts provider DB is uninstalled, any user, group and computer account is erased.

- A list of users and groups in TSV format is dumped to `/var/lib/nethserver/backup/users.tsv` and `/var/lib/nethserver/backup/groups.tsv`. See also *Import accounts from plain-text files*.
- Existing files owned by users and groups must be removed manually. This is the list of system directories containing users and groups data:

```
/var/lib/nethserver/home
/var/lib/nethserver/vmail
/var/lib/nethserver/ibay
```

Join an existing Active Directory domain

Here NethServer is bound to a remote Active Directory account provider. It can be provided by either Samba or Microsoft implementations. In this scenario NethServer becomes a trusted server of an existing Active Directory domain. When accessing a NethServer resource from a domain workstation, user credentials are checked against one of the domain controllers, and the access to the resource is granted.

Joining an Active Directory domain has the following pre-requisite:

> The Kerberos protocol requires the difference between systems clocks in the network is less than 5 minutes. Configure the network clients to align their clocks to a common time source. For NethServer go to *Date and time* page.

After the prerequisite is fulfilled, proceed to the page *Accounts provider* > *Active Directory* > *Join a domain*.

- Enter the *DNS domain name* of the AD domain. The NetBIOS domain name (domain short name) is probed automatically.
- Fill the *AD DNS server* field. Usually it is the IP address of an AD domain controller.
- Provide the *User name* and *Password* of an AD account with the privilege of joining a computer to the domain. Remember that the default *administrator* account could be disabled!

[2] https://technet.microsoft.com/en-us/library/ff458341.aspx

Warning: Some additional modules, like *Nextcloud*, *WebTop*, *Roundcube*, *Ejabberd* require read-only access to AD LDAP services. To be fully operational they require an additional account to perform simple LDAP binds.

Create a **dedicated user account** in AD, and set a complex *non-expiring* password for it.

Once NethServer has successfuly joined AD, specify the **dedicated user account** credentials in *Accounts provider* > *Authentication credentials for LDAP applications*.

Bind to a remote LDAP server

To configure a remote LDAP accounts provider, go to page *Accounts provider* > *LDAP* > *Bind remotely*.

Type the LDAP server IP address in the field *Host name or IP*. If the LDAP service runs on a non-standard TCP port, specify it in *TCP port*.

Then an LDAP *rootDSE* query is sent to the specified host and a form is filled with returned data. Check the values are correct then press the *Save* button to confirm.

If the LDAP server requires authentication, fill in the fields under *Authenticated bind*. Enable either `ldaps://` or STARTTLS to encrypt the connection.

Tip: If the remote LDAP server is also a NethServer installation and it is in the LAN (green) network, select *Anonymous bind*

3.3.2 Users

A newly created user account remains locked until it has set a password. Disabled users are denied to access system services.

When creating a user, following fields are mandatory:

- User name
- Full name (name and surname)

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 services without deleting the account. This can be achieved using the *Lock* and *Unlock* actions.

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

Changing the password

If there wasn't given an initial password during user creation, the user account is disabled. To enable it, set a password using the *Change password* button.

When a user is enabled, the user can access the Server Manager and change his/her own password by going to the *user@domain.com* label on the upper right corner of the screen and clicking on *Profile*.

If the system is bound to an Active Directory account provider, users can change their password also using the Windows tools. In this 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 it is evaluated according to the *configured policies*.

Credentials for services

The user's credentials are the **user name** and his **password**. Credentials are required to access the services installed on the system.

The user name can be issued in two forms: *long* (default) and *short*. The *long* form is always accepted by services. It depends on the service to accept also the *short* form.

For instance if the domain is *example.com* and the user is *goofy*:

User long name form *goofy@example.com*

User short name form *goofy*

To access a shared folder, see also *Network access*.

User home directories

User home directories are stored inside `/var/lib/nethserver/home` directory, in order to simplify the deployment of a single-growing partition system.

The administrator can still restore the well-known `/home` path using the bind mount:

```
echo "/var/lib/nethserver/home       /home   none    defaults,bind   0 0" >> /etc/
↪fstab
mount -a
```

3.3.3 Groups

A group of users can be granted some permission, such as authorize access over a *shared folder*. The granted permission is propagated to all group members.

Two special groups can be created. Members of these groups are granted access to the panels of the Server Manager:

- *domain admins*: members of this group have the same permissions as the *root* user from the Server Manager.
- *managers*: members of this group are granted access to the *Management* section of the Server Manager.

3.3.4 Admin account

If a **local AD or LDAP provider** is installed, an *admin* user, member of the *domain admins* group is created automatically. This account allows access to all configuration pages within the Server Manager. It is initially *disabled* and has no access from the console.

Tip: To enable the *admin* account set its password.

Where applicable, the *admin* account is granted special privileges on some specific services, such as joining a workstation to an Active Directory domain.

If NethServer is bound to a **remote account provider**, the *admin* user and *domain admins* group could be created manually, if they do not already exist.

If a user or group with a similar purpose is already present in the remote account provider database, but it is named differently, NethServer can be configured to rely on it with the following commands:

```
config setprop admins user customadmin group customadmins
/etc/e-smith/events/actions/system-adjust custom
```

3.3.5 Password management

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

Password policies can be changed from web interface.

Complexity

The password complexity is a set of minimum conditions for password 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)
- If Samba Active Directory is installed, also the system will enable password history

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.

Expiration

The password expiration is enabled by default to 6 months from the time when the password is set.

Note: The system will refer to the date of the last password change, if password is older 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.

Effects of expired passwords

After password expiration, the user is still able to read and send email messages.

If NethServer has an Active Directory account provider, the user cannot access shared folders, printers (by Samba) and other domain computers.

3.3.6 Import accounts from plain-text files

Import users

It is possible to create user accounts from a TSV (Tab Separated Values) file with the following format:

```
username <TAB> fullName <TAB> password <NEWLINE>
```

Example:

```
mario <TAB> Mario Rossi <TAB> 112233 <NEWLINE>
```

then execute:

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

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

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

Alternative separator character:

```
import_users users.tsv ','
```

Import emails

It is possible to create mail aliases from a TSV (Tab Separated Values) file with the following format:

```
username <TAB> emailaddress <NEWLINE>
```

Then you can use the `import_emails` script. See *Import accounts from plain-text files* for a sample script invocation.

Import groups

Group management is available from the command line through `group-create` and `group-modify` events

```
signal-event group-create group1 user1 user2 user3
signal-event group-modify group1 user1 user3 user4
```

3.4 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

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

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

3.4.1 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.

3.4.2 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.

3.5 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.

[1] Dynamic Host Configuration Protocol (DHCP) https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

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.

3.5.1 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`.

Advanced options

There are seven advanced options for DHCP. You can assign zero options, one option or all seven options.

For the servers – DNS, NTP, WINS and TFTP – you can assign zero, one or more for each server; if you place more than one, use a comma between each server with no space.

3.5.2 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.

3.5.3 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:

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

[3] Preboot eXecution Environment https://en.wikipedia.org/wiki/Preboot_Execution_Environment
[2] Trivial File Transfer Protocol https://en.wikipedia.org/wiki/Tftp

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

3.6 TLS policy

The *TLS policy* page controls how individual services configure the Transport Layer Security (TLS) protocol, by selecting a *policy identifier*.

If not otherwise stated, the TLS settings of policies are always *cumulative*: **newer policies extend older ones**.

Each module implementation decides how to implement a specific policy identifier, providing a trade off between security and client compatibility. Newer policies are biased towards security, whilst older ones provide better compatibility with old clients.

The following sections describe each policy identifier.

3.6.1 Policy 2018-10-01

This policy restricts the TLS settings of the default Ejabberd configuration. It applies only to Ejabberd version 18 and greater.

Ejabberd (XMPP)

- See https://bettercrypto.org/static/applied-crypto-hardening.pdf category B
- Disabled SSLv3 and TLSv1.0

- Cipher server priority
- ECC certificate
- Ciphers suite

```
ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-ECDSA-
↪AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-
↪SHA256:EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:+
↪aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:CAMELLIA256-
↪SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA
```

3.6.2 Policy 2018-06-21

This policy extends `2018-03-30` by adding the support for ECC certificates to

- Apache
- Dovecot
- OpenSSH
- Postfix

Slapd (openldap-servers)

- Reference https://access.redhat.com/articles/1474813
- Disabled SSLv3 and TLSv1.0
- Cipher suite

```
ECDHE:EDH:CAMELLIA:ECDH:RSA:ECDSA:!eNULL:!SSLv2:!RC4:!DES:!EXP:!SEED:!IDEA:!
↪3DES:!ADH
```

3.6.3 Policy 2018-03-30

The goal of this policy is to harden the cipher set provided by the default upstream policy. It is not compatible with IE 8 XP and Java 6u45 and 7u25 clients. It does not support ECC certificates.

Apache

- See https://bettercrypto.org/static/applied-crypto-hardening.pdf category B
- Cipher suite

```
EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
```

- Disabled SSLv2 and SSLv3
- Ignore `httpd/SSLCipherSuite` property settings (see *Default upstream policy*)

Dovecot

- See https://bettercrypto.org/static/applied-crypto-hardening.pdf category B
- Cipher suite

```
EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:+CAMELLIA2
↪aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-
↪SHA:AES256-SHA:CAMELLIA128-SHA:AES128-SHA
```

- Disabled SSLv2 and SSLv3

OpenSSH

- See https://github.com/NethServer/nethserver-openssh/pull/6
- Configuration snippet

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
↪gcm@openssh.com,aes256-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-
↪etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-ripemd160
KexAlgorithms curve25519-sha256@libssh.org,diffie-hellman-group-exchange-
↪sha256,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1
```

Postfix

- See https://bettercrypto.org/static/applied-crypto-hardening.pdf category B
- Use TLS in outbound connections, if remote server supports it
- Disable SSLv2 and SSLv3 on submission ports
- Cipher suite

```
EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA256:EECDH:+CAMELLIA128:+AES128:+SSLv3:
↪SHA:AES128-SHA
```

- Exclude ciphers

```
aNULL:eNULL:LOW:3DES:MD5:EXP:PSK:DSS:RC4:SEED:IDEA:ECDSA
```

3.6.4 Default upstream policy

The goal of this policy is retaining upstream settings. This is the original goal since NethServer 7.

This policy allows to customize `httpd` (Apache) with a given cipher list, by issuing the following commands:

```
config setprop httpd SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
signal-event nethserver-httpd-update
```

CHAPTER 4

Modules

4.1 Backup

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

- configuration backup
- data backup

Configuration backup contains only system configuration files. 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 by installing the "Backup" module and, by default, contains all the data stored in the system (user's home directories, shared folders, emails, etc). The *single backup* runs once a day and can be full or incremental on a weekly basis. This backup also contains the archive of the configuration backup. More backups can be configured to save different data at different intervals.

4.1.1 Configuration backup

From page *Backup (configuration)* the system configuration can be saved, downloaded, uploaded and restored again.

Furthermore, an automated task runs every night at 00.15 and creates a new archive, `/var/lib/nethserver/backup/backup-config.tar.xz`, if the configuration has changed during the previous 24 hours. Under *Backup (configuration)* > *Configure* page, specify the number of *Automatic backups to keep*.

The list of installed modules is included in the backup archive. The restore procedure can download and install the listed modules automatically.

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 a custom httpd configuration. In this case you can add the file that contains the customization 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/httpd/conf.d/mycustom.conf` file, add this line:

```
/etc/httpd/conf.d/mycustom.conf
```

Do not add big directories or files to the configuration backup.

Exclusion

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

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

4.1.2 Data backup

NethServer implements 2 types of data backup:

- Single backup (primary, default, backward compatible)
- Multiple backups (multi-backup, multi-engine)

The data backup can be performed using different engines:

- duplicity (default) - http://duplicity.nongnu.org/
- restic - https://restic.net/
- rsync - https://rsync.samba.org/

When selecting an engine, the system administrator should carefully evaluate multiple aspects:

- Compression: data is compressed on the destination, disk usage can vary in function of compression efficiency which depends also on the data set
- Deduplication: instead of compressing files, data is split into chunks and only a copy of each chunk is kept. Efficiency depends highly on the data set
- Encryption: data saved inside the destination storage is encrypted. Usually data is encrypted before transfer
- Size: space used on the destination for each backup, may be smaller or equal than the original data set. When using engines without encryption support, the destination should always be bigger than the source
- Retention: the policy which sets the amount of time in which a given set of data will remain available for restore
- Integrity: it's the engine ability to check if the performed backup is valid in case of restore
- Type: a backup can be full, incremental or snapshot based (incremental-forever):
  - full: all files are copied to the destination each time
  - incremental: compare the data with last full backup and copy only changed or added items. The full backup and all the intermediate incrementals are needed for the restore process. A full backup is required on a regular basis.
  - snapshot: create a full backup only the first time, then create differential backups. Snapshots can be deleted and consolidated and only one full backup is needed

Engine	Compression	Deduplication	Encryption	Integrity	Type
duplicity	Yes	No	No	Yes	full / incremental
restic	No	Yes	Yes	Yes	snapshot
rsync	No	Partial	No	No	snapshot

Engines

Duplicity

Duplicity is the well-known default engine for NethServer. It has a good compression algorithm which will reduce storage usage on the destination. Duplicity requires a full backup once a week, when the data set is very big the process may take more than 24 hours to complete. NethServer doesn't implement backup encryption if the engine is Duplicity.

Supported storage backends:

- CIFS
- NFS
- USB
- WebDAV (only when used as single backup)

Restic

Restic implements a snapshot-based and always-encrypted backup. It has support for deduplication and can perform backup on cloud services. Since Restic requires only one full backup, all runs after the first should be fast and could be scheduled multiple times a day.

Supported storage backends:

- CIFS
- NFS
- USB
- WebDAV (only when used as *single backup*)
- SFTP (SSH File Transfer Protocol)
- Amazon S3 (or any compatible server like Minio)
- Backblaze B2
- Restic REST server

Rsync

Time machine-style backup engine using rsync. After the first full backup, it copies only modified or new files using fast incremental file transfer. On the destination, partial deduplication is obtained using hard links. If the backup destination directory is full, the oldest backups are automatically deleted to free space.

Supported storage backends:

- CIFS

- NFS
- USB
- WebDAV (only when used as *single backup*)
- SFTP (SSH File Transfer Protocol)

Rsync doesn't support encryption nor compression on the destination. During data transfer, SFTP assures encryption and data is compressed to minimize bandwidth usage.

Note: When using rsync engine, make sure the storage backend supports symbolic and hard links. Please note that NethServer doesn't support links on Samba shares due to security implications. Also symlinks are not supported on WebDAV.

Single backup

This is the default system backup which can be configured and restored using the web interface. It can be scheduled once a day, can include system logs and implements notifications to the system administrator or to an external mail address.

Storage backends

Single backup can be saved on a destination chosen between:

- USB: disk connected to a local USB port (See: *Data backup*)
- CIFS: Windows shared folder, it's available on all NAS (Network Attached Storage). Use access credentials like: MyBindUser,domain=mydomain.com
- NFS: Linux shared folder, it's available on all NAS, usually faster than CIFS
- WebDAV: available on many NAS and remote servers (use a server with a valid SSL certificate as WebDAV target, otherwise the system will fail mounting the filesystem)

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

Change backup engine

Duplicity is the default engine for the *single backup*. You can change it executing one of the commands below.

To use restic:

```
config setprop backup-data Program restic
```

To use rsync:

```
config setprop backup-data Program rsync
```

To use duplicity:

```
config setprop backup-data Program duplicity
```

The backup will use the selected engine on next run. When the new engine has completed at least one backup, remember to cleanup the destination by removing data from the old engine.

Multiple backups

The administrator can schedule multiple backups using different engines and destinations. A valid policy could be creating a weekly backup to a local destination using duplicity, while scheduling a daily backup to a cloud storage using restic.

Note: Multiple backups can't be configured using the server-manager web user interface. All operations should be performed from command line.

When configuring multiple backups, please bear in mind two golden rules:

- always use different destinations for each engine
- avoid scheduling concurrent backups, each backup should run when the previous one has been completed

Limitation of multiple backups:

- disk usage report is not implemented
- WebDAV can't be used as storage backend

Every backup record is saved inside the `backups` database. Each record can have 3 different types:

- `duplicity`
- `restic`
- `rsync`

Common properties:

- `status` : enable or disable the backup, can be `enabled` or `disabled`
- `Notify`: if set to `always`, always send a notification with backup status; if set to `error`, send a notification only on error; if set to `never`, never send a notification
- `NotifyFrom`: set a different sender than `root@localhost`
- `NotifyTo`: send the notification to given mail address, default is `root@localhost`
- `VFSType` : set the storage backend

To list all configured backups:

```
db backups show
```

Output example:

```
mybackup=rsync
  BackupTime=1 7 * * *
  Notify=error
  NotifyFrom=
  NotifyTo=root@localhost
  SMBHost=192.168.1.234
  SMBLogin=test
```

(continues on next page)

(continued from previous page)

```
  SMBPassword=test
  SMBShare=test
  VFSType=cifs
  status=enabled
```

Schedule

The backup schedule uses the cron syntax saved inside the `BackupTime` property. Below, some examples.

Every night at 3:

```
db backups setprop mybackup BackupTime '0 3 * * *'
```

Every hour, at minute 15:

```
db backups setprop mybackup BackupTime '15 * * * *'
```

At 04:05 on every Sunday:

```
db backups setprop mybackup BackupTime '5 4 * * 0'
```

For more examples, see:

- https://crontab-generator.org/
- https://crontab.guru

Retention policy

Each engine can implement its own retention policy. The policy can be set using the `CleanupOlderThan` property.

The property takes a number followed by D, M or Y (Days, Months, or Years respectively).

Example: cleanup after 30 days:

```
db backups setprop mybackup CleanupOlderThan 30D
```

The retention policy is not supported by the rsync backend.

Storage backends

Multiple backups support different storage backends. Some backends are engine-specific.

CIFS

Samba or Windows share, `VFSType` is `cifs`. Supported by all backends.

Properties:

- `SMBShare`: Samba share name
- `SMBHost`: Samba server host name or IP address
- `SMBLogin`: Samba login user

- `SMBPassword`: Samba password for the given user

USB

USB-attached disk, `VFSType` is `usb`. Supported by all backends.

Properties:

- `USBLabel`

NFS

Network File System, `VFSType` is `nfs`. Supported by all backends.

Properties:

- `NFSHost`: NFS server host name or IP address
- `NFSShare`: NFS share name

SFTP

SSH File Transfer Protocol, `VFSType` is `sftp`. Supported only by restic and rsync.

Properties:

- `SftpHost`: SSH host name or IP address
- `SftpUser`: SSH user
- `SftpPort`: SSH port
- `SftpDirectory`: destination directory, must be writable by the SSH user

S3

Amazon S3 (or compatible), `VFSType` is `s3`. Supported only by restic.

Properties:

- `S3AccessKey`: user access key
- `S3Bucket`: bucket (directory) name
- `S3Host`: S3 host, use `s3.amazonaws.com` for Amazon
- `S3SecretKey`: secret access key

How to setup Amazon S3 access keys: https://restic.readthedocs.io/en/stable/080_examples.html

B2

Backblaze B2, `VFSType` is `b2`. Supported only by restic.

Properties:

- `B2AccountId`: B2 account name

- `B2AccountKey`: B2 account secret key
- `B2Bucket`: B2 bucket (directory)

Rest

Restic REST server, `VFSType` is `rest`. Supported only by restic.

Properties:

- `RestDirectory`: destination directory
- `RestHost`: REST server hostname or IP address
- `RestPort`: REST sever port (default for server is 8000)
- `RestProtocol`: REST protocol, can be `http` or `https`
- `RestUser`: user for authentication (optional)
- `RestPassword`: password for authentication (optional)

Examples

Rsync backup, every day at 7:15 to a remote server. The SFTP backend requires the password of the remote server to execute SSH key exchange.

```
db backups set mybackup1 rsync status enabled BackupTime '15 7 * * *' Notify error␣
↪NotifyFrom '' NotifyTo root@localhost \
VFSType sftp SftpHost 192.168.1.2 SftpUser root SftpPort 22 SftpDirectory /mnt/
↪mybackup1
echo -e "Nethesis,1234" > /tmp/mybackup1-password; signal-event nethserver-backup-
↪data-save mybackup1 /tmp/mybackup1-password
```

Restic backup every day at 3:00 to Amazon S3, no retention limit:

```
db backups set mybackup1 restic VFSType s3 BackupTime '0 3 * * *' CleanupOlderThan␣
↪never Notify error NotifyFrom '' NotifyTo root@localhost status enabled \
S3AccessKey XXXXXXXXXXXXXXXXXXX S3Bucket restic-demo S3Host s3.amazonaws.com␣
↪S3SecretKey xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx Prune 0
signal-event nethserver-backup-data-save mybackup1
```

Duplicity backup every day at 22:00 to CIFS, 10 days retention:

```
db backups set mybackup1 duplicity VFSType cifs BackupTime '0 22 * * *'␣
↪CleanupOlderThan 10D Notify error NotifyFrom '' NotifyTo root@localhost status␣
↪enabled \
SMBHost nas.localnethserver.org SMBLogin myuser SMBPassword mypassword SMBShare␣
↪mybackup
signal-event nethserver-backup-data-save mybackup1
```

To manually start a backup, execute:

```
backup-data -b <name>
```

Where `name` is the backup name. For the examples above, the name is `mybackup1`.

Data backup customization

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

Single backup

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
```

The same syntax applies to configuration backup. Modifications should be done inside the file `/etc/backup-config.d/custom.include`.

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/
```

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

Multiple backups

All multiple backups read the same configuration of the single backup, but the list of saved and excluded files can be customized using two special files, where `name` is the name of the multiple backup:

- `/etc/backup-data/<name>.include`
- `/etc/backup-data/<name>.exclude`

Both files will override the list of included and excluded data set from the single backup. The accepted syntax is the same as the single backup (see paragraph above).

For example, given a backup named `mybackup1` create the following files:

- `/etc/backup-data/mybackup1.include`
- `/etc/backup-data/mybackup1.exclude`

Example

It's possible to configure the single backup to save all data and create a multiple backup which includes only the mail and is scheduled each our.

1. Configure the new `mymailbackup`:

```
db backups set mymailbackup restic status enabled BackupTime '0 * * * *' Notify␣
↪error NotifyFrom '' NotifyTo root@localhost \
VFSType nfs NFSHost nsfs.server.loc NFSShare test CleanupOlderThan 1d Prune 0
```

2. Create a custom include containing only the mail directory:

```
echo "/var/lib/nethserver/vmail" > /etc/backup-data/mymailbackup.include
```

3. Create an empty custom exclude file:

```
touch /etc/backup-data/mymailbackup.exclude
```

4. Apply the configuration:

```
signal-event nethserver-backup-save mymailbackup
```

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

4.1.3 Selective restore of files

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

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

By default, the latest backup tree is shown. If you want to restore a file from a previous backup, select the backup date from *Backup File* selector.

There are two options when restoring:

- Restore files in the original path, the current files in the filesystem are overwritten by the restored files from backup
- Restore files in original path but the restored files from backup are moved to 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 the **Restore** button.

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

Command line procedure

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>`

Single backup

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

```
backup-data-list
```

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

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). When used with snapshot-based engines, the `-t` option requires the name of the snapshot to restore.

Multiple backups

To list data inside a multiple backup, use:

```
backup-data-list -b <name>
```

To restore all data in the original location, use:

```
restore-data -b <name>
```

To restore a file or directory, use:

```
restore-file -b <name> <position> <path>
```

Note: When you are using *CIFS* to access the share, and the command doesn't work as expected, verify that user and password for the network share are correct. If user or password are wrong, you will find NT_STATUS_LOGON_FAILURE errors in `/var/log/messages`. Also, you can use the **`backup-data-list`** to check if the backup is accessible.

4.1.4 USB disk configuration

The best filesystem for USB backup disks is EXT3 or EXT4. FAT filesystem is supported but *not recommended*, while NTFS is **not supported**. EXT3 or EXT4 is mandatory for the rsync engine.

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
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*. The filesystem should be tuned on the backup engine used: rsync and restic require a lot of inodes, where duplicity performs better on file systems optimized for large files.

  For duplicity use:

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

  For rsync and restic use:

  ```
  mkfs.ext4 -v /dev/sdc1 -L backup -E lazy_itable_init
  ```

- 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.

4.1.5 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 the proper packages are installed. You can install additional packages before or after the restore. For example, if the mail-server is installed, the system can send and receive mails.

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. If possible, enable a network connection at boot (refer to *Interactive and Manual modes* section) to automatically re-install the required modules
2. Access the Server Manager and follow the *First configuration wizard* procedure
3. At step *Restore configuration*, upload the configuration archive. The option *Download modules automatically* should be enabled.
4. If a warning message requires it, reconfigure the network roles assignment. See *Restore network roles* below.
5. Verify the system is functional
6. Restore data backup executing on the console

```
restore-data
```

Please note that the disaster recovery should be always performed from a local media (eg. NFS or USB) to speed up the process.

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 automatic procedure attempts to fix the configuration at boot-time, to ensure a minimal network connectivity and login again on the Server Manager.

4.2 Email

The Email module is split into 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]
- DKIM signature[8]

Note: Since NethServer 7.5.1804 new *Email*, *POP3 connector* and *POP3 proxy* installations are based on the Rspamd filter engine. Previous NethServer installations are automatically upgraded to Rspamd as described in *Email module transition to Rspamd*

4.2.1 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[9] format.
- *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 custom email address. The hidden copy is enabled by the *Always send a copy (Bcc)* check box.

[1] Postfix mail server http://www.postfix.org/
[2] Dovecot Secure IMAP server http://www.dovecot.org/
[3] Sieve mail filtering language https://en.wikipedia.org/wiki/Sieve_(mail_filtering_language)
[4] Rspamd – Fast, free and open-source spam filtering system. https://rspamd.com/
[5] Email, https://en.wikipedia.org/wiki/Email
[6] The MX DNS record, https://en.wikipedia.org/wiki/MX_record
[7] SMTP, https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
[8] Domain Keys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing – Wikipedia
[9] The Maildir format, https://en.wikipedia.org/wiki/Maildir

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

If the final recipient cannot be established (i.e. the recipient address does not exist), the message is normally rejected. Sometimes (i.e. when a mail domain is migrated) it could be useful to accept it and silently deliver the message to a catch-all mailbox. This behavior can be obtained by enabling the *Accept unknown recipients* option.

Append a legal notice

Warning: Since NethServer 7.5.1804 this feature is shipped in a separate, optional package: `nethserver-mail2-disclaimer`. It is considered *deprecated* because the alterMIME[10] project which provides the actual implementation is no longer developed and can stop working at any time.

If the optional `nethserver-mail2-disclaimer` package was installed from the *Software center*, NethServer can automatically *append a legal notice to sent messages*. This text is also known as "disclaimer" and it can be used to meet some legal requirements.

The disclaimer text can contain Markdown[11] code to format the text.

Please note *signature* and *disclaimer* are very different concepts.

In general, the **disclaimer** is a fixed text and should be *attached* (not added) to messages by the mail server. This technique helps in 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 **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
```

DKIM signature

DomainKeys Identified Mail (DKIM)[8] provides a way to validate the sending MTA, which adds a cryptographic signature to the outbound message MIME headers.

To enable the DKIM signature for a mail domain, enable *Email > Domains > Sign outbound messages with DomainKeys Identified Mail (DKIM)*.

The DKIM signature headers are added only to messages sent through TCP ports 587 (submission) and 465 (smtps).

To work effectively, the public DNS must be configured properly. Refer to the instructions of your DNS provider to run the following steps:

[10] alterMIME is a small program which is used to alter your mime-encoded mailpack – https://pldaniels.com/altermime/
[11] The Markdown plain text formatting syntax, https://en.wikipedia.org/wiki/Markdown

1. Add a TXT record to your public DNS service provider with key "default._domainKey"
2. Copy and paste the given key text in the DNS record data (RDATA) section

4.2.2 Email addresses

Each user has a personal *mailbox* and any user name in the form <*username*>@<*domain*> is also a valid email address to deliver messages into it.

The list of mailboxes is shown by the *Email addresses* > *User mailboxes* page. The *Edit* button allows disabling the *Access to email services* (IMAP, POP3, SMTP/AUTH) for a specific user. Messages delivered to that user's mailbox can be forwarded to an external email address.

Warning: If the system is bound to a *remote account provider* and a user account is remotely deleted, the associated mailbox must be erased manually. The file system path prefix is `/var/lib/nethserver/vmail/` .

Mailboxes can be shared among groups of users. The *Email addresses* > *Shared mailboxes* page allows creating a new *shared mailbox* and defining one or more owning groups. Shared mailboxes can also be created by any IMAP client supporting IMAP ACL protocol extension (RFC 4314).

The system enables the creation of an unlimited number of additional email addresses, from the *Email addresses* > *Mail aliases* page. Each *mail alias* is associated with one or more destinations. A *destination* can be of the following types:

- user mailbox,
- shared mailbox,
- external email address.

A mail alias can be bound to any mail domain or be specific to one mail domain. 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.

4.2.3 Mailbox configuration

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

- IMAP[12] (recommended)
- POP3[13] (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.

[12] IMAP https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol
[13] POP3 https://en.wikipedia.org/wiki/Post_Office_Protocol

Warning: Do not allow unencrypted connections on production environments!

From the same page, the *disk space* of each mailbox can be limited to a default *quota*. If the mailbox quota is enabled, the *Dashboard* > *Mail quota* page summarizes the quota usage for each user. This summary is updated when a user logs in or a message is delivered. The quota can be customized for a specific user in *Email addresses* > *User mailboxes* > *Edit* > *Custom mailbox quota*.

Messages marked as **spam** (see *Filter*) can be automatically moved into the *Junk* folder by enabling the option *Move to "Junk" 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 *Email addresses* > *User mailboxes* > *Edit* > *Customize spam message retention*.

The `root` user can impersonate another user, gaining full rights to any mailbox contents and folder permissions. The *Root can log in as another user* option controls this empowerment, known also as *master user* in Dovecot[2].

When *Root can log in as another user* is enabled, the following credentials are accepted by the IMAP server:

- user name with `*root` suffix appended
- root's password

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

- user name: `john*root`
- password: `secr3t`

4.2.4 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.

4.2.5 Smarthost

The *Email* > *Smarthost* page, configures 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[14], or normal SMTP access is restricted by the ISP.

4.2.6 Filter

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

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

Block of attachments

The system can inspect mail attachments, denying access to messages carrying forbidden file formats. The server can check 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[4] analyzes emails by detecting and classifying *spam*[15] messages using heuristic criteria, predetermined rules and statistical evaluations on the content of messages.

The filter can also check if sender server is listed in one or more blacklists (DNSBL[14]). A score is associated to each rule.

Total spam score collected at the end of the analysis allows the server to decide what to do with a message, according to three **thresholds** that can be adjusted under *Email* > *Filter* > *Anti spam*.

1. If the spam score is above *Greylist threshold* the message is **temporarily rejected**. The *greylisting*[16] technique assumes that a spammer is in hurry and is likely to give up, whilst a SMTP-compliant MTA will attempt to deliver the deferred message again.

[14] DNSBL https://en.wikipedia.org/wiki/DNSBL
[15] SPAM https://en.wikipedia.org/wiki/Spamming
[16] Greylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using greylisting will "temporarily reject" any email from a sender it does not recognize – Wikipedia

2. If the spam score is above *Spam threshold* the message is **marked as spam** by adding the special header `X-Spam: Yes` for specific treatments, then it is delivered like other messages. As an alternative, the *Add a prefix to spam messages subject* option makes the spam flag visible on the subject of the message, by prefixing the given string to the `Subject` header.
3. If the spam score is above *Deny message spam threshold* the message is **rejected**.

Statistical filters, called Bayesian[17], 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 *Junk folder*. As a prerequisite, the Junk folder must be enabled from *Email* > *Mailboxes* page by checking *Move to "Junk" folder"* option.

- By *putting a message into the Junk 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 Junk*, 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.

The bayesian filter training applies to all users on the system, not only the user that marked an email as spam or ham.

It is important to understand how the Bayesian tests really work:

- It does not outright flag messages as spam if they contain a specific subject, or sender address. It is only collecting specific characteristics of the message.
- A message can only be flagged one time. If the same message is flagged multiple times, it will not affect anything as the dynamic tests have already been trained by that message.
- The Bayesian tests **are not active until it has received enough information. This includes a minimum of 200 spams AND 200 hams (false positives).**

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

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

Rspamd web interface

The anti-spam component is implemented by Rspamd[4] which provides its administrative web interface at

[17] Bayesian filtering https://en.wikipedia.org/wiki/Naive_Bayes_spam_filtering

```
https://<HOST_IP>:980/rspamd
```

The actual URL is listed under the *Applications* page. By default access is granted to members of the `domain admins` group and to the `admin` user (see also *Admin account*). An additional special login `rspamd` can be used to access it. Its credentials are available from *Email* > *Filter* > *Rspamd user interface (Web URL)*: just follow the given link.

The Rspamd web UI:

- displays messages and actions counters,
- shows the server configuration,
- tracks the history of recent messages,
- allows training the Bayes filter by submitting a message from the web form.

4.2.7 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
- GSSAPI (only if NethServer is bound to Samba/Microsoft Active Directory)

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. Mail user agents (MUA) must use the submission port.

4.2.8 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.

4.2.9 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.

4.2.10 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 folder using the 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.

4.2.11 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

NethServer configuration uses Rspamd as milter. It runs an Rspamd proxy worker in "self-scan" mode[19].

The key to track the whole SMTP transaction, including Rspamd decisions is the message ID header, or the Postfix Queue ID (QID). Both are available from the message source. The `Message-ID` header is generated by the sender, whilst the QID is assigned by the receiving MTA. For instance

```
Received: from my.example.com (my.example.com [10.154.200.17])
      by mail.mynethserver.org (Postfix) with ESMTP id A785B308622AB
      for <jsmith@example.com>; Tue, 15 May 2018 02:05:02 +0200 (CEST)
...
Message-ID: <5afa242e.hP5p/mry+fTNNjms%no-reply@example.com>
User-Agent: Heirloom mailx 12.5 7/5/10
```

Here `A785B308622AB` is the QID, whilst `5afa242e.hP5p/mry+fTNNjms%no-reply@example.com` is the Message ID.

Both strings can be used with the `grep` command to find relevant log lines in `/var/log/maillog*` (note the ending "*" to search also in archived log files). For instance

```
grep -F 'A785B308622AB' /var/log/maillog*
```

Yields

```
/var/log/maillog:May 15 02:05:02 mail postfix/smtpd[25846]: A785B308622AB: client=my.
↪example.com[10.154.200.17]
/var/log/maillog:May 15 02:05:02 mail postfix/cleanup[25849]: A785B308622AB: message-
↪id=<5afa242e.hP5p/mry+fTNNjms%no-reply@example.com>
/var/log/maillog:May 15 02:05:02 mail rspamd[27538]: <8ae27d>; proxy; rspamd_message_
↪parse: loaded message; id: <5afa242e.hP5p/mry+fTNNjms%no-reply@example.com>; queue-
↪id: <A785B308622AB>; size: 2348; checksum: <b1035f4fb07162ba88053d9e38df9c93>
/var/log/maillog:May 15 02:05:03 mail rspamd[27538]: <8ae27d>; proxy; rspamd_task_
↪write_log: id: <5afa242e.hP5p/mry+fTNNjms%no-reply@example.com>, qid:
↪<A785B308622AB>, ip: 10.154.200.17, from: <no-reply@example.com>, (default: F (no␣
↪action): [-0.64/20.00] [BAYES_HAM(-3.00){100.00%;},AUTH_NA(1.00){},MID_CONTAINS_
↪FROM(1.00){},MX_INVALID(0.50){},MIME_GOOD(-0.10){text/plain;},IP_SCORE(-0.04){ip:␣
↪(0.22), ipnet: 10.154.192.0/20(0.18), asn: 14061(0.23), country: US(-0.81);},ASN(0.
↪00){asn:14061, ipnet:10.154.192.0/20, country:US;},DMARC_NA(0.00){example.com;},
↪FROM_EQ_ENVFROM(0.00){},FROM_NO_DN(0.00){},NEURAL_HAM(-0.00){-0.656;0;},RCPT_COUNT_
↪ONE(0.00){1;},RCVD_COUNT_TWO(0.00){2;},RCVD_NO_TLS_LAST(0.00){},R_DKIM_NA(0.00){},R_
↪SPF_NA(0.00){},TO_DN_NONE(0.00){},TO_DOM_EQ_FROM_DOM(0.00){},TO_MATCH_ENVRCPT_ALL(0.
↪00){}]), len: 2348, time: 750.636ms real, 5.680ms virtual, dns req: 47, digest:
↪<b1035f4fb07162ba88053d9e38df9c93>, rcpts: <jsmith@example.com>, mime_rcpts:
↪<jsmith@example.com>
/var/log/maillog:May 15 02:05:03 mail postfix/qmgr[27757]: A785B308622AB: from=<no-
↪reply@example.com>, size=2597, nrcpt=1 (queue active)
/var/log/maillog:May 15 02:05:03 mail postfix/lmtp[25854]: A785B308622AB: to=
↪<vmail+jsmith@mail.mynethserver.org>, orig_to=<jsmith@example.com>, relay=mail.
↪mynethserver.org[/var/run/dovecot/lmtp], delay=0.82, delays=0.8/0.01/0.01/0.01,␣
↪dsn=2.0.0, status=sent (250 2.0.0 <vmail+jsmith@mail.mynethserver.org> gK8pHS8k+lr/
↪ZAAAJc5BcA Saved)
/var/log/maillog:May 15 02:05:03 mail postfix/qmgr[27757]: A785B308622AB: removed
```

[19] https://rspamd.com/doc/workers/rspamd_proxy.html

References

4.3 Webmail

The default webmail client is Roundcube. Roundcube's 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

Note: If NethServer is bound to a remote Active Directory account provider a dedicated user account in AD is required by the module to be fully operational! See *Join an existing Active Directory domain*.

4.3.1 Plugins

Roundcube supports many plugins that are already bundled within the installation.

The plugins that are enabled by default are:

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

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
```

4.3.2 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
```

4.3.3 Removing

If you want remove Roundcube, run the following command on the server command line.

```
yum autoremove nethserver-roundcubemail
```

4.4 WebTop 5

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

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

Note: If NethServer is bound to a remote Active Directory account provider a dedicated user account in AD is required by the module to be fully operational! See *Join an existing Active Directory domain*.

4.4.1 Authentication

Always use the full user name format `<user>@<domain>` for login to the web application and Active Sync.

Example

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

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 using the administrator user. The administrator user can change global settings and login as any other user, however, it's not a system user and can't access any other service like Mail, Calendar, etc.

Default credentials are:

- User: *admin*
- Password: *admin*

The administrator user's password must be changed from within the WebTop interface.

Warning: Remember to change the admin password after installation!

To check the mail of the system's user admin account 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

Change admin password

Access WebTop using the `admin` user, then open user settings by clicking on the menu in the top-right corner.

Go to *Settings* then click on guilabel:*Change password*.

If you want to reset the admin password from command line, use the following commands:

```
curl -s https://git.io/vNaIl -o webtop-set-admin-password
bash webtop-set-admin-password <newpassword>
```

Remember to replace `<newpassword>` with your actual new password, example:

```
bash webtop-set-admin-password VeryInsecurePass
```

4.4.2 Two factor authentication (2FA)

WebTop support two factor authentication. The user can choose between:

- Google Authenticator: the code will be generated using Google Authenticator app (https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid)
- Secondary mail: the access code will be sent to selected mail address

To enable 2FA:

- Click on the menu button on the top-right corner and select the *Settings* icon
- Then select *Security* and click on the *Activate button*.

4.4.3 Synchronization with ActiveSync (EAS)

Mobile devices can be synchronized using ActiveSync. ActiveSync can be used only for **contacts** and **calendars**.

Note: To synchronize **e-mails** you should configure an IMAP account.

Apple iOS

Access your iOS device, navigate to Settings and add an Exchange account following the official guide: https://support.apple.com/en-us/HT201729

Fill the required fields with:

- **E-mail**: add your mail address, eg: goofy@nethserver.org
- **Server**: add your server public name, eg: mail.nethserver.org
- **Domain**: leave blank
- **User name**: enter your full user name, eg: goofy@nethserver.org
- **Password**: enter your password

Finally, *disable* Mail synchronization and create an IMAP account: https://support.apple.com/en-us/HT201320

Note: iOS devices require a valid SSL certificate on the server. See *Server certificate*

Google Android

Access your Android device, navigate to Settings, then select *Add account* -> *Exchange* (or "Company" for older releases).

Fill the required fields with:

- **User name**: enter your full user name, eg: goofy@nethserver.org
- **Password**: enter your password

Then select *Manual configuration* and change the name of the *Server* field accordingly to your server public name. Finally, if you have a self-signed certificate on your server, make sure to select *SSL/TLS (accept all certificates)* option.

Finally, *disable* Mail synchronization and create an IMAP account.

Note: On some Android releases (notably Samsung), the User name and Domain must be entered in the same line. In this case, leave blank the field before the backslash character (), and enter the user name in the following format: `\goofy@nethserver.org`

Multiple calendars and contacts

Calendars and address books shared by others with the user can be synchronized using the ActiveSync protocol.

Shared resources are displayed with the owner's name and category (the number in square brackets is the internal id). Private events are not synchronized.

Mobile devices based on Apple iOS fully support folders / categories for calendar, contacts and activities (called reminders), including original colors.

Mobile devices based on Android support only calendars and contacts (activities are not supported), but using the Google Calendar application all items will have the same colour.

Installing and using the CloudCal application, you can change the colors associated with each calendar, including shared ones.

On Android devices, contacts from shared phone books are merged with the personal phone book and displayed in a single view. Contacts can be modified and changes will be saved it the original source.

Note: In order to receive data via EAS on mobile devices, it is necessary to verify that the shared resources (Calendars and Contacts) have synchronization enabled (Full or Read only):

It is possible to enable or disable the synchronization for each shared resource (calendars and contacts). The user can customize every resource sharing with him by deciding the type of synchronization.

To do so, just right click on the shared resource → Customize → Devices sync.:

The default setting is "Not active".

4.4.4 Synchronization with CalDAV and CardDAV

Calendars and address books can be synchronized also through CalDAV and CardDAV protocols.

To synchronize a calendar, pick up its `URL` link right-clicking on the calendar and selecting *Links to this calendar*, then use it to configure your third-party client.

To synchronize an address book, pick up its `URL` link right-clicking on the address book and selecting *Links to this addressbook*, then use it to configure your third-party client.

To authenticate, provide your credentials in the following form:

- **User name**: enter your full user name (i.e. *goofy@nethserver.org*)
- **Password**: enter your password

Some third-party clients allow to simplify the configuration through the *autodiscovery* feature that automatically discovers the synchronizable resources, as in the case of mobile devices clients (i.e. Android or iOS devices).

Note: If you are using clients that do not support autodiscovery, you need to use the full URL: `https://<server_name>/webtop-dav/server.php`

If you are using clients that support autodiscovery use URL: `https://<server_name>`

Google Android

A good, free, Android third-party client is Opensync.

- install the suggested app from the market;
- add a new account clicking on + key and select *Login with URL and username* method;
- insert the `URL` (`https://<server_name>`), complete username (i.e. *goofy@nethserver.org*) and password;
- click on the new profile and select the resources you want to synchronize.

Apple iOS

CalDAV/CardDAV support is built-in on iOS, so to configure it:

- go to Settings -> Account and Password -> Add account;
- select *Other* -> Add *CalDAV* or *CardDAV* account;
- insert the server name (i.e. *server.nethserver.org*), complete username (i.e. *goofy@nethserver.org*) and password.

By default the syncronization `URL` uses the server principal name (`FQDN`), if you need to change it:

```
config setprop webtop DavServerUrl https://<new_name_server>/webtop-dav/server.php
signal-event nethserver-webtop5-update
```

Desktop clients

Thunderbird

To use CalDAV and CardDAV on Thunderbird you need third-party add-ons like *Cardbook* (for contacts) and *Lightning* (for calendars).

- *Cardbook* add-on works fine, with easy setup and autodiscovery support.
- *Lightning* add-on doesn't support autodiscovery: any calendar must be manually added.

Outlook

- open source *Outlook CalDav Synchronizer* client works fine, supporting both CardDAV and CalDAV.

Note: At the moment CalDAV and CardDAV support **only personal resources synchronization**.

Warning: Webtop is a **clientless groupware**: its functionalities are fully available **only using the web interface**!

The use of CalDAV/CardDAV through third-party clients **cannot be considered a web interface alternative**.

4.4.5 Sharing email folders or the entire account

It is possible to share a single folder or the entire account with all the subfolders included. Select the folder to share -> right click -> "Manage sharing":

- select the user to share the resource (1).
- select if you want to share your identity with the user and possibly even if you force your signature (2).
- choose the level of permissions associated with this share (3).
- if you need to change the permission levels more granularly, select "Advanced" (4).
- finally, choose whether to apply sharing only to the folder from which you started, or only to the branch of subfolders or to the entire account (5).

Note: If you also select "Force signature", when this identity is used, the user signature from which the shared mail was received will be automatically inserted.

In this case, however, it is necessary that the personalized signature of the User from which it originates has been associated to the Email address and not to the User.

4.4.6 Sharing calendars and contacts

Sharing Calendar

You can share each personal calendar individually. Select the calendar to share -> right click -> "Sharing and permissions":

Select the recipient user of the share (or Group) and enable permissions for both the folder and the individual items:

Sharing Contacts

In the same way, you can always share your contacts by selecting the directory you want to share -> right click -> "Sharing and permissions". Select the recipient user of the share (or Group), and enable permissions for both the folder and the individual items.

4.4.7 Mail tags

You can tag each message with different colored labels. Just select a message, right-click and select *Tag*.

You can edit existing tags or add new ones selecting *Manage tags*.

Tags can be used to filter messages using the filter top bar.

4.4.8 Mail inline preview

By default, the mail page will display a preview of the content of latest received messages.

This feature can be enabled or disabled from the *Settings* menu, under the *Mail* tab, the check box is named *Show quick preview on message row*.

4.4.9 Mail archiving

Archiving is useful for keeping your inbox folder organized by manually moving messages.

Note: Mail archiving is not a backup.

The system automatically creates a new special Archives folder

If the *Archives* folder does not appear immediately upon login, it will appear at the first archiving.

There are three archiving criteria in *Settings -> Mail -> Archiving*

- **Single folder:** a single root for all archived emails
- **Per year:** a root for each year
- **By year / month:** a root for each year and month

To maintain the original structure of the folders is possible to activate *Keep folder structure*

The archiving operation is accessible from the contextual menu (right click). Click on *Archive*

The system will process archiving according to the last settings chosen.

4.4.10 Subscription of IMAP folders

On WebTop, by default, all IMAP folders on the server are automatically subscribed and therefore visible since the first login.

If you want to hide from the view some folders, which is equivalent to removing the subscription, you can do so by simply clicking the right mouse button on the folder to hide and select from the interactive menu the item “Hide from the list”.

For example, if you want to hide the subfolder “folder1” from this list, just right-click on it and select “Hide from the list”:

It is possible to manage the visibility of hidden folders by selecting the "Manage visibility" function:

For example, if you want to restore the subscription of the "folder1" just hidden, just select it from the list of hidden folders and click on the icon on the left:

4.4.11 Export events (CSV)

To export calendars events in CSV (Comma Separated Value) format, click on the icon on top right corner.

Finally, select a time interval and click on *Next* to export into a CSV file.

4.4.12 Nextcloud integration

Note: Before proceeding, verify that the "Nextcloud" module has been installed from *Software Center*

By default, Nextcloud integration is disabled for all users. To enable it, use the administration panel which can be accessed using the webtop admin password

For example, if you want to activate the service for all webtop users, proceed as follows:

1. access the administrative panel and select "Groups":

2. modify the properties of the "users" group by double clicking and select the button related to the Authorizations:

3. add to existing authorizations those relating to both the `STORE_CLOUD` and `STORE_OTHER` resources by selecting the items as shown below:

   so get this:

4. save and close.

At this point from any user it will be possible to insert the Nextcloud resource (local or remote) in your personal Cloud.

To do this, simply select the Cloud button and add a new **"Nextcloud"** resource by right clicking on **"My resources"** and then **"Add resource"** in this way:

A precompiled wizard will open:

Note: Remember to fill in the User name and Password fields related to access to the Nextcloud resource, otherwise it will not be possible to use the public link to the shared files

Proceed with the Next button until the Wizard is complete.

4.4.13 Use the personal Cloud to send and receive documents

Cloud module allows you to send and receive documents throug web links.

Note: The server must be reachable in HTTP on port 80

How to create a link to send a document

To create the link, select the button at the top right:

Follow the wizard to generate the link, use field *date* to set the deadline.

you can create a *password* to protect it:

The link will be generated and will be inserted in the new mail:

Downloading the file, generates a notification to the sender:

Request for a document

To create the request, insert the subject of the email than select the button at the top right:

Follow the wizard. You can set both an expiration date and a password. The link will be automatically inserted into the message:

A request email will be sent to upload the document to the Cloud:

The sender will receive a notification for each file that will be uploaded:

To download the files just access your personal *Cloud* → *Uploads* → *Folder* with date and name:

4.4.14 Chat integration

Web chat integration installation is disabled by default for all users.

To enable chat integration:

1. Install "Instant messaging"" module from *Software Center*.
2. Access WebTop as admin user then enable the web chat authorization:
   - Access the *Administration* menu, then *Domains* → *NethServer* → *Groups* → *Users* → *Authorizations*
   - *Add (+)* → *Services* → *com.sonicle.webtop.core (WebTop)* → *Resource* → *WEBCHAT* → *Action* → *ACCESS*
   - Click *OK* then save and close

4.4.15 Audio and video WebRTC calls with chat (Beta)

Warning: This feature is currently released in Beta. When the final version will be released it is likely that the configurations previously made will be reset.

Configuration is currently only possible via the WebTop administration panel. The settings to be inserted are documented here In addition to the WebRTC settings, it is also necessary to add the **XMPP BOSH** public URL as shown here

From web interface by accessing the administration panel -> *Properties (system)* -> *Add* -> select *com.sonicle.webtop.core (WebTop)* and enter the data in the *Key* and *Value* fields according to the key to be configured:

`webrtc.ice.servers` : defines the list of ICE servers as JSON arrays

`xmpp.bosh.url` : specifies the XMPP URL that can be accessed via the BOSH protocol

For the key field `webrtc.ice.servers` as "Value" insert the content in json format that shows the values of these variables:

`url` : URL ice server

`username` : server username (optional)

`credential` : server password (optional)

For example:

```
[
 {
   'url': 'stun:stun.l.google.com:19302'
 }, {
   'url': 'stun:stun.mystunserver.com:19302'
 }, {
   'url': 'turn:myturnserver.com:80?transport=tcp',
   'username': 'my_turn_username',
   'credential': 'my_turn_password'
 }
]
```

For the key field `xmpp.bosh.url` as "Value" enter this type of URL: `https://<public_server_name>/http-bind`

With these configurations, every user authorized to use the **WEBCHAT** service can perform audio and video calls with other users that are available on the same chat server through the buttons available on the chat window.

Note: If the buttons are grayed out, the requirements for activating the call are not satisfied. For example: XMPP BOSH URL unreachable or ICE server unreachable.

4.4.16 Send SMS from contacts

It is possible to send SMS messages to a contact that has the mobile number in the addressbook. To activate sending SMS, first you need to choose one of the two supported providers: SMSHOSTING or TWILIO.

Once registered to the service of the chosen provider, retrieve the API keys (AUTH_KEY and AUTH_SECRET) to be inserted in the WebTop configuration db. The settings to configure are those shown here .

It is possible to do this in two ways:

1. from web interface by accessing the administration panel -> *Properties (system)* -> *Add* -> select *com.sonicle.webtop.core (WebTop)* and enter the data in the *Key* and *Value* fields according to the key to be configured:

`sms.provider` = smshosting or twilio

`sms.provider.webrest.user` = API AUTH_KEY

`sms.provider.webrest.password` = API AUTH_SECRET

`sms.sender` = (default optional)

2. through shell commands:

to configure the `sms.provider` key (smshosting for example):

```
su - postgres -c "psql webtop5 -c \"insert into core.settings (\"service_id\",\"key\",
↪\"value\") values ('com.sonicle.webtop.core','sms.provider','smshosting');\""
```

to configure the `sms.provider.webrest.user` key:

```
su - postgres -c "psql webtop5 -c \"insert into core.settings (\"service_id\",\"key\",
↪\"value\") values ('com.sonicle.webtop.core','sms.provider.webrest.user','API_AUTH_
↪KEY');\""
```

to configure the `sms.provider.webrest.password` key:

```
su - postgres -c "psql webtop5 -c \"insert into core.settings (\"service_id\",\"key\",
↪\"value\") values ('com.sonicle.webtop.core','sms.provider.webrest.password','API␣
↪AUTH_SECRET');\""
```

substituting the key obtained from the provider instead of 'API_AUTH_KEY' and 'API AUTH_SECRET'

The `sms.sender` key is optional and is used to specify the default sender when sending SMS. It is possible to indicate a number (max 16 characters) or a text (max 11 characters).

to configure the `sms.sender` key:

```
su - postgres -c "psql webtop5 -c \"insert into core.settings (\"service_id\",\"key\",
↪\"value\") values ('com.sonicle.webtop.core','sms.sender','XXXXXXXXXX');\""
```

replacing 'XXXXXXXXXX' with the number or text of the default sender.

Note: Each user always has the possibility to overwrite the sender by customizing it as desired through its settings panel: *WebTop -> Switchboard VOIP and SMS -> SMS Hosting service configured -> Default sender*

To send SMS from the addressbook, right-click on a contact that has the mobile field filled in -> *Send SMS*

4.4.17 Custom link buttons in launcher (Beta)

Warning: This feature is currently released in Beta. When the final version will be released it is likely that the configurations previously made will be reset.

Configuration is currently only possible via the WebTop administration panel -> *Properties (system)* -> *Add* -> select *com.sonicle.webtop.core (WebTop)* and enter the data in the *Key* and *Value* fields according to the key to be configured:

`launcher.links` : json array of link objects

In the "Value" field, enter the content in json format that shows the values of these variables:

`href` : URL opened in a new browser tab

`text` : descriptive text that appears with mouseover

`icon` : icon image URL (to avoid scaling problems, use vector images)

For example:

```
[
 {
   'href': 'https://www.google.it/',
   'text': 'Google',
   'icon': 'https://upload.wikimedia.org/wikipedia/commons/5/53/Google_%22G%22_Logo.
↪svg'
 }, {
   'href': 'https://the/url/to/open',
   'text': 'The link text',
   'icon': 'https://the/icon/url'
 }
]
```

Warning: The URL of the icon from which to retrieve the vector image must always be publicly reachable by the browser with which you connect.

If you can not retrieve an Internet link of the icon image, you can copy the image locally on the server in two different ways:

1. copying the file (for example `icon.svg`) directly into the `/var/www/html/` directory of the server and using this type of URL for the 'icon' field of the Json file:

   ```
   'icon': 'https://<public_name_server>/<icon.svg>'
   ```

2. uploading the icon file to the public cloud of WebTop (where images are uploaded for mailcards) via the administration panel -> *Cloud* -> :guilabel:'Public Images'and insert a URL of this type for the 'icon' field of the Json file:

   ```
   'icon': 'https://<public_name_server>/webtop/resources/156c0407/images/<icon.svg>'
   ```

Note: The configured custom link buttons will be shown to all users at the next login.

4.4.18 Browser notifications

With WebTop, the desktop notification mode integrated with the browser was introduced.

To activate it, simply access the general settings of your user:

_static/webtop-desktop_notifications.png

It is possible to enable desktop notification in two modes:

- **Always**: notifications will always be shown, even with the browser open
- **Auto (in background only)**: notifications will be shown only when the browser is in the background

Once the mode is selected, a browser consent request will appear at the top left:

_static/webtop-chrome_notifications.png

If you need to enable this consent later on a different browser just click on the appropriate button:

_static/webtop-button_desktop_notifications.png

4.4.19 Mailcards of user and domain

One of the main features of managing signatures on WebTop is the opportunity to integrate images or custom fields profiled per user.

To use the images you need to upload them to the public cloud through the WebTop admin user like this:

You can use the *Upload* button to load an image which is at the bottom or simply via a drag & drop.

Note: Remember that the public images inserted in the signature are actually connected with a public link. To be visible to email recipients, the server must be reachable remotely on port 80 (http) and its FQDN name must be publicly resolvable.

To change your signature, each user can access the *Settings* → *Mail* → *Editing* → *Edit User mailcard*:

The public image just uploaded will be able to recall it in the HTML editor of the mailcard with this button:

Note: The personal mailcard can be associated with the user or his email: by associating it by email it will also be possible to share the mailcard to other users with whom the identity is shared.

Through the webtop5_impersonate-section you can also set a general domain mailcard that will be automatically set for all users who have not configured their personal mailcard:

Furthermore, it will also be possible to modify personal information:

that can be used within the parameterized fields within the domain mailcard editor:

In this way it is possible to create a single mailcard that will be automatically customized for every user who does not use his own mailcard.

4.4.20 Configure multiple mailcards for a single user

It is possible to configure multiple mailcards (HTML signatures) for each individual user.

Access the *Settings* → *Mail* → *Identities* and create multiple identities:

To edit every single signature select *Settings* → *Mail* → *Identities* then select each individual signature and click on the *edit mailcard* button

When finished, close the window and click YES:

to use multiple mailcards, create a new email, and choose the signature:

_static/webtop-sig_sig5.png

4.4.21 Manage identities

In *settings* → *mail* → *identities* click *Add* and fill in the fields

_static/webtop_manageident1.png

It is possible to associate the new identity with a folder in your account or of a shared account

Local account:

_static/webtop_manageident2.png

Shared account:

_static/webtop_manageident3.png

Otherwise the sent mails will always end up in the "Sent Items" folder of your personal account.

4.4.22 Subscribing remote resources

WebTop supports subscription to remote calendars and contacts (directory) using cardDAV, calDav and iCal.

Remote calendars

An Internet Calendar can be added and synchronized. To do so just click the right button on personal calendars, *Add Internet Calendar*. Two types of remote calendars are supported: Webcal (ics format) and CalDAV.

Note: Synchronization of Webcal calendars (ics) is always done by downloading every event on the remote resource every time, while only the differences are synchronized with the CalDAV mode

---

Example of Google Cal remote calendar (Webcal only - ICS)

1. Take the public access ICS link from your Google calendar: *Calendar options -> Settings and sharing -> Secret address in iCal format*
2. On WebTop, add an Internet calendar of type Webcal and paste the copied URL without entering the authentication credentials in step 1 of the wizard.
3. The wizard will connect to the calendar, giving the possibility to change the name and color, and then perform the first synchronization.

Note: The first synchronization may fail due to Google's security settings. If you receive a notification that warns you about accessing your resources you need to allow them to be used confirming that it is a legitimate attempt.

Remote contacts (directory)

Example of Google CardDAV remote address book

1) On Webtop, configure a new Internet address book, right-click on *Personal Categories -> Add Internet address book* and enter a URL of this type in step 1 of the wizard: https://www.googleapis.com/carddav/v1/principals/XXXXXXXXXX@gmail.XXX/lists/default/ (replace the X your gmail account)

2. Enter the authentication credentials (as user name use the full address of gmail):

_static/webtop-remote_phonebook.png

3. The wizard in the following steps will connect to the phonebook, giving the possibility to change the name and color, and then perform the first synchronization.

Note: To be able to complete the synchronization it is necessary to enable on your account Google, in the security settings, the use of apps considered less secure (here a guide on how to do: https://support.google.com/accounts/answer/6010255?hl=it).

Synchronization of remote resources can be performed manually or automatically.

Automatic synchronization

To synchronize automatically you can choose between three time intervals: 15, 30 and 60 minutes. The choice of the time interval can be made in the creation phase or later by changing the options. To do this, right-click on the phonebook (or on the calendar), *Edit Category*, *Internet Addressbook* (or *Internet Calendar*):

_static/webtop-sync_automatic.png

Manual synchronization

To update a remote address book, for example, click on it with the right mouse button and then select the item "Synchronize":

For CardDav address books, as well as for remote CalDAV calendars, you can select whether to perform a full synchronization or only for changes. To do this, right-click on the phonebook (or on the calendar), *Edit Category*:

Select the desired mode next to the synchronization button:

4.4.23 User settings management

Most user settings can be directly managed by the user itself via the settings menu. Locked settings require administration privileges.

The administrator can impersonate users, to check the correctness and functionalities of the account, through a specific login:

- **User name**: admin!<username>
- **Password**: <WebTop admin password>

While impersonating you receive similar user privileges, allowing you to control exactly what the user can see. Full administration of user settings is available directly in the administration interface, by right clicking on a user: the settings menu will open the full user settings panel, with all options unlocked.

It is also possible to make a massive change of the email domain of the selected users: select the users (Click + CTRL for multiple selection) to which you want to apply this change then right-click on *Bulk update email domain*.

4.4.24 SMTP setting

The default configuration for sending mail to the SMTP server is anonymous and without encryption on port 587. It is possible to enable authenticated sending in this way:

```
config setprop webtop SmtpAuth enabled
```

to enable encryption also:

```
config setprop webtop SmtpStarttls enabled
```

To apply the new settings launch this event which will also restart the application:

```
signal-event nethserver-webtop5-update
```

4.4.25 Changing the logo

To modify and customize the initial logo that appears on the login page of WebTop, you must upload the custom image file on the public images of the admin user and rename it with "login.png".

Proceed as follows:

1. log in with the WebTop user admin
2. select the cloud service and public images:

3. upload the image (via the Upload button at the bottom left or simply dragging with a drag & drop)
4. rename the loaded image so that its name is **"login.png"** (use right click -> Rename):

5. the next login will show the new logo on the login page

4.4.26 Change the public URL

By default, the public WebTop URL is configured with the FQDN name set in the server-manager.

If you want to change URL from this: `http://server.domain.local/webtop` to: `http://mail.publicdomain.com/webtop`

execute these commands

```
config setprop webtop PublicUrl http://mail.publicdomain.com/webtop
signal-event nethserver-webtop5-update
```

4.4.27 Change default limit "Maximum file size"

There are hard-coded configured limits related to the maximum file size:

- Maximum file size for chat uploads (internal default = 10 MB)
- Maximum file size single message attachment (internal default = 10 MB)
- Maximum file size for cloud internal uploads (internal default = 500 MB)
- Maximum file size for cloud public uploads (internal default = 100 MB)

To change these default values for all users, the following keys can be added via the admin interface: *Properties (system) -> Add*

Maximum file size for chat uploads

- Service: `com.sonicle.webtop.core`
- Key: `im.upload.maxfilesize`

Maximum file size for single message attachment

- Service: `com.sonicle.webtop.mail`
- Key: `attachment.maxfilesize`

Maximum file size for cloud internal uploads

- Service: `com.sonicle.webtop.vfs`
- Key: `upload.private.maxfilesize`

Maximum file size for cloud public uploads

- Service: `com.sonicle.webtop.vfs`
- Key: `upload.public.maxfilesize`

Note: The value must be expressed in Bytes (Example 10MB = 10485760)

4.4.28 Importing contacts and calendars

WebTop supports importing contacts and calendars from various file formats.

Contacts

Supported contacts format:

- CSV - Comma Separated values (*.txt, *.csv)
- Excel (.*xls, *.xlsx)
- VCard (*.vcf, *.vcard)
- LDIF (*.ldif)

To import contacts:

1. Right click on the target phone book, then select *Import contacts*

2. Select the import format and make sure that fields on the file match the ones available on WebTop

If you are importing a phone book exported from Outlook, make sure to set *Text qualifier* to `"` value.

Calendars

Supported calendar format: iCalendar (*.ics, *.ical, *.icalendar)

To import events:

1. Right click on the target calendar, then select *Import events*

2. Select the import format

3. Then choose if you want to delete all existings events and import new ones, or just append imported data to existing calendar events

4.4.29 Importing from Outlook PST

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

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

```
yum install libpst -y
```

Also make sure the PHP timezone corresponds to the server timezone:

```
config getprop php DateTimezone
```

PHP time zone can be updated using the following command:

```
config setprop php DateTimezone Europe/Rome
signal-event nethserver-php-update
```

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>
```

Example:

```
# /usr/share/webtop/doc/pst2webtop.sh data.pst goofy
Do you wish to import email? [Y]es/[N]o:
```

All mail messages will be imported. Contacts and calendars will be saved inside a temporary file and the script will output further commands to import contacts and calendars.

Example:

```
Events Folder found: Outlook/Calendar/calendar
pst2webtop_cal.php goody '/tmp/tmp.Szorhi5nUJ/Outlook/Calendar/calendar' <foldername>

...

log created: /tmp/pst2webtop14271.log
```

All commands are saved also in the reported log.

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: Personal folders/Contacts/contacts
 Import to webtop:
./pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/Contacts/contacts'
↪<foldername>
```

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

```
/usr/share/webtop/doc/pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/
↪Contacts/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: Personal folders/Calendar/calendar
 Import to webtop:
./pst2webtop_cal.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/Calendar/calendar'
↪<foldername>
```

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

```
/usr/share/webtop/doc/pst2webtop_cal.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/
↪Calendar/calendar' WebTop
```

Known limitations:

- only the first occurrence of recurrent events will be imported
- Outlook reminders will be ignored

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

4.4.30 Troubleshooting

After login a "mail account authentication error" is displayed

If an entire mail account is shared among different users, a Dovecot connection limit can be reached. This is the displayed error:

In `/var/log/imap` there are lines like the following:

```
xxxxxx dovecot: imap-login: Maximum number of connections from user+IP exceeded (mail_
↪max_userip_connections=12): user=<mail@dominio.com>, method=PLAIN, rip=127.0.0.1,␣
↪lip=127.0.0.1, secured, session=<zz/8iz1M1AB/AAAB>
```

To list active IMAP connections per user, execute:

```
doveadm who
```

To fix the problem, just raise the limit (eg. 50 connections for each user/IP):

```
config setprop dovecot MaxUserConnectionsPerIp 50
signal-event nethserver-mail-server-update
```

At the end, logout and login again in WebTop.

Blank page after login

You can access WebTop using system admin user (NethServer Administrator) using the full login name, eg: `admin@nethserver.org`.

If the login fails, mostly when upgrading from WebTop 4, it means that the admin user doesn't have a mail address.

To fix the problem, execute the following command:

```
curl -s https://git.io/vNuPf | bash -x
```

Synchronized events have different time

Sometimes calendar events created on mobile devices and synchronized via EAS, are shown with a wrong time, for example with a difference of 1 or 2 hours.

The problem is due to the PHP time zone which can be different from the system time zone.

With this command you can see the current time zone set for PHP:

```
config getprop php DateTimezone
```

Output example:

```
# config getprop php DateTimezone
UTC
```

If the Time Zone is not the desired one, you can changed it using these commands:

```
config setprop php DateTimezone "Europe/Rome"
signal-event nethserver-php-update
```

To apply the changes, execute:

```
signal-event nethserver-httpd-update
signal-event nethserver-webtop5-update
```

List of PHP supported time zones: http://php.net/manual/it/timezones.php

Delete automatically suggested email addresses

When compiling the recipient of a mail, some automatically saved email addresses are suggested. If you need to delete someone because it is wrong, move with the arrow keys until you select the one you want to delete (without clicking on it), then delete it with *Shift* + *Canc*

4.4.31 WebTop vs SOGo

WebTop and SOGo can be installed on the same machine, although it is discouraged to keep such setup on the long run.

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-webtop5-update
```

All incoming mail filters configured within SOGo, must be manually recreated inside WebTop interface. This also applies if the user is switching from WebTop to SOGo.

4.4.32 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 the shell, access webtop database:

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

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

```
UPDATE core.settings SET value = '__value__' WHERE service_id = 'com.sonicle.webtop.
↪core' AND key = 'googledrive.clientid';
UPDATE core.settings SET value = '__value__' WHERE service_id = 'com.sonicle.webtop.
↪core' AND key = 'googledrive.clientsecret';
```

(continues on next page)

(continued from previous page)

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:

```
UPDATE core.settings SET value = '__value__' WHERE service_id = 'com.sonicle.webtop.
↪core' AND key = 'dropbox.appkey';
UPDATE core.settings SET value = '__value__' WHERE service_id = 'com.sonicle.webtop.
↪core' AND key = 'dropbox.appsecret';
```

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

4.5 POP3 proxy

Note: Since NethServer 7.5.1804 new *Email*, *POP3 connector* and *POP3 proxy* installations are based on the Rspamd filter engine. Previous NethServer installations are automatically upgraded to Rspamd as described in *Email module transition to Rspamd*

A user on the LAN can configure an email client in order to connect to an external POP3 server and download mail messages. Please note that 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 will believe that they are connected 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 the 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

4.5.1 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 and will have to turn off encryption.

4.6 POP3 connector

Note: Since NethServer 7.5.1804 new *Email*, *POP3 connector* and *POP3 proxy* installations are based on the Rspamd filter engine. Previous NethServer installations are automatically upgraded to Rspamd as described in *Email module transition to Rspamd*

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

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

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

- the email address (as unique account identifier)
- the protocol (IMAP/POP3/IMAP with SSL/POP3 with SSL)
- the remote server address
- the account credentials
- the local user account where to deliver messages
- if a message has to be deleted from the remote server after delivery
- anti-spam and anti-virus checks

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

After the account configuration has been completed, the account is automatically checked for new mail.

The underneath implementation is based on *Getmail*[1]. After fetching mail messages from the POP3/IMAP provider Getmail applies all required filters (SPAM and virus) prior to delivering the mail locally. All messages are filtered according to the *configured rules*.

All operations are logged in `/var/log/maillog`.

Warning: If an account was selected for delivery and has been subsequently deleted the configuration becomes inconsistent. If this should happen then existing account configuration in *POP3 connector* page must be disabled or deleted.

References

4.7 Chat

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

The main features are:

- Messaging between users of the system

[1] Getmail is a remote-mail retrieval utility http://pyropus.ca/software/getmail/

- Chat server administration
- Broadcast messages
- Group chat
- Offline messages
- Transfer files over LAN
- S2S
- Message archiving

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

Note: If NethServer is bound to a remote Active Directory account provider a dedicated user account in AD is required by the module to be fully operational! See *Join an existing Active Directory domain*.

4.7.1 Server to server (S2S)

The XMPP system is federated by nature. If S2S is enabled, users with accounts on one server can communicate with users on remote servers. S2S allows for servers communicating seamlessly with each other, forming a global 'federated' IM network.

For this purpose, the SRV DNS record must be configured for your domain (https://wiki.xmpp.org/web/SRV_Records#XMPP_SRV_records) and the server must have a valid SSL/TLS certificate.

4.7.2 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.

With TLS capabilities, strictly configured servers or clients could reject connections with your Ejabberd server if the SSL/TLS certificate doesn't match the domain name. Also, the certificate should contain two sub-domains `pubsub.*` and `conference.*`. This certificate can be obtained for free with Let's Encrypt (see *Server certificate*).

4.7.3 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.

4.7.4 Message Archive Management

Message Archive Management (mod_mam) implements Message Archive Management as described in XEP-0313. When enabled, all messages will be stored inside the server and compatible XMPP clients can use it to store their chat history on the server.

The database can store a maximum of 2GB of messages, archived messages can be purged automatically. To configure message retention policy, set *Clean messages older than X days* option.

Note: If enabled, this module will store every message sent between users. This behavior will affect the privacy of your users.

4.8 Team chat (Mattermost)

The team chat module installs Mattermost Team Edition platform inside NethServer.

Mattermost is an Open Source, private cloud Slack-alternative. Check out the excellent official documentation: https://docs.mattermost.com/.

4.8.1 Configuration

Mattermost installation needs a dedicated virtual host, an FQDN like `chat.nethserver.org`.

Before proceeding with the configuration, make sure to create the corresponding DNS record. If NethServer act as the DNS server of your LAN, please refer to *DNS*.

If your server is using a Let's Encrypt certificate as default, make also sure to have a corresponding public DNS record. See *Server certificate* for more info.

How to configure:

1. Access *Team chat* page inside the Server Manager
2. Check *Enable Mattermost Team Edition*, then enter a valid FQDN inside *Virtual host name* field (eg. `chat.nethserver.org`)
3. Open the entered host name inside the browser, eg: `https://chat.nethserver.org`. At first access, a wizard will create the administrator user

The following features are enabled by default:

- mail notifications
- push notifications for mobile apps
- redirect from HTTP to HTTPS

4.8.2 Authentication

Mattermost authentication is *not* integrated with any Account Provider. The Mattermost administrator should take care of users and teams creation.

Note: The administrator should always use Mattermost wizard to create the admin user, then send team invitation link to each user.

Importing users

If the system administrator still needs bulk user creation, he/she can rely on `mattermost-bulk-user-create` command.

The command will:

- create a default team named as the Company from *Organization contacts*
- read all users from local or remote Account Providers and create them inside Mattermost

Please note that:

- users disabled in the Server Manager or already existing in Mattermost will be skipped
- a random password will be generated for each user
- the first imported user will be set as administrator if no admin has been already created

Invocation example:

```
mattermost-bulk-user-create

...
Creating default team: example (Example Org) ... OK
Skipping locked user: 'goofy'
Skipping locked user: 'admin'
Creating user: 'pluto' with password '6aW221o7' ... OK
...
```

Note: Users are not automatically synced inside Mattermost. Each time a user is created or removed, remember to execute `mattermost-bulk-user-create` command or manually create the user using Mattermost administration web interface.

Forcing a common default password

It's possible to set a default password for each new Mattermost user, just append the default password to command invocation.

Example:

```
mattermost-bulk-user-create Password,1234
```

4.9 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 center* 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.

4.9.1 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
```

4.9.2 UPS statistics

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

4.10 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

4.10.1 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.

4.10.2 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*. The *faxmaster* group must be explicitly created.

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

4.10.3 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 "Numero Fax:", containing the fax number, for example:

```
Numero Fax: 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.

4.10.4 Mail2Fax

Warning: To enable this function, make sure that `Email` module is installed.

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 mails from the green network.

4.10.5 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

4.11 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)
- Deep packet inspection (DPI)

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

4.11.1 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.

4.11.2 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
- Source
- Destination
- Service
- Time condition

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*.
- *Hi-Prio*: mark the traffic as high priority. See *Traffic shaping*.
- *Low-Prio*: mark the traffic as low priority. See *Traffic shaping*.

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.

Deep Packet Inspection (DPI)

The Deep Packet Inspection (DPI)[1] is an advanced packet filtering technique.

When the DPI module is active, new items for the *Service* field are available in the *Edit rule* form. Those items are labeled *DPI protocol*, among the usual *network service* and *service object* items.

The complete list of available DPI protocols can be obtained from the Dashboard or with the following command:

```
db NethServer::Database::Ndpi keys
```

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: -

[1] Deep Packet Inspection https://en.wikipedia.org/wiki/Deep_packet_inspection

4.11.3 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 correctly fill *Link weight*, *Inbound bandwidth* and *Outbound bandwidth* fields from the *Network* 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.

4.11.4 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 possible to specify a port range using a colon as separator in the source port field (eg: 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 between 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 between 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 between 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

4.11.5 sNAT 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.

This feature only applies to traffic from the network specific host to internet.

It doesn't affect in any way the traffic from internet toward the Alias IP, if you need to route some specific traffic to the internal host use the port forward as usual.

If you need to route all traffic to the internal host (not recommended!) use a port forward with protocol TCP & UDP and source port 1:65535.

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.

4.11.6 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 exact amount of available download and upload bandwidth. Access the *Network* page and carefully set bandwidth values.

If download and upload bandwidth are not set for a red interface, traffic shaping rules will not be enabled for that interface.

Note: Be sure to specify an accurate estimate of the bandwidth on network interfaces. To pick an appropriate setting, please do not trust the nominal value, but use online tools to test the real provider speed.

In case of congestion by the provider, there is nothing to do in order to improve performance.

Configuration of traffic shaping is composed by 2 steps:

- creation of traffic shaping classes
- assignment of network traffic to a specific class

Classes

Traffic shaping is achieved by controlling how bandwidth is allocated to classes.

Each class can have a reserved rate. A reserved rate is the bandwidth a class will get only when it needs it. The spare bandwidth is the sum of not commited bandwidth, plus the committed bandwidth of a class but not currently used by the class itself.

Each class can have also a maximum rate. If set, the class can exceed its committed rate, up to the maximum rate. A class will exceed its committed rate only if there is spare bandwidth available.

Traffic shaping classes can be defined under *Traffic shaping* page. When creating a new class, fill the following fields:

- *Class name*: a representative name
- *Min download (%)*: minimum reserved download bandwidth, if empty no download reservation will be created
- *Max download (%)*: maximum allowed download bandwidth, if empty no upper limit will be set
- *Min upload (%)*: minimum reserved upload bandwidth, if empty no upload reservation will be created
- *Max upload (%)*: maximum allowed download bandwidth, if empty no upper limit will be created
- *Description*: optional description for the class

The system provides two pre-configured classes:

- *high*: generic high priority traffic, can be assigned to something like SSH
- *low*: low priority traffic, can be assigned to something like peer to peer file exchange

The system always tries to prevent traffic starvation under high network load.

Classes will get spare bandwidth proportionally to their committed rate. So if class A has 1Mbit committed rate and class B has 2Mbit committed rate, class B will get twice the spare bandwidth of class A. In all cases all spare bandwidth will be given to them.

For more info, see[2] .

4.11.7 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.

- Time conditions: can be associated to firewall rules to limit their effectiveness to a given period of time.

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

[2] FireQOS tutorial: https://github.com/firehol/firehol/wiki/FireQOS-Tutorial

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.

Note: Rules which have time conditions are enforced only for new connections. Example: if you are blocking HTTP connections from 09:00 to 18:00, connections established before 09:00 will be allowed until closed. Any new connection after 09:00 will be dropped.

4.11.8 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.

4.12 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

4.12.1 Authenticated mode

Before enabling the web proxy in authenticated mode, please make sure to configure a local or remote account provider.

When Samba Active Directory is installed, or the server is joined to a remote Active Directory, Windows machines can use integrated authentication with Kerberos. All Windows clients **must** access the proxy server using the FQDN.

All other clients can use basic authentication mechanism.

Note: NTLM authentications is deprecated and it's not supported.

4.12.2 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.

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.

4.12.3 SSL Proxy

In transparent SSL mode, the proxy implements the so-called "peek and splice" behavior: it establishes the SSL connection with remote sites and checks the validity of certificates without decrypting the traffic. Then the server can filter requested URLs using the web filter and return back the response to the client.

Note: There is no need to install any certificate into the clients, just enabling the SSL proxy is enough.

4.12.4 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 domains
- bypass by source
- bypass by destination

Bypass by domains

Bypass by domains can be configured from *Domains without proxy* section. All domains listed inside this page can be directly accessed from LAN clients. No antivirus or content filtering is applied to these domains.

Every domain listed will be expanded also for its own sub-domains. For example, adding *nethserver.org* will bypass also *www.nethserver.org*, *mirror.nethserver.org*, etc.

Note: All LAN clients must use the server itself as DNS, either directly or as a forwarder.

Bypass by source and destinations

A source bypass allows direct access to any HTTP/HTTPS sites from selected hosts, host groups, IP ranges and network CIDR. Source bypasses are configurable from *Hosts without proxy* section.

A destination bypass allows direct access from any LAN clients to HTTP/HTTPS sites hosted on specific hosts, host groups or network CIDR. Destination bypasses are configurable from *Sites without proxy* section.

These bypass rules are also configured inside the WPAD file.

4.12.5 Priority and divert rules

Firewall rules for routing traffic to a specific provider, or decrease/increase priority, are applied only to network traffic which traverse the gateway. These rules don't apply if the traffic goes through the proxy because the traffic is generated from the gateway itself.

In a scenario where the web proxy is enabled in transparent mode and the firewall contains a rule to lower the priority for a given host, the rule applies only to non-HTTP services like SSH.

The *Rules* tab allows the creation of priority and divert rules also for the traffic intercepted by the proxy.

The web interface allow the creation of rules for HTTP/S traffic to:

- raise the priority of an host or network
- lower the priority of an host or network
- divert the source to a specific provider with automatic fail over if the provider fails
- force the source to a specific provider without automatic fail over

4.12.6 Report

Install `nethserver-lightsquid` package to generate web proxy stats.

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. Lightsquid web interface can be found at the *Applications* tab inside the *Dashboard*.

4.12.7 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 free 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
```

4.12.8 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 Antivirus

Web browsing can be checked for malicious content, but only for clear text HTTP protocol. If the proxy is configured in SSL transparent mode (*SSL Proxy*), content downloaded via HTTPS will not be scanned.

4.13.3 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 IPS (Suricata)

Suricata is a *IPS* (Intrusion Prevention System), a system for the network intrusion analysis. The software analyzes all traffic on 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 (`/var/log/suricata/fast.log`).

Suricata can be configured using sets of rules organized in uniform categories. Each category can be set to:

- Enable: traffic matching rules from this categories will be reported
- Block: traffic matching rules from this categories will be dropped

- Disable: rules from this categories are ignored

Note: The use of an IPS impacts on all traffic passing on the firewall. Make sure you fully understand all the implications before enabling it. In particular, pay attention to blocking rules that may stop updates to the system itself.

4.14.1 Rule categories

Suricata is configured to use free rules from https://rules.emergingthreats.net/.[1]

Rules are divided into categories listed below.

Activex Attacks and vulnerabilities(CVE, etc.) regarding ActiveX.

Attack Response Responses indicative of intrusion—LMHost file download, certain banners, Metasploit Meterpreter kill command detected, etc. These are designed to catch the results of a successful attack. Things like "id=root", or error messages that indicate a compromise may have happened.

Botcc (Bot Command and Control) These are autogenerated from several sources of known and confirmed active Botnet and other Command and Control hosts. Updated daily, primary data source is Shadowserver.org. Bot command and control block rules generated from shadowserver.org, as well as spyeyetracker, palevotracker, and zeustracker. Port grouped rules offer higher fidelity with destination port modified in rule.

Botcc Portgrouped Same as above, but grouped by destination port.

Chat Identification of traffic related to numerous chat clients, irc, and possible check-in activity.

CIArmy Collective Intelligence generated IP rules for blocking based upon www.cinsscore.com.

Compromised This is a list of known compromised hosts, confirmed and updated daily as well. This set varied from a hundred to several hunderd rules depending on the data sources. This is a compilation of several private but highly reliable data sources. Warming: Snort does not handle IP matches well load-wise. If your sensor is already pushed to the limits this set will add significant load. We recommend staying with just the botcc rules in a high load case.

Current Events Category for active and short lived campaigns. This category covers exploit kits and malware that will be aged and removed quickly due to the short lived nature of the threat. High profile items that we don't expect to be there long—fraud campaigns related to disasters for instance. These are rules that we don't intend to keep in the ruleset for long, or that need to be tested before they are considered for inclusion. Most often these will be simple sigs for the Storm binary URL of the day, sigs to catch CLSID's of newly found vulnerable apps where we don't have any detail on the exploit, etc.

Decoder-events Suricata specific. These rules log normalization events related to decoding.

Deleted Rules removed from the rule set.

DNS Rules for attacks and vulnerabilities regarding DNS. Also category for abuse of the service for things such as tunneling.

DOS Denial of Service attempt detection. Intended to catch inbound DOS activity, and outbound indications.

Drop Rules to block spamhaus "drop" listed networks. IP based. This is a daily updated list of the Spamhaus DROP (Don't Route or Peer) list. Primarily known professional spammers. More info at http://www.spamhaus.org.

Dshield IP based rules for Dshield Identified attackers. Daily updated list of the DShield top attackers list. Also very reliable. More information can be found at http://www.dshield.org.

[1] Categories documentation source: proofpoint - ETPro Category Descriptions

Exploit Exploits that are not covered in specific service category. Rules to detect direct exploits. Generally if you're looking for a windows exploit, Veritas, etc, they'll be here. Things like SQL injection and the like, whie they are exploits, have their own category.

Files Example rules for using the file handling and extraction functionality in Suricata.

FTP Rules for attacks, exploits, and vulnerabilities regarding FTP. Also includes basic none malicious FTP activity for logging purposes, such as login, etc.

Games Rules for the Identification of gaming traffic and attacks against those games. World of Warcraft, Starcraft, and other popular online games have sigs here. We don't intend to label these things evil, just that they're not appropriate for all environments.

HTTP-Events Rules to log HTTP protocol specific events, typically normal operation.

Info General rules to track suspicious host network traffic.

Inappropriate Rules for the identification of pornography related activity. Includes Porn, Kiddy porn, sites you shouldn't visit at work, etc. Warning: These are generally quite Regex heavy and thus high load and frequent false positives. Only run these if you're really interested.

Malware Malware and Spyware related, no clear criminal intent. The threshold for inclusion in this set is typically some form of tracking that stops short of obvious criminal activity. This set was originally intended to be just spyware. That's enough to several rule categories really. The line between spyware and outright malicious bad stuff has blurred to much since we originally started this set. There is more than just spyware in here, but rest assured nothing in here is something you want running on your net or PC. There are URL hooks for known update schemed, User-Agent strings of known malware, and a load of others.

Misc. Miscellaneous rules for those rules not covered in other categories.

Mobile Malware Specific to mobile platforms: Malware and Spyware related, no clear criminal intent.

Netbios Rules for the identification, as well as attacks, exploits and vulnerabilities regarding Netbios. Also included are rules detecting basic activity of the protocol for logging purposes.

P2P Rules for the identification of Peer-to-Peer traffic and attacks against. Including torrents, edonkey, Bittorrent, Gnutella, Limewire, etc. We're not labeling these things malicious, just not appropriate for all networks and environments.

Policy Application Identification category. Includes signatures for applications like DropBox and Google Apps, etc. Also covers off port protocols, basic DLP such as credit card numbers and social security numbers. Included in this set are rules for things that are often disallowed by company or organizational policy. Myspace, Ebay, etc.

SCADA Signatures for SCADA attacks, exploits and vulnerabilities, as well as protocol detection.

SCAN Things to detect reconnaissance and probing. Nessus, Nikto, portscanning, etc. Early warning stuff.

Shellcode Remote Shellcode detection. Remote shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections to allow the attacker access to the shell on the target machine. Such shellcode can be categorised based on how this connection is set up: if the shellcode can establish this connection, it is called a "reverse shell" or a connect-back shellcode because the shellcode connects back to the attacker's machine.

SMTP Rules for attacks, exploits, and vulnerabilities regarding SMTP. Also included are rules detecting basic activity of the protocol for logging purposes.

SMTP-events Rules that will log SMTP operations.

SNMP Rules for attacks, exploits, and vulnerabilities regarding SNMP. Also included are rules detecting basic activity of the protocol for logging purposes.

SQL Rules for attacks, exploits, and vulnerabilities regarding SQL. Also included are rules detecting basic activity of the protocol for logging purposes.

Stream-events Rules for matching TCP stream engine events.

TELNET Rules for attacks and vulnerabilities regarding the TELNET service. Also included are rules detecting basic activity of the protocol for logging purposes.

TFTP Rules for attacks and vulnerabilities regarding the TFTP service. Also included are rules detecting basic activity of the protocol for logging purposes.

TLS-Events Rules for matching on TLS events and anomal

TOR IP Based rules for the identification of traffic to and from TOR exit nodes.

Trojan Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and whatever else we can detect on the wire. This is also a highly important ruleset to run if you have to choose.

User Agents User agent identification and detection.

VOIP Rules for attacks and vulnerabilities regarding the VOIP environment. SIP, h.323, RTP, etc.

Web Client Web client side attacks and vulnerabilities.

Web Server Rules for attacks and vulnerabilities against web servers.

Web Specific Apps Rules for very specific web applications.

WORM Traffic indicative of network based worm activity.

4.14.2 EveBox

EveBox is a web based alert and event management tool for events generated by the Suricata.

It can be accessed from the Server Manager under the *Applications* page.

4.15 Reverse proxy

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

4.15.1 Path and virtual host rules

A web client request can be forwarded to another web server transparently, according to two types of matching rules:

- Requests matching an URL path, like `http://mydomain.com/mysite`
- Requests matching a virtual host name, like `http://my.secondary-domain.com`

The typical scenario for a **URL path rule** is the following:

- 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)

In this scenario, create a new record under *Reverse proxy* > *Paths* page. Set the *Name* of the item to `mysite` and the *Target URL* to `http://192.168.2.100`.

If only encrypted connections are allowed, enable the *Require SSL encrypted connection*.

Only clients from certain networks can be allowed to connect, by specifying a comma-separated list of CIDR networks under the *Access from CIDR networks* field.

A **virtual host name rule** can be forward HTTP requests to another web server, and is defined in the *Reverse proxy* > *Virtual hosts* page. For instance:

- NethServer is the firewall of your LAN
- You have a domain `http://my.secondary-domain.com`
- You would like `http://my.secondary-domain.com` to be forwarded to the internal web server `192.168.2.101`, port 9000.

In this scenario, set the *Name* of a new virtual host item to `my.secondary-domain.com` and the *Target URL* to `http://192.168.2.101:9000`.

Refer also to *the UI description of Reverse Proxy* for additional information about advanced features, like *Forward HTTP "Host" header to target* and :guilabel'Accept invalid SSL certificate from target'.

4.15.2 Manual configuration

If *Reverse proxy* page is not enough, you can always configure Apache manually, 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: https://httpd.apache.org/docs/2.4/mod/mod_proxy.html

4.16 Virtual hosts

Virtual hosting allows to host multiple domain names on a single server. On NethServer, from *Virtual hosts* page, is possible to configure web sites as Apache named virtual hosts.

4.16.1 Virtual host names (FQDN)

Is the list of Fully Qualified Domain Names that are associated to the virtual host. Values must be separated with a "," (comma). To access virtual host, is also needed a DNS record. If enabled under "Additional actions" an alias for the server is automatically created on "DNS > Server alias", but it's useful only for clients that use the server as DNS.

4.16.2 Configuring a web application

When a new virtual host is created, also the folder /var/lib/nethserver/vhost/*NAME* is created. If FTP access is enabled, is possible to upload files to this folder using an FTP client and, virtual host name as username.

Warning: FTP access is disabled by default, you also need to enable it from FTP configuration page

HTTP authentication password should be different from FTP ones, because FTP is used for upload content on virtual host and HTTP to read content.

4.16.3 Apache permissions

FTP uploaded files are owned by the "apache" group. If you need to allow apache write or execution access, you can change group permissions using the FTP client

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

4.17 Shared folders

A *shared folder* is a place where files can be accessed by a group of people using Samba (SMB/CIFS).

To create, edit and delete a shared folder go to the *Shared folders* page.

4.17.1 Requirements

Shared folders use ACL (Access Control List) to provide flexible permission on files and directories.

To enable ACL, the filesystem must be mounted with the `acl` option. The `acl` option is already enabled on `XFS`, the default CentOS filesystem, and usually even on `Ext3` and `Ext4` filesystems.

Enabling ACL

On Ext2/3/4 filesystems, use `tune2fs` command to check if `acl` option is already enabled:

```
tune2fs -l /dev/sdXY | grep "Default mount options:"
```

Where `sdXY` is the name of your partition, the output should look like this:

```
Default mount options:    user_xattr acl
```

If the `acl` option is not enabled, add the option inside the `/etc/fstab`:

```
/dev/mapper/VolGroup-lv_root /                       ext4     defaults,acl        0
```

Or use `tune2fs` to enable as default mount option:

```
tune2fs -o acl /dev/sdXY
```

4.17.2 Authorizations

If **Active directory** is selected as account provider, a shared folder is 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.

ACLs can also be set on individual files and directories from a Windows client, if the user has enough permissions – see section *Change resource permissions from Windows clients* for details.

Warning: Some ACLs settings supported by Windows clients cannot be translated to POSIX ACLs supported by NethServer, thus they will be lost when they are applied

At any time, the *Reset permissions* button propagates the shared folder UNIX permissions and POSIX ACLs to its contents.

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

If an **LDAP** account provider is selected or there is no account provider at all, any access to shared folders is considered as *Guest access* so that everyone is allowed to read and write its content.

4.17.3 Network access

SMB/CIFS is a widely adopted protocol that allows to share files across a computer network. 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
```

Warning: Authenticated access to shared folders is available with an Active Directory accounts provider. LDAP provider allows guest access only.

When accessing a SMB share, some user interfaces provide a single user name field. In that case, specify the **user short name** prefixed with the **NetBIOS domain name**. For instance, if the NetBIOS domain name is "DOMAIN" and the user name is "john.smith", the domain-prefixed user name to access a SMB share is:

```
DOMAIN\john.smith
```

On the contrary, some applications provide separate input fields for the NetBIOS domain name and the user name; in that case fill in the input fields individually.

4.17.4 Network recycle bin

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

4.17.5 Hide a shared folder

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

4.17.6 Home share

Each NethServer user has a personal shared folder that is mapped to his Unix home directory. The SMB share name correspond to the **user short name**. For example:

- user short name `john.smith`
- server name `MYSERVER`
- server address `192.168.1.2`

The SMB network address is:

```
\\MYSERVER\john.smith
\\192.168.1.2\john.smith
```

Provide John's credentials as explained in *Network access*.

Tip: The Unix home directory is created the first time the user accesses it by either SMB or SFTP/SSH protocol.

4.17.7 Change resource permissions from Windows clients

When an user connects to a shared folder with a Windows client, he can change permissions on individual files and directories. Permissions are expressed by Access Control Lists (ACLs).

Warning: Some ACLs settings supported by Windows clients cannot be translated to POSIX ACLs implemented by NethServer, thus they will be lost when they are applied

Only the owner of a resource (being it either file or directory) has full control over it (read, write, change permissions). The permission to delete a resource is granted to users with write permissions on the parent directory. The only exception to this rule is described in the *Administrative access* section.

When a new resource is created, the owner can be defined by one of the following rules:

- the owner is the user that creates the resource
- the owner is inherited from the parent directory

To enforce one of those rules, go to *Windows file server* page and select the corresponding radio button under *When a new file or directory is created in a shared folder* section.

Warning: The *Owning group* setting of a shared folder does not affect the owner of a resource. See also the *Authorizations* section above

4.17.8 Administrative access

The *Windows file server* page allows to grant special privileges to members of the `Domain Admins` group:

- extend the owner permission by enabling the *Grant full control on shared folders to Domain Admins group* checkbox
- access other users' home directories by enabling the *Grant full control on home directories to Domain Admins group (home$ share)* checkbox. To access home directories connect to the hidden share `home$`. For instance, the SMB network address is:

```
\\MYSERVER\home$
\\192.168.1.2\home$
```

4.18 Bandwidth monitor

4.18.1 ntopng

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

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

Port The port where to view the ntopng web interface.

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

Interfaces Interfaces on which ntopng will listens 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 called

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

The web interface can be accessed from the *Graphs*.

After installation, the system will gather following statistics:

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

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

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

4.19.1 Network latency

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

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

Example:

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

4.20 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

4.20.1 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, a server will have the master role. All other servers are considered as slaves (clients).

A client can be connected to another NethServer or any other firewall which uses OpenVPN.

All tunnels use OpenVPN routed mode, but there are two kind of topologies: *subnet* and *p2p* (Point to Point)

Topology: subnet

This is the recommended topology. In subnet topology, the server will accept connections and will act as DHCP server for every connected clients.

In this scenario

- the server will authenticate clients using TLS certificates
- the server can push local routes to remote clients
- the client will be able to authenticate with TLS certificates or user name and password

Topology: P2P

In p2p topology, the administrator must configure one server for each client.

In this scenario:

- the only supported authentication method is the PSK (Pre-Shared Key). Please make sure to exchange the PSK using a secure channel (like SSH or HTTPS)
- the administrator must select an IP for both end points
- routes to remote networks must be configured on each end point

To configure a tunnel, proceed as follow:

1. Access the tunnel server and open the *OpenVPN tunnels* page, move to *Tunnel servers* tab and click on *Create new* button
2. Insert all required fields, but please note:
   - *Public IPs and/or public FQDN*, it's a list of public IP addresses or host names which will be used by clients to connect to the server over the public Internet
   - *Local networks*, it's a list of local networks which will be accessible from the remote server. If topology is set to p2p, the same list will be reported inside the client *Remote networks* field
   - *Remote networks*, it's a list of networks behind the remote server which will be accessible from hosts in the local network

3. After the configuration is saved, click on the *Download* action and select *Client configuration*
4. Access the tunnel client, open the *OpenVPN tunnels* page, move to *Tunnel clients* tab, click on *Upload* button

Advanced features

The web interface allows the configuration of advanced features like:

- on the client, multiple addresses can be specified inside the *Remote hosts* field for redundancy; the OpenVPN client will try to connect to each host in the given order
- WAN priority: if the client has multiple WAN (red interfaces), the option allows to select the order in which the WAN will be used to connect to the remote server
- protocol: please bear in mind that OpenVPN is designed to operate optimally over UDP, but TCP capability is provided for situations where UDP cannot be used
- cipher: the cryptographic algorithm used to encrypt all the traffic. If not explicitly selected, the server and client will try to negotiate the best cipher available on both sides
- LZO compression: enabled by default, can be disabled when using legacy servers or clients

Legacy mode

Tunnels can still be created also using Roadwarriors accounts.

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.

4.20.2 IPsec

IPsec (IP Security) protocol is the 'de facto' standard in VPN tunnels, it's tipically used to create net to net tunnels and it's supported from all manufacturers. You can use this protocol to create VPN tunnels between a NethServer and a device from another manufacturer as well as VPN tunnels between 2 NethServer.

Note: IPSec is not designed to connect single hosts but for net2net configuration, this implies two gateways on both ends (at least one red and one green interface).

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.

4.21 Nextcloud

Nextcloud 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 Nextcloud with MariaDB and default access credential
- integration with NethServer system users and groups
- automatic backup data with nethserver-backup-data tool
- customize https access url (custom virtual host)

4.21.1 Installation

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

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

All users configured inside any user provider (see *Users and groups*) can automatically access the NextCloud installation. After the installation a new application widget is added to the NethServer web interface dashboard.

Note: Nextcloud update/upgrade procedure disables the apps to avoid incompatibility problems. Server logs keep track of which apps were disabled. After a successful update/upgrade procedure you can use the Applications page to update and re-enable the apps.

Note: Nextcloud version 13 uses new PHP 7.1 (*nethserver-rh-php71-php-fpm*) while older version uses PHP 5.6 (*nethserver-rh-php56-php-fpm*). You can remove php56 version (if there are no dependency problems) with the command "yum remove nethserver-rh-php56-php-fpm".

User list

All users are listed inside the administrator panel of NextCloud using a unique identifier containing letters and numbers. This is because the system ensures that there are no duplicate internal user names as reported in section *Internal Username* of Official NextCloud documentation.

Note: If NethServer is bound to a remote Active Directory account provider a dedicated user account in AD is required by the module to be fully operational! See *Join an existing Active Directory domain*.

4.21.2 Custom Virtual Host

To customize the Nextcloud web url:

```
config setprop nextcloud VirtualHost mynextcloud.domain.com
config setprop nextcloud TrustedDomains mynextcloud.domain.com
signal-event nethserver-nextcloud-update
```

If you use *let's encrypt* remember to add the domain name to the proper list.

4.21.3 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 nextcloud TrustedDomains server.domain.com
signal-event nethserver-nextcloud-update
```

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

4.22 FTP

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

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

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

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

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

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

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

4.22.1 System users

Warning: This configuration is highly discouraged

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

Enable system users:

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

Given a user name *goofy*, first make sure the user has Remote shell access. 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
```

4.23 Phone Home

During the first configuration wizard, you can opt-out from contributing to usage statistics. Phone home is used to track all NethServer's installations around the world. Each time a new NethServer is installed, this tool sends some installation details to a central server. The information is stored in a database and used to display nice markers in a Google Map view with number of installation grouped by country and release.

4.23.1 Overview

The tool is *enabled* by default.

To disable it at a later time, run: `config setprop phone-home status disabled`

If phone home is *enabled* the details sent are:

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

All the data is used to populate the map.

4.24 SNMP

The 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.

To enable it, you should set three main options:

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

The implementation is based on the Net-SNMP project. Please refer to the official project page for more information:

http://www.net-snmp.org/

References

4.25 Hotspot (Dedalo)

Hotspot main goal is to provide internet connectivity via wi-fi to casual users. Users are sent to a captive portal from which they can access the network by authenticating themselves via social login, sms or email. The hotspot service allows the regulation, accountability and pricing of Internet access in public places, like internet points, hotels and fairs.

Main features:

- network isolation between corporate and guests
- guests can authenticate themselves using social login (Facebook, Instagram, Linkedin) as well as sms or email login
- paid service based on vouchers
- hotspot manager with different accesses type (admin, customer, desk)
- bandwidth Limit for each user
- export account list and connections report (not yet implemented)

4.25.1 How it works?

The implementation is based on 2 components:

- a remote hotspot manager with a Web GUI running on a cloud server that allows you to:
  - create a hotspot instance: usually each instance is referred to a specific location (e.g. Art Cafè, Ritz Hotel and so on)
  - edit the captive portal page
  - choose what type of login to use
  - see session and users logged
- a client part (dedalo) installed in NethServer physically connected to the Access Points network : it assigns IP addresses to the clients of the Wi-Fi Network and redirects them to the captive portal for authentication.

For more detailed information please refer to https://nethesis.github.io/icaro/docs/components/ .

4.25.2 How to install it

- install the server component: https://nethesis.github.io/icaro/docs/provisioning/ This procedure uses Vagrant to provision a Digital Ocean (DO) droplet. If you prefere to use another cloud provider, edit Vagrantfile accordingly.
- configure the server in order to make it possibile to login: https://nethesis.github.io/icaro/docs/configuration/
- install the client component in your NethServer: https://nethesis.github.io/icaro/docs/client_installation/
- please remind that the installation requires at least 3 ethernet interfaces:
  - 1 for normal LAN clients, marked with green role (you need it even if unused, it can be a VLAN)
  - 1 (or more) for Internet connection, marked with red role
  - 1 one for the Dedalo, marked with hotspot role

4.25.3 Configuration

Hotspot manager interface

- go to the hotspot manager
- go to the *Managers* section and create a new *Manager* of type *Reseller* or *Customer*. More info about *Roles* here : https://nethesis.github.io/icaro/docs/manager/.
- do logout and login with the new manager just created
- go in the *Hotspot* section and create a new hotspot instance
- click on the hotspot name and configure the captive portal

Hotspot Unit on NethServer

- go to the section *Hotspot Unit* on NethServer
- edit the parameters in the *Hotspot unit registration* page:
  - `Host name` : Public name of the Hotspot Manager
  - `User name` : user of a working account (reseller or customer)
  - `Password` : password

After that just choose the ethernet interface where the hotspot will be active.

If you have the proxy web active a specific flag in the hotspot unit page will allow you to forward all the hotspot traffic (http and httpas protocols) to the web proxy for logging purposes (Be aware of the privacy implications!).

- connect an AP to the hostpot interface.

Access Point Configuration

The Access Point (AP) must perform the sole function of enabling the connection with the firewall, they should behave like an ordinary network switch. Follow these recommendations:

- configure the access point without authentication and without DHCP
- disable any service (security services, etc.) in order to avoid interference with hotspot behavior

- if you use more AP configure them with different SSID (eg: 1-SCHOOL / SCHOOL-2 / . . .) in order to easily identify any malfunctioning AP
- configure the AP with a static IP address on a network segment (rfc-1918) different from the one used by the hotspot
- if possible, enable the "client isolation", to avoid traffic between clients connected to the access point
- configure the AP to work on different channels to minimize interference, a good AP allow you to manage the channels automatically or manually select them
- do not use too shoddy products, low quality AP can cause frequent disconnections which impact on the quality of the overall service, the recommendation is even more important if you are using repeaters

For test purposes only you can also connect a laptop or a pc via ethernet cable to the hotspot interface instead of a Wi-Fi network. This can be very useful if you are experiencing problems and you want to check if they are caused by the hotspot service or by the AP network.

Free Mode and Voucher Mode

The free mode (default) allows you to make login by yourself without the need of any code, just click on the desired social (or sms, email).

The voucher mode force you to create a voucher (basically "a code") and give it to every user, only users with the voucher will be allowed to make login.

4.26 FreePBX

FreePBX is a web-based open source GUI (graphical user interface) that controls and manages Asterisk (PBX), an open source communication server (https://www.freepbx.org/).

4.26.1 Installation

You can install FreePBX from the package manager of NethServer, the module named "FreePBX".

All FreePBX configurations and data are saved inside configuration and data backup.

4.26.2 Web Access

After installed, FreePBX will be accessible at `https://ip_address/freepbx` from green interfaces. You can also configure the access from the red interface under the "PBX Access" page of the NethServer Server Manager.

4.26.3 FwConsole

The `fwconsole` is a tool that allows the user to perform some FreePBX administrative tasks (see FreePBX wiki). In order to use it with NethServer you have to use it in conjunction with scl:

```
/usr/bin/scl enable rh-php56 "/usr/sbin/fwconsole"
```

4.26.4 Advanced Documentation

For further information you can read the FreePBX documentation at: https://wiki.freepbx.org

4.27 HotSync

Warning: HotSync should be considered a beta release. Please test it on your environment before using in production.

HotSync aims to reduce downtime in case of failure, syncing your NethServer with another one, that will be manually activated in case of master server failure.

Normally, when a hardware damage occurs, the time needed to restore service is:

1. fix/buy another server: from 4h to 2 days
2. install OS: 30 minutes
3. restore backup: from 10 minutes to 8 hours

In summary, users are able to start working again with data from the night before failure after a few hours/days. Using hotsync, time 1 and 3 are 0, 2 is 5 minutes (time to activate spare server). Users are able to start working again in few minutes, using data from a few minutes before the crash.

By default all data included in backup are synchronized every 15 minutes. MariaDB databases are synchronized too, unless databases synchronization isn't disabled. Applications that use PostgreSQL are synchronized (Mattermost, Webtop5) unless databases synchronization isn't disabled.

4.27.1 Terminology

- MASTER is the production system SLAVE is the spare server
- SLAVE is switched on, with an IP address different than MASTER
- Every 15 minutes, MASTER makes a backup on SLAVE
- An email is sent to root (admin if mail server is installed)

4.27.2 Installation

Install nethserver-hotsync on both MASTER and SLAVE, execute from command line:

```
yum install nethserver-hotsync
```

If you want to tests the Cockpit-based web interface, execute also:

```
yum --enablerepo=nethserver-testing install nethserver-cockpit-hotsync
```

4.27.3 Configuration

Master

```
[root@master]# config setprop rsyncd password <PASSWORD>
[root@master]# config setprop hotsync role master
[root@master]# config setprop hotsync SlaveHost <SLAVE_IP>
[root@master]# signal-event nethserver-hotsync-save
```

Slave

```
[root@slave]# config setprop rsyncd password <PASSWORD>
[root@slave]# config setprop hotsync role slave
[root@slave]# config setprop hotsync MasterHost <MASTER_IP>
[root@slave]# signal-event nethserver-hotsync-save
```

The `<PASSWORD>` must be the same on master and slave.

If mysql or postgresql are installed, they will be synchronized by default. To disable databases sync

```
[root@master]# config setprop hotsync databases disabled
[root@master]# signal-event nethserver-hotsync-save
```

Enabling/Disabling

Hotsync is enabled by default. To disable it:

```
[root@slave]# config setprop hotsync status disabled
[root@slave]# signal-event nethserver-hotsync-save
```

and to re-enable it:

```
[root@slave]# config setprop hotsync status enabled
[root@slave]# signal-event nethserver-hotsync-save
```

4.27.4 Restore: put SLAVE in production

The following procedure puts the SLAVE in production when the master has crashed.

1. switch off MASTER
2. if the SLAVE machine must run as network gateway, connect it to the router/modem with a network cable
3. on SLAVE, if you are connected through an ssh console, launch the `screen` command, to make your session survive to network outages:

   ```
   [root@slave]# screen
   ```

4. on SLAVE launch the following command, and read carefully its output

   ```
   [root@slave]# hotsync-promote
   ```

5. go to Server Manager, in page `Network` and reassign roles to network interfaces as required
6. launch the command

   ```
   [root@slave]# /sbin/e-smith/signal-event post-restore-data
   ```

7. update the system to the latest packages version

   ```
   [root@slave]# yum clean all && yum -y update
   ```

8. if an USB backup is configured on MASTER, connect the backup HD to SLAVE

4.27.5 Supported packages

- nethserver-nextcloud
- nethserver-mysql
- nethserver-dnsmasq
- nethserver-squidguard
- nethserver-pulledpork
- nethserver-antivirus
- nethserver-samba-audit
- nethserver-freepbx > 14.0.3
- nethserver-webtop5 (z-push state is not synchronized)
- nethserver-collectd
- nethserver-cups
- nethserver-dc
- nethserver-letsencrypt
- nethserver-nextcloud
- nethserver-sssd
- nethserver-directory
- nethserver-ibays
- nethserver-mail-server

4.28 Virtual machines

NethServer is capable of running virtual machines using KVM and libvirt.

Virtualization software can be installed and started using the command line:

```
yum -y install qemu-kvm libvirt virt-install libvirt-client
systemctl enable libvirtd
systemctl start libvirtd
```

If NethServer is used as DHCP server, the dnsmasq instance launched by libvirtd will conflict with the default one. To avoid the conflict, remove the `default` libvirt NAT network:

```
systemctl stop dnsmasq
systemctl start libvirtd
virsh net-destroy default
virsh net-autostart default --disable
systemctl start dnsmasq
```

The recommended client to manage virtual machines is Virtual Machine Manager (virt-manager).

Install virt-manager in your Linux desktop, then create a new connection to your NethServer using the SSH protocol.

Alternatively, virt-manager can be directly installed on NethServer:

```
yum -y install virt-manager
```

Then, use X11 Forwarding through SSH to view virt-manager graphical interface.

4.28.1 External resources

For more info see:

- Virtual Machine Manager official site
- Virtual Machine Manager on RHEL
- Introduction to virtualization
- KVM/Libvirt FAQ

4.29 Fail2ban

Fail2ban scans log files (e.g. `/var/log/apache/error_log`) and bans IPs that show the malicious signs – too many password failures, seeking for exploits, etc. Generally Fail2Ban is then used to update firewall rules to reject the IP addresses for a specified amount of time, although any arbitrary other action (e.g. sending an email) could also be configured. Out of the box Fail2Ban comes with filters for various services (Apache, Dovecot, Ssh, Postfix, etc).

Fail2Ban is able to reduce the rate of incorrect authentications attempts however, it cannot eliminate the risk that weak authentication presents. To improve the security, open the access to service only for secure networks using the firewall.

4.29.1 Installation

Install from the Software Center or use the command line:

```
yum install nethserver-fail2ban
```

4.29.2 Settings

Fail2ban is configurable in the security category of the server-manager. Most of settings can be changed in the *Configuration* tab, only really advanced settings must be configured by the terminal.

Jails

A jail is enabled and start to protect a service when you install a new module, the relevant jail (if existing) is automatically activated after the package installation.

All jails can be disabled individually in the Jails settings.

Number of attempts Number of matches (i.e. value of the counter) which triggers ban action on the IP.

Time span The counter is set to zero if no match is found within "findtime" seconds.

Ban Time Duration for IP to be banned for.

Recidive jail is perpetual When an IP goes several time in jail, the recidive jail bans it for a much longer time. If enabled, it is perpetual.

Network

Allow bans on the LAN By default the failed attempts from your Local Network are ignored, except when you enabled the option.

IP/Network Whitelisting IP listed in the text area will be never banned by fail2ban (one IP per line). Network could be allowed in the Trusted-Network panel.

Email

Send email notifications Enable to send administrative emails.

Administrators emails List of email addresses of administrators (one address per line).

Notify jail start/stop events Send email notifications when a jail is started or stopped.

4.29.3 Unban IP

IPs are banned when they are found several times in log, during a specific find time. They are stored in a database to be banned again each time your restart the server or the service. To unban an IP you can use the *Unban IP* tab in the status category of the server-manager.

4.29.4 Statistics

The *Ban statistics* tab is available in the status category of the server-manager, it gives you the total number of bans per jail as well as the total of all bans.

4.29.5 Tools

Fail2ban-client

Fail2ban-client is part of the fail2ban rpm, it gives the state of fail2ban and all available jails:

```
fail2ban-client status
```

To see a specific jail :

```
fail2ban-client status sshd
```

To see which logfiles are monitored for a jail:

```
fail2ban-client get nginx-http-auth logpath
```

Fail2ban-listban

Fail2ban-listban counts the IPs currently and totally banned in all activated jails, at the end it shows the IPs which are still banned by shorewall.

```
fail2ban-listban
```

Fail2ban-regex

Fail2ban-regex is a tool which is used to test the regex on you logs, it is a part of fail2ban software. Only one filter is allowed per jail, but it is possible to specify several actions, on separate lines.

The documentation is readable at the fail2ban project.

```
fail2ban-regex /var/log/YOUR_LOG /etc/fail2ban/filter.d/YOUR_JAIL.conf --print-all-
↪matched
```

You can also test custom regex directly:

```
fail2ban-regex /var/log/secure '^%(__prefix_line)s(?:error: PAM: )?[aA]uthentication␣
↪(?:failure|error) for .* from <HOST>( via \S+)?\s*$'
```

Fail2ban-unban

Fail2ban-unban is used to unban an IP when the ban must be removed manually.

```
fail2ban-unban <IP>
```

You can use also the built-in command with fail2ban-client:

```
fail2ban-client set <JAIL> unbanip <IP>
```

4.29.6 Whois

If you desire to query the IP `whois` database and obtain the origin of the banned IP by email, you could Install the `whois` rpm.

4.30 Email module transition to Rspamd

Since NethServer 7.5.1804 new *Email*, *POP3 connector* and *POP3 proxy* installations are based on the Rspamd[1] filter engine.

- Previous NethServer installations are automatically upgraded to Rspamd as described by this section.
- New configuration features, specific to the Rspamd-based implementation, are documented in *Email*. Here is a brief list:
  - DKIM signature
  - Rspamd web UI
  - Greylist threshold[3]

[1] Rspamd – Fast, free and open-source spam filtering system. https://rspamd.com/

[3] Greylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using greylisting will "temporarily reject" any email from a sender it does not recognize – Wikipedia

4.30.1 Feature changes

Append a legal notice

The *Email* > *Domains* > *Append a legal note to sent messages* (also known as "Disclaimer") feature was split in a separate, optional package: `nethserver-mail2-disclaimer`. New installations should avoid it, as it relies on an old package[4] that can be removed in future releases.

Block port 25

The block of port 25 can prevent abuse/misuse by LAN machines. If the system is acting as the LAN network gateway, the administrator can create a firewall rule inside the *Rules* page.

Additional host name aliases

The following host name aliases were automatically registered in the local DNS service, if the `postfix/MxRecordStatus` was `enabled`:

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

When upgraded from an old Email module based on Amavisd, the `postfix/MxRecordStatus` is removed and those aliases are pushed as `self` records in the `hosts` DB. They can be edited from *DNS* > *Server alias* page.

MX record for LAN clients

The new Email module implementation based on Rspamd does not push the MX record override for LAN hosts any more. Ensure the LAN mail user agents are configured to use SMTP/AUTH or are listed in *Email* > *SMTP access* > *Allow relay from IP addresses* before upgrading.

4.30.2 Upgrade procedures

Manual upgrade procedures are no longer needed: upgrade occurs automatically.

References

[4] alterMIME is a small program which is used to alter your mime-encoded mailpack – https://pldaniels.com/altermime/

CHAPTER 5

NethForge modules

5.1 SOGo

Note: This package is not supported in NethServer Enterprise

SOGo is a fully supported and trusted groupware server with a focus on scalability and open standards. SOGo is released under the GNU GPL/LGPL v2 and above. SOGo provides a rich AJAX-based Web interface and supports multiple native clients through the use of standard protocols such as CalDAV, CardDAV and GroupDAV, as well as Microsoft ActiveSync. SOGo is the missing component of your infrastructure; it sits in the middle of your servers to offer your users a uniform and complete interface to access their information. It has been deployed in production environments where thousands of users are involved.

Note: SOGo provides EAS (Exchange ActiveSync) support, but not EWS (Exchange Web Service). Outlook 2013, 2016 for Windows works well with EAS. Mainstream mobile devices (iOS, Android, BlackBerry 10) work well with EAS, they can sync mails, calendars, contacts, tasks. Apple Mail.app, and Outlook for Mac support EWS. But not EAS. **Clients work very well with POP3/IMAP account, caldav/carddav account**

Warning: `nethserver-sogo` doesn't integrate OpenChange and Samba4 for native MAPI support, so SOGo groupware doesn't provide full support for Microsoft Outlook clients, Mac OS X Mail.app and all iOS devices, don't try to add your mail account as an Exchange account in these mail clients. You have to add account as POP3/IMAP account, caldav/carddav account instead.

5.1.1 Installation

Note: You need first to set an account provider which can be local (nethserver-directory for openldap or nethserver-dc for Samba AD) or remote (whatever openldap or samba AD choice). You cannot mix your choice by openldap and

Samba AD, preferably if you plan to host samba shares with user authentication, you need samba AD (nethserver-dc)

Then install from the Software Center or use the command line:

```
yum install nethserver-sogo
```

5.1.2 Official documentation

Please read official documentation: your solution is in this book.

5.1.3 Usage

The URL of the groupware is https://yourdomain.com/SOGo. You can use the 'username or username@domain.com for login.

5.1.4 Esmith database

You can modify the available properties of SOGo:

```
sogod=service
  ActiveSync=enabled
  AdminUsers=admin
  BackupTime=30 0
  Certificate=
  Dav=enabled
  DraftsFolder=Drafts
  IMAPLoginFieldName=userPrincipalName
  MailAuxiliaryUserAccountsEnabled=YES
  Notifications=Appointment,EMail              #'Folder'/'ACLs'/'Appointment'
  SOGoInternalSyncInterval=10
  SOGoMaximumPingInterval=10
  SOGoMaximumSyncInterval=30
  SOGoMaximumSyncResponseSize=2048
  SOGoMaximumSyncWindowSize=100
  SentFolder=Sent
  SxVMemLimit=512
  TrashFolder=Trash
  VirtualHost=
  WOWatchDogRequestTimeout=10
  WOWorkersCount=10
  status=enabled
```

Properties:

- AdminUsers: Parameter used to set which usernames require administrative privileges over all the users tables.
- BackupTime: Time to launch the backup, by default ('30 0')each day at 00h30, you can change it if you set a cron compatible value * *
- DraftsFolder: name of draft folder, default is 'Drafts'
- IMAPLoginFieldName: adjust the imap login field to your good trusted value in your ldap (see https://community.nethserver.org/t/sogo-and-ad-brainstorming/8024/31)
- SentFolder: name of the sent folder, default is 'Sent'

- TrashFolder: name of the trash folder, default is 'Trash'
- WOWorkersCount: The amount of instances of SOGo that will be spawned to handle multiple requests simultaneously
- MailAuxiliaryUserAccountsEnabled: Parameter used to activate the auxiliary IMAP accounts in SOGo. When set to YES, users can add other IMAP accounts that will be visible from the SOGo Webmail interface.
- Notifications: enabled notifications. The value is a comma separated list. Default value is "Appointment, EMail"

Notes

Terms highlighted in **bold** are documented in SOGo installation and configuration guide.

- `AdminUsers` comma separated list of accounts allowed to bypass SOGo ACLs. See **SOGoSuperUsernames** key
- Notifications comma separated list of values (no spaces between commas). Known item names are `ACLs`, `Folders`, `Appointments`. See **SOGoSendEMailNotifications**
- `{Drafts,Sent,Trash}Folder` See respective **SOGoFolderName** parameters
- `VirtualHosts` SOGo is reachable from the default host name plus the host (FQDN) listed here. The host key is generated/removed in `hosts` DB, with `type=self` automatically.

5.1.5 Access SOGo on an exclusive hostname

To make SOGo accessible with an exclusive DNS hostname:

- In "DNS and DHCP" UI module (Hosts), create the DNS host name as a server alias (i.e. webmail.example.com)
- Add the host name to sogod/VirtualHost prop list:

```
config setprop sogod VirtualHost webmail.example.com
signal-event nethserver-sogo-update
```

Same rule applies if SOGo must be accessible using server IP address. For example:

```
config setprop sogod VirtualHost 192.168.1.1
signal-event nethserver-sogo-update
```

If the VirtualHost prop is set, requests to the root (i.e. webmail.example.com) are redirected to the (mandatory) /SOGo subfolder (webmail.example.com/SOGo).

It is also possible to use a custom certificate for this virtualhost:

```
config setprop sogod Certificate example.crt
signal-event nethserver-sogo-update
```

5.1.6 Maximum IMAP command

Maximum IMAP command line length in kilo bytes. Some clients generate very long command lines with huge mailboxes, so you may need to raise this if you get "Too long argument" or "IMAP command line too large" errors often.

Set by default to 2048KB:

```
config setprop dovecot ImapMaxLineLenght 2048
signal-event nethserver-sogo-update
```

5.1.7 ActiveSync

According to this *WebTop vs SOGo*, WebTop and SOGo can be installed on the same machine, although it is discouraged to keep such setup on the long run.

ActiveSync is enabled by default on SOGo and WebTop. At installation of SOGo, Webtop-ActiveSync is disabled and SOGo will take precedence.

SOGo-ActiveSync can be disabled in the server-manager at the SOGo-panel or with:

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

To enable ActiveSync on WebTop:

```
config setprop webtop ActiveSync enabled
signal-event nethserver-webtop5-update
```

To enable ActiveSync on SOGo again:

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

5.1.8 Backup

Each night (by default) a cron run to backup user data (filter rules, specific settings, events, contacts) and save it to `/var/lib/sogo/backups` you can restore the data with a tool `sogo-restore-user`, for example:

```
sogo-restore-user /var/lib/sogo/backups/sogo-2017-12-10_0030/ stephane
```

or for all users

```
sogo-restore-user /var/lib/sogo/backups/sogo-2017-12-10_0030/ -A
```

if you want to change the time of your backup for example (in this example, run at 4h01 AM):

```
config setprop sogod BackupTime '1 4'
signal-event nethserver-sogo-update
```

5.1.9 Fine tuning

Adjust Setting

SOGo must be tuned following the number of users, some settings can be tested.

Note: Keep in mind to set one worker per user for the activesync connection.

100 users, 10 EAS devices:

```
config setprop sogod WOWorkersCount 15
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 30
signal-event nethserver-sogo-update
```

100 users, 20 EAS devices:

```
config setprop sogod WOWorkersCount 25
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 40
signal-event nethserver-sogo-update
```

1000 users, 100 EAS devices:

```
config setprop sogod WOWorkersCount 120
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 60
signal-event nethserver-sogo-update
```

Increase sogod log verbosity

Read the SOGo FAQ for other debugging features.

SOGo floods /var/log/messages

You can see this log noise in `/var/log/message`:

```
Dec  4 12:36:01 ns7ad1 systemd: Created slice User Slice of sogo.
Dec  4 12:36:01 ns7ad1 systemd: Starting User Slice of sogo.
Dec  4 12:36:01 ns7ad1 systemd: Started Session 163 of user sogo.
Dec  4 12:36:01 ns7ad1 systemd: Starting Session 163 of user sogo.
Dec  4 12:36:01 ns7ad1 systemd: Removed slice User Slice of sogo.
Dec  4 12:36:01 ns7ad1 systemd: Stopping User Slice of sogo.
```

These messages are normal and expected – they will be seen any time a user logs in. To suppress these log entries in `/var/log/messages`, create a discard filter with rsyslog, e.g., run the following command:

```
echo 'if $programname == "systemd" and ($msg contains "Starting Session" or $msg␣
↪contains "Started Session" or $msg contains "Created slice" or $msg contains
↪"Starting User" or $msg contains "Removed slice User" or $msg contains "Stopping␣
↪User") then stop' > /etc/rsyslog.d/ignore-systemd-session-slice-sogo.conf
```

and restart rsyslog

```
systemctl restart rsyslog
```

this solution comes from RedHat solution

5.1.10 Clients

Android

Currently you have 2 ways to integrate your Android device with Sogo.

Integration via Caldav /Cardav/imap

Note: The drawback is that you need to set all settings (Url/Username/Password) in each application.

- Email

Imaps(over ssl) is a good choice, you can use the K9-mail software to retrieve your email or the default email application

- Contacts and calendars

There are various working clients, including DAVdroid (open-source) and CalDAV-Sync/CardDav-Sync. Advantages Full integration into Android, so that almost all calendar and contacts apps can access synchronized data.

Integration via ExchangeActiveSync

Note: The advantage is that you set the Url/Username/Password only in one location

Step-by-step configuration

- Open the account menu, choose add an exchange account
- Fill your full email address and password in Account Setup page:
- If it asks you to choose Account Type, please choose Exchange:
- In detailed account setup page, fill up the form with your server address and email account credential
  - DomainUsername: your full email address
  - Password: password of your email account
  - Server: your server name or IP address
  - Port: 443

Note: Please also check Use secure connection (SSL) and Accept all SSL certificates

- In Account Settings page, you can choose Push. it's all up to you.
- Choose a name for your Exchange account.
- Click Next to finish account setup. That's all.

Mozilla Thunderbird and Lightning

Alternatively, you can access SOGo with a GroupDAV and a CalDAV client. A typical well-integrated setup is to use Mozilla Thunderbird and Mozilla Lightning along with Inverse's SOGo Connector plug in to synchronize your address books and the Inverse's SOGo Integrator plug in to provide a complete integration of the features of SOGo into Thunderbird and Lightning. Refer to the documentation of Thunderbird to configure an initial IMAP account pointing to your SOGo server and using the user name and password mentioned above.

With the SOGo Integrator plug in, your calendars and address books will be automatically discovered when you login in Thunderbird. This plug in can also propagate specific extensions and default user settings among your site. However, be aware that in order to use the SOGo Integrator plug in, you will need to repackage it with specific modifications. Please refer to the documentation published online.

If you only use the SOGo Connector plug in, you can still easily access your data.

- To access your personal address book:
- Choose Go > Address Book.
- Choose File > New > Remote Address Book.
- Enter a significant name for your calendar in the Name field.
- Type the following URL in the URL field: http://localhost/SOGo/dav/jdoe/Contacts/personal/
- Click on OK.

To access your personal calendar:

- Choose Go > Calendar.
- Choose Calendar > New Calendar.
- Select On the Network and click on Continue.
- Select CalDAV.
- Type the following URL in the URL field: http://localhost/SOGo/dav/jdoe/Calendar/personal/
- Click on Continue.

Windows Mobile

The following steps are required to configure Microsoft Exchange ActiveSync on a Windows Phone:

Locate the Settings options from within your application menu.

- Select Email + Accounts.
- Select Add an Account.
- Select the option for Advanced Setup.
- Enter your full email address and password for your account. Then press the sign in button.
- Select Exchange ActiveSync.
- Ensure your email address remains correct.
- Leave the Domain field blank.
- Enter the address for Server (domain name or IP)
- Select the sign in button.
- You might need to accept all certificats, if you are not able to sync

Once connected, you will see a new icon within your settings menu with the name of your new email account.

Outlook

You can use it with

- IMAP + commercial plugin as cfos or outlookdav for calendars/contacts
- ActiveSync since Outlook 2013

There is no support for Openchange/OutlookMAPI.

5.1.11 Nightly build

SOGo is built by the community, if you look to the last version, then you must use the nightly built. This version is not considered as stable, but bugs are fixed quicker than in stable version. You are the QA testers :)

NethServer 7 - SOGo 3

Execute:

```
sudo rpm --import 'http://pgp.mit.edu/pks/lookup?op=get&search=0xCB2D3A2AA0030E2C'
sudo rpm -ivh http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
sudo cat >/etc/yum.repos.d/SOGo.repo <<EOF
[sogo3]
name=SOGo Repository
baseurl=https://packages.inverse.ca/SOGo/nightly/3/rhel/7/\$basearch
gpgcheck=1
EOF
```

Then to install:

```
yum install nethserver-sogo --enablerepo=sogo3
```

5.1.12 Issues

Please raise issues on community.nethserver.org.

5.1.13 Sources

Source are available https://github.com/NethServer/nethserver-sogo

Developer manual on github.

CHAPTER 6

Best practices

6.1 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
```

6.1.1 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`.

6.1.2 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*.

6.1.3 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 green
signal-event firewall-adjust
signal-event runlevel-adjust
```

6.1.4 Starting and stopping

NethServer uses the standard systemd multiuser target.

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

To enable a service on boot:

```
systemctl enable mysoftware
```

To disable a service on boot:

```
systemctl disable mysoftware
```

CHAPTER 7

Appendix

7.1 Migration from NethService/SME Server

Migration is the process to convert a SME Server/NethService machine (*source*) into a NethServer (*destination*). It can be achieved from a *backup* or *using rsync*.

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

Warning: Before running the migration procedure, read carefully all the sections of this chapter.

7.1.1 Accounts provider

You should configure an *accounts provider* before starting the migration procedure.

- If the source system was joined to an Active Directory domain (Samba server role was ADS), configure a *remote Active Directory* accounts provider.
- If the source system was a NT Primary Domain Controller (Samba server role was PDC) install a *local Active Directory* accounts provider.
- If access to Shared Folders on the destination system requires user authentication, install a *local Active Directory* accounts provider.
- In any other case, install a *local LDAP* accounts provider.

If you choose a *local Active Directory* accounts provider, remember to fully configure and start the DC before executing the `migration-import` event. See *Account providers*.

Furthermore, the following accounts are ignored by the migration procedure because they are already provided by Active Directory:

- administrator
- guest
- krbtgt

7.1.2 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 information.

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 script based on `rsync` is provided by package `nethserver-mail-server`. It runs on the destination host and synchronizes destination mailboxes with the source host:

```
Usage:
    /usr/share/doc/nethserver-mail-server-<VERSION>/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
        -t TYPE     source type: sme8 (default), ns6
```

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

7.1.3 Apache

The SSL cipher suite configuration is not migrated automatically because the source system uses a weak cipher suite by default. To migrate it manually, execute the following commands:

```
MIGRATION_PATH=/var/lib/migration
config setprop httpd SSLCipherSuite $(db $MIGRATION_PATH/home/e-smith/db/
↪configuration getprop modSSL CipherSuite)
signal-event nethserver-httpd-update
```

7.1.4 Ibays

The *ibay* concept has been superseded by *Shared folders*. Supported protocols for accessing Shared folders are:

- SFTP, provided by the `sshd` daemon
- SMB file sharing protocol, typical of Windows networking, implemented by Samba

Warning: Read carefully the *Shared folders* section in the *Upgrade from NethServer 6* chapter, because the connection credentials may change when migrating to NethServer 7.

Starting from NethServer 7, Shared folders are not configurable for HTTP access. After `migration-import` event, old ibays could be migrated according to the following rules of thumb:

1. If the ibay was a **virtual host**, install the "Web server" module from the *Software center* page. Copy the ibay contents to the virtual host root directory. Refer to *Virtual hosts*.
2. If the ibay access was restricted with a **secret password** (for instance, to share contents with a group of people across the internet), the *Virtual hosts* page still offers the same feature. Also the *Nextcloud* module could be a good replacement.
3. If the ibay contents were accessible with an URL like `http://<IP>/ibayname` the easiest procedure to keep it working is moving it to Apache document root:

```
mv -iv /var/lib/nethserver/ibay/ibayname /var/www/html/ibayname
chmod -c -R o+rX /var/www/html/ibayname
db accounts delete ibayname
signal-event nethserver-samba-update
```

After migration, ibays will retain a backward compatibile profile. To take advantage of new features, including Samba Audit, the ibay configuration must be switched to the new profile. From command line execute:

```
db accounts ibay_name SmbProfileType default
signal-event ibay-mody ibay_name
```

Where `ibay_name` is the name of the ibay to configure.

7.1.5 Migration from backup

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 destination host, 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
   ```

7.1.6 Migration with rsync

The process is much faster than migrating from a backup.

Before starting make sure to have:

- a running NethService/SME installation, we will call it original server or source server
- a running NethServer 7 installation with at least the same disk space of the source server, we will call it destination server
- a working network connection between the two severs

Please also make sure the source server allows root login via SSH key and password.

Sync files

The synchronization script copies all data using rsync over SSH. Files are saved inside `/var/lib/migration` directory. If the destination server doesn't have any SSH keys, the script will also create a pair of RSA keys and copy the public key to the source server. All directories excluded from the backup data will not be synced.

On the target machine, execute the following command:

```
screen rsync-migrate <source_server_name> [ssh_port]
```

Where

- `source_server_name` is the host name or IP of the original server
- `ssh_port` is the SSH port of the original server (default is 22)

Example:

```
screen rsync-migrate mail.nethserver.org 2222
```

When asked, insert the root password of the source server, make a coffee and wait patiently.

The script will not perform any action on the source machine and can be invoked multiple times.

Sync and migrate

If called with `-m` option, `rsync-migrate` will execute a final synchronization and upgrade the target machine.

Example:

```
screen rsync-migrate -m mail.nethserver.org 2222
```

The script will:

- stop every service on the source machine (except for SSH)
- execute the `pre-backup` event on the source machine
- sync all remaining data
- execute the `migration-import` event on the destination machine

At the end, check for any error message in `/var/log/messages`:

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

7.2 Upgrade from NethServer 6

The upgrade from NethServer 6 to NethServer 7 can be achieved from a *backup* (see also *Disaster recovery*) or *using rsync*.

Warning: Before running the upgrade procedure, read carefully all the sections of this chapter. Please also read *Discontinued packages*.

Note: During the whole upgrade process, all network services will be inaccessible.

7.2.1 Accounts provider

There are different upgrade scenarios, depending on how the source machine was configured.

- If the source system was a NT Primary Domain Controller (Samba server role was *Primary Domain Controller* – PDC) or a standalone file server (role was *Workstation* – WS), refer to *Primary Domain Controller and Workstation upgrade*.
- If the source system was joined to an Active Directory domain (Samba server role was *Active Directory member* – ADS), refer to *Active Directory member upgrade*.
- In any other case, the LDAP server is upgraded automatically to *local LDAP accounts provider*, preserving existing users, passwords and groups.

Primary Domain Controller and Workstation upgrade

After the restore procedure, go to *Accounts provider* page and select the *Upgrade to Active Directory* procedure. The button will be available only if network configuration has already been fixed accordingly to the new hardware.

The following accounts are ignored by the upgrade procedure because they are already provided by Samba Active Directory:

- `administrator`
- `guest`
- `krbtgt`

An additional, free, IP address from the *green* network is required by the Linux container to run the local Active Directory accounts provider.

For instance:

- server IP (green): `192.168.98.252`
- free additional IP in green network: `192.168.98.7`

Ensure there is a working Internet connection:

```
# curl -I http://packages.nethserver.org/nethserver/
HTTP/1.1 200 OK
```

For more information about the local Active Directory accounts provider, see *Samba Active Directory local provider installation*.

Shared folder connections may require further adjustment.

Warning: Read carefully the *Shared folders* section, because the connection credentials may change when upgrading to NethServer 7.

The upgrade procedure preserves user, group and computer accounts.

Warning: Users not enabled for Samba in NethServer 6 will be migrated as locked users. To enable these locked users, the administrator will have to set a new password.

Active Directory member upgrade

After **restoring the configuration**, join the server to the existing Active Directory domain from the web interface. For more information see *Join an existing Active Directory domain*.

At the end, proceed with **data restore**.

Warning: Mail aliases from AD server are not imported automatically!

7.2.2 Shared folders

Shared folders have been split into two packages:

- "Shared folders" page configures only Samba SMB shares; it provides data access using CIFS/SMB protocol and can be used to share files among Windows and Linux workstations
- The "Virtual hosts" panel provides HTTP and FTP access, it has been designed to host web sites and web applications

SMB access

In NethServer 7 the SMB security model is based on Active Directory. As consequence when upgrading (or migrating) a file server in Primary Domain Controller (PDC) or Standalone Workstation (WS) role the following rule apply:

> When connecting to a shared folder, the NetBIOS domain name must be either prefixed to the user name (i.e. `MYDOMAIN\username`), or inserted in the specific form field.

The upgrade procedure enables the deprecated[1] NTLM authentication method to preserve backward compatibility with legacy network clients, like printers and scanners.

Warning: Fix the legacy SMB clients configuration, then disable NTLM authentication.

- Edit `/var/lib/machines/nsdc/etc/samba/smb.conf`
- Remove the `ntlm auth = yes` line
- Restart the samba DC with `systemctl -M nsdc restart samba`

HTTP access

Every shared folder with web access configured in NethServer 6 can be migrated to a virtual host directly from the web interface by selecting the action *Migrate to virtual host*. After the migration, data inside the new virtual host will be accessible using only FTP and HTTP protocols.

See also *Virtual hosts* for more information about *Virtual hosts* page.

7.2.3 Mail server

All mailboxes options like SPAM retention and quota, along with ACLs, user shared mailboxes and subscriptions are preserved.

[1] Badlock vulnerability http://badlock.org/

Mailboxes associated to groups with *Deliver the message into a shared folder* option enabled, will be converted to public shared mailboxes. The public shared folder will be automatically subscribed by all group members, but all messages will be marked as unread.

7.2.4 TLS policy

In NethServer 7 the services configuration can adhere to *TLS policy*. Before upgrading, the network clients must be checked against the available policy identifiers.

Warning: An old network client can fail to connect if its TLS ciphers are considered invalid

The policy identifier selected by the upgrade procedure depends on the NethServer version and is documented in *Release notes 7*.

7.2.5 Let's Encrypt

Let's Encrypt certificates are restored during the process, but will not be automatically renewed.

After the upgrade process has been completed, access the web interface and reconfigure Let's Encrypt from the *Server certificate* page.

7.2.6 Owncloud and Nextcloud

In NethServer 7, Owncloud has officially been replaced by Nextcloud.

However Owncloud 7 is still available to avoid service disruption after the upgrade.

Note: In case of *upgrade from local LDAP to Samba AD*, user data inside Owncloud will not be accessible either from the web interface or desktop/mobile clients. In such case, install and migrate to Nextcloud after the upgrade to Samba Active Directory has been completed.

From Nextcloud 13, the migration from Owncloud to Nextcloud is not supported anymore.

Users should replace Owncloud clients with Nextcloud ones[2], then make sure to set the new application URL: `https://<your_server_address>/nextcloud`.

7.2.7 Perl libraries

In NethServer 7, perl library `NethServer::Directory` has been replaced by `NethServer::Password`. Please update your custom scripts accordingly.

Example of old code:

```
use NethServer::Directory;
NethServer::Directory::getUserPassword('myservice', 0);
```

New code:

[2] Nextcloud clients download https://nextcloud.com/install/#install-clients

```
use NethServer::Password;
my $password = NethServer::Password::store('myservice');
```

Documentation available via perldoc command:

```
perldoc NethServer::Password
```

7.2.8 Upgrade from backup

1. Make sure to have an updated backup of the original installation.
2. Install NethServer 7 and complete the initial steps using the first configuration wizard. The new machine must have the same hostname of the old one, to access the backup set correctly. Install and configure the backup module.
3. Restore the configuration backup using the web interface. The network configuration is restored, too! If any error occurs, check the `/var/log/messages` log file for further information:

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

4. If needed, go to *Network* page and fix the network configuration accordingly to the new hardware. If the machine was joined to an existing Active Directory domain, read *Active Directory member upgrade*.
5. Complete the restore procedure with the following command:

   ```
   restore-data
   ```

6. Check the restore logs:

   ```
   /var/log/restore-data.log
   /var/log/messages
   ```

7. Each file under `/etc/e-smith/templates-custom/` must be manually checked for compatibility with version 7.

Warning: Do not reboot the machine before executing the restore-data procedure.

7.2.9 Upgrade with rsync

The process is much faster than a traditional backup and restore, also it minimizes the downtime for the users.

Before starting make sure to have:

- a running NethServer 6 installation, we will call it original server or source server
- a running NethServer 7 installation with at least the same disk space of the source server, we will call it destination server
- a working network connection between the two severs

Please also make sure the source server allows root login via SSH key and password.

Sync files

The synchronization script copies all data using rsync over SSH. If the destination server doesn't have any SSH keys, the script will also a pair of RSA keys and copy the public key to the source server. All directories excluded from the backup data will not be synced.

On the target machine, execute the following command:

```
screen rsync-upgrade <source_server_name> [ssh_port]
```

Where

- `source_server_name` is the host name or IP of the original server
- `ssh_port` is the SSH port of the original server (default is 22)

Example:

```
screen rsync-upgrade mail.nethserver.org 2222
```

When asked, insert the root password of the source server, make a coffee and wait patiently.

The script will not perform any action on the source machine and can be invoked multiple times.

Sync and upgrade

If called with `-u` option, `rsync-upgrade` will execute a final synchronization and upgrade the target machine.

Example:

```
screen rsync-upgrade -u mail.nethserver.org 2222
```

The script will:

- close access to every network service on the source machine (except for SSH and httpd-admin)
- execute `pre-backup-config` and `pre-backup-data` event on the source machine
- sync all remaining data
- execute `restore-config` on the destination machine

If `rsync-upgrade` terminates without loosing the network connection,

1. Disconnect the original ns6 from network, to avoid IP conflict with the destination server
2. Access the server manager UI and fix the network configuration from the *Network* page

Otherwise, if during `rsync-upgrade` **the network connection is lost**, it is likely that the source and destination servers have an **IP conflict**:

1. Disconnect the original ns6 from network,
2. From a ns7 root console run the command:

   ```
   systemctl restart network
   ```

3. Then grab the screen device:

   ```
   screen -r -D
   ```

At the end of `rsync-upgrade` run the following steps:

1. If the source system was a NT Primary Domain Controller (Samba server role was *Primary Domain Controller* – PDC) or a standalone file server (role was *Workstation* – WS), refer to *Primary Domain Controller and Workstation upgrade*.
2. If the source system was joined to an Active Directory domain (Samba server role was *Active Directory member* – ADS), refer to *Active Directory member upgrade*.
3. Go back to the CLI and call the `post-restore-data` event on the destination machine:

```
signal-event post-restore-data
```

4. Check the restore logs for any `ERROR` or `FAIL` message:

```
/var/log/restore-data.log
/var/log/messages
```

5. Each file under `/etc/e-smith/templates-custom/` must be manually checked for compatibility with version 7.

Warning: Do not reboot the machine before executing the post-restore-data event.

7.3 Documentation license

7.4 List of NethServer 7 ISO releases

Each subsection corresponds to an upstream ISO release. See also the ISO releases on Developer's manual.

7.4.1 7.5.1804

- 2018-06-11 final
- 2018-05-31 rc
- 2018-05-21 beta

7.4.2 7.4.1708

- 2017-10-26 final - GA 2017-10-30
- 2017-09-21 beta1

7.4.3 7.3.1611

- 2017-07-31 update 1
- 2017-01-30 final - GA 2017-02-08
- 2017-01-18 rc4
- 2016-12-16 rc3

7.4.4 7.2.1511

- 2016-11-09 rc2
- 2016-10-18 rc1
- 2016-09-02 beta2
- 2016-07-12 beta1
- 2016-05-23 alpha3
- 2016-02-12 alpha2

7.5 Chat

The chat service uses the standard protocol Jabber/XMPP. See also *Chat*.

Administration web Interface The Jaber server comes with a web administrative interface for members of the jabberadmins group.

Federation (S2S) XMPP allows for servers communicating seamlessly with each other, forming a global 'federated' IM network.

File transfer maximum speed Limit in Byte/second the maximum file transfer.

File transfer normal speed Limit in Byte/second the normal file transfer.

7.6 Windows file server

See also *Shared folders*

Workgroup/NetBIOS domain name The value can be changed only with LDAP accounts provider and defines the Windows workgroup name visible from Network neighborhood panel in Windows systems. With Active Directory accounts provider the value is determined by the joined domain

When a new file or directory is created in a shared folder Decide who owns a newly created file or directory: either the resource creator or the current owner of the directory containing the new resource (also known as parent directory)

Grant full control on home directories to Domain Admins group (home$ share) Allow members of `Domain Admins` group to connect the hidden `home$` share and grant them administrative access to any home folder inside of it

Grant full control on shared folders to Domain Admins group Allow members of `Domain Admins` group to connect any shared folder and grant them administrative access on its content

7.7 Reverse proxy

This page configures certain paths and virtual host names under Apache to be served by forwarding the original web request to another URL. See also *Reverse proxy*.

7.7.1 Create / Edit

Name The URL **path name** or the **virtual host name** (an host FQDN). A path name will match URLs like `http://somehost/<path name>/...`, whilst a virtual host name will match an URL like `http://<virtual host name>/...`. Matching URLs are forwarded to the *Target URL*.

Access from CIDR networks Restrict the access from the given list of CIDR networks. Elements must be separated with a "," (comma).

SSL/TLS certificate Select a certificate that is compatible with the virtual host name.

Require SSL encrypted connection If enabled, the URL path or virtual host name can be accessed only with an SSL/TLS connection.

Target URL The URL where the original request is forwarded. An URL has the form `<scheme>://<hostname>:<port>/<path>`.

Accept invalid SSL certificate from target If the *Target URL* has the `https` scheme, accept its certificate even if it is not valid.

Forward HTTP "Host" header to target When enabled, this option will pass the HTTP "Host" header line from the incoming request to the proxied host, instead of the "hostname" specified in the *Target URL* field.

7.7.2 Delete

Removes the selected entry.

7.8 SOGo Groupware

See also *SOGo*.

Enable CalDAV and CardDAV CalDAV allow users to access and share calendar data on a server. CardDAV allows users to access and share contact data on a server.

Enable Microsoft ActiveSync ActiveSync is a mobile data (email, calendar, task, contact) synchronization app developed by Microsoft.

Allow Users to add other IMAP accounts Allow users to add other IMAP accounts that will be visible from the SOGo Webmail interface.

Administrators List of users with administrative privileges over all the user datas.

Notifications Several different types of notifications(email-based) are available. Activate them according your needs.

Make SOGO reachable only from this domain(FQDN) SOGo is per default accessible from all server's virtualhosts, If you specify a domain name here, SOGo will be usable only from this domaine name.

Number of workers This is the amount of instances of SOGo that will be spawned to handle multiple requests simultaneously. You should have at least one worker per activesync device connected.

Maximum time in second Parameter used to set the maximum amount of time, in seconds, SOGo will wait before doing an internal check for data changes (add, delete, and update).

7.9 TLS policy

Enforced security level Configures the system services as described in the *TLS policy* section

CHAPTER 8

Indices

- General index

Index

N

O

P

Q

R

S

T

U

V

W

X

Z