NethServer Documentation

Release 7 Final

Nethesis

Oct 14, 2020

Release notes

See also

- Web site
- Community
- Wiki
- Developer manual

CHAPTER 1

Release notes 7

NethServer release 7

- ISO release 7.8.2003 “final” replaces any previous ISO 7.7.1908
- This release is based on CentOS 7 (2003)
- 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

1.1 Major changes on 2020-05-05

- ISO release 7.8.2003 “final” replaces any previous ISO 7.7.1908
- The new Server Manager implementation based on Cockpit is now marked as stable
- On new installations, the *System* > *Settings* > *Shell policy* > *Override the shell of users* option is enabled by default. Normal users will be able to log in to the new Server Manager only if *System* > *Settings* > *User settings page* > *Enable user settings page* option has been enabled, or if the user has been delegated to access at least one module.

  SSH access is limited to `root` and users inside the designated administrative group (`Domain Admins` by default). More granular permissions can be tuned from the *SSH* page.
- All IMAP actions will be logged by default into `/var/log/imap`
- Shared seen flag is enabled by default for shared mail folders
- Mail server connection limit for each user has been increased to avoid errors on web mail clients
- When creating a new POP3 connector, filter check is disabled by default

- OpenVPN roadwarrior server will use the `subnet` topology as default
- To increase security, when authentication mode is set to `Username, Password and Certificate`, OpenVPN roadwarrior server will enforce a match between user name and certificate CN
- Default maximum PHP memory size has been increased from 128MB to 512MB
- Nextcloud now uses PHP 7.3 stack to improve performance and support widely used plugins
- Ejabberd has been upgraded to 20.03
- POP3 proxy (P3Scan) has been deprecated and can't be installed anymore from Software Center
- PHP 7.1 is now obsolete and has been removed from upstream repositories: restored machines will need to migrate custom applications to PHP 7.2 or higher

1.2 Major changes on 2019-10-07

- ISO release 7.7.1908 "final" replaces any previous ISO 7.6.1810
- The new Server Manager implementation based on Cockpit reached Beta stage and is available by default on new installations. Existing systems can add the new Server Manager module from the Software Center page. See also *Accessing the Server Manager*.
- The *Software updates origin* (locked/unlocked) feature was removed from the "Software Center" page. NethServer can be upgraded manually from the Software Center page when the next "point release" is released. See also *Software center*.
- Delta RPM files have been removed by the upstream distribution and are no longer available from YUM repositories
- OpenSSH configuration was removed from TLS policy settings and reverted to upstream defaults.
- Starting with the new Server Manager based on Cockpit, the Mail module feature *Shared mailboxes* has been renamed to *Public mailboxes*.
- The *Junk* public mailbox is created during the Mail module installation, granting IMAP access to the root user; further permissions can be added from the new Server Manager Email application or with an IMAP/ACL client, like Roundcube.
- Only users with enabled shell can access the new Server Manager. From the old Server Manager, go to the *Users and groups* page and enable the *Remote shell (SSH)* option for the selected user. From the new Server Manager, go to the *Users and groups* page and enable the *Shell* option for the selected user.
- Official ClamAV antivirus signatures are disabled by default.
- The web interface for selective restore has been removed from the old Server Manager. A new one is available inside Cockpit, see *Selective restore of files*.
- As default, the disk usage analyzer (duc) scans only the root file system contents. Other mount points are ignored.

1.3 Major changes on 2018-12-17

- ISO release 7.6.1810 "final" replaces any previous ISO 7.5.1804
- PHP 5.6 from SCL has reached end-of-life and is thus deprecated. See *PHP 5.6 SCL*
- Default TLS policy is `2018-10-01`

- Default systems log retention has been increased to 52 weeks
- The Zeroconf network protocol is now disabled by default
- By default, Evebox events are retained for 30 days. The new default is applied to upgraded systems as a bug fix
- NDPI module has been updated to version 2.4 which no longer recognize some old protocols. See *NDPI 2.4* for the list of removed protocols
- SMTP server can be directly accessed from trusted networks
- PPPoE connections use rp-pppoe plugin by default to improve network speed
- For repositories that support GPG metadata signature, YUM runs now an integrity check (`repo_gpgcheck=1`) for additional security. This new default setting is applied automatically unless a `.repo` file was changed locally. In that case an `.rpmnew` file is created instead of overwriting the local changes. Rename the `.rpmnew` to `.repo` to apply the new defaults. This is the list of files to be checked:
  - `/etc/nethserver/yum-update.d/NsReleaseLock.repo`
  - `/etc/yum.repos.d/NethServer.repo`
  - `/etc/yum.repos.d/NsReleaseLock.repo`

1.4 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*. 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

1.5 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

1.6 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

1.7 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

1.8 Deprecated features and packages

1.8.1 PHP 5.6 SCL

PHP 5.6 from the SCL repository has reached end-of-life (EOL)[1][2].

To avoid problems with existing legacy applications, the PHP 5.6 SCL packages from CentOS 7.5.1804 will be still available from NethServer repositories during the 7.6.1810 lifetime.

Warning: PHP 5.6 SCL packages will **not** receive any security update. Very limited support will be provided as best-effort

The `nethserver-rh-php56-php-fpm` package will be removed from the next NethServer release.

Developers are invited to update their modules, replacing `nethserver-rh-php56-php-fpm` with `nethserver-rh-php71-php-fpm` as soon as possible.

1.8.2 NDPI 2.4

The following protocols have been removed:

- tds
- winmx
- imesh
- http_app_veohtv
- quake
- meebo
- skyfile_prepaid
- skyfile_rudics
- skyfile_postpaid
- socks4
- timmeu
- torcedor
- tim
- simet
- opensignal

[1] Red Hat Software Collections Product Life Cycle – https://access.redhat.com/support/policy/updates/rhscl
[2] PHP supported versions – http://php.net/supported-versions.php

- 99taxi
- easytaxi
- globotv
- timsomdechamada
- timmenu
- timportasabertas
- timrecarga
- timbeta

Rules using the above protocols, will be automatically disabled.

1.9 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.

1.9.1 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
```

1.9.2 User shared mailbox

If you want to enable user shared mailbox, execute:

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

1.9.3 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

References

CHAPTER 2

Installation

2.1 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.

2.1.1 Hardware compatibility

NethServer is compatible with any hardware certified by Red Hat® Enterprise Linux® (RHEL®), listed on the hardware vendor website or at Red Hat Customer Portal.

2.2 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

2.3 Installing from ISO

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

2.3.1 Media creation

Download the latest 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.

2.3.2 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*.

2.3.3 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.

2.3.4 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*

2.4 Install on CentOS

It is possible to install NethServer on a fresh CentOS minimal installation using a couple of commands. 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
```

2.5 Next steps

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

CHAPTER 3

Accessing the Server Manager

Note: Documentation about the old Server Manager is available here.

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:9090` or `https://server_name:9090` where *a.b.c.d* and *server_name* respectively are the server IP address and name configured during installation.

Since the Server Manager uses a self-signed SSL certificate as default, the first time you access the server you should explicitly accept the certificate. Despite the warning, the connection is safe and encrypted, but you are advised to configure a valid certificate, later.

3.1 Login

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`.

Besides root, all users with a *delegated* panel can access the Server Manager.

The web interface language is automatically chosen depending on your browser configuration. If you wish to change the language, go to your user name on the upper right corner of the screen and select *Display Language*.

3.1.1 Login to remote servers

The login page allows access the local machine (default) or a remote one. To access a remote server, first make sure the server is accessible using SSH. Then click on *Other options* and enter the host name (or IP address) of the remote server inside the *Connect to* field.

The Server Manager will try to access the remote machine using SSH on port 22. If the remote server use a different port, you can specify it with the `host:port` syntax (eg. `a.b.c.d:222`).

3.2 Hints

After login, the system is ready to be used but you're advised to review the list of hints which will guide you to correctly configure the machine. Hints are shown as yellow markers with a number over the left menu items.

As best practice you should at least:

- change the default root password
- set the correct date and time

3.3 Change the current password

All users with access to the Server Manager can change their own password from the *Settings* menu.

Users without shell access should use the old Server Manager. See access-section.

3.4 Logout

Terminate the current Server Manager session by going to your user name on the upper right corner of the screen and by clicking on *Log Out*.

CHAPTER 4

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.

4.1 Registering the system

1. Access *Subscription* page from the old or new 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.

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

4.2 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 nethserver-subscription-save
```

If you have installed the *new server manager* AKA *cockpit*, you can unsubscribe the machine in the *Subscription* page, clicking on **Unsubscribe** button.

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

CHAPTER 5

Software center

Note: For the old Server Manager see software_center_legacy-section.

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

An *application* 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.

5.1 Applications installation

The *Applications* section lists all modules that can be installed. This list can be filtered by category. To **install an application**, check the corresponding box and click on *Install applications*.

Once a module has been installed, it is listed under the *Applications* page.

5.2 Software updates

5.2.1 Enterprise and community subscriptions

NethServer receives controlled updates from a set of managed software repositories. See *Automatic update procedure* to receive new features and fix bugs and security issues.

[1] RPM Package Manager – http://rpm.org

5.2.2 Community without subscription

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. Only updates for the current system release (i.e. "7.6.1804") are considered, until a manual upgrade to the next system release is started.

More info about CentOS updates:

- 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 immediately available from the official EPEL mirrors. As EPEL is not bound to the current system release number, the *Software Center* always installs the latest available software versions from EPEL.

More info about EPEL updates:

- https://fedoraproject.org/wiki/EPEL

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]

Manual update procedure

When updates are available, the list of new packages is available under the *Updates* section.

Further details are available clicking the *Changelog* button.

To expand the list of updates, cick on the *Details* button, you can then update a single NethServer package by clicking on the *Update* button. To start a full system update click the *Update all* button.

Hint: On community machines without any type of subscription, remember to regularly update the installed software to fix bugs, security issues and receive new features

---

[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

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. To configure the update policy click on the *Configure* button.

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

References

CHAPTER 6

Base system

Note: Documentation about the old Server Manager is available here.

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

The default installation includes the following main modules:

- *System*
- *Applications*
- *Software center*
- *Terminal*
- *Subscription*

While the *root* user can see all configuration pages, access of each section and application may be also delegated to specific users. See *Role delegation*.

Many Server Manager applications use netdata to display useful charts. Since netdata is not installed by default, you can install it from *Software center*.

6.1 System

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

From the system dashboard, the administrator can:

- change the machine FQDN and server *Alias*
- set upstream *DNS* servers
- configure date-time-section

- customize the organization details

The basic system includes also:

- *Network*
- *Services*
- *Backup*
- server_certificate-section
- *Users and groups*
- *TLS policy*
- *DHCP and PXE server*
- *DNS*
- *SSH*
- *Storage*
- trusted_networks-section
- duc-section
- *Settings*
- *Logs*

6.1.1 Network

Besides all features available in the old Server Manager (see network-section), this page allows to:

- check network status with integrated diagnostic tools like ping, trace route and name lookup
- create a logical network interface without a role: such an interface can be used later in other modules like Dedalo hotspot

6.1.2 Services

A remote system can connect to a network service, which is a software running on NethServer itself.

Each service can have a list of "open" ports accepting local or remote connections. To control which zones or hosts can access a network service, see *Firewall*.

Existing services can be started and stopped directly from the *Services* page.

6.1.3 Storage

The storage section configures and monitors disks. The administrator can mount new local or remote disks, manage RAID arrays and LVM volumes.

6.1.4 SSH

The SSH page displays the number of current SSH connections. From this section the administrator can change the OpenSSH listening port, disable root login and password authentication.

By default, SSH access is limited to `root` user and all users inside the designated administrative group (`Domain Admins`). It is possible to selectively grant SSH and SFTP access to some groups, while administrators are always granted access to SSH and SFTP.

SSH and SFTP permissions are available once the *System* > *Settings* > *Shell policy* > *Override the shell of users* has been enabled. If *Override the shell of users* is disabled, only users with *Shell* option can access the Server Manager, and delegation is not required any more.

6.1.5 Settings

The settings page allows the configuration of some options which could impact multiple system applications.

Smart host

Many system applications, like cron, can generate mail notification. If the server can't directly deliver those mails, the administrator can configure a SMTP relay. When the smarthost is enabled, all mail messages will be delivered to the configured server.

Email notifications

As default, notifications are sent to the local root maildir. The administrator can change the root forward address adding one or more mail address to the *Destination* field.

It's also a good practice to set a custom *Sender address*: messages from the root user (like cron notifications) will be sent using the specified address. A good value could be: `no-reply@<domain>` (where `<domain>` is the domain of the server). If not set, messages will be sent using `root@<fqdn>` as sender address.

Server Manager

As default, access to the Server Manager is granted from all firewall zones. From this section the administrator can restrict the access to the Server Manager only to a list of trusted IP addresses.

Log files

All log files are managed by logrotate. Logrotate is designed to ease administration of a large numbers of log files. It allows automatic rotation, compression, and removal of log files. Each log file may be handled daily, weekly, monthly.

The administrator can set logrotate defaults from this page. The configuration will apply to all applications. But please note that some applications can override such configuration to meet specific needs.

Configuration hints

Most Server Manager pages can display some configuration hints to help guide the administrator on a better system configuration. Hints are just suggestions and can be disabled from this menu.

Password change

The settings page also includes a panel to let users change their password, including the root user.

Shell policy

This setting can be used to enable or disable the shell that is needed to use new Server Manager and the SSH service. If this option is enabled the user's shell setting under the *Users and Groups* page is ignored and it is considered always enabled.

User settings page

When the *Enable user settings page* options is enabled, users can change their password and other settings on a web page outside Cockpit (on port 443). The default page is */user-settings*. This feature can be enabled only if *Shell Policy* is enabled as well.

The access to the page can be limited only from Trusted Networks.

6.1.6 Logs

The system provides an indexed log named journal. Journal can be browsed from this page: messages can be filtered by service, severity and date.

6.2 Applications

The *Applications* page lists all installed applications. An application is a Server Manager module usually composed by multiple pages including a dashboard, one or more configuration sections and the access to application logs. A click on the *Settings* button will open the application.

There are also simpler applications which include only a link to an external web pages. To access such applications click on the *Open* button.

6.2.1 Shortcuts

The administrator can add shortcuts to applications which are frequently used. Applications with a shortcut, will be linked to the left menu.

Only *root* user has access to this feature.

6.2.2 Add to home page

Launcher is an application of the new Server Manager available to all users on HTTPS and HTTP ports. The launcher is accessible on the server FQDN (eg. `https://my.server.com`) and it's enabled if there is no home page already configured inside the web server (no index page in `/var/www/html`)

Installed applications can be added to the launcher by clicking on the *Add to home page* button. All users will be able to access the public link of the application.

Only *root* user has access to this feature.

6.2.3 Removing applications

To remove an installed module click *Remove* button on the corresponding application.

> **Warning:** When removing a module other modules could be removed, too! Read carefully the list of affected packages to avoid removing required features.
>
> This feature is not available in NethServer Enterprise.

6.3 Terminal

Execute a standard shell inside a terminal directly accessible from the browser. The shell and the processes will run with the user privileges.

6.4 Role delegation

On complex environments, the *root* user can delegate the access of some section to specific groups of local users.

A local user can be delegated to access:

- one or more pages of the *System* section
- one or more installed applications
- one or more main sections between *Subscription*, *Software Center*

Role delegation is based on local groups, each user belonging to the group will be delegated. Users inside the *domains admins* are automatically delegated to all panels.

To create a new delegation, access the *User & Groups* page under the group section, then edit an existing group or create a new one. Select one or more items from the *System views* and *Applications* menus.

Even if a user has been delegated, it must be explicitly granted the shell access before being able to log into the Server Manager.

The following pages are always accessible to all users:

- dashboard
- applications
- terminal

6.5 Two-factor authentication (2FA)

Two-factor authentication (2FA) can be used to add an extra layer of security required to access the new Server Manager. First, users will enter user name and password, then they will be required to provide a temporary verification code generated by an application running on their smartphone.

2FA is disabled by default. Each user can enable it by accessing the *Two-factor authentication* section under *Settings* page, then following these steps:

1. download and install the preferred 2FA application inside the smartphone
2. scan the QR code with the 2FA application

3. generate a new code and copy it inside *Verification code* field, than click *Check code*
4. if the verification code is correct, click on the *Save* button

Two-factor authentication can be enabled for:

- the new Server Manager
- SSH when using username and password (access with public key will never require 2FA)

6.5.1 Recovery codes

Recovery codes can be used instead of temporary codes if the user cannot access the 2FA application on the smartphone. Each recovery code is a one-time password and can be used only once.

To generate new recovery codes, disable 2FA, then re-enable it by registering the application again following the above steps.

6.5.2 Smartphone applications

There are several commercial and open source 2FA applications:

Available for both Android and iOS:

- FreeOTP: available for both Android and iOS
- Authenticator: available on iOS only
- andOTP: available for both Android and iOS https://github.com/andOTP/andOTP

6.5.3 Emergency recovery

In case of emergency, 2FA can be disabled accessing the server from a physical console like a keyboard and a monitor, a serial cable or a VNC-like connection for virtual machines:

1. access the system with user name and password
2. execute:

```
rm -f ~/.2fa.secret
sudo /sbin/e-smith/signal-event -j otp-save
```

Eventually, the root user can retrieve recovery codes for a user. Use the following command and replace `<user>` with the actual user name :

```
oathtool -w 4 $(cat ~<user>/.2fa.secret)
```

Example for user `goofy`:

```
# oathtool -w 4 $(cat ~goofy/.2fa.secret)
984147
754680
540025
425645
016250
```

CHAPTER 7

Users and groups

7.1 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.

7.1.1 Choosing the right account provider

Besides 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.

7.1.2 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.

Warning: The NethServer OpenLDAP account provider does not fully support the user password expiration. Refer to *Effects of expired passwords* for more information

7.1.3 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.

The Linux Container root directory is `/var/lib/machines/nsdc/` and requires the filesystem support to Posix ACLs. The default XFS filesystem has a builtin support for Posix ACLs and no special configuration is required. For other filesystems (i.e. EXT4) enable the ACLs as explained in *Shared folders requirements*.

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.

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

VMWare

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

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]

7.1.4 Local accounts provider uninstall

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 and delete 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
```

7.1.5 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.

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

- 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!

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 successfully joined AD, specify the **dedicated user account** credentials in *Accounts provider* > *Authentication credentials for LDAP applications*.

7.1.6 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*

7.2 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 access to services without deleting the account. The safest approach is:

- lock the user using the *Lock* action
- (optionally) change the user's password with a random one

Note: When a user is deleted, the home directory and personal mail box will be also deleted.

7.2.1 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*.

7.2.2 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*.

7.2.3 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
```

7.3 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.

7.4 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 a password. Also remember to enable the shell if the admin user must access the new Server Manager.

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
```

7.5 Password management

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

Password policies can be changed from web interface.

7.5.1 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.

7.5.2 Expiration

The password expiration is **NOT** enabled by default.

Each time a user changes his password, the date of the password change is recorded and, if *Password expiration for users* option is enabled, the password is considered expired when the *Maximum Password Age* has elapsed.

For example, given that

- last password was set in January,
- in October the *Maximum Password Age* is set to `180 days` and *Password expiration for users* is enabled

thus the password is **immediately considered expired** (January + 180 days = June!).

7.5.3 Effects of expired passwords

> **Warning:** **no email notification related to password expiration** is sent by the server!

The effects of an expired password depend on the configured accounts provider.

When a password is expired

- with `Active Directory` (both local and remote) a user **cannot authenticate** himself **with any service**;
- with a NethServer `LDAP` accounts provider (both local and remote) **some services ignore the password expiration** and grant access in any case.

Examples of services that do not fully support the password expiration with NethServer LDAP accounts provider:

- NextCloud
- WebTop (contacts and calendars are available)
- SOGo

. . . and other services that authenticate directly with LDAP

7.6 Import and delete accounts from plain-text files

7.6.1 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>/scripts/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 ','
```

7.6.2 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 and delete accounts from plain-text files* for a sample script invocation.

7.6.3 Import groups

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

```
group1 <TAB> user1 <TAB> user2 <NEWLINE>
group2 <TAB> user1 <TAB> user2 <TAB> user3 <NEWLINE>
```

Example:

```
faxmaster <TAB> matteo <TAB> luca <NEWLINE>
managers <TAB> marco <TAB> francesco <TAB> luca <NEWLINE>
```

then execute:

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

For example, if the group file is `/root/groups.tsv`, execute following command:

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

Group management is also 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
```

7.6.4 Delete users

It is possible to delete user accounts from a file with the following format:

```
user1
user2
...
userN
```

Example:

```
mario <NEWLINE>
```

then execute:

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

Tip: You can also use the same import users file to delete the users.

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/delete_users /root/users.tsv
```

Alternative separator character:

```
delete_users users.tsv ','
```

CHAPTER 8

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 from the old Server Manager. Otherwise click on the DNS address inside the *Dashboard* of the new Server Manager.

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

8.1 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.

8.2 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.

8.3 Domain redirection

The administrator can override the upstream DNS for specific domains. A typical usage scenario is setting the Active Directory server as resolver for the queries to the internal domain.

Such changes can be done by editing the `DomainRedirection` property via command line. The property accepts a comma-separated list of couples in the form `<domain>:<ip_address>`.

Example:

```
config setprop dnsmasq DomainRedirection my.local.domain.org:192.168.1.1,my.domain.
↪com:192.168.1.2
signal-event nethserver-dnsmasq-save
```

The `my.domain.org:192.168.1.1` configuration will send all queries for `my.local.domain.org` to `192.168.1.1`.

The special server address `#` can be used to send queries to the default DNS server. Example:

```
config setprop dnsmasq DomainRedirection domain.org:1.1.1.1,sub.domain.org:#
signal-event nethserver-dnsmasq-save
```

In this example all queries for `domain.org` will be sent to `1.1.1.1`, while queries for `sub.domain.org` will be sent to default upstream DNS.

CHAPTER 9

DHCP and PXE server

The *Dynamic Host Configuration Protocol* (DHCP)[1] server centralizes the management of the local network configuration for any device connected to it. When a computer (or a device such as a printer, smartphone, etc.) connects to the local network, it can ask the network configuration parameters by means of the DHCP protocol. The DHCP server replies, providing the IP, DNS, and other relevant network parameters.

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

The *Preboot eXecution Environment* (PXE)[3] specification allows a network device to retrieve the operating system from a centralized network location while starting up, through the DHCP and TFTP protocols. See *Boot from network configuration* for an example about configuring a such case.

9.1 DHCP configuration

The DHCP server can be enabled on all *green* and *blue* interfaces (see network-section). 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`.

9.1.1 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.

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

9.2 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.

9.3 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
```

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:

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

```
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

CHAPTER 10

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.

10.1 Policy 2020-05-10

This policy disables the TLS protocol versions 1.0 and 1.1. It applies to the following services:

- Apache (httpd, httpd-admin)
- Ejabberd
- Cockpit
- Slapd (openldap-servers)
- Postfix
- Dovecot

Reference: https://access.redhat.com/articles/1462183

10.2 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
```

10.3 Policy 2018-06-21

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

- Apache
- Dovecot
- 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
```

10.4 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

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
```

10.5 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 11

Web server

Note: This chapter describes the features of the *Web server* application, available in the new Server Manager.

After NethServer has been installed the *Web server* application is already available. It configures and starts the Apache HTTP web server.

The *Web server* application provides the following features:

- Apache HTTP web server
- Integration with system certificates for HTTPS
- Hosting of multiple web sites
- HTTP reverse proxy
- PHP scripting language to run web applications
- FTP server

The following sections describe the pages of the *Web server* application. Some of them require additional software components that are automatically downloaded, installed and configured when they are required for the first time.

11.1 Web server dashboard

The *Web server dashboard* page shows the current web server status and statistics. It also lists the additional components installed on the system.

The default Apache configuration serves the contents of `/var/www/html` and is capable of executing PHP scripts by running them on the *Default web stack*.

11.2 Settings

The *Settings* page allows to change the PHP configuration parameters for resources allocation (e.g. script maximum memory and execution time).

Changes affect the global PHP configuration: as such they are valid for both web applications and command line scripts, unless they are overridden by some means.

PHP settings can also be adjusted for a specific web site from the *Virtual hosts* page (see also *PHP versions and configuration*), or overridden with a custom configuration file. To this end,

1. for PHP 7.2, look at current PHP-FPM settings in `/etc/opt/rh/rh-php72/php-fpm.d/000-virtualhost.conf`;
2. create a file under the same directory (e.g. `/etc/opt/rh/rh-php72/php-fpm.d/001-custom.conf`) and refer to the official PHP-FPM documentation to adjust the pool directives;
3. add the created file to your *configuration backup*.

11.3 Virtual hosts

Multiple web sites can be hosted on NethServer. It is possible to configure the web site hosting space in the *Virtual hosts* page.

When a new virtual host is created with one or more *server names* the new Server Manager contextually creates a server alias name in the local DNS service for each of them.

Note: A server alias name is accessible from web clients if they use the NethServer itself as their DNS server. For public web sites, refer to your DNS provider documentation and ensure the server alias name is correctly set in the public DNS.

Server alias names are listed and can be changed from the new Server Manager *dashboard*.

11.3.1 Web site access restrictions

It is possible to limit how the web clients access the web site with the following options, available under the *Advanced settings* section.

1. Enable the option *Allow access from trusted networks only*. Refer to trusted_networks-section for more information.
2. Enable the switch *Require HTTP authentication* to grant access only if the specified password is provided by the client. Web applications usually provide an authentication method by themselves: this option could be useful to protect the contents of static web sites.
3. If the web site must be always accessed through an encrypted channel it is possible to enable the *Require SSL encrypted connection* option. Any resource request received over the HTTP protocol is redirected over HTTPS.

11.3.2 SSL/TLS certificate

Each virtual host can be assigned a reserved *SSL/TLS certificate* or rely on the default system one. In any case, the virtual host names must be present among the certificate alternative names, otherwise the web clients can refuse to connect.

11.3.3 Configuring a web application

When a new virtual host is created a web root directory is created as well. The full web root path is displayed under *Virtual hosts* > *List* > *Web root path*.

If the switch *Enable FTP access* is enabled, it is possible to upload data, configuration and script files to the web root path using a FTP client.

Hint: HTTP authentication password should be different from the FTP one, because FTP is used to upload the virtual host contents whilst HTTP is used to see them from the web.

The web site displays a "Welcome" page until a file named `index.html` or `index.php` is uploaded under the web root directory. If this is not desired, it is possible to enable the option *Root directory file listings*, as alternative to the "Welcome" page.

FTP uploaded files are owned by the *apache* group with read-only permissions. If write or execution permissions are needed, a FTP client can be used to grant them.

Warning: If a web site contains executable code, such as PHP scripts, the security implications of file permissions must be evaluated carefully. Grant write access to a limited set of special files and directories, as required by the web application documentation.

The Apache configuration can be overridden by uploading a file named `.htaccess`. Refer to the official Apache documentation for more information about this feature[1].

11.3.4 PHP versions and configuration

If the PHP version provided by the *Default web stack* does not fit a web application it is possible to select and install an alternative one and override the global PHP default settings, as explained by the *Settings* section.

11.3.5 Disabling a virtual host

The *Disable* action hides the virtual host, making it not accessible from web clients. This operation is reversible, by selecting the *Enable* action.

11.3.6 Deleting a virtual host

The *Delete* action removes the virtual host configuration and erases the web root directory. This operation is not reversible.

11.4 Reverse proxy

As alternative to a virtual host, which stores static files or a PHP web application under a local web root directory, it is possible to forward web requests to another HTTP server and serve responses in behalf of it. This behavior can be configured from the *Reverse proxy* page.

Each reverse proxy item is actually a rule that can match an incoming web request. Depending on the rule *Name* field value, the match can occur in either:

[1] Apache documentation for `.htaccess` files https://httpd.apache.org/docs/2.4/howto/htaccess.html

A) the requested **web site name**, if *Name* starts with any character, but the slash /, or

B) the requested **resource path**, if *Name* starts with a slash / character.

If the rule matches, the request is forwarded to another web server, defined by the *Destination URL* field.

11.4.1 Advanced reverse proxy settings

When the reverse proxy rule matches a **web site name** it is possible to assign it a dedicated certificate, choosing one from the *SSL/TLS certificate* list.

It is not possible to select the certificate if the rule matches a **resource path**. In this case only the default certificate can be used.

Regardless the rule type, the following settings are also available:

- *Access from CIDR networks*: restricts the access from the given list of CIDR networks. Only web clients connecting from those networks are allowed to open the web site.
- *Require SSL encrypted connection*: if enabled, any *http://* request is redirected to *https://*.
- *Accept invalid SSL certificate from target*: if the destination URL starts with *https://* and an invalid certificate is returned, enabling this option ignores the certificate validation error.
- *Forward HTTP "Host" header to target*: if enabled, a HTTP *Host* header containing the original request host name is forwarded to the destination URL. This could be required by the destination server application to work properly.

11.5 FTP server

Warning: The FTP protocol is unsecure. Passwords and file data are sent in clear text over the network.

The File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server[2]. The *FTP* page enables the FTP service and configures additional user accounts limited to the FTP service only.

Users of the FTP service can be restricted to access their own home directory by enabling *Chroot user on home directory*. When this option is enabled the user cannot see the other system directories. This configuration is also known as *jailing*.

When a virtual host is created, a random FTP user name is assigned to it. It is possible to upload the virtual host file contents with FTP. Refer to *Configuring a web application* for more information.

References

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

CHAPTER 12

Firewall

NethServer can act as firewall and gateway inside the network where it 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. Firewall mode is enabled only if the system has at least one network interface configured with red role.

The Firewall application can be installed from *Software center* and includes:

- Multi WAN support up to 15 connections
- Firewall rules management
- Traffic shaping (QoS)
- Port forwarding
- Routing rules to divert traffic on a specific WAN
- Deep packet inspection (DPI)
- Smart search to quickly find existing rules or objects
- Real time charts

Real time charts display traffic and service statistics collected by Netdata. To avoid performance penalty on slow hardware, Netdata is not part of the firewall application and can be installed from *Software center*.

12.1 Apply and revert

Every time the firewall configuration has been changed, modifications are not applied immediately but saved in a temporary store. For the changes to take effect, click on the *Apply* button at the top right corner of the page.

As long as the new rules created have not been applied, you can revert all changes by clicking the *Revert* button at the top right corner of the page.

12.2 Policy

Each interface is identified with a color indicating its role within the system. See network-section.

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:

- *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.

To change the default policy for Internet access, enable or disable the *Traffic to Internet (red interface)* option from the *Settings* page. Policies can be changed also by creating specific rules between zones from the *Rules* page.

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.

To display the list of active policies click on the *Policies* button inside the *Rules* page.

12.3 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 matches 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 five main parts:

- Action
- Source
- Destination
- Service (optional)
- Time condition (optional)

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

Source and destination fields accept built-in roles, *Firewall objects* and raw IPv4 addresses or CIDR. Such raw addresses can be later converted to firewall objects using the *Create Host* and *Create CIDR subnet* actions which will appear next to the address itself.

If *VPN* application is installed, there are also two extra zones available:

- *ivpn*: all traffic from IPSec VPNs
- *ovpn*: all traffic from OpenVPN VPNs

The configuration of firewall rules is split into two different pages:

- **Rules**: manage rules applied only to the network traffic traversing the firewall.
- **Local rules**: manage rules applied only to the network traffic generated from the firewall, or directed to the firewall itself.

When creating new rules, only the most common fields are shown. To show other less common parameters click the *Advanced* label.

Note: If no red interface has been configured, the firewall will not generate rules for blue and orange zones.

12.3.1 REJECT vs DROP

As a general rule, you should use REJECT when you want to inform the source host that the port 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 disclosed to any attacker.

12.3.2 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. The log can be inspected from the command line or using the *Logs* page.

12.3.3 Deep Packet Inspection (DPI)

Deep Packet Inspection (DPI) 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 DPI module uses the nDPI library which can identify around 250 types of network traffic split in network protocols (eg. OpenVPN, DNS) and web applications (eg. Netflix, Spotify).

Firewall rules using DPI services are generated inside the mangle table, for this reason such rules have some limitations:

- *reject* action is not supported, use *drop* to block traffic
- *any* and *firewall* can't be used as source or destination
- *route to provider X* action is not supported: the identification of the protocol often begins after the connection has been already established, so the routing decision can't be changed

Even if DPI can identify traffic to/from specific web sites such as Facebook, it is better suited to block or shape protocols like VPN, FTP, etc. Web site access should be regulated using *Web proxy*.

Note that some DPI protocols (such as Amazon) can match large CDNs, so please do not block such protocols using DPI rules unless you want to prevent access to thousands of sites.

DPI markers are automatically applied also to the traffic which originates from the firewall itself, like HTTP traffic from the web proxy.

The complete list of DPI protocols, along with counters for matched traffic, is available inside the *DPI* page under the *Status* category on the left menu.

12.3.4 Rules on existing connections

When a new rule is created, as default, it is applied only to new connections. But in some scenarios, the administrator may need to apply the rule also on established connections.

If the option *Apply to existing connections* is enabled, the rule will be applied to all connections including already established ones.

12.3.5 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: -

12.4 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 that actually manages the WAN link.

All WAN network interfaces are labeled with the red role and are listed on the top of the page, just below bandwidth usage charts. Rules can be created under the *Rules* section on the same page.

If the server has two or more configured red interfaces, it is required to correctly fill, *Download bandwidth* and *Upload bandwidth* fields from the *Network* page. Download and upload bandwidth can be automatically calculated using the *Speedtest* button.

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

The system can use WAN connections in two modes:

- *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

To change WAN mode and link monitoring options click on *Configure* button.

The network traffic can be routed to specific WANs by creating rules inside the *Rules* section on this page. After creating or editing rules, make sure to apply the changes. See <apply_revert-section> for details.

12.4.1 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.

12.5 Port forward

The firewall blocks requests from public networks to private ones. For example, if a web server is running inside the LAN, only computers on the local network can access the service in 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 network protocol like TCP, UDP, TCP & UDP, AH, ESP or GRE
- 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 the separator in the source port field (eg: 1000:2000), in this case, the destination port field must be left empty

Port forwards are grouped by destination host and support raw IP addresses along with firewall objects.

By default, all port forwards are available only for hosts inside the WAN. Check the *Enable hairpin NAT* option under the *Settings* page to make all port forwards available also from local networks.

12.5.1 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 the 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 the 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 the firewall's red interfaces on the port range between 5000 and 6000 will be redirected to the same ports on Server1.

12.5.2 Limiting access

By default, the field access to port forward is granted to anyone. You can restrict access to port forward only from some IP addresses or networks by adding entries to *Restrict access to* field. This configuration is useful when services should be available only from trusted IPs or networks.

Example of valid entries:

- `10.2.10.4`: enable port forward for traffic coming from 10.2.10.4 IP
- `10.2.10.0/24`: enable port forward only for traffic coming from 10.2.10.0/24 network

12.6 SNAT 1:1

One-to-one source NAT (SNAT) 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. SNAT is available only if there is at least one IP alias configured on red network interfaces.

This feature only applies to network traffic from a host inside the local network to the public Internet. It does not affect in any way the traffic from the 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.

12.6.1 Example

In our network we have a 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.

12.7 Traffic shaping

Traffic shaping allows applying priority rules on network traffic through the firewall. In this way, it is possible to optimize the transmission, control 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 the *Speedtest* button or 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.

Traffic shaping classes are used to commit bandwidth for specific network traffic. Configuration of traffic shaping is composed of 2 steps:

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

12.7.1 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 committed 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
- *Description*: optional description for the class

Limits under *Download bandwidth limits* section:

- *Min*: minimum reserved download bandwidth, if empty no download reservation will be created
- *Max*: maximum allowed download bandwidth, if empty no upper limit will be set

Limits under *Upload bandwidth limits* section:

- *Min*: minimum reserved upload bandwidth, if empty no upload reservation will be created

- *Max*: maximum allowed download bandwidth, if empty no upper limit will be created

For each class the bandwidth can be specified using the percentage of available network bandwidth or with absolutes values expressed in kbps. As default, a traffic shaping class is applied to all red network interfaces. Such behavior can be changed by selecting an existing red interfaces under the *Bind to* menu inside the *Advanced* section.

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.

Network traffic can be shaped by creating rules under the *Rules* section in this page. After creating or editing rules, make sure to *apply* the changes.

For more info, see FireQOS tutorial.

12.8 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`, `goofy_pc`
- **Groups of hosts**: representing homogeneous groups of computers. Hosts in a host group should always be reachable using the same interface. Example: `servers`, `router`
- **IP ranges**: a list of IP addresses expressed as a range. Example: `myrange`, composed by IPs from `192.168.1.100` to `192.168.1.120`
- **CIDR Networks**: you can express a CIDR network in order to simplify firewall rules.

  Example 1 : last 14 IP addresses 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 intended 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.

  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.

- **Services**: a service listening on a host with at least one port and protocol. Example: `ssh`, `https`

- **MAC addresses**: a host identified by a MAC address. The MAC address must be bound to an existing zone.

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.

12.9 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 the 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.

12.10 Connections

This page keeps track of all active connections. Connections can be filter by *Protocol* and *State*. The list of connections is not refreshed in real time. To list new connections click the *Refresh* button.

The administrator can delete a single connection or flush the whole connection tracking table using *Delete all connections* button.

CHAPTER 13

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]
- Antispam filter, antivirus 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 antivirus and antispam 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-section installations are based on the Rspamd filter engine. Previous NethServer installations are automatically upgraded to Rspamd as described in *Email*

[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

module transition to Rspamd

13.1 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 *Copy inbound messages* switch (formerly *Always send a copy (Bcc)* check box).

Warning: On some countries, enabling the *Copy inbound messages* switch 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.

13.1.1 Append a legal notice

Warning: Since NethServer 7.5.1804 this feature is shipped in a separate, optional package: `nethserver-mail-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-mail-disclaimer` RPM was installed from the terminal, 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.

To configure and enable the *disclaimer attachment*, turn on the option switch *Email* > *Domains [List item]* > *Edit* > *Append a legal note to sent messages*.

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:

[9] The Maildir format, https://en.wikipedia.org/wiki/Maildir
[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

```
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
```

13.1.2 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 the *Signature* switch under *Email* > *Domains* > *[list item]* > *Configure 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:

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

13.2 Filter

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

- Attachments
- Antivirus
- Antispam

13.2.1 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.

13.2.2 Antivirus

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

13.2.3 Antispam

The antispam 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.
2. If the spam score is above *Spam flag 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 the *Email* > *Mailboxes [General settings]* > *Configure [Advanced options]* > *Move spam to "Junk" folder* check box (formerly *Email* > *Mailboxes* > *Move to "Junk" folder"* check box).

- 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.

[15] SPAM https://en.wikipedia.org/wiki/Spamming
[14] DNSBL https://en.wikipedia.org/wiki/DNSBL
[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
[17] Bayesian filtering https://en.wikipedia.org/wiki/Naive_Bayes_spam_filtering

- The Bayesian filter **is not active until it has received enough information. This includes a minimum of 200 spams AND 200 hams (false positives).**

  As the system receives that information, the progress of bayesian filter training can be monitored from the *Email* > *Filter [Statistics]* > *Bayes training* progress bar.

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

13.2.4 Rules for white and black lists

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 *Email* > *Filter [Rules]* > *Details* (formerly *Rules by mail address*) allows creating three types of rules:

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

The *Allow* rules have higher precedence over the *Block* ones. As soon as an *Allow* rule matches, the antispam and antivirus checks are skipped, the *Block* rule is not evaluated and the message is accepted.

Warning: **Antivirus and antispam checks are skipped** if an *Allow* rule matches

It is possible to create an *Allow* or *Block* rule even for an entire domain, not just for a single email address: you just need to specify the domain name (e.g. `dev.nethserver.org`).

When a second level domain domain name is specified it matches also its subdomains. For instance `nethserver.org` matches `nethserver.org` itself, `dev.nethserver.org`, `demo.nethserver.org` and so on.

13.2.5 Rspamd web interface

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

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

For more information on Rspamd, please read the *Rspamd* page.

13.2.6 Quarantine (beta)

NethServer scans all incomaing email messages before they are delivered to the user mailbox. The messages that are identified as spam will be sent to a specific user mailbox. The purpose of this feature is to verify the email before deleting it. If enabled, a mail notification is also sent to the postmaster (root alias) for each quarantined email.

Note: The quarantined messages can be accessed using a web mail or an IMAP account

Warning: The mailbox used for quarantine, must be able to accept spam. It should be a local shared mailbox or a user mailbox. If an external account is used, make sure the account exists on the remote server. Please make sure the quarantine mailbox has been created only for this specific purpose, otherwise the mailbox will be overloaded with unwanted spam.

Quarantine is provided by an optional RPM named `nethserver-mail-quarantine`. Once it has been installed from the terminal you must manually set its database properties.

The properties are under the `rspamd` key (configuration database):

```
rspamd=service
...
QuarantineAccount=spam@domain.org
QuarantineStatus=enabled
SpamNotificationStatus=disabled
```

- `QuarantineAccount`: The user or the shared mailbox where to send all spam messages (spam check is automatically disabled on this account). You must create it manually. You could send it to an external mailbox but then make sure to disable the spam check on the remote server
- `QuarantineStatus`: Enable the quarantine, spam are no more rejected: enabled/disabled. Disabled by default
- `SpamNotificationStatus`: Enable the email notification when email are quarantined: enabled/disabled. Disabled by default

For example, the following commands enable the quarantine and the mail notification to root:

```
config setprop rspamd QuarantineAccount spam@domain.org QuarantineStatus enabled␣
↪SpamNotificationStatus enabled
signal-event nethserver-mail-quarantine-save
```

13.3 Mailboxes

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* > *Mailboxes* page. There are three types of mailboxes: Users, Groups and Public mailboxes.

13.3.1 Users mailboxes

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 multiple external email addresses.

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/` .

13.3.2 Groups mailboxes

The *automatic aliases for groups mailboxes* are initially disabled. If enabled, addresses like <*group-name*>@<*domain*> become valid email addresses. A specific group address can be disabled and enabled again in a later stage, once Groups mailboxes are enabled. To disable the automatic aliases globally, refer to *General settings*.

A group mailbox has no disk space for it. When a message is sent to a group mailbox, a copy of it is delivered to the group members, according to their delivery and forward preferences.

13.3.3 Public mailboxes

Note: In the old Server Manager the *Shared mailboxes* label was used in place of *Public mailboxes*.

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

13.3.4 General settings

The *Email* > *Mailboxes [General settings]* > *Configure* page controls what protocols are available to access the user's mailbox:

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

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

Warning: Do not allow unencrypted connections on production environments!

From the same page, the *Quota limit* for each mailbox can be limited to a default quota. If the general mailbox quota is enabled, the *Email* > *Mailboxes* list 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* > *Mailboxes [users item]* > *Edit* > *Custom mailbox quota*.

Messages marked as **spam** (see *Filter*) can be automatically moved into the *Junk* folder by enabling the option *Move spam to "Junk" folder*. Spam messages are expunged automatically after the *Keep spam for* period has elapsed. The spam retention period can be customized for a specific user in *Email* > *Mailboxes [users item]* > *Edit* > *Custom spam 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:

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

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

Additional options:

- If *Groups mailboxes* were enabled in *Email* > *Mailboxes* > *Groups*, unselect the *Automatic alias for groups* check box to disable them again.
- It is possible to record the IMAP actions by enabling *Log IMAP actions*. See also *Logs*.
- Unlike almost any IMAP client, Outlook does not move deleted messages to the trash folder, but simply marks them as "deleted".

  It is possibile to automatically move messages inside the trash folder, by enabling *Move deleted email to trash (Outlook)*.

  You should also change Outlook configuration to hide deleted messages from the inbox folder. This configuration is available in the Outlook options menu.
- *Max user connections per IP* changes the limit of connections for a user coming from the same IP address. This limit could be increased if messages like *Maximum number of connections* appear in the log files (see *Logs*).

13.3.5 *Shared seen* configuration

Users could share their mailbox (or some parts of it, folders) with selected accounts on the system. Everyone who is given access to a shared mailbox can read or delete messages according to permissions granted by the mailbox owner.

An IMAP flag named `/Seen` is used to mark if a message has been read or not. In a shared mailbox, each user has their copy of the messages they have read, but sometimes a team sharing a mailbox could prefer to know if a mail has already been read by someone else. To enable sharing of the `/Seen` flag for all shared mailboxes use the following commands:

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

Please note that changing the `SharedSeen` status resets the `/Seen` flag for all users on all mailboxes.

Public folders are created by the administrator and are usually visible to all users (or large groups). The `/Seen` flag is kept for each user and it cannot be shared.

13.4 Addresses

In addition to the Users, Groups and Public mailboxes addresses, described in the previous section, the system enables the creation of an unlimited number of email addresses, from the *Email* > *Addresses* page. Each *mail address* is associated with one or more destinations. A *destination* can be of the following types:

- user mailbox
- groups mailbox
- public mailbox
- external email address

A mail address 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* bound to any domain: `info@mydomain.net`, `info@example.com`
- Email address *goofy* specific to one domain: `goofy@example.com`

Sometimes a company forbids communications from outside the organization using personal email addresses. The *Internal* check box (formerly *Local network only*) and the *Make internal* and *Make public* action buttons block the possibility of an address to receive messages from the outside. Still an *internal* address can be used to exchange messages with other accounts of the system.

13.5 Connectors

The *Email* > *Connectors* page is described in *POP3 connector*.

13.6 Synchronization

The *Email* > *Synchronization* page is based on an IMAP transfer tool called Imapsync. The purpose is to migrate email messages from a remote IMAP account to a local one.

The migration is recursive and incremental and can be repeated as many times as needed. The emails will be copied locally if they do not exist on the local server.

The system administrator of the local NethServer does not need to know the password of the local user. However, the administrator has to know the password of the remote IMAP account, unless the IMAP admin authentication is implemented also for the remote email server.

If the remote IMAP server is also a NethServer, the IMAP admin user is `vmail` and its password can be read from `/var/lib/nethserver/secrets/vmail`. The username with a `*vmail` suffix (e.g. `username@domain.com*vmail`) and the `vmail` password has to be set in the IMAP synchronization panel.

Note: List of IMAP servers with admin authentication in Imapsync documentation

---

13.7 Queue

The *Email* > *Queue* page lists the messages that are waiting to be relayed in the SMTP mail queue. In normal conditions, this queue should be empty or contain just a few messages.

The *Email* > *Queue [Charts]* > *Show charts* link shows a real-time chart of the mail queue status in the last minutes, updated as the page is left opened. The chart shows the number of message in the queue and the total queue size in kilobytes.

While messages are in the queue, the administrator can request an immediate message relay attempt, by pressing the button *Resend all* (formerly *Attempt to send*), or empty the queue with the *Delete all* button.

It is also possible to selectively *Resend* or *Delete* a queued message, from the action buttons of *Email* > *Queue [List]* items.

13.8 Relay

The *Email* > *Relay* page configures how messages are accepted and routed from the NethServer SMTP server to other SMTP servers.

13.8.1 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. See also *Client configuration*.

To ease the configuration of legacy environments, the *Email* > *Relay [Configuration]* > *Details* section (formerly 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.

Warning: The listed IP addresses are excluded from all mail filtering checks: use this feature only as a last resort

Moreover, in the same section 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.
- By default an authenticated SMTP client has no particular restrictions on setting the SMTP sender address.

  To avoid the unauthorized use of email addresses and the sender address spoofing, enable the *Enforce sender/login match* option.

  If enabled, only addresses associated to the current SMTP login are allowed.

13.8.2 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 the public DNS, the HELO can be changed in the *Custom HELO* text field.

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

13.8.3 Relay hosts

The *Email* > *Relay* page allows to describe the route of an email message, by sending it through an external relay host with specific port, authentication, and TLS settings.

Create a relay host description under *Email* > *Relay* > *Create relay host*.

The relay host is identified by **the SMTP sender address**. It is possible to match the full sender address or only the domain part of it.

13.8.4 Default relay host settings

If the sender address does not match the relay rules described in the above section it is possible (though not recommended) to configure a default relay host instead of relying on the standard SMTP relay rules.

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.

The *System* > *Settings* > *Smart host* section, configures the 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

Refer also to *Smart host* for more information.

13.9 Settings

From the *Email* > *Settings* page, the *Maximum message size* (formerly *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 *Message queue lifetime* (formerly *Queue message lifetime*) slider changes this limit. By default it is set to *4 days*.

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

Warning: On some countries, enabling the *Forward a copy of all messages* can be against privacy laws.

13.10 Logs

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, plus the IMAP actions, if enabled in *General settings*

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

13.11 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.

References

CHAPTER 14

Shared folders

A *shared folder* is a place where files can be accessed by a group of people using Samba (SMB/CIFS).

Shared folder are part of the File server application in the new Server Manager. The application dashboard now integrates the Samba status module, which displays shared folder usage in real time.

To create, edit and delete a shared folder go to the *Shared folders* page.

14.1 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.

14.1.1 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
```

14.2 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.

14.3 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.

14.4 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.

14.5 Hide a shared folder

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

14.6 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.

14.7 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

14.8 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$
```

14.9 Auditing

Note: The audit module has been integrated inside the File server application of the new Server Manager.

Samba audit is a module that keeps track of all users activities on shared folders. Auditing is disabled by default and must be explicitly enabled for each folder.

Actions are logged to a file during the the day and are moved to a browseable database overnight. By default, to avoid the database overloading, read actions like access to files and directories are saved only inside `/var/log/smbaudit.log`. To change this behavior and store read actions inside the database, access the *Settings* page and enable the *Enable auditing of read actions*.

The auditing report is available under the *Audit* page.

The same report is also available from the old Server Manager inside the *Applications* page.

CHAPTER 15

Backup

The backup documentation is split into the following chapters:

- *Settings*: general data backup settings
- *Legacy backup*: configuration from the old Server Manager
- *Disaster recovery*: how to recover a failed system
- *Backup customization*: advanced customization, best practices and command line tools

The system handles two kinds of backups:

- configuration backup
- data backup

Configuration backup

Configuration backup contains only system configuration files and it's fully automatic. The purpose of this kind of backup is to quickly restore a machine in case of *disaster recovery*. From page *Backup* the system configuration can be saved, downloaded, uploaded and restored again. The retention of configuration backup can be changed by clicking the *Configure* button. Make sure to regularly download the configuration backup and save it to a secure place.

Data backup

Data backup contains all data stored in the system (user's home directories, shared folders, emails, etc). The administrator can schedule multiple data backups.

15.1 Settings

The data backup can be performed using different engines:

- **restic**: very fast, deduplication and encryption enabled by default, best suited for cloud storage

- **rsync**: fast and simple, partial deduplication, perfect for USB and SFTP storage
- **duplicity**: old and reliable, it uses compression and can execute full or incremental backups, no encryption, best choice for local network filesystem

Available storage backend:

- network filesystems for LAN: Windows File Share (CIFS), Network File System (NFS)
- remote network filesystems: WebDAV, SSH File Transfer Protocol (SFTP)
- local disk connected to a local USB/SATA port
- cloud providers: Amazon S3 (or any compatible S3 server)
- Backblaze B2

When using WebDAV as storage backend, make sure the server has a valid SSL certificate, otherwise the system will fail mounting the filesystem

15.1.1 Scheduling

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.

When configuring 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

To configure a new backup, access the *Backup* page and click on the *Schedule* button. The web interface will start a configuration wizard which will automatically suggest the best engine based on the destination type.

15.1.2 Data backup customization

Every time a new NethServer module is installed, all directories containing data are added to the data backup.

The list of paths included inside the backup are visible clicking the *Configure* button from the *Backup* page. From the same page, it's also possible to customize what is included or excluded.

When the *Include logs* option is enabled, all logs will be automatically added to the backup set.

For further customization see *Backup customization*.

15.1.3 Notifications

At the end of the backup a mail notification can be sent to the system administrator or to a list of custom email addresses.

Usually notifications are sent in case of backup failure. You can suppress all notifications or enable them even for successful backup by accessing the *Notify on* field in the final step of the backup configuration wizard.

Please refer to *Settings* chapter if you need to tune global notifications options such a SMTP rely.

15.2 Selective restore of files

Restore data application must be explicitly installed from the Software Center. Please note that selective restore will be available only for backups executed after the application installation.

First, make sure the backup destination is reachable (for example, the USB disk must be connected), then access *Restore data* application.

Access the *Restore data* application, select the name of the backup and the execution date. Then search a file or directory by entering the name inside the *Field or directory* field. For better results, select the search mode from the *Choose mode* menu: the search can be restricted only to mail folders, normal files from applications like Nextcloud. If the *Advanced* mode is selected, you can use regular expressions inside the *Pattern* field.

Finally, select the files to restore and click the *Restore* button.

If the *Overwrite* option is checked, the restored files will overwrite the existing ones. Otherwise the restored files will be created in the same path with date included in the name and `.restore`, like *.restore-20190729-153318-myfile*.

CHAPTER 16

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. When the machine is functional, a full data restore can be performed while the machine is already in production. 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

Warning: Do not restore a configuration backup from an old minor version into a newer version. The backup should come from a NethServer having the same operating system version of the new installation, i.e., avoid restoring a configuration backup from a 7.4.1708 installation on a new 7.6.1810 system, as it may lead to unexpected results.

Note: Third-party repositories are not restored by the disaster recovery procedure. If the original machine has some third-party repositories enabled, remember to install them before proceeding with the restore.

16.1 New Server Manager

Please, follow below steps:

1. Install the new machine (refer to *installation* section), access the new Server Manager and make sure the machine is able to access the internet and resolve public names correctly
2. If the machine has a Community subscription entitlement, please follow *Subscription*, otherwise you can skip this step
3. Install all the available core updates from the *Software updates*

4. Access the *Backup* page and click on the *Restore* button under the **Configuration Backup** section, then upload the configuration backup or download it directly from an HTTP/S URL.

   For NethServer Enterprise, all cloud backups will be automatically downloaded and ready to be restored directly from the *From backup* field.

5. Map network interface names from the backup to the running system. This step is required only if *Restore network configuration* option is enabled.

6. Click the *Restore* to start the restore process.

   Note: If you're connected to a network interface that will change the IP address during the restore, you will be disconnected from the Server Manager and you will need to login again using the new IP address.

   ---

7. Verify the system is functional and then access the *Backup* page. To restore all files, click on *Restore* button under the **Data Backup** section, select the name of the backup and click the *Restore* button.

Please bear in mind that the restore process can last from minutes to hours depending on the storage backend speed.

If the *Restore network configuration* was not enabled, further steps may be required to restore all applications. See *Skip network restore* for more details.

16.2 Old Server Manager

Please, follow below steps:

1. Install the new machine (refer to *installation* section), access the Server Manager and follow the first configuration wizard procedure to complete the basic server configuration
2. Ensure that NethServer is able to access the internet and resolve public names correctly
3. Install all the available core updates in the *Software Center*
4. Restore the configuration backup using the *Backup (configuration)* panel
5. If a warning message requires it, reconfigure the network roles assignment. See *Restore network roles* below.
6. Verify the system is functional
7. Restore data backup executing on the console

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

   where `name` is the name of the data backup you want to restore from.

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

Note: The root/admin password is not restored.

16.2.1 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 message 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.

16.3 Skip network restore

Network configuration is restored by default, but sometimes it is necessary to restore an installation on a different hardware without migrating the network configuration. This is a common scenario when moving a virtual machine from a VPS provider to another.

To disable the network restore, make sure to disable the *Restore network configuration* option from the new Server Manager.

Since some application configurations depend on network interface names, not everything can be automatically restored.

16.3.1 DHCP

DHCP servers on non-existing interfaces will be deleted. If needed, please reconfigure the DHCP from the Server Manager. See also *DHCP and PXE server* for more general information.

16.3.2 Samba Active Directory

Warning: Restoring a local Samba Active Directory without the *Restore network configuration* option enabled is highly discouraged. Read carefully this section.

Samba Active Directory requires a network bridge and an additional, free IP address in the green zone for the local running container.

If both the bridge exists and the IP address suits the current network configuration, the container will continue running after the restore.

Otherwise Samba Active Directory is forcibly stopped. To enable it again:

- from the *Network* page, create the bridge, e.g. `br0`

- find an unused IP address in your green network, e.g. `192.168.1.11`
- reconfigure the container from command line:

```
config setprop nsdc bridge br0 status enabled
signal-event nethserver-dc-change-ip 192.168.1.11
```

- fix the DC sysvol ACLs:

```
/etc/e-smith/events/actions/nethserver-dc-sysvolreset
```

More info about *Samba Active Directory local provider installation*.

16.3.3 Firewall

At the end of restore the firewall will:

- delete all WAN providers
- delete all zones connected to non-existing network interface
- disable all rules using a non-existing zone or a non-existing role

The administrator can access the Server Manager to create missing zones and roles. Finally, all previously disabled rules can be manually enabled again.

See firewall_new-section.

16.3.4 Web proxy

Web proxy priority rules using non-existing zones will be disabled. Before re-enabling such rules, make sure the zones have been created.

More info on priority rules: *Priority and divert rules*.

16.3.5 OpenVPN tunnels

OpenVPN tunnel servers contain a field named *Public address*. If such field uses only public DNS names, no action is required. Otherwise, insert the new public IP address inside the field and update tunnel clients accordingly.

See also OpenVPN *Tunnel (net2net)*.

16.3.6 OpenVPN roadwarrior

OpenVPN roadwarrior server exposes a field named *Contact this server on public IP / host*. If such field uses only public DNS names, no action is required. Otherwise, insert the new public IP address inside the field and update roadwarrior clients accordingly.

See also OpenVPN *Roadwarrior*.

16.3.7 IPSec tunnels

Only IPSec tunnels configured with a dynamic red interface will be disabled. Access the Server Manager, edit the disabled tunnel by selecting a new red interface and enable it again.

More info at *IPsec*.

16.3.8 Dedalo hotspot

Dedalo hotspot will be disabled if the system does not have a network interface configured with the `hotspot` role. If the Dedalo is disabled, just reconfigure following *Hotspot (Dedalo)* chapter.

16.3.9 ntopng

ntopng must be reconfigured. Access the *Bandwidth monitor* page inside the old Server Manager. Then enable the service and select network interfaces to monitor.

See also *Bandwidth monitor*.

CHAPTER 17

Backup customization

Basic customization can be done directly from the new Server Manager. See *Data backup customization*.

17.1 Data backup

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 compression 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

17.1.1 Storage backends

Supported by all engines:

- 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)
- USB: disk connected to a local USB/SATA port

Supported by restic and rsync:

- SFTP: SSH File Transfer Protocol

Supported only by restic:

- Amazon S3 (or any compatible server like Minio)
- Backblaze B2

17.1.2 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)

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

---

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

When configuring a backup using the restic engine and a remote storage backend, please ensure you have enough bandwidth to complete the first backup within 24 hours. Otherwise restic will create multiple different snapshots. If you have a slow connection and you still want to use a remote storage backend, follow this procedure:

- configure the restic backup
- manually execute the backup by clicking on *Run now*
- disable the configured backup, so it will not start at next scheduled execution
- when the backup is over, re-enable it to allow scheduled execution

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:

- 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.

The destination must be accessed with `root` user.

17.1.3 Command line execution

To run a backup from command line, use:

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

where `name` is the name of the backup you want to run.

Note: By default, the name of the *first* data backup configured on NethServer is `backup-data`

17.1.4 Data backup customization

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

Inclusion

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

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

```
/opt/mysoftware
```

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`.

Override inclusions and exclusions

All backups read the same configuration, but the list of saved and excluded files can be overridden using two special files:

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

Where `name` is the name of the backup.

Both files will override the list of included and excluded data set. The accepted syntax is the same as reported in the 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 a backup which includes only the mail and is scheduled each our.

1. Configure the new `mymailbackup` using the UI
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-data-save mymailbackup
```

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

Note: This type of backup can't be used in case of disaster recovery.

17.2 Configuration backup

Configuration backup is an automated task that 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.

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

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.

17.2.1 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.

17.2.2 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.

17.3 Restore from command line

When the *Selective restore of files* web interface is not enough, the restore can be done via command line.

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

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

To list data inside a 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>
```

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

```
restore-file -b <name> -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.

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.

17.4 Formatting a local disk

Local disks can be formatted directly from the *web interface*. If something goes wrong, or a custom partitioning is required, please follow the below steps.

The best filesystem for SATA/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:

  ```
  sgdisk --zap-all /dev/sdc
  sgdisk --largest-new=1 /dev/sdc
  ```

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

  ```
  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* page.

CHAPTER 18

Legacy backup

Note: A new backup module is available inside the new Server Manager. See *Backup*.

NethServer handles two kinds of backups: configuration backup and data backup. See *Backup* for more details.

18.1 Configuration backup

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

The page allows the creation of a new on-demand backup by clicking on the *Create backup* button. As default, the system retains the latest three configuration backups. The retention policy can be changed using the *Configure* button.

18.2 Data backup

Note: The old Server Manager can handle only a single backup. Such configuration can be managed also from the new Server Manager by editing the backup named `backup-data`.

The data backup is performed using Duplicity engine and can be configured from *Backup (data)* page. 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 when using Duplicity.

Supported storage backends:

- 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)
- USB: disk connected to a local USB/SATA port

The selective restore of files can be performed only form the new Server Manager. See *Selective restore of files*.

CHAPTER 19

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*.

19.1 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
```

19.2 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
```

19.3 Removing

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

```
yum autoremove nethserver-roundcubemail
```

CHAPTER 20

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*.

20.1 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.

20.1.1 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 -sL https://git.io/fjhn8 -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
```

20.2 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*.

20.3 Synchronization with ActiveSync (EAS)

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

20.3.1 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

Note: iOS devices require a valid SSL certificate on the server. See server_certificate-section

20.3.2 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.

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`

20.3.3 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".

20.4 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>`

20.4.1 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.

20.4.2 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
```

20.4.3 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.

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**.

20.5 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.

20.6 Sharing calendars and contacts

20.6.1 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:

20.6.2 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.

20.7 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.

20.8 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*.

20.9 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.

20.10 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:

20.11 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.

20.12 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.

20.13 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

20.13.1 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:

20.13.2 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:

20.14 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

20.15 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 inside webrtc settings section. In addition to the WebRTC settings, it is also necessary to add the **XMPP BOSH** public URL as shown inside xmpp settings.

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'
 }, {
```

(continues on next page)

(continued from previous page)

```
    '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.

20.16 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 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)

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).

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*

20.17 Custom link buttons in launcher

To configure the buttons access the WebTop administration panel and select -> *Domains* -> *NethServer* -> *Launcher* :

For each button, enter these three values

`Name` : tab descriptive text that appears with mouseover

`Link URL` : URL opened in a new browser

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

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 URL' field: `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* -> *Public Images* and insert a URL of this type for the 'Icon URL' field: `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.

20.18 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:

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:

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

20.19 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.

Alternatively, you can configure a global setting to turn images automatically into inline attachments instead of public internet links

It is possible to do this from web interface by accessing the administration panel -> *Properties (system)* -> *Add* -> select *com.sonicle.webtop.mail (Mail)* and enter the data in the *Key* and *Value* fields according to the key to be configured:

`public.resource.links.as.inline.attachments` = true (default = false)

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.

By accessing the user settings from the WebTop administration panel (*Domains* → *NethServer* → *Users* → *Right click on user*) it is also possible to set up 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.

20.20 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:

20.21 Manage identities

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

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

Local account:

Shared account:

_static/webtop_manageident3.png

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

20.22 Subscribing remote resources

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

20.22.1 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.

20.22.2 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):

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*):

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:

20.23 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*.

20.24 Changing the logo

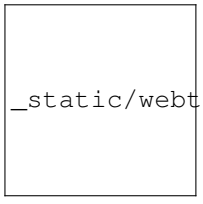
To modify and customize the initial logo that appears on the login page of WebTop, you must upload the custom image file on the public images of the admin user and rename it with "login.png".

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

20.25 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
```

20.26 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)

20.27 Importing contacts and calendars

WebTop supports importing contacts and calendars from various file formats.

20.27.1 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.

20.27.2 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

20.28 Hide auto-suggested recipient in lookups

To disable the suggestion of automatically saved addresses, access the web 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:

`recipient.provider.auto.enabled` = false (default is true)

20.29 Edit subject of a mail and save it

To enable the modification of the subject for received and sent emails, access the web administration panel -> *Properties (system)* -> *Add* -> select *com.sonicle.webtop.mail (Mail)* and enter the data in the *Key* and *Value* fields according to the key to be configured:

`message.edit.subject` = true (default is false)

20.30 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
```

20.30.1 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.

20.30.2 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
```

20.30.3 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.

20.31 Troubleshooting

20.31.1 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.

20.31.2 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
```

20.31.3 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

20.31.4 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*

20.32 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 change `/etc/httpd/conf.d/webtop5-zpush.conf` config file.

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.

20.33 Google integration

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

20.33.1 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

It is possible to do this 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:

`googledrive.clientid` = (Google API client_ID)

`googledrive.clientsecret` = (Google API client_secret)

CHAPTER 21

POP3 connector

Note: Since NethServer 7.5.1804 new *Email*, *POP3 connector* and pop3_proxy-section 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 is part of the *Email* application inside the new Server Manager and it is accessible from the list of user mailboxes. The same configuration is accessible from the old Server Manager, from the *POP3 connector* page.

Configured external accounts will be checked regularly and retrieved messages 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
- antispam and antivirus 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

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

CHAPTER 22

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
- 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*.

22.1 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.

22.2 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-section).

22.3 Administrators

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

The group `jabberadmins` must be created and configured from the *Groups* page.

Administrators can:

- Send broadcast messages
- Check the status of connected users

22.4 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.

22.5 Other options

From the new Server Manager the administrator can configure all the options described above.

Other available options:

- upload and dowload transfer speed

- enable/disable the administrator web interface

CHAPTER 23

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/.

23.1 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-section for more info.

Warning: Please note that the mobile app **cannot connect to servers with self-signed certificates**!

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

23.2 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.

23.2.1 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-section
- 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.

23.2.2 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
```

CHAPTER 24

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.

24.1 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
```

24.2 UPS statistics

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

CHAPTER 25

Report

Note: The configuration page of this module is available only in the new Server Manager.

This module manages the configuration of Dante.

Dante collects data from logs, databases and services, aggregates and displays them on a report structured as a customizable dashboard. The report can be sent via e-mail, with configurable scheduling and recipients.

25.1 Dashboard

The *Dashboard* page is composed by a set of widgets, each showing a piece of information on the system. The user can customize the layout of the dashboard by adding, removing, resizing and drag & dropping widgets.

The types of widgets currently supported are:

- **Chart**: pie, bar, line or area charts
- **Counter**: a card that displays an aggregated numerical value and a trend on a time interval
- **Table**: a table with optional row and column headers
- **Ranking**: a list of the top N items, ordered by their value
- **Label**: a text showing a piece of information
- **Title**: a simple text typed by the user to organize the layout of the dashboard

25.2 Settings

The *Settings* page manages the configuration of the module.

25.2.1 Host configuration

- **Public host**: this is the hostname where the report is hosted. It must be a name that can be resolved from the internet
- **Final url**: this field displays the public URL where the report is hosted

25.2.2 Report configuration

- **Theme**: the themes available for the dashboard are *light* and *dark*
- **Palette**: there are 9 color palettes to choose from
- **Interval**: time interval on which the data are aggregated. It can be *Week*, *Month* or *Six-months*
- **Language**: language used to display the report
- **Anonymization**: boolean flag that controls the anonymization of sensible data in the report
- **Max Entries**: maximum number of items to display on ranking widgets
- **Addresses**: configuration of report e-mail recipients and scheduling of e-mail dispatch

25.2.3 Test mail

- **Address**: e-mail recipient of the test e-mail containing the report
- **Include configured addresses**: boolean flag to control whether the test e-mail should be sent to the addresses configured in *Report configuration* in addition to *Address*

CHAPTER 26

Fax server

Note: The configuration page of this module is available only in the old Server Manager and will not be ported to the new one.

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

26.1 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.

26.2 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

26.2.1 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.

26.3 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.

26.4 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.

26.5 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

CHAPTER 27

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

27.1 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.

27.2 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.

27.3 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.

27.4 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

27.4.1 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.

27.4.2 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.

27.5 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

27.6 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*.

27.7 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.

27.7.1 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
```

27.8 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
```

27.9 Logs

Squid logs are kept for 5 weeks in compressed format, to control disk space usage. Web proxy logs are verbose to help troubleshoot problems. Web browsing activities are logged in aggregate and readable format by Lightsquid.

In environments where logs need to be preserved for more than 5 weeks, you could manually edit the logrotate configuration `/etc/logrotate.d/squid`. Finally, remember to add `/etc/logrotate.d/squid` to the configuration backup using the custom include.

```
echo '/etc/logrotate.d/squid' >> /etc/backup-config.d/custom.include
```

CHAPTER 28

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.

Web content filter is included inside the "Web Proxy & Filter" application of the new Server Manager.

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.

28.1 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.

28.1.1 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`.

28.2 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. See *Antivirus* for more info.

28.3 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

CHAPTER 29

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.

29.1 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 auto-generated from several sources of known and confirmed active Botnet and other Command and Control hosts. Updated daily, primary data source is Shadowserver.org. Bot

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

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 hundreds 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 rule set 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.

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, while 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 categorized 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 anomalies

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 rule set 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.

29.2 Bypass

The bypass disables IPS protection for selected hosts: all traffic from/to the given host will not be analyzed.

To create a bypass access the new Server Manager and open the *IPS* application, then go to the *Bypass* page and click on *Add bypass* button.

Fill the *Bypass* field and click on *Save* button. The *Bypass* field supports:

- host objects
- host groups objects
- IP range objects
- raw IP addresses

29.3 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.

CHAPTER 30

Reverse proxy

Note: The reverse proxy configuration is part of the *Web server* application inside the new Server Manager.

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

30.1 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'.

30.2 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

CHAPTER 31

Virtual hosts

Note: The virtual host configuration is part of the *Web server* application inside the new Server Manager.

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.

31.1 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.

31.2 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.

31.3 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.

CHAPTER 32

Bandwidth monitor

Bandwidth monitor module allows you to analyze real-time network traffic using ntopng under the hood. **ntopng** is a powerful tool that evaluates the bandwidth used by individual hosts and identifies the most commonly used network protocols.

32.1 Dashboard

Dashboard page provides an overview on network usage displaying traffic information on some graphical widgets.

32.1.1 Status

Status section informs you whether bandwidth monitor is currently enabled and provides *Open bandwidth monitor app* button to access **ntopng** web interface.

32.1.2 Top local hosts

This table shows the list of hosts belonging to local networks that are currently generating most throughput, either downloading or uploading. This widget can help identify any hosts that are using a lot of bandwidth.

32.1.3 Top remote hosts

This table shows the list of remote hosts that are currently generating most throughput, either downloading or uploading.

32.1.4 Traffic by interface

This chart plots the throughput generated by monitored interfaces during the last 5 minutes.

32.1.5 Traffic by protocol

This chart plots the traffic divided by protocol during the last 5 minutes. **ntopng** tries to recognize various layer 7 protocols such as HTTP, TLS, DNS, SIP, Facebook, Spotify, Zoom, etc.

32.2 Settings

In *Settings* page you can manage **Bandwidth monitor** configuration through the following controls:

- *Enable bandwidth monitor*: if enabled, all traffic passing through selected network interfaces will be analyzed. Depending on the capabilities of your server, it may cause a slowdown of the network and an increase in system load.
- *Interfaces*: the network interfaces **ntopng** will listen to.
- *Web interface port*: the TCP port where **ntopng** web interface should be available. By default TCP port is **3000** and can be accessed from green zone.
- *Enable authentication*: if enabled, **ntopng** web interface will require login credentials. Username is `admin` and default password is `admin`.

When **Bandwidth monitor** is enabled, **ntopng** web interface is available at: `http://<SERVER_NAME>:<WEB_INTERFACE_PORT>`. A link to **ntopng** web interface is provided in *Dashboard* and *Settings* pages.

32.3 Logs

In *Logs* page you can examine systemd journal of **ntopng** unit.

CHAPTER 33

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.

33.1 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
```

CHAPTER 34

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

Roadwarrior OpenVPN, IPSec tunnel and OpenVPN tunnels are part of the VPN application in the new Server Manager.

By default, the network traffic between VPNs is blocked by the firewall. To allow such traffic go to the *Firewall* application and enable the *Allowed* field under *Settings* > *Traffic between OpenVPN roadwarrior, OpenVPN tunnels and IPSec tunnels*.

34.1 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

34.1.1 Roadwarrior

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

Supported authentication methods are:

- System user and password

- Certificate
- System user name, password and certificate
- System user name, One Time Password (OTP) 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 or with one time password (2FA).

2. Download the file containing the configuration and certificates. As an alternative, the file can be sent to the user by mail (available only on the new Server Manager).
3. Import the file into the client and start the VPN.

Note: When using OTP-based authentication, users will be required to enable *2FA* before accessing the VPN. Also make sure users will not enable the "Save password" option on their clients, because a new OTP must be entered every time the VPN is started. A password saved inside a VPN client can be seen as a login failure by *Fail2ban*.

Accounting

Every time a client connects to the OpenVPN server, the access is logged inside an accounting database. Access statistics are available from the new Server Manager. For each user, statistics include:

- client name
- virtual IP address
- real IP address
- time of connection
- time of disconnection
- transferred bytes

34.1.2 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.

34.2 IPsec

IPsec (IP Security) protocol is the 'de facto' standard in VPN tunnels, it's typically 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).

34.2.1 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.

CHAPTER 35

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:

- configure 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)

35.1 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.

35.1.1 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*.

35.2 Configuration

After installation, the application can be configured from the new Server Manager.

35.2.1 Custom virtual host

Sometimes it's better to reserve a full virtual host for accessing Nextcloud like `nextcloud.nethserver.org`.

Please note that after the configuration of a custom virtual host, Nextcloud will no longer be accessible from the default URL `https://your_nethserver_ip/nextcloud`.

If the machine is using Let's Encrypt, remember to add the virtual host domain name to list of valid certificate domains.

35.2.2 Trusted domains

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

- domain name
- IP address

The list of trusted domains can be customized using *Trusted domains* field: add one domain per line.

35.2.3 CalDAV and CardDAV

Some CalDAV and CardDAV clients may have problems finding the proper sync URL and need automatic service discovery. Service discovery is enabled by default if a custom virtual host for Nextcloud has been configured.

To enable the service discovery even if Nextcloud is running on the default URL, check the *Enable CalDAV and CardDAV auto-discovery* field.

Note: When enabling DAV auto-discovery, please make sure WebTop or SOGo are *not* already installed.

35.2.4 Collabora Online

See *Collabora Online module from NethForge*.

35.2.5 ONLYOFFICE

Since Nextcloud 18, ONLYOFFICE Community Document Server can be installed directly to the system without further configuration. To enable built-in ONLYOFFICE integration, access Nextcloud with the `admin` user then:

- Go to *Apps* page and access *Office & text* section
- Download and enable the `ONLYOFFICE` application
- Download and enable the `Community Document Server` application. Please be patient, download and install will take a while.
- Go to the *Settings* page and access the *ONLYOFFICE* application under *Administration* section
- Verify the *Document Editing Service address* already contains the public address of your Nextcloud server

---

Note: Installation of full ONLYOFFICE server is not supported on NethServer.

CHAPTER 36

FTP

Note: The FTP server is part of the *Web server* application inside the new Server Manager.

Warning: 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.

36.1 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
```

CHAPTER 37

Phone Home

Phone home is used to track all NethServer 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 the number of installations grouped by country and release: https://www.nethserver.org/phone-home/index.html

The phone home is enabled by default and it sends the following data:

- UUID stored in `/var/lib/yum/uuid`
- RELEASE from `/sbin/e-smith/config getprop sysconfig Version`
- TYPE of installation like `subscription`, `enterprise` or `community`

37.1 Disabling

The phone home can be disabled from command line. Just run the following command in a root shell:

```
config setprop phone-home status disabled
```

CHAPTER 38

SNMP

Note: The configuration page of this module is available only in the old Server Manager and will not be ported to the new one.

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/

CHAPTER 39

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)

39.1 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/ .

39.2 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

39.3 Configuration

39.3.1 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

39.3.2 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.

39.3.3 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.

39.3.4 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.

CHAPTER 40

FreePBX

Note: The configuration page of this module is available only in the old Server Manager.

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/).

40.1 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.

40.2 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.

40.3 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"
```

40.4 Advanced Documentation

For further information you can read the FreePBX documentation at: https://wiki.freepbx.org

CHAPTER 41

Virtual machines

NethServer is capable of running virtual machines using KVM and libvirt, but it doesn't provide a Web interface for it.

Virtualization software can be installed and started using the command line, just execute:

```
yum install --setopt=base.enablegroups=1 @virtualization-hypervisor @virtualization-
↪tools @virtualization-platform
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 such conflict, remove `default` libvirt NAT network:

```
systemctl stop dnsmasq
systemctl start libvirtd
virsh net-destroy default
virsh net-autostart default --disable
systemctl start dnsmasq
```

Finally, the system is ready to be managed using Virtual Machine Manager (virt-manager), a Linux desktop user interface for managing virtual machines through libvirt.

Access virt-manager in your Linux desktop, then create a new connection to your NethServer using SSH protocol.

41.1 External resources

For more info see:

- Virtual Machine Manager official site
- Virtual Machine Manager on RHEL
- Introduction to virtualization
- KVM/Libvirt FAQ

CHAPTER 42

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.

42.1 Installation

Install from the Software Center or use the command line:

```
yum install nethserver-fail2ban
```

42.2 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.

42.2.1 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 ban Extend the ban of persistent abusers. Recidive ban can have 2 different behaviors:

- *Static ban time*: ban recidive hosts for 2 weeks, like brute force attack bots. The rule applies when an IP address has been already banned multiple times.
- *Incremental ban time*: increase the ban time after each failure found in log. When enabled, if you set a short ban time, a valid user can be banned for a a little while but a brute force attacker will be banned for a very long time.

42.2.2 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.

42.2.3 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.

42.3 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.

42.4 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.

42.5 Tools

42.5.1 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 log files are monitored for a jail:

```
fail2ban-client get nginx-http-auth logpath
```

42.5.2 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
```

42.5.3 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*$'
```

42.5.4 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>
```

42.6 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.

CHAPTER 43

Rspamd

Rspamd is the new antispam engine of NethServer, it replaces SpamAssassin and Amavisd-new.

The official documentation of Rspamd is available at https://rspamd.com

You need to install the *Email* module from the *Software center* page. The menu where to activate it and modify its settings is on the *Email* > *Filter* page. You can read more in the *Email filter* section.

43.1 Rspamd Web Interface

The antispam component is implemented by Rspamd which provides its administrative web interface at

```
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.

43.1.1 Status

It is the landing menu, the global statistics are available on the Rspamd service.

43.1.2 Troughput

The graphics are displayed in this menu to explain the activity of the antispam software. You can adjust the time scale (hourly, daily, weekly, montly) and modify some other settings to refine the graphics

43.1.3 Configuration

The *Configuration* > *Lists* menu is useful to edit lists of allowed IP/Domain/mime for the modules, you will find:

- SURBL
- mime list types
- SPF_DKIM
- DMARC
- DKIM
- SPF

When you want to create an exception list in a module, you could give the path `/var/lib/rspamd/`, the list will be editable by the Rspamd web interface.

43.1.4 Symbols

Rspamd use a concept of symbols which will increase or decrease the spam score when the rule has matched. The symbol weight is modifiable, negative score are for good email, positive are for spam.

Find the matching symbols

The convenient way is to use the *History* > *History* menu.

Modify a symbol weight

An easier way to change the symbol weight is to use the Rspamd WebUI: *Symbols* > *Symbols and rules*. A search box is available, you could use it to display the symbol and modify its weight.

- Symbol score for spam is in red (positive score)
- Symbol score for ham is in green (negative score)

If you want to remove the custom settings, you could edit the file `/var/lib/rspamd/rspamd_dynamic` or remove them in the Rspamd Web Interface: *Configuration* > *Lists* > *rspamd_dynamic*

You could redefine manually the scores defined in `/etc/rspamd/scores.d/*_group.conf` where they are placed by a symbol's group. Like for the modules, you could overwrite the setting in `/etc/rspamd/local.d/*_group.conf` or `/etc/rspamd/override.d/*_group.conf`.

Priority order

```
scores.d/*_group.conf < local.d/*_group.conf < override.d/*_group.conf
```

43.1.5 Learning

The purpose of the *Learning* Menu is to train the Bayes filter, you could use directly the source of the email in the relevant text area to make learn to rspamd if the email is a spam or a ham.

43.1.6 Scan

The *Scan* menu can be used to scan directly an email and check its score and the matching symbols.

43.1.7 History

The Rspamd web Interface could be used to display the action done and the spam score against an email, see *History* > *History*

You could display a list of symbols by clicking on the email field, it will help you to understand the action done (reject, add_header, no_action, rewrite_subject, greylist) and gather useful informations like:

- the sender
- the recipient
- the subject
- the full score

43.2 Modules

Rspamd comes with a modular approach, all modules are not enabled by default and are customisable by the system administrator. The default settings are in the file `/etc/rspamd/modules.d/MODULE_NAME.conf`, relevant to the module name.

For a particular need, you can look the documentation with the list of modules.

43.2.1 Disable a module

You must disable a module only with a good reason. For example the ip_score module could give a high spam score due to the IP of the email sender, if it is blacklisted.

In that example we could disable the module but many modules (like ip_score) implement a white list to do not check an ip or a domain against the spam filter.

Create a file (relevant to the module name) `/etc/rspamd/override.d/MODULE_NAME.conf` with

```
enabled = false;
```

Restart Rspamd

```
systemctl restart rspamd
```

43.2.2 Modify the settings of a module

All the default settings of a module are in `/etc/rspamd/modules.d/MODULE_NAME.conf`, NethServer uses `/etc/rspamd/local.d/MODULE_NAME.conf` to modify these parameters. Therefore the prefered way is to use `/etc/rspamd/override.d/MODULE_NAME.conf` to either change the Rspamd and NethServer default settings. The override file uses the new parameter with a high preference, all former settings are kept.

Priority order:

```
modules.d/MODULE_NAME.conf < local.d/MODULE_NAME.conf < override.d/MODULE_NAME.conf
```

In that example we want to implement a list of IP to allow them in the ip_score module.

Create a file `/etc/rspamd/override.d/ip_score.conf` with

```
whitelist = "file:///var/lib/rspamd/ip_score_whitelist";
```

Restart rspamd

```
systemctl restart rspamd
```

The whitelist is editable in the rspamd UI at *Configuration* > *Lists* > *ip_score_whitelist*

Note: The folder `/var/lib/rspamd` is owned by Rspamd, all files here are modifiable by the software

43.3 Frequently asked questions

The official Rspamd FAQ could have the answer to your questions. Please see https://rspamd.com/doc/faq.html

CHAPTER 44

Antivirus

Note: The configuration page of this module is available only in the new Server Manager.

ClamAV is the open source antivirus engine of NethServer. The server runs two different ClamAV instances: one for scanning received mail (see *Email*) and the other one for analyzing HTTP web traffic (see *Web content filter*).

The antivirus engine can be configured from the new Server Manager. Since virus signatures are downloaded about once per hour, changes to the configuration will take effect on next automatic signatures download.

Available options:

- *ClamAV official signatures*: enable or disable official signatures. These signatures detect many old threats but are not very effective against the latest malware. Usage of official signatures is discouraged on machines with less than 4GB of RAM.
- *Third-party signatures rating*: choose the rating of unofficial signatures downloaded from multiple verified sources like SaneSecurity. Higher rating means more blocked threats but also a higher probability of false positives. Recommended ratings are `Low` and `Medium`.

CHAPTER 45

Threat shield

Note: The configuration page of this module is available only in the new Server Manager.

The Threat shield blocks connections to and from malicious hosts, preventing attacks, service abuse, malware, and other cybercrime activities using IP blacklists. It also blocks DNS requests for malicious domains using DNS blacklists. The package can be installed both on firewalls and on machines without a red interface, like mail servers or PBXs.

45.1 Configuration

IP blacklist and *DNS blacklist* can be enabled and configured on the corresponding pages in the menu. Their configuration is almost identical.

First, set the *Download URL* for the blacklists. After setting the URL, the administrator can choose which blacklist categories should be enabled. Each category can have a *Confidence* score between 0 and 10. Categories with a higher confidence are less prone to false positives.

Enabled categories will be automatically updated at regular intervals.

The download URL must contain a valid GIT repository. Administrators can choose a public repository or subscribe to a commercial service. If the machine has a Community or an Enterprise subscription, the access to the URL will be authenticated using system id and secret.

A popular free IP blacklist is Firehol. Experienced administrators can also setup their own IP blacklist server.

An example of DNS blacklist is available at dns-community-blacklist.

Warning: If *Web proxy* is enabled, in any mode, *DNS blacklist* will not work for proxied hosts.

45.1.1 Whitelist

In case of a false positive, an IP address or a CIDR subnet can be added to the local *Whitelist*. If the firewall module is installed, the whitelist will also accept host and CIDR firewall objects.

Hosts should be added to the whitelist only for a limited period of time. As a best practice, when a false positive is found, please report it to the blacklist maintainer.

45.2 Incident response

The *Analysis* page displays most recent attacks and DNS requests which can be easily filtered by source, destination and other attributes. Using the *Check IP address or domain* section, administrators can also check if a given IP or domain has been blacklisted by enabled categories.

For advanced log analysis with regular expressions support, use the *Logs* page.

45.3 Statistics

The *Dashboard* page provides an overview on current status of IP and DNS blacklists and displays graphical information about blocked attacks.

IP blacklist dashboard provides:

- Today's total number of threats blocked
- Today's most blocked source hosts
- Today's most blocked destination hosts

DNS blacklist dashboard provides:

- Today's total number of threats blocked
- Today's total number of DNS requests
- Today's threats percentage
- Top clients performing most DNS requests
- Top blocked domains
- Top requested domains

CHAPTER 46

Email module transition to Rspamd

Since NethServer 7.5.1804 new *Email*, *POP3 connector* and pop3_proxy-section 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]

46.1 Feature changes

46.1.1 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.

46.1.2 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.

[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] alterMIME is a small program which is used to alter your mime-encoded mailpack – https://pldaniels.com/altermime/

46.1.3 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.

46.1.4 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.

46.2 Upgrade procedures

Manual upgrade procedures are no longer needed: upgrade occurs automatically.

After the upgrade the old antispam engine services provided by amavisd and spamassassin are stopped and their packages can be removed.

To clean up the old antispam rpms type

```
yum remove amavisd-new spamassassin
```

References

CHAPTER 47

Collabora Online

Note: This package is not supported in NethServer Enterprise

Collabora Online Collabora Online is a powerful LibreOffice-based online office that supports all major document, spreadsheet and presentation file formats, which you can integrate in your own infrastructure. Please see the official website.

47.1 Installation

Install from the Software Center or use the command line:

```
yum install nethserver-collabora
```

47.1.1 Virtual host configuration

Collabora Online requires a dedicated virtual host and it's only accessible from HTTPS with a valid certificate.

Note: Collabora Online will **not be enabled** without a dedicated virtual host

To configure Collobora Online, execute:

```
config setprop loolwsd VirtualHost collabora.yourdomain.com
signal-event nethserver-collabora-update
```

After virtual host configuration, obtain a valid HTTPS certificate via Let's Encrypt from `Server certificate` section of Server Manager interface.

47.1.2 Usage

Collabora Online will be automatically enabled in Nextcloud if the package `nethserver-nextcloud` is present when the virtual host is configured, otherwise you can enable with:

```
yum install nethserver-nextcloud
signal-event nethserver-collabora-update
```

If your instance of Nextcloud is not installed in the same server of Collabora Online, you must set the host name of Nextcloud in the prop `AllowWopiHost`:

```
config setprop loolwsd AllowWopiHost nextcloud-office.yourdomain.com
signal-event nethserver-collabora-update
```

And manually configure the Nextcloud richdocuments app.

47.2 Admin user

After installation, admin dashboard can be enabled with `loolconfig set-admin-password` and accessible at:

```
https://collabora.yourdomain.com/loleaflet/dist/admin/admin.html
```

CHAPTER 48

Docker

Note: This package is not supported in NethServer Enterprise

Docker is an open platform for developing, shipping, and running applications. Docker enables you to separate your applications from your infrastructure so you can deliver software quickly. With Docker, you can manage your infrastructure in the same ways you manage your applications.

Warning: Docker is customised to NethServer and the firewall layer. The default bridge `docker0` is enabled to provide compatibility, however the official docker documentation stated on why you should not use it. Docker with NethServer comes with 3 other networks called `aqua`, `aeria` and `macvlan`.

48.1 Official documentation

The purpose of this documentation is to help you to install docker and enable the Portainer user interface. However all docker relative issues should be reported to the documentation or to the docker community.

The official documentation of docker can be found at : https://docs.docker.com/get-started/overview/

48.2 Installation

Install from the Software Center or use the command line:

```
yum install nethserver-docker
```

48.3 Docker repository

The official repository of docker is bundled but not enabled, the upgrade might break the running containers. It is advised to stop all containers before to upgrade `docker-ce`.

To upgrade to the latest stable version of docker:

```
yum update --enablerepo=docker-ce-stable
```

to enable it permanently:

```
config setprop docker enableRepository enabled
signal-event nethserver-docker-update
```

48.4 Configuration

If you have a free block device (required for production environments) assign it to Docker before starting it for the first time

```
config setprop docker DirectLvmDevice /dev/sdb
signal-event nethserver-docker-update
```

Review the current settings with

```
config show docker
```

Network, is the IP network address of the aqua zone IpAddress, is the IP address of the Docker host in the Network above

After each change, you have to restart docker

```
signal-event nethserver-docker-update
```

48.5 Web user Interface

Portainer is an interface to manage all containers running on this host or eventually on remote hosts, a property must be enabled before to create the portainer

```
config setprop portainer status enabled
signal-event nethserver-docker-update
```

The URL of portainer is `https://<IP>:980/portainer/` . The first time it is accessed, it asks to generate the administrative credentials.

Portainer is itself a container without important data, except the admin credential. Therefore if you need to do a clean installation you can remove the container and the data stored in `/var/lib/nethserver/portainer`.

The official documentation of portainer can be found at : https://www.portainer.io/documentation/

48.6 Default network

The default bridge docker0 is allowed in the firewall of NethServer, any ports or the containers will be opened through shorewall. Any docker howto is supposed to be compatible.

Example of nginx container on port `9001`:

```
docker run  -dit --name nginx-test-01 -p 9001:80 --restart=unless-stopped␣
↪nginx:alpine nginx-debug -g 'daemon off;'
```

48.7 Aqua network

A new firewall zone and docker network, `aqua`. Basically, containers are attached to aqua and they can talk each other. IP traffic from other zones, like green and red must be configured with the usual Firewall rules and Port forwarding pages.

For an integration with system services, connections from the aqua zone are allowed to the MySQL/MariaDB port `3306`. it means that a docker running on `aqua` can use the mysql database on the server. More port rules can be opened to the system services running on the server with a esmith db command (these rules allow **only** the containers to connect to a service running on the server):

```
db dockrules set customName aqua TCPPorts 5141,5142 UDPPorts 5143,5144 status enabled
signal-event firewall-adjust
```

You have to specify to use the network `aqua` for your container, the default `docker0` is another network. Each container on the network `aqua` will have an IP from the network `172.28.0.0/16`. They can communicate each other and the server can ping each container.

For example (pihole on aqua with a static IP):

```
docker run -d --name nxfilter -v nxfilter-conf:/nxfilter/conf -v nxfilter-log:/
↪nxfilter/log \
-v nxfilter-db:/nxfilter/db -e TZ=Europe/Vienna \
--net=aqua --ip=172.28.0.10/16 --restart=unless-stopped packetworks/nxfilter-
↪base:latest
```

48.8 Aeria network

NethServer docker provides a docker network named `Aeria` that is bound to a bridge. The container will have an IP attributed by the dhcp server of your local network, all containers will communicate like any servers on your network.

For the bridge creation the server manager could be used, if you have already installed the account provider Samba AD (nethserver-dc), you have already a bridge called `br0`.

Warning: A bridge is mandatory to `aeria`, you must accomplish this step before to go further: `ip a` can valid that the bridge is up and workable. The same bridge cannot be shared among `aeria` and `macvlan`, it is a docker limitation.

To enable the Aeria network, the `bridgeAeria` property has to be set to the name of the bridge

```
config setprop docker bridgeAeria br0
signal-event nethserver-docker-update
```

The NethServer DHCP module can be used to set IP addresses for the docker containers. By default docker containers use random MAC addresses so fixed ones need to be set for the containers to make DHCP reservations work.

Here is an example for starting pihole in the Aeria network and set the MAC address

```
docker run -d --name pihole -e TZ="Europe/Vienna" -e WEBPASSWORD="admin" \
-v "$(pwd)/etc-pihole/:/etc/pihole/" \
-v "$(pwd)/etc-dnsmasq.d/:/etc/dnsmasq.d/" --cap-add NET_ADMIN \
--net=aeria --mac-address=0e:6f:47:f7:26:1a --restart=unless-stopped pihole/
↪pihole:latest
```

Aeria uses a docker plugin. To update the plugin

```
signal-event nethserver-docker-plugin-update
```

48.9 Macvlan

A container use TCP/UDP ports to communicate outside of the server, this is the default networking. However your container could need to get a real IP on your network. Like this it will be reachable with `http://IPofYourContainer` instead of `http://IPofYourServer:port`. A specific configuration like a DNS sinkhole (as pihole) must have an IP, because it might break the DNS resolution of your server. Therefore with a different IP, all hosts of your network will use the services of pihole like if it was on another server.

Note: The difference between macvlan and aeria is that macvlan is not a plugin, it is an official network driver.

NethServer docker provides a docker network named `macvlan` that must be bound to a bridge. Each container on the network `macvlan` must have a relevant IP in the range assigned to macvlan, all containers will communicate like any servers on your network.

For the bridge creation the server manager could be used, if you have already installed the account provider Samba AD (nethserver-dc), you have already a bridge called `br0`.

Warning: A bridge is mandatory to `macvlan`, you must accomplish this step before to go further: `ip a` can valid that the bridge is up and workable. The same bridge cannot be shared among `aeria` and `macvlan`, it is a docker limitation.

Macvlan must be created by filling some important parameters, the goal is to create a container with an IP on your network, each parameter depends from your network setting.

- macVlanGateway : It is the gateway of your network, generally speaking it is your router (here **192.168.1.1**)
- macVlanLocalNetwork : It is the full network of your router (here **192.168.1.0/24** from **192.168.1.1** to **192.168.1.255**)
- macVlanNetwork : It is the restricted IP for `macVlan0` (here **192.168.1.224/27**, you can use **30 IP** for your containers from **192.168.1.225** to **192.168.1.254**)
- macVlanNic : It is the network interface where to run macvlan (**br0** here)

Create the network

```
config setprop  docker macVlanGateway 192.168.1.1 macVlanLocalNetwork 192.168.1.0/24␣
↪macVlanNetwork 192.168.1.224/27 macVlanNic br0
```

Then trigger the event

```
signal-event nethserver-docker-update
```

You have to specify to use the network `macvlan` for your container, the default `docker0` is another network.

Docker creation example on macvlan

```
docker run --net=macvlan -dit --name nginx-test-02 --ip=192.168.1.225 --
↪restart=unless-stopped nginx:alpine nginx-debug -g 'daemon off;'
```

The container can be contacted at the relevant IP

```
curl http://192.168.1.225
```

In case of the proposed CIDR doesn't fit your need, you should have a look to an IP calculator

48.10 Issues

Please raise issues on community.nethserver.org.

48.11 Sources

Source are available https://github.com/NethServer/nethserver-docker

CHAPTER 49

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.

49.1 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
```

49.2 Official documentation

Please read official documentation: your solution is in this book.

49.3 Usage

The URL of the groupware is https://yourdomain.com/SOGo. You can use the 'username or username@domain.com for login.

49.4 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.

49.5 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
```

49.6 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
```

49.7 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 SOGo again:

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

49.8 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
```

49.9 Fine tuning

49.9.1 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 active user for the activesync connection. The SxVMemLimit could be be adjusted also, between 25MB to 45 MB per active user with the activesync service.

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
```

SxVMemLimit (default 512MB):

```
config setprop sogod SxVMemLimit 1024
signal-event nethserver-sogo-update
```

49.9.2 Increase sogod log verbosity

Read the SOGo FAQ for other debugging features.

49.9.3 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

49.10 Clients

49.10.1 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.

49.10.2 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.

49.10.3 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.

49.10.4 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.

49.11 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 :)

49.11.1 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
```

49.12 Issues

Please raise issues on community.nethserver.org.

49.13 Sources

Source are available https://github.com/NethServer/nethserver-sogo

Developer manual on github.

CHAPTER 50

PhpVirtualBox

Note: This package is not supported in NethServer Enterprise

VirtualBox VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. It is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. Please see the official website

phpVirtualBox A web-based front-end to VirtualBox. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License version 3 as published by the Free Software Foundation. Please see the github page

50.1 Installation

nethserver-virtualbox-X.X-phpvirtualbox requires nethserver-virtualbox-X.X-VirtualBox. The versions are bound togheter: nethserver-virtualbox-5.2-phpvirtualbox requires nethserver-virtualbox-5.2-VirtualBox

Warning: VirtualBox compile its modules with the latest kernel, you must have the most updated kernel and start on it at boot. If the installer cannot compile the modules, then you should reboot your server and launch again the compilation using : `/sbin/vboxconfig`

Install from the Software Center or use the command line:

```
yum install nethserver-virtualbox-5.2-phpvirtualbox
```

50.1.1 Usage

The URL of the phpVirtualBox application can be found at https://yourdomain.com/phpvirtualbox. The default credentials are :

- username: `admin`
- password: `admin`

More information are available at the Authentication section

50.1.2 Network access

The application is restricted to your local network (default is `private`), to enable phpVirtualBox to the external IP

```
config setprop phpvirtualbox access public
signal-event phpvirtualbox-save
```

50.1.3 Access on an exclusive hostname

To make phpVirtualBox accessible with an exclusive DNS name, for example https://webmail.example.com :

- 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 `DomainName` prop list (default is ''):

```
config setprop phpvirtualhost DomainName webmail.example.com
signal-event phpvirtualbox-save
```

50.1.4 Advanced settings

phpVirtualBox attempts to look like the user interface of VirtualBox, but you can enable the `AdvancedSettings` property (default is `false`) and get more settings, only available by the command line

```
config setprop phpvirtualhost AdvancedSettings true
signal-event phpvirtualbox-save
```

50.1.5 VM ownership and quota

The administrator users are not limited on the virtual machine quota and can manage VM of other users. The VMs are visible only to the owner, as long as the property `VMOwnerShip` is to true (default is `true`).

```
config setprop phpvirtualhost VMOwnerShip false
signal-event phpvirtualbox-save
```

Maximum number of VMs allowed for non admin user (default is `5`)

```
config setprop phpvirtualhost QuotaPerUser 10
signal-event phpvirtualbox-save
```

50.2 User permissions

phpVirtualBox essentially has two access levels. `admin` and `non-admin` users. The administrator users have access to the Users section of phpVirtualBox and can add, edit, remove other users (only for the internal method). They can also perform actions that change VM group memberships and manipulate VM groups (Rename, Group, Ungroup).

The administrator users are also not limited with the virtual machine quota and can manage VM of other users. The VMs are visible only by the owner, as long as the property `VMOwnerShip` is set to true.

50.3 Authentication

You can change the authentication method by the property `Authentication` (`internal`, `LDAP`, `AD`, default is `internal`). For LDAP and AD, phpVirtualBox will connect the NethServer Account providers and grant or not the authorization to the web application.

Example:

```
config setprop phpvirtualbox Authentication AD
signal-event phpvirtualbox-save
```

50.3.1 internal

The default credentials are :

- username: `admin`
- password: `admin`

Once logged in the first time, you should change the default password in the menu *File -> Change Password*.

In the phpvirtualbox user menu, you can create users, and set their permissions (only for the internal authentication method).

50.3.2 LDAP (openldap)

This authentication method is simple, all users from Openldap can login, but only users in the property `AdminUser` are administrators (comma separated list, default is `admin`)

50.3.3 AD (active directory)

This authentication method is the most complete, group based (you have to create manually the two groups in the group panel of NethServer and associate members to these groups):

- members of `vboxadmin` are administrators
- members of `vboxuser` are non privilegied users

The users who do not belong to s `vboxadmin` or `vboxuser` groups, can't use the phpVirtualBox web application. You can change the group name with the properties `UserGroup` and `AdminGroup`

50.4 Uploading ISOs

The user who runs virtualbox is `vboxweb`, a home is created (`/home/vboxweb`) to store all the virtual machines (in VirtualBox VMs) and also the needed ISOs for creating your VM. The password of this user is stored in `/var/lib/nethserver/secrets/virtualbox`.

You could open a session by ssh to download directly the ISO with wget, or push them by rsync or scp, directly from your computer. You could provide to the `vboxweb user` a ssh key and open a ssh session without password.

```
rsync -avz XXXXXXX.iso vboxweb@IpOfServer:/home/vboxweb/
scp XXXXXXX.iso vboxweb@IpOfServer:/home/vboxweb/
```

50.5 Oracle VM VirtualBox Extension Pack

This Extension Pack provides some good features like the usb support, Virtualbox RDP, disk encryption, NVMe and PXE boot for Intel cards. It is installed by the event nethserver-virtualbox-X.X-virtualbox-update automatically (by the installation or a rpm update). The pack is relevant of the VirtualBox version, if you need to update it, then trigger the event virtualbox-save :

```
signal-event virtualbox-save
```

50.6 The RDP console

You could use your own RDP software client for the installations of your guests, but phpVirtualBox comes with a Flash RDP console that you could use with your browser.

- The RDP console is restricted to the local network (default is green), the ports are between `[19000-19100]`. If you want to enable RDP for the external IP

```
config setprop phpvirtualhost accessRDP red
signal-event phpvirtualbox-save
```

- For specific needs you could specify the IP (default is ‘’) of the integrated RDP console

```
config setprop phpvirtualhost ipaddrRDP xxx.xxx.xxx.xxx
signal-event phpvirtualbox-save
```

50.7 VM networking

The networking side is probably the most difficult part of the virtualization, you should consult the VirtualBox Documentation

Promiscuous way Enable the promiscuous mode policy, select “Allow all” from the drop down list located in the network settings section.

W10 When you want to join a virtualized W10 to the sambaAD container, bridge the guest NIC to br0 and create a script

Example script

```
VBoxTunctl -u root -g vboxusers -t vbox0
ifconfig vbox0 up
brctl addif br0 vbox0
sudo -H -u vboxweb VBoxManage startvm VMname --type headless
```

50.8 Esmith database

You can modify the available properties of phpvirtualhost:

```
AdminGroup=vboxadmin        # members of this group can authenticate in  `AD` as␣
↪administrators
AdminUser=admin             # User list (comma separated) of administrators that can␣
↪authenticate in `LDAP`
AdvancedSettings=false      # Display the advanced settings in phpvirtualbox (true,␣
↪false)
Authentication=internal     # Authentication in phpvirtualbox: internal (builtin), AD␣
↪(SAMBA AD), LDAP (openldap)
DomainName=                 # If set, a domain name or FQDN is used instead of https://
↪server/phpvirtualbox
QuotaPerUser=5              # Number maximal of VMs allowed for non admin user
TCPPortsRDP=19000-19100       # RDP ports for the console RDP of phpvirtualbox (the␣
↪firewall is opened)
URL=                        # If set, the path is modified to https://server/URL
UserGroup=vboxuser          # members of this group can authenticate in  `AD` as␣
↪simple users
VMOwnerShip=true            # If set to true, users can see only their VM (true, false)
access=private              # Restric phpvirtualbox access (private, public)
accessRDP=green             # Access usage of the integrated RDP console (green, red)
ipaddrRDP=                  # Set the IP of the integrated RDP console for specific␣
↪need
status=enabled              # Enable phpvirtualbox (disabled, enabled)
```

Example:

```
config setprop phpvirtualbox accessRDP red AdvancedSettings enabled
signal-event phpvirtualbox-save
```

50.9 Documentation

VirtualBox The official VirtualBox documentation is available on the VirtualBox website.

phpVirtualbox The official phpVirtualbox documentation is available on the github website.

CHAPTER 51

HotSync

Note: This package is not supported in NethServer Enterprise

Warning: HotSync should be considered a beta release. Please test it on your environment before using in production.

Warning: For a correct restore, it's suggested to configure HotSync on two identical servers or two servers with same network cards number, name and position. If the master and slave servers differ, the restore procedure may behave unexpectedly (see *Troubleshooting*).

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.

51.1 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
- If an error occurs, an email is sent to root (admin if mail server is installed)
- SLAVE check updates and makes some system operations every 60 minutes

51.2 Installation

Install nethserver-hotsync on both MASTER and SLAVE from Software Center or execute from command line:

```
yum install -y nethserver-hotsync --enablerepo=nethforge
```

51.3 Configuration

You can configure HotSync from Cockpit interface: access it from Master and Slave, select role and fill required fields with password and IP. The `<PASSWORD>` must be the same on master and slave.

You can also configure HotSync from command line using these commands:

51.3.1 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
```

51.3.2 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
```

If mysql or postgresql are installed, they will be synchronized by default. You can disable databases sync from Master Cockpit interface or from command line on master machine with this command:

```
[root@master]# config setprop hotsync databases disabled
[root@master]# signal-event nethserver-hotsync-save
```

Note: If you are using HotSync to restore FreePBX leave databases enabled, otherwise FreePBX database will not be restored properly.

51.3.3 Enabling/Disabling

HotSync is enabled by default. To disable it uncheck the checkbox into HotSync Cockpit GUI or use this command:

```
[root@slave]# config setprop hotsync status disabled
[root@slave]# signal-event nethserver-hotsync-save
```

and to re-enable it re-check the checkbox on interface or use CLI:

```
[root@slave]# config setprop hotsync status enabled
[root@slave]# signal-event nethserver-hotsync-save
```

Note: After HotSync is configured, it's a good practice to launch `hotsync` command on master host. After master has properly syncronized, access the slave and execute `hotsync-slave`. You can force these commands also from Cockpit GUI and check `/var/log/messages` logs. As best practice, the first syncrhonization should be done via command line to better check if everything is properly configured.

Warning: After HotSync is configured and `hotsync` command executed properly, note that `hotsync-slave` command must be executed at least one time before proceed with `hotsync-promote`. You can launch it manually or wait 60 minutes for automatic execution.

51.4 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
   ```

   As best practice, execute following procedure using a local console and not via SSH connection.
4. on SLAVE launch the following command, and read carefully its output

   ```
   [root@slave]# hotsync-promote
   ```

   If no Internet connection is detected (e.g. you are restoring a firewall on a machine that was passing through crashed master for Internet connection), the scripts will purpose you some options

   ```
   1. Restore master network configuration (IMPORTANT: use this option only if two␣
   ↪servers are identical - NIC number, names and positions must be identical)
   2. Fix network configuration from Cockpit GUI (when restoring on different␣
   ↪hardware)
   3. Continue without internet: assign correct roles before proceed with this␣
   ↪option. Some events could fails (not recommended)
   ```

   else restore will start automatically. If you are restore on different hardware you could encounter DC errors.

Warning: When restoring on identical hardware choose option 1 and network configuration will be overwritten, else choose option 2. It's not recommended to start the promote procedure without Internet access. When restoring on a different hardware and you've choosed option 2, you can encounter DC errors. Please see *Troubleshooting*.

5. If necessary go to Server Manager or Cockpit GUI, in page `Network` and reassign roles to network interfaces as master one. Remember also to recreate bridge if you have configured DC. In case of DC errors consult troubleshooting section before proceed with network restore.
6. After everything has been restored, 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

51.5 Troubleshooting

51.5.1 After restore on different hardware DC is not working

Console could report some errors like these

```
[ERROR] /usr/libexec/nethserver/sambads: failed to add service primaries to system␣
↪keytab
Action: /etc/e-smith/events/nethserver-mail-server-update/S50nethserver-sssd-
↪initkeytabs FAILED
```

To solve this, restore network configuration as master (including bridges) and then launch

```
/sbin/e-smith/signal-event nethserver-dc-save
/sbin/e-smith/signal-event nethserver-sssd-save
```

51.5.2 After restore permissions on ibays are not correct

Restore permissions from Cockpit GUI, under File Server, open shared folder menu and click on `Restore permissions`.

51.5.3 After network restore server is unreachable

If you cannot reach server after a network reconfiguration, check configuration and, if it's correct, try launching this commands

```
/sbin/e-smith/signal-event interface-update
/sbin/e-smith/signal-event nethserver-firewall-base-update
```

If you cannot reach the server yet, use `network-recovery` tool.

51.5.4 Suggested check after restore

When all issues have been solved, please make that: - configuration is restored properly - all enabled services are working - applications interfaces (e.g. freepbx, webtop) are working - file server is working and users can log into shared folders - email server is working and users can send and receive emails - asterisk is working and users can make calls

Finally, reboot the system and check all services are working after boot.

51.6 Supported packages

All nethserver packages are supported. Here is a list of major NethServer packages:

- nethserver-antivirus
- nethserver-backup-config
- nethserver-backup-data
- nethserver-base
- nethserver-c-icap
- nethserver-cockpit
- nethserver-collectd
- nethserver-cups
- nethserver-dante
- nethserver-dc
- nethserver-dedalo
- nethserver-directory
- nethserver-dnsmasq
- nethserver-duc
- nethserver-ejabberd
- nethserver-evebox
- nethserver-fail2ban
- nethserver-firewall-base
- nethserver-freepbx > 14.0.3
- nethserver-httpd
- nethserver-hylafax
- nethserver-iaxmodem
- nethserver-ipsec-tunnels
- nethserver-janus
- nethserver-letsencrypt
- nethserver-lightsquid
- nethserver-mail

- nethserver-mattermost
- nethserver-mysql
- nethserver-ndpi
- nethserver-netdata
- nethserver-nextcloud
- nethserver-ntopng
- nethserver-nut
- nethserver-openssh
- nethserver-openvpn
- nethserver-pulledpork
- nethserver-restore-data
- nethserver-roundcubemail
- nethserver-samba
- nethserver-samba-audit
- nethserver-squid
- nethserver-squidclamav
- nethserver-squidguard
- nethserver-sssd
- nethserver-subscription
- nethserver-suricata
- nethserver-vpn-ui
- nethserver-vsftpd
- nethserver-webtop5 (z-push state is not synchronized)

Packages nethserver-ntopng and nethserver-evebox are reinstalled without migrating history.

Warning: To avoid errors on the slave host, do not make any changes to the modules from the Cockpit GUI except the HotSync module.

CHAPTER 52

Microsoft SQL Server

Note: This package is not supported in NethServer Enterprise

With this package you can install Microsoft SQL Server on NethServer: it will automatically configure Microsoft repository and default configuration.

52.1 Installation

To install this package go on Software Center and install Microsoft SQL Server application. Otherwise use this command:

```
yum install -y nethserver-mssql --enablerepo=nethforge
```

52.2 Default configuration

When installed the module generates a default configuration as follow: * Auto-generated SA password saved in /var/lib/nethserver/secrets/mssql * Create default MSSQL databases (master, model, msdb, tempdb) * Allow access to SQL service from Green network on default port 1433

User can change access network from Cockpit Services page or from Firewall section.

Database example:

```
mssql-server=service
    ProductId=express
    ProductKey=
    TCPPort=1433
    access=green
    status=enabled
```

52.3 Install mssql-server service

The package needs a first configuration. Please access the Cockpit application and select MSSQL edition between these options: Evaluation, Developer, Web, Express, Standard, Enterprise. Alternatively it is possibile also to insert a product key.

You can do this also from command line:

```
config setprop mssql-server ProductId <version>
signal-event nethserver-mssql-save
```

Instead, if you want to configure a product key use these commands:

```
config setprop mssql-server ProductId key
config setprop mssql-server ProductKey <ProductKey>
signal-event nethserver-mssql-save
```

Note: After save event is launched, Microsoft package download will starts: this phase can be long, depending on Internet connection.

Now your SQL Server is ready to use!

52.4 Helpful actions

Directly from Cockpit interface you can: * create a new database under Databases page * view and change SA password under Settings page * see SQL Server status in MSSQL Dashboard page * change SQL Server edition from Settings page

Warning: Don't change SA password from SQL Server, but use Cockpit interface. Otherwise NethServer will not able to load correct informations and perform backup-data.

52.5 Backup and restore

Configuration is saved with backup-config event. After you've restored configuration on new server download of MSSQL package will starts in post-config-restore event. Database are automatically saved in backup-data event. They will be restored in post-restore-data.

52.6 SQLCMD utility

You can use also classic SQLCMD utility by accessing it with this absolute path:

```
/opt/mssql-tools/bin/sqlcmd
```

CHAPTER 53

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
```

53.1 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`.

53.2 Backup

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

53.3 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
```

53.4 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 54

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.

54.1 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

54.2 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 mail client configuration and *Special SMTP access policies* section 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.

54.3 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
```

54.4 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 setprop ibay_name SmbProfileType default
signal-event ibay-mody ibay_name
```

Where `ibay_name` is the name of the ibay to configure.

54.5 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 NethServer 7 **using the most recent ISO**, register it then apply **all the latest core updates available**.
3. In the destination host, install all packages that cover the same features of the source.
4. Explode the full backup archive into some directory; for instance, create the directory `/var/lib/migration`.
5. In destination host, signal the event `migration-import`:

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

   This step will require some time.
6. Check for any error message in `/var/log/messages`:

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

54.6 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 **all the latest updates installed** and 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.

54.6.1 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.

54.6.2 Sync and migrate

If called with `-m` option, `rsync-migrate` will execute a final synchronization and upgrade the target machine.

Before executing the final migration, install all packages that cover the same features of the source.

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
```

CHAPTER 55

Upgrade from NethServer 6

The upgrade from NethServer 6 to NethServer 7 is obtained by means of three methods:

- *backup* (see also *Disaster recovery*)
- *rsync*
- *upgrade-tool*

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.

55.1 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.

55.1.1 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.

55.1.2 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!

55.2 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

55.2.1 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`

55.2.2 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.

55.3 Mail server

All mailboxes options like SPAM retention and quota, along with ACLs, user shared mailboxes and subscriptions are preserved.

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.

55.4 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

[1] Badlock vulnerability http://badlock.org/

The policy identifier selected by the upgrade procedure depends on the NethServer version and is documented in *Release notes 7*.

55.5 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.

55.6 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`.

55.7 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:

```
use NethServer::Password;
my $password = NethServer::Password::store('myservice');
```

Documentation available via perldoc command:

```
perldoc NethServer::Password
```

55.8 Upgrade from backup

1. Make sure to have an updated backup of the original installation.

[2] Nextcloud clients download https://nextcloud.com/install/#install-clients

2. Install NethServer 7 **using the most recent ISO** 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 -b <name>
```

   where *name* is the name of the configured data backup.

   Note: By default, the name of the *backup-data* configured on NethServer 6 is `backup-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.

55.9 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, and **latest updates installed**; 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.

55.9.1 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.

55.9.2 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.

55.10 Upgrade with Upgrade tool

The Upgrade tool module make it possible an **in-place upgrade** of NethServer from version 6 to version 7 with an automated procedure.

Please refer to the Upgrade tool page of NethServer 6 Administrator Manual.

CHAPTER 56

Documentation license

This documentation is distributed under the terms of **Creative Commons - Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)** license.

You are free to:

- **Share** — copy and redistribute the material in any medium or format
- **Adapt** — remix, transform, and build upon the material

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- **Attribution** — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **NonCommercial** — You may not use the material for commercial purposes.
- **ShareAlike** — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

This is a human-readable summary of (and not a substitute for) the full license available at: http://creativecommons.org/licenses/by-nc-sa/4.0/

Architecture documentation is from SME Server project and is licensed under GNU Free Documentation License 1.3 (http://www.gnu.org/copyleft/fdl.html). See http://wiki.contribs.org/ for original documentation.

CHAPTER 57

List of NethServer 7 ISO releases

Each subsection corresponds to an upstream ISO release. See also the ISO releases on Developer's manual.

57.1 7.8.2003

- 2020-05-05 final

57.2 7.7.1908

- 2019-10-07 final

57.3 7.6.1810

- 2018-12-17 final
- 2018-12-10 beta2

57.4 7.5.1804

- 2018-06-11 final
- 2018-05-31 rc
- 2018-05-21 beta

57.5 7.4.1708

- 2017-10-26 final - GA 2017-10-30
- 2017-09-21 beta1

57.6 7.3.1611

- 2017-07-31 update 1
- 2017-01-30 final - GA 2017-02-08
- 2017-01-18 rc4
- 2016-12-16 rc3

57.7 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

CHAPTER 58

Public issue trackers

List of public issue trackers related to NethServer.

- NethServer 7: https://github.com/NethServer/dev/issues
- NethServer 6: http://dev.nethserver.org/projects/nethserver/issues
- NethServer Enterprise: https://github.com/nethesis/dev/issues
- CentOS: https://bugs.centos.org/
- Red Hat: https://bugzilla.redhat.com

CHAPTER 59

Index

CHAPTER 60

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.

CHAPTER 61

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

CHAPTER 62

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*.

62.1 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.

62.2 Delete

Removes the selected entry.

CHAPTER 63

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 virtual-hosts, 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).

CHAPTER 64

TLS policy

Enforced security level Configures the system services as described in the *TLS policy* section

Index

N

O

P

Q

R

S

T

U

V

W

X

Z