NethServer Documentation

Versión 6.10 Final

Nethesis

01 de diciembre de 2020

Índice general

Sitio oficial: www.nethserver.org

Advertencia: On November 30, 2020 NethServer 6 entered the End-Of-Life (EOL) phase. See the instructions to upgrade to NethServer 7.

CAPÍTULO 1

Notas de lanzamiento 6.10 Final

1.1 Notas de la versión

NethServer versión 6.10 Final

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

1.1.1 Major changes on 2018-07-23

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

1.1.2 Upgrade of version 6.9 to 6.10

Inicie la actualización como de costumbre en la página *Centro de software*. Se recomienda reiniciar el sistema al final del procedimiento de actualización.

CAPÍTULO 2

Instalación

2.1 Tipos de instalación

2.1.1 Requerimientos mínimos

Los requisitos mínimos son:

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

Consejo: Recomendamos utilizar al menos 2 discos para configurar un RAID 1. El software RAID garantizará la integridad de los datos en caso de fallo del disco.

Compatibilidad de hardware

NethServer es compatible con cualquier hardware certificado por Red Hat® Enterprise Linux® (RHEL®), que aparezca en hardware.redhat.com

2.1.2 Tipos de instalación

NethServer admite dos modos de instalación. En resumen:

Instalación desde ISO

- Descargar la imagen ISO
- Prepare a CD / DVD
- Seguir el asistente

Instalación desde YUM

- Instalar CentOS Minimal
- Configurar la red
- Instalar desde la red

2.1.3 Instalación desde ISO

Advertencia: ¡La instalación ISO borrará todos los datos existentes en los discos duros!

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

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

Al iniciar un menú se mostrarán diferentes tipos de instalación:

NethServer interactive install

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

Other / Unattended NethServer install

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

Las instalaciones estándar de CentOS

> Use the standard CentOS installation procedure.

Herramientas

> Inicie el sistema en el modo *rescate* (recuperación), ejecute una prueba de memoria o inicie la herramienta de detección de hardware.

Arranque desde una unidad local

> Intente iniciar un sistema que ya esté instalado en el disco duro.

Al final del proceso de instalación, se le pedirá que reinicie la máquina. Asegúrese de retirar el soporte de instalación antes de reiniciar.

Modo desatendido

After installation, the system will be configured as follows:

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

- Time zone: `Greenwich`
- Language: English
- Disks: if there are two or more disks, a RAID 1 will be created on first two disks

Install options

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

Para deshabilitar la raid, simplemente añada esta opción a la línea de comandos:

```
raid=none
```

Si necesita seleccionar los discos duros de instalación, utilice:

```
disks=sdx,sdy
```

Other available options:

- lang: system language, default is en_US
- keyboard: keyboard layout, default is us
- timezone: default is UTC Greenwich
- fspassword: enable file system encryption with given password This option can be used even in Interactive Mode

Interactive Mode

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

- Idioma
- Software RAID
- Network configuration

Idioma

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

System language is always set to English.

Software RAID

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

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

Available levels:

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

Spare disk

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

Contraseña del administrador del sistema

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

A good password is:

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

Default password is `Nethesis,1234`.

Encrypted file system

Al activar esta opción, todos los datos escritos en el disco se cifrarán mediante cifrado simétrico. En caso de robo, un atacante no podrá leer los datos sin la clave de cifrado.

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

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

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

Network interfaces

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

Network configuration

Host and Domain Name (FQDN)

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

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

IP Address

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

Netmask

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

Gateway

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

DNS

Type a valid DNS. Example: 8.8.8.8

End of installation procedure

After parameters input, the procedure will start the installation. See also *Próximos pasos*.

2.1.4 Instalar en CentOS

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

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

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

Enable specific YUM repositories with this command:

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

Para instalar el sistema base, ejecute:

```
nethserver-install
```

Alternativamente, para instalar el sistema base *and* módulos adicionales, pase el nombre del módulo como parámetro al script de instalación. Ejemplo:

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

2.1.5 Próximos pasos

Al final del procedimiento de instalación, *acceda por el administrador del servidor* a: ref:*Instalar software adicional <package_manager-section>*.

2.2 Accediendo al administrador del servidor

NethServer puede ser configurado mediante la interfaz web de *Server Manager*. Necesitas un navegador web como Mozilla Firefox o Google Chrome para acceder a la interfaz web mediante la dirección (URL) `https://a.b.c.d:980` o `https://server_name:980` donde *abcd* y *Server_name* son respectivamente la dirección IP y el nombre del servidor configurados durante la instalación.

Si el módulo del servidor web está instalado, también puede acceder a la interfaz web utilizando esta dirección `https://server_name/server-manager`.

El Administrador del Servidor utiliza certificados SSL autofirmados. Debe aceptarlos explícitamente la primera vez que acceda al servidor. La conexión es segura y encriptada.

2.2.1 Iniciar sesión

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

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

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

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

2.2.2 Session timeouts

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

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

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

To disable the timeouts

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

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

CAPÍTULO 3

Configuración

3.1 Sistema base

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

3.1.1 Dashboard

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

Analizador de disco

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

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

Las carpetas conocidas son:

- Carpetas compartidas: `/var/lib/nethserver/ibay`
- Directorios de los usuarios: `/var/lib/nethserver/home`
- Windows roaming profiles: `/var/lib/nethserver/profile`
- Correo: `/var/lib/nethserver/vmail`
- Faxes: `/var/lib/nethserver/fax`
- Bases de datos MySQL: `/var/lib/mysql`

3.1.2 Red

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

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

NethServer soporta un número ilimitado de interfaces de red. Cualquier red administrada por el sistema debe seguir estas reglas:

- Las redes deben estar físicamente separadas (no se pueden conectar múltiples redes al mismo conmutador/concentrador)
- Las redes deben estar lógicamente separadas: cada red debe tener direcciones diferentes
- private networks, like LANs, must follow address's convention from RFC1918 document. See *Dirección para redes privadas (RFC1918)*

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

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

Consulte *Política* para obtener más información sobre las funciones y las reglas de firewall.

Nota: El servidor debe tener al menos una interfaz de red. Cuando el servidor tiene sólo una interfaz, esta interfaz debe tener rol verde.

Si el servidor está instalado en un VPS público (Virtual Private Server), debe estar configurado con una interfaz verde. Todos los servicios críticos deben cerrarse mediante el panel *Servicios de red*.

Alias IP

Utilice alias IP para asignar más direcciones IP a la misma NIC.

El uso más común es con una interfaz roja: cuando el ISP proporciona un grupo de direcciones IP públicas (dentro de la misma subred), puede agregar algunas (o todas) a la misma interfaz en rojo y administrarlas individualmente (por ejemplo, en la configuración de reenvío de puertos).

La sección IP de alias se puede encontrar en el menú desplegable de la interfaz de red relacionada.

Nota: Los Alias de las IP en la interfaz PPPoE podrían no funcionar correctamente, debido a las diferentes implementaciones del servicio realizado por los proveedores de Internet.

Interfaces lógicas

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

- bond: arrange two or more network interfaces, provides load balancing and fault tolerance

- bridge: connect two different networks, it's often used for bridged VPN and virtual machine
- VLAN (Virtual Local Area Network): crea dos o más redes separadas lógicamente utilizando una sola interfaz
- PPPoE (Point-to-Point Protocol over Etherne): conéctese a Internet a través de un módem DSL

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

Modos que proporcionan equilibrio de carga y tolerancia a fallos:

- Balance Round Robin (recomendado)
- Balance XOR
- 802.3ad (LACP): requiere soporte a nivel de controlador y un conmutador con IEEE 802.3ad Modo de agregación de vínculo dinámico habilitado
- Balance TLB: requiere soporte a nivel de driver
- Balance ALB

Modos que proporcionan tolerancia a fallos solamente:

- Copia de seguridad activa (recomendado)
- Política de difusión

Un **puente** tiene la función de conectar los diferentes segmentos de la red, por ejemplo, permitiendo máquinas virtuales, o un cliente conectado a través de una VPN, para acceder a la red local (verde).

Cuando no es posible separar físicamente dos redes diferentes, puede utilizar una **VLAN** etiquetada. El tráfico de las dos redes se puede transmitir en el mismo cable, pero se manejará como si fuera enviado y recibido en tarjetas de red separadas. El uso de VLAN, requiere switches configurados correctamente.

Advertencia: La interfaz lógica **PPPoE** debe asignarse al rol rojo, por lo que se requiere la funcionalidad de la pasarela o gateway. Véase *Firewall y gateway / Cortafuego y Puerta de enlace* para más detalles.

Dirección para redes privadas (RFC1918)

Las redes privadas TCP/IP que no estén conectadas directamente a Internet deben utilizar direcciones especiales seleccionadas por la Autoridad de Números Asignados de Internet (IANA).

Red privada	Máscara de subred	Intervalo de direcciones IP
10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 - 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

3.1.3 Servicios de red

Un servicio de red es un servicio que se ejecuta en el propio firewall.

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

Available policies are:

- Access only from green networks (private): all hosts from green networks and from VPNs

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

Custom access

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

Example

Given the following configuration:

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

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

3.1.4 Redes de confianza

Las redes de confianza son redes especiales (locales, VPN o remotas) que pueden acceder a los servicios de un servidor especial.

Por ejemplo, los hosts dentro de redes de confianza pueden acceder a:

- Administrador del servidor
- Carpetas compartidas (SAMBA)

Si la red remota es accesible mediante un router, recuerde agregar una ruta estática dentro de la página *Rutas estáticas*.

3.1.5 Rutas estáticas

Esta página permite crear rutas estáticas especiales que usará la puerta de enlace especificada. Estas rutas se utilizan generalmente para conectar la red privada.

Recuerde agregar la red a *Redes de confianza*, si desea permitir que los hosts remotos tengan acceso a los servicios locales.

3.1.6 Organización contactos

Los campos de la página *Organización contactos* se utilizan como valores predeterminados para las cuentas de usuario. El nombre y la dirección de la organización también se muestran en la pantalla de inicio de sesión del Administrador del servidor.

3.1.7 Certificado del servidor

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

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

Nota: Para evitar problemas al importar el certificado en Internet Explorer, el campo Nombre Común (CN) debe coincidir con el FQDN de servidor.

Install a custom certificate

Custom certificates should be placed inside the following standard directories:

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

Set the private key and certificate file paths:

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

You can also set a SSL certificate chain file:

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

Notify registered daemons about certificate update:

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

Custom certificate backup

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

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

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

Let's Encrypt certificate

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

From https://letsencrypt.readthedocs.org:

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

Prerequisites

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

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

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

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

How it works

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

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

Ejemplo

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

The server must:

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

Installation

Install the package from command line:

```
yum install nethserver-letsencrypt
```

Configuration

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

Certificate for FQDN

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

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

Certificate for server alias (optional)

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

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

Example for “”alias.mydomain.com”” alias:

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

Options

You can customize the following options by using config command:

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

Example:

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

Test certificate creation

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

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

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

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

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

Obtaining a valid certificate

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

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

Access your http server and check your certificate is valid.

3.1.8 Change user password

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

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

- Name and surname
- External mail address

The user can also overwrite fields set by the administrator:

- Company
- Office
- Address
- City

3.1.9 Apagar

La máquina donde NethServer está instalado puede reiniciarse o detenerse desde la página *Apagar*. Seleccione una opción (reiniciar o detener) y, a continuación, haga clic en el botón Enviar.

Utilice siempre este módulo para evitar un apagado incorrecto que pueda causar daños en los datos.

3.1.10 Visor de registro

Todos los servicios guardarán las operaciones dentro de los archivos llamados *logs*. El análisis de log es la herramienta principal para encontrar y resolver problemas. Para analizar los archivos de registro, haga clic en *Visor de registro*.

Este módulo permite:

- Iniciar la búsqueda en todos los registros del servidor
- Mostrar un solo registro
- Seguir el contenido de un registro en tiempo real

3.1.11 Fecha y hora

Después de la instalación, asegúrese de que el servidor esté configurado con la zona horaria correcta. El reloj de la máquina puede configurarse manual o automáticamente utilizando servidores públicos NTP (de preferencia).

El reloj de la máquina es muy importante en muchos protocolos. Para evitar problemas, todos los hosts en LAN se pueden configurar para utilizar el servidor como servidor NTP.

3.1.12 Ayuda en línea

Todos los paquetes dentro del Administrador del servidor contienen una ayuda en línea. La ayuda en línea explica cómo funciona el módulo y todas las opciones disponibles.

Estas páginas de ayuda están disponibles en todos los idiomas del Administrador de servidores.

Puede encontrar una lista de todas las páginas de ayuda en línea disponibles en la dirección:

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

Ejemplo

Si el servidor tiene la dirección «192.168.1.2», y desea ver todas las páginas de ayuda en inglés, use esta dirección:

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

3.2 Centro de software

NethServer es altamente modular: al final de la instalación sólo el sistema base estará listo para ser utilizado. El sistema básico incluye módulos como la configuración de la red y el visor de registros. El administrador puede instalar módulos adicionales como *Correo electrónico*, :ref:dhcp-section‘ y *Firewall y gateway / Cortafuego y Puerta de enlace*.

La página principal muestra todos los módulos disponibles e instalados (comprobados). La vista puede filtrarse por categoría.

Para instalar un módulo, marque la casilla correspondiente y haga clic en *Aplicar*. Para quitar un módulo, desmarque la casilla correspondiente y haga clic en :guilabel: *Aplicar*. La página siguiente reanudará todas las modificaciones y mostrará todos los paquetes opcionales.

Nota: Los paquetes opcionales se pueden agregar al sistema *después* de la instalación del componente principal. Simplemente haga clic de nuevo en *Aplicar* y seleccione paquetes opcionales desde la página de confirmación.

La sección *Software instalado* muestra todos los paquetes ya instalados en el sistema.

CAPÍTULO 4

Módulos

4.1 Copia de seguridad

Backup es la única manera de restaurar una máquina cuando ocurren desastres. El sistema maneja dos tipos de copia de seguridad:

- copia de seguridad configuración
- copia de seguridad datos

La copia de seguridad de la configuración sólo contiene los archivos de configuración del sistema. Está programada para ser ejecutada cada noche y creará un nuevo archivo, `/var/lib/nethserver/backup/backup-config.tar.xz`, sólo si algún archivo se cambia en las últimas 24 horas. La copia de seguridad de la configuración también guarda una lista de módulos instalados. Todos los módulos se reinstalarán durante el proceso de restauración de la configuración. El propósito de este tipo de copia de seguridad es restaurar rápidamente una máquina en caso de recuperación de desastres. Cuando la máquina está funcionando, se puede realizar una restauración completa de los datos incluso si la máquina ya está en producción.

La copia de seguridad de datos está habilitada para instalar el módulo de «copia de seguridad» y contiene todos los datos como los directorios y correos de inicio del usuario. Se ejecuta cada noche y puede ser completa o incremental sobre una base semanal. Esta copia de seguridad también contiene el archivo de la copia de seguridad de configuración.

Data backup can be saved on three different destinations:

- USB: disco conectado a un puerto USB local (Ver: *Configuración del disco USB*)
- CIFS: Carpeta compartida de Windows, está disponible en todas las NAS (Network Attached Storage)
- NFS: Carpeta compartida de Linux, está disponible en todas las NAS, generalmente más rápido que CIFS

El estado de la copia de seguridad se puede notificar al administrador del sistema o a una dirección de correo externa.

Nota: El directorio de destino se basa en el nombre de host del servidor: en caso de cambio de FQDN, el administrador debe tener cuidado de copiar los datos de copia de seguridad del directorio antiguo al nuevo.

4.1.1 Restauración de datos

Asegúrese de que el destino de la copia de seguridad está accesible (por ejemplo, debe estar conectado el disco USB).

Linea de comandos

Listado de archivos

Es posible listar todos los archivos dentro de la última copia de seguridad usando este comando:

```
backup-data-list
```

El comando puede tomar algún tiempo dependiendo del tamaño de la copia de seguridad.

Archivo y directorio

Todos los archivos relevantes se guardan en el directorio `/var/lib/nethserver/`

- Correos: `/var/lib/nethserver/vmail/<user>`
- Carpetas compartidas: `/var/lib/nethserver/ibay/<name>`
- Página de inicio del usuarios: `/var/lib/nethserver/home/<user>`

Para restaurar un archivo/directorio, utilice el comando:

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

Ejemplo, restaure la cuenta de correo *prueba* al directorio `/tmp`:

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

Ejemplo, restaure la cuenta del correo *prueba* a la posición original:

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

El sistema puede restaurar una versión anterior de directorio (o archivo).

Ejemplo, restaure la versión de un archivo de hace 15 días:

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

La opción `-t` permite especificar el número de días (15 en este escenario).

Interfaz gráfica

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

Hay dos opciones para restaurar:

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

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

Para usar el campo de búsqueda, simplemente inserte al menos 3 caracteres y la búsqueda se inicia automáticamente, resaltando los directorios coincidentes

Es posible restaurar los directorios haciendo clic en el botón **Restaurar**.

Nota: La selección múltiple se puede hacer con la tecla Ctrl presionada.

4.1.2 Recuperación de desastres

El sistema se restablece en dos fases: primero configuración, luego datos. Justo después de la restauración de la configuración, el sistema está listo para ser utilizado si se instalan paquetes adecuados. Puede instalar paquetes adicionales antes o después de la restauración. Por ejemplo, si el servidor de correo está instalado, el sistema puede enviar y recibir correo.

Otras configuraciones restauradas:

- Usuarios y grupos
- Certificados SSL

Nota: La contraseña de root/admin no se ha restaurado.

Pasos a ejecutar:

1. Instale la nueva máquina con el mismo nombre de host que el antiguo
2. Configurar una copia de seguridad de datos, para que el sistema pueda recuperar datos guardados y configuración
3. If the old machine was the network gateway, remember to re-install firewall module
4. Restaurar la copia de seguridad de la configuración desde la página *Copia de seguridad (configuración)* > *Restaurar* en el Administrador de servidores, o ejecutar: **`restore-config`**
5. Si un mensaje de advertencia lo requiere, reconfigure la asignación de roles de red. Ver *Restaurar funciones de red* a continuación.
6. Verificar que el sistema es funcional
7. Restaurar la copia de seguridad de datos ejecutando: **`restore-data`**

Restaurar funciones de red

Si la configuración de roles apunta a una placa de red ausente, las páginas *Dashboard*, *Copia de seguridad (configuración)* > *Restaurar* y *Red* muestran una advertencia. Esto podría suceder en los siguientes casos:

- La copia de seguridad de la configuración se ha restaurado en un nuevo hardware
- Una o más tarjetas de red han sido sustituidas
- Los discos del sistema se mueven a una nueva máquina

La advertencia sugiere una página que muestra una lista de placas de red instaladas en el sistema, resaltando las que no tienen asignadas un rol *rol*. A estas últimas, se les puede restaurar el rol desde el menú desplegable.

Por ejemplo, si una placa de red de rol «naranja» ha sido reemplazada; en el menú desplegable aparecerá listado un elemento «naranja» cerca de la placa de red.

Lo mismo se aplica si la tarjeta antigua era un componente de una interfaz lógica, como un puente o enlace.

Escogiendo un elemento del menú desplegable, el rol antiguo se transfiere a la nueva interfaz física.

Haga clic en el botón *Submit* para aplicar los cambios.

Advertencia: Elija cuidadosamente la nueva asignación de interfaces: ¡cometer un error aquí podría conducir a tener un sistema aislado de la red!

Si el papel que falta es `green`, un procedimiento interactivo pide que se fije la configuración durante el arranque, para asegurar una conectividad de red mínima y volver a iniciar sesión en el Administrador del servidor.

Restaure los módulos instalados

De forma predeterminada, el proceso de restauración de la configuración también restaurará todos los módulos previamente instalados.

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

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

4.1.3 Personalización de la copia de seguridad de datos

Si se instala software adicional, el administrador puede editar la lista de archivos y directorios incluidos (o excluidos).

Inclusion

Si desea agregar un archivo o carpeta para copias de seguridad, agregue una línea al archivo `/etc/backup-data.d/custom.include`.

Por ejemplo, para hacer una copia de seguridad de un software instalado en el directorio `/opt`, agregue esta línea:

```
/opt/mysoftware
```

Exclusion

Si desea excluir un archivo o carpeta de hacer copias de seguridad, agregue una línea al archivo `/etc/backup-data.d/custom.exclude`.

Por ejemplo, para excluir todos los directorios llamados *Download*, agregue esta línea:

```
**Download**
```

Para excluir un listado de direcciones llamado *test*, agregue la siguiente línea:

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

La misma sintaxis se aplica a la copia de seguridad de configuración. Modificar el archivo `/etc/backup-config.d/custom.exclude`.

Nota: Asegúrese de no dejar líneas vacías dentro de los archivos editados.

4.1.4 Personalización de la copia de seguridad de la configuración

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

Inclusion

Si desea agregar un archivo o directorio a la copia de seguridad de la configuración, agregue una línea al archivo `/etc/backup-config.d/custom.include`.

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

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

No agregue directorios o archivos grandes a la copia de seguridad de la configuración.

Exclusion

Si desea excluir un archivo o directorio a la copia de seguridad de la configuración, agregue una línea al archivo `/etc/backup-config.d/custom.exclude`.

Nota: Asegúrese de no dejar líneas vacías dentro de los archivos editados. La sintaxis de la copia de seguridad de configuración sólo admite rutas de directorio y de archivos simples.

4.1.5 Configuración del disco USB

El mejor sistema de archivos para copias de seguridad en unidades USB es EXT3. El sistema FAT se puede usar pero *no es recomendado*. Con NTFS directamente **no funciona**.

Antes de formatear el disco, adjúntelo al servidor y busque el nombre del dispositivo:

```
# 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
```

(continué en la próxima página)

(proviene de la página anterior)

```
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
```

Otro buen comando podría ser:

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

En este escenario, el disco es accesible como dispositivo *sdc*.

- Crear una partición Linux en todo el disco:

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

- Cree el sistema de archivos en la partición *sdc1* con una etiqueta denominada *backup*:

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

- Desconecte y vuelva a conectar el disco USB:

  Puede simularlo con el siguiente comando:

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

- Ahora la etiqueta *backup* aparecerá en la página *Copia de seguridad (datos)*.

4.2 Usuarios y grupos

4.2.1 Usuarios

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

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

Cuando se crea un usuario, los siguientes campos son obligatorios.

- Username
- Name
- Surname

Optional fields:

- Company
- Office
- Address
- City

- Phone

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

Un usuario puede ser agregado a uno o mas grupos de la pagina *Usuarios* o de la pagina *Grupos* .

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

Nota: Cuando se elimina un usuario, también se eliminarán todos los datos del usuario.

Access to services

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

4.2.2 Grupos

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

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

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

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

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

4.2.3 Cuenta de administrador

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

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

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

4.2.4 Gestión de contraseñas

El sistema proporciona la capacidad de establecer restricciones en la contraseña *complejidad* y *expiración*.

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

Complejidad

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

- *none*: no hay control específico sobre la contraseña introducida, pero la longitud mínima es de 7 caracteres
- *strong*

La directiva strong requiere que la contraseña cumpla con las siguientes reglas:

- Longitud mínima de 7 caracteres
- Contiene al menos 1 número
- Contiene al menos 1 carácter en mayúscula
- Contiene al menos 1 carácter minúscula
- Contiene al menos 1 carácter especial
- Al menos 5 caracteres diferentes
- No debe estar presente en los diccionarios de palabras comunes
- Debe ser diferente del nombre de usuario
- No se pueden realizar repeticiones de patrones formados por 3 o más caracteres (por ejemplo, la contraseña As1.$ AS1. $ No es válida)

La directiva predeterminada es: dfn:*strong*.

Advertencia: El cambio de las políticas predeterminadas es contraindicado. El uso de contraseñas débiles a menudo conduce a servidores comprometidos por atacantes externos.

To change the setting to none

```
config setprop passwordstrength Users none
```

To change the setting to strong

```
config setprop passwordstrength Users strong
```

Check the policy currently in use on the server

```
config getprop passwordstrength Users
```

Vencimiento

La Caducidad de contraseña está habilitada de forma predeterminada a 6 meses desde el momento en que se establece la contraseña. El sistema enviará un correo electrónico para informar a los usuarios cuando su contraseña está a punto de expirar.

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

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

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

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

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

Below are the commands to view enabled policies.

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

```
config getprop passwordstrength MaxPassAge
```

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

```
config getprop passwordstrength MinPassAge
```

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

```
config getprop passwordstrength PassWarning
```

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

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

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

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

Effects of expired password

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

Domain password

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

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

4.2.5 Notification language

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

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

Example for Italian:

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

4.2.6 Importar usuarios

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

```
username    firstName    lastName    email    password
```

Ejemplo:

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

Make sure the mail server is installed, then execute:

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

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

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

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

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

4.3 Correo electrónico

The Email module is split in three main parts:

- Servidor SMTP para enviar y recibir[1]
- Servidor IMAP y POP3 para leer el correo electrónico[2], y el lenguaje Sieve para organizarlo[3]
- Filtro anti-spam, antivirus y bloqueador de archivos adjuntos[4]

Los beneficios son

- autonomía completa en la gestión del correo electrónico
- evitar problemas por el Proveedor de Servicios de Internet
- capacidad de seguimiento de la ruta de los mensajes con el fin de detectar errores
- análisis antivirus y antispam optimizados

Consulte también los siguientes temas relacionados:

- Cómo funciona el correo electrónico[5]
- Registro MX DNS[6]

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

- Simple Mail Transfer Protocol (SMTP)[7]

4.3.1 Dominios

NethServer puede manejar un número ilimitado de dominios de correo, configurable desde la página *Correo electrónico* > *Dominios*. Para cada dominio hay dos alternativas:

- *Entregar* mensajes a buzones locales, de acuerdo con el formato Maildir[8].
- *Retransmitir* mensajes a otro servidor de correo.

Nota: Si se elimina un dominio, el correo electrónico no se eliminará; Se conserva cualquier mensaje recibido.

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

Advertencia: En algunos países, habilitar la opción *Enviar siempre una copia (Cco)* puede estar en contra de las leyes de privacidad.

NethServer puede automáticamente *añadir un aviso legal a los mensajes enviados*. Este texto se llama *renuncia* y puede utilizarse para cumplir con algunos requisitos legales. Tenga en cuenta *firma* y renuncia son conceptos muy diferentes.

La firma debe insertarse dentro del texto del mensaje sólo por el cliente de correo (MUA, Mail User Agent): Outlook, Thunderbird, etc. Normalmente es un texto definido por el usuario que contiene información como direcciones de remitente y números de teléfono.

Ejemplo de firma:

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

La «renuncia» es un texto fijo y solo puede ser *adjunto* (no añadido) a los mensajes del servidor de correo.

Esta técnica permite mantener la integridad del mensaje en caso de firma digital.

Ejemplo de renuncia:

```
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.
```

El texto de la renuncia puede contener el código Markdown[9] para dar formato al texto.

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

4.3.2 Correos electrónicos

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

- Primer dominio: mydomain.net
- Segundo dominio: example.com
- La dirección de correo electrónico *info* es válida para ambos dominios: info@mydomain.net, info@example.com
- Dirección de correo electrónico *goofy* válido sólo para un dominio: goofy@example.com

A veces una compañía prohíbe las comunicaciones de fuera de la organización usando direcciones de correo electrónico personales. La opción *Sólo red local* bloquea la posibilidad de una dirección para recibir correo electrónico desde el exterior. Sin embargo, la dirección «sólo de red local» se puede utilizar para intercambiar mensajes con otras cuentas del sistema.

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

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

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

4.3.3 User and group mailboxes

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

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

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

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

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

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

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

- IMAP[10] (recomendado)
- POP3[11] (obsoleto)

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

Por razones de seguridad, todos los protocolos requieren el cifrado STARTTLS de forma predeterminada. El comando *Permitir conexiones sin cifrar*, desactiva este requisito importante y permite pasar contraseñas y contenido de correo de texto claro en la red.

Advertencia: ¡No permita conexiones no cifradas en entornos de producción!

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

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

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

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

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

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

4.3.4 Mensajes

Desde la página *Correo electrónico* > *Mensajes*, el cursor *Máximo tamaño del mensajes de cola* ajusta el tamaño máximo de los mensajes que atraviesan el sistema. Si se excede este límite, un mensaje no puede entrar en el sistema en absoluto y se rechaza.

Una vez que un mensaje entra en NethServer, se mantiene en una *cola*, esperando la entrega final o la retransmisión. Cuando NethServer retransmite un mensaje a un servidor remoto, pueden producirse errores. Por ejemplo,

- La conexión de red falla, o
- El otro servidor está inactivo o está sobrecargado.

Estos y otros errores son *temporales*: en tales casos, NethServer intenta volver a conectar el host remoto a intervalos regulares hasta que se alcance un límite. El control deslizante *Vida del mensaje de cola* cambia este límite. De forma predeterminada, se establece en *4 días*.

Mientras los mensajes están en la cola, el administrador puede solicitar un intento inmediato de retransmisión de mensajes, pulsando el botón *Intento de envío* desde la página *Correo electrónico* > *Gestión de colas*. De lo contrario, el administrador puede eliminar de forma selectiva los mensajes en cola o vaciarla con el botón *Borrar todo*.

Para mantener una copia oculta de cualquier mensaje que atraviese el servidor de correo, active la casilla de verificación *Enviar siempre una copia (Cco)*. Esta característica es diferente de la misma casilla de verificación en *Correo electrónico* > *Dominio*, ya que no diferencia entre dominios de correo y captura también cualquier mensaje saliente.

Advertencia: En algunos países, habilitar la opción *Enviar siempre una copia (Cco)* puede estar en contra de las leyes de privacidad.

La opción *Enviar usando un host inteligente*, obliga a dirigir todos los mensajes salientes a través de un servidor SMTP especial, llamado técnicamente *smarthost*. Un smarthost acepta transmitir mensajes bajo algunas restricciones. Se podría comprobar:

- La dirección IP del cliente,
- Las credenciales SMTP AUTH del cliente.

Nota: Por lo general, no se recomiendan envíos a través de *smarthost*. Puede ser utilizado sólo si el servidor está temporalmente en la lista negra[12], o el acceso SMTP normal está restringido por el ISP.

4.3.5 Filtro

Todos los mensajes de correo electrónico en tránsito están sujetos a una lista de comprobaciones que se pueden activar selectivamente en la página: *Correo electrónico* > *Filtro*

- Bloque de archivos adjuntos
- Anti-virus
- Anti-spam

Bloque de archivos adjuntos

El sistema puede inspeccionar los archivos adjuntos de correo, denegando el acceso a mensajes que contengan formatos de archivo prohibidos. El servidor puede comprobar las siguientes clases de datos adjuntos:

- ejecutables (eg. exe, msi)
- archivos (eg. zip, tar.gz, docx)
- Lista de formato de archivo personalizado

El sistema reconoce los tipos de archivo mirando su contenido, independientemente del nombre del archivo adjunto. Por lo tanto, es posible que el archivo MS Word (docx) y OpenOffice (odt) estén bloqueados porque en realidad también son archivos zip.

Anti-virus

El componente antivirus detecta mensajes de correo electrónico que contienen virus. Los mensajes infectados se descartan. La base de datos de firmas de virus se actualiza periódicamente.

Anti-spam

El componente anti-spam[14] analiza los correos electrónicos detectando y clasificando mensajes *spam*[13] usando criterios heurísticos, reglas predeterminadas y evaluaciones estadísticas sobre el contenido de los mensajes. Las reglas son públicas y se actualizan regularmente. El filtro también puede comprobar si el servidor remitente aparece en una o más listas negras (DNSBL). Una puntuación está asociada a cada regla.

[12] DNSBL http://en.wikipedia.org/wiki/DNSBL
[14] Página de inicio de Spamassassin http://wiki.apache.org/spamassassin/Spam
[13] SPAM http://en.wikipedia.org/wiki/Spamming

La puntuación total de spam recogida al final del análisis permite al servidor decidir si *rechazar* el mensaje o *marcarlo* como spam y entregarlo de todos modos. Los umbrales de puntuación se controlan mediante los siguientes controles *Umbral de spam* y *Denegar el umbral de spam de mensajes* en la página *Correo electrónico* > *Filtro*.

Los mensajes marcados como spam tienen una cabecera especial `X-Spam-Flag: SI`. La opción *Añadir un prefijo al asunto de los mensajes de spam* hace que el indicador de spam sea visible en el asunto del mensaje, prefijando la cadena dada al encabezado‘‘Asunto‘‘.

Los filtros estadísticos, llamados Bayesian[15], son reglas especiales que evolucionan y se adaptan rápidamente al análisis de mensajes marcados como **spam** o **ham**.

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

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

De forma predeterminada, todos los usuarios pueden entrenar los filtros utilizando esta técnica. Si existe un grupo llamado `spamtrainers`, sólo los usuarios de este grupo podrán entrenar los filtros.

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

Si el sistema no reconoce el spam correctamente incluso después del entrenamiento, las *listas blancas* y *listas negras* pueden ayudar. Esas son listas de direcciones de correo electrónico o dominios respectivamente siempre permitidos y siempre bloqueados para enviar o recibir mensajes.

La sección *Reglas por correo electrónico* permite crear tres tipos de reglas:

- *Bloquear de*: cualquier mensaje del remitente especificado está bloqueado
- *Permitir de*: se acepta cualquier mensaje del remitente especificado
- *Permitir a*: se acepta cualquier mensaje al destinatario especificado

Es posible crear una regla de «Permitir» o «Bloquear» incluso para un dominio de correo electrónico completo, no sólo para una dirección de correo electrónico única: solo necesita especificar el dominio deseado (por ejemplo: nethserver.org).

Nota: Las verificaciones de antivirus se aplican a pesar de la configuración de *lista blanca*.

4.3.6 Bloquear el puerto 25

Si el sistema actúa como puerta de enlace de red, las zonas verde y azul no podrán enviar correo a servidores externos a través del puerto 25 (SMTP). El bloqueo del puerto 25 podría impedir que las máquinas controladas remotamente dentro de la LAN enviasen SPAM.

El administrador puede cambiar esta política creando una regla de firewall personalizada dentro de la página *Reglas*.

[15] Bayesian filtering http://en.wikipedia.org/wiki/Naive_Bayes_spam_filtering

4.3.7 Configuración del cliente

El servidor admite clientes de correo electrónico estándar que cumplan con los siguientes puertos IANA:

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

La autenticación requiere el comando STARTTLS y admite las siguientes variantes:

- LOGIN
- PLAIN

También los siguientes puertos habilitados para SSL están disponibles para software heredado que aún no admite STARTTLS:

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

Advertencia: El puerto estándar SMTP 25 está reservado para transferencias de correo entre servidores MTA. En los clientes sólo utilizan puertos de envío.

Si NethServer actúa también como servidor DNS en la LAN, registra su nombre como registro MX junto con los siguientes alias:

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

Por ejemplo:

- Dominio: `mysite.com`
- Hostname: `mail.mysite.com`
- MX record: `mail.mysite.com`
- Aliases disponibles: `smtp.mysite.com`, `imap.mysite.com`, `pop.mysite.com`, `pop3.mysite.com`.

Nota: Algunos clientes de correo electrónico (por ejemplo, Mozilla Thunderbird) pueden utilizar alias de DNS y registro MX para configurar automáticamente las cuentas de correo electrónico simplemente escribiendo la dirección de correo electrónico.

Para deshabilitar MX locales y alias, acceda a la consola de root y escriba:

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

4.3.8 Políticas especiales de acceso SMTP

La configuración predeterminada de NethServer requiere que todos los clientes utilicen el puerto de envío (587) con cifrado y autenticación habilitados para enviar correo a través del servidor SMTP.

Para facilitar la configuración de los entornos heredados, la página *Correo electrónico* > *Acceso SMTP* permite realizar algunas excepciones en la directiva de acceso SMTP predeterminada.

Advertencia: ¡No cambie la política predeterminada en nuevos entornos!

Por ejemplo, hay algunos dispositivos (impresoras, escáneres, . . .) que no son compatibles con la autenticación SMTP, el cifrado o la configuración de puertos. Estos pueden estar habilitado para enviar mensajes de correo electrónico por lista de su dirección IP en: guilabel:*Permitir la retransmisión de direcciones IP* area de texto

Además, bajo *Opciones avanzadas* hay otras opciones:

- La opción *Permitir la retransmisión desde redes de confianza* permite a cualquier cliente de las redes de confianza enviar mensajes de correo electrónico sin ninguna restricción.
- La opción *Habilitar la autenticación en el puerto 25* permite a los clientes SMTP autenticados enviar mensajes de correo electrónico también en el puerto 25.

4.3.9 HELO personalizada

El primer paso de una sesión SMTP es el intercambio de comando *HELO* (o *EHLO*). Este comando toma un nombre de servidor válido como parámetro requerido (RFC 1123).

NethServer y otros servidores de correo intentan reducir el spam al no aceptar dominios HELO que no estén registrados en un DNS público.

Al hablar con otro servidor de correo, NethServer utiliza su nombre de host completo (FQDN) como el valor para el comando HELO. Si el FQDN no está registrado en el DNS público, el HELO se puede fijar estableciendo un *apoyo* especial. Por ejemplo, asumiendo que «myhelo.example.com» es el registro DNS registrado públicamente, escriba los siguientes comandos:

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

Esta configuración también es valiosa si el servidor de correo está utilizando un servicio DNS dinámico gratuito.

4.3.10 Email in Active Directory

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

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

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

```
dn: CN=John Smith,OU=Sviluppo,OU=Nethesis,DC=adnethesis,DC=it
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
```

(continué en la próxima página)

(proviene de la página anterior)

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

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

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

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

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

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

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

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

4.3.11 Correo eliminado de Outlook

A diferencia de casi cualquier cliente IMAP, Outlook no mueve los mensajes eliminados a la papelera, pero simplemente los marca como «eliminados».

Es posible mover automáticamente mensajes dentro de la papelera utilizando los siguientes comandos:

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

También debe cambiar la configuración de Outlook para ocultar mensajes eliminados de la carpeta Bandeja de entrada. Esta configuración está disponible en el menú de opciones.

4.3.12 Registro

Cada operación del servidor de correo se guarda en los siguientes archivos de registro:

- `/var/log/maillog` registra todas las transacciones de correo
- `/var/log/imap` contiene las operaciones de inicio de sesión y cierre de sesión de los usuarios

Una transacción registrada en el archivo `maillog` normalmente implica diferentes componentes del servidor de correo. Cada línea contiene respectivamente

- La marca de tiempo,
- El nombre de host,
- El nombre del componente y el ID de proceso de la instancia de componente
- Un mensaje de texto que detalla la operación

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

`transfer/smtpd`

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

`submission/smtpd`

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

`amavis`

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

`queue/smtpd`

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

`relay/smtp`

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

`delivery/lmtp`

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

`dovecot`

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

Una imagen de todo el sistema está disponible en *workaround.org*[16].

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

Referencias

4.4 Webmail

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

- Simple y rápido
- Libreta de direcciones integradas adaptado con LDAP interno
- Soporte para mensajes HTML
- Soporte para carpetas compartidas
- Plugins

El webmail está disponible en las siguientes URL:

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

Por ejemplo, dado un servidor con dirección IP *192.168.1.1 * y nombre *mail.mydomain.com*, las direcciones válidas son:

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

4.4.1 Plugins

Roundcube supports many plugins already bundled within the installation.

Plugins enabled by default:

- Administrar filtros: gestionar filtros para el correo entrante
- Marcar como basura: marque los mensajes seleccionados como basura y muévalos a la carpeta de correo no deseado configurada

Other recommended plugins:

- Notificador de nuevo correo
- Emoticonos
- Soporte VCard

Los complementos se pueden agregar o eliminar editando la lista separada por comas dentro de la propiedad `Plugins`. Por ejemplo, para habilitar «notificación de correo», «marcar como basura» y «administrar filtrado», ejecute desde la línea de comandos:

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

Se puede encontrar una lista de complementos agrupados dentro del directorio `/usr/share/roundcubemail/plugins`. Para obtener la lista, ejecute:

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

4.4.2 Acceso

Con la configuración predeterminada webmail es accesible mediante HTTPS desde cualquier red.

Si desea restringir el acceso sólo a redes verdes y de confianza, ejecute:

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

Si desea abrir el acceso desde cualquier red:

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

4.5 Conector POP3

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

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

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

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

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

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

The underneath implementation is based on *Fetchmail*[1]. After fetching mail messages from the POP3/IMAP provider, Fetchmail delivers them locally by connecting directly to the local mail-filter server. All messages are filtered accordingly to the *configured rules*.

All operations are logged to the following files:

- `/var/log/fetchmail.log`

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

- `/var/log/maillog`

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

Referencias

4.6 POP3 proxy

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

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

It's possible to selectively activate following controls:

- antivirus: los mensajes que contienen virus son rechazados y se envía un correo electrónico de notificación al usuario
- spam: los mensajes serán marcados con las puntuaciones anti-spam apropiadas

4.6.1 POP3s

El proxy también puede interceptar conexiones POP3 en el puerto 995. El proxy establecerá una conexión segura con el servidor externo, pero el intercambio de datos con el cliente LAN estará en texto claro.

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

4.7 Carpetas compartidas

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

The available methods/protocols are:

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

4.7.1 Access privileges

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

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

4.7.2 Web access

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

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

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

Each URL has three components:

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

The *Web address* radio group defines the «path» component.

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

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

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

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

4.7.3 Configuring a web application

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

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

If the check box is enabled

- any file named `.htaccess` is loaded as configuration for Apache.
- a text file named `.htwritable` positioned in the root level of the shared folder may contain a list of sub-directories where Apache is granted write permission. The syntax of the file is one sub-directory for each line.

Lines beginning with `#` are comments. When the content of `.htwritable` changes, the *Reset permission* button must be pressed again to propagate the file system permissions.

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

4.7.4 Samba

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

Por ejemplo, las direcciones de red SMB de la carpeta `documentos` podrían ser

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

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

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

Si *Guest access* está habilitado, las credenciales de autenticación proporcionadas se consideran válidas.

Si *Navegable* está habilitado, la carpeta compartida aparece públicamente. Esto no afecta al permiso para usar este recurso.

4.8 Windows network

Microsoft Windows™ interoperability is provided by Samba[1]. To install it, select the *File Server* module, or any other module that requires it.

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

Currently the following roles are available:

- Workstation
- Primary Domain Controller
- Active Directory Member

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

Workstation

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

Primary Domain Controller

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

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

Active Directory member

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

4.8.1 Workstation

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

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

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

4.8.2 Primary domain controller

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

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

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

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

   For more information refer to Microsoft Naming conventions[2].

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

   Some versions of Windows may require applying a system registry patch to join the domain. From the Server Manager, follow *Client registry settings* link to download the appropriate `.reg` file. Refer to the official Samba documentation[3] for more information.

4.8.3 Active Directory member

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

[2] Naming conventions in Active Directory for computers, domains, sites, and OUs http://support.microsoft.com/kb/909264
[3] Registry changes for NT4-style domains https://wiki.samba.org/index.php/Registry_changes_for_NT4-style_domains

Joining an Active Directory domain has some pre-requisites:

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

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

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

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

4.9 Chat

El servicio: index:*chat* utiliza el protocolo estándar: index:*Jabber*/XMPP y soporta TLS en puertos estándar (5222 o 5223).

Las características principales son:

- Messages between users of the system
- Posibilidad de dividir a los usuarios en grupos, de acuerdo a la empresa o departamento / oficina
- Chat server's administrators
- Mensajes de difusión
- Grupo de chat
- Mensajes sin conexión
- Transferencia de archivos a través de LAN

Todos los usuarios del sistema pueden acceder al chat usando sus propias credenciales.

4.9.1 Cliente

Los clientes Jabber están disponibles para todas las plataformas de escritorio y móviles.

Algunos clientes comunes:

- Pidgin está disponible para Windows y Linux
- Adium para Mac OS X
- BeejibelIM para Android e iOS, Xabber sólo para Android

Cuando configure el cliente, asegúrese de que TLS (o SSL) esté habilitado. Introduzca el nombre de usuario y el dominio de la máquina.

Si NethServer Es también el servidor DNS de la red, el cliente debe buscar automáticamente la dirección del servidor a través de los registros DNS especiales preconfigurados. De lo contrario, especifique la dirección del servidor en las opciones avanzadas.

4.9.2 Administradores

Todos los usuarios dentro del grupo `jabberadmins` son considerados administradores del servidor de chat.

Los administradores pueden:

- Enviar mensajes de difusión
- Compruebe el estatus de los usuarios conectados

El grupo `jabberadmins` es configurable desde la página *Grupos*.

4.10 UPS

NethServer soporta la gestión de UPS (Uninterruptible Power Supply - Fuente de Poder Ininterrumpible) conectado al sistema.

El servidor se puede configurar de dos maneras:

- *maestro*: UPS está conectado directamente al servidor, el servidor acepta conexiones de esclavos
- *esclavo*: El UPS está conectado a otro servidor accesible a través de la red

---

Nota: Debes consultar la lista de modelos compatibles antes de comprar uno. A través de *Administración/Centro de software* instala el paquete de UPS. En *Configuración* aparece la nueva entrada *UPS* donde se puede encontrar el modelo compatible escribiendo en el campo *Buscar controlador para el modelo*.

En modo maestro, el UPS puede conectarse al servidor:

- en un puerto serial
- en un puerto USB
- con un adaptador USB a serial

En modo esclavo, deberá proporcionar la dirección IP del servidor maestro

La configuración predeterminada proporciona un apagado controlado en caso de ausencia de alimentación.

4.10.1 Dispositivo personalizado

Si el UPS está conectado a un puerto que no aparece en la interfaz web, puede configurar un dispositivo personalizado con los siguientes comandos:

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

4.10.2 Estadísticas del UPS

Si el módulo estadístico (collectd) está instalado y funcionando, el módulo recopilará automáticamente datos estadísticos sobre el estado del UPS.

4.11 Servidor de fax

El servidor de fax le permite enviar y recibir faxes a través de un módem conectado directamente a un puerto de servidor o a través de modem virtual.

La interfaz web le permite configurar:

- Código de área y número de fax
- Remitente (TSI)
- Un módem físico con parámetros de línea telefónica y cómo enviar / recibir faxes
- Uno o más *Módems virtuales*
- Notificaciones por correo electrónico para los faxes enviados y recibidos, con el documento adjunto en varios formatos (PDF, PostScript, TIFF)
- Imprimir faxes recibidos
- Impresora Virtual Samba
- Informe diario de los faxes enviados
- Envío de faxes por correo electrónico

4.11.1 Modem

Aunque HylaFAX admite un gran número de marcas y modelos, recomendamos el uso de un módem externo en serie o USB.

Si se bloquea un módem interno, debe reiniciar todo el servidor, mientras que un módem externo se puede desactivar por separado. Además, la mayoría de los módems internos del mercado pertenece a la llamada familia de winmodem, módems «de software» que necesitan un controlador, usualmente disponible sólo en Windows.

También tenga en cuenta que muchos módems externos USB también son winmodem.

Debe preferir los módems en Clase 1 o 1.0, especialmente si se basan en chips Rockwell/Conexant o Lucent/Agere. El sistema también admite módems en las clases 2, 2.0 y 2.1.

4.11.2 Cliente

Recomendamos utilizar el cliente de fax YajHFC (http://www.yajhfc.de/) que se conecta directamente al servidor y permite:

- El uso de una libreta de direcciones LDAP
- capacidad de seleccionar el módem para enviar
- Ver el estado de los módems

Autenticación

El sistema admite dos métodos de autenticación para enviar faxes:

- Basado en host: utiliza la dirección IP del equipo que envía la solicitud
- PAM: uses username and password, users must belong to the group *faxmaster*

Asegúrese también de habilitar la opción *Ver faxes de clientes*.

4.11.3 Impresora virtual Samba

Si la opción SambaFax está habilitada, el servidor creará una impresora virtual llamada «sambafax» disponible para la red local.

Cada cliente debe configurar la impresora mediante el controlador Apple LaserWriter 16/600 PS.

Los documentos enviados deben cumplir los siguientes requisitos previos:

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

```
Fax Number: 12345678
```

- La cadena puede estar presente en cualquier posición del documento, pero en una sola línea
- La cadena debe escribirse en fuentes sin mapa de bits (por ejemplo, Truetype)

Los faxes se enviarán mediante el ID de usuario que envía. Esta información se mostrará en la cola de faxes.

4.11.4 Mail2Fax

Todos los correos electrónicos enviados a la red local en `sendfax@<domainname>` serán transformados en un fax y enviados al destinatario.

El `<domainname>` debe coincidir con un dominio de correo local configurado para la entrega local.

El correo electrónico debe cumplir con este formato:

- El número del destinatario debe especificarse en el objeto (o asunto)
- El correo electrónico debe estar en formato de texto sin formato
- Puede contener archivos adjuntos como PDF o PS que se convertirán y enviarán con su fax

---

Nota: Este servicio está habilitado sólo para clientes que envían correo electrónico desde la red verde.

4.11.5 Módems virtuales

Los módems virtuales son módems de software conectados a un PBX (Asterisk usualmente) utilizando una extensión IAX.

La configuración de los módems virtuales consta de dos partes:

1. Creación de la extensión IAX dentro de la PBX
2. Configuración del módem virtual

4.12 Proxy web

El proxy web es un servidor que se encuentra entre las PCs de LAN y los sitios de Internet. Los clientes hacen peticiones al proxy que se comunica con sitios externos y luego envían la respuesta al cliente.

Las ventajas de un proxy web son:

- capacidad de filtrar contenido
- reducir el uso del ancho de banda mediante el almacenamiento en caché de las páginas que visita

El proxy sólo se puede activar en zonas verdes y azules. Los modos admitidos son:

- Manual: todos los clientes deben configurarse manualmente
- Los usuarios autenticados deben ingresar un nombre de usuario y una contraseña para navegar
- Transparente: todos los clientes se ven obligados automáticamente a usar el proxy para las conexiones HTTP
- SSL transparente: todos los clientes se obligan automáticamente a utilizar el proxy para las conexiones HTTP y HTTPS

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

4.12.1 Configuración del cliente

El proxy está siempre escuchando en el puerto **3128**. Cuando se utilizan modos manuales o autenticados, todos los clientes deben estar configurados explícitamente para usar el proxy. El panel de configuración es accesible desde la configuración del navegador. Por cierto, la mayoría de los clientes serán configurados automáticamente usando el protocolo WPAD. En este caso, es útil habilitar la opción *Bloquear puertos HTTP y HTTPS* para evitar el bypass de proxy.

Si el proxy está instalado en modo transparente, todo el tráfico web procedente de clientes se desvía a través del proxy. No se requiere configuración en los clientes individuales.

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

Nota: Para que el archivo WPAD sea accesible desde la red de invitados, agregue la dirección de la red azul dentro del campo *Permitir hosts* para el servicio httpd desde la página :guilabel:‘ Servicios de red‘.

4.12.2 Proxy SSL

Advertencia: Decrypting HTTPS connection without user consent is illegal in many countries.

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

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

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

4.12.3 Bypass

En algunos casos, puede ser necesario garantizar que el tráfico procedente de una dirección IP específica o destinado a algunos sitios no se enrute a través del proxy HTTP / HTTPS.

El proxy le permite crear:

- bypass por origen, configurable desde la sección *Hosts sin proxy*
- bypass por destino, configurable desde la sección *Sitios sin proxy*

Las reglas de bypass también se configuran dentro del archivo WPAD.

4.12.4 Reporte

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

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

4.12.5 Cache

En la pestaña *Cache* hay un formulario para configurar los parámetros del caché:

- El caché puede ser activado o desactivado (*desactivado* por defecto)
- **Tamaño de caché de disco**: valor máximo de caché de squid en disco (en MB)
- **Tamaño mínimo de objeto**: se puede dejar en 0 para almacenar en caché todo, pero puede ser elevado si no se desean objetos pequeños en la caché (en kB)
- **Tamaño máximo del objeto**: los objetos mayores que este valor no se guardarán en el disco. Si la velocidad es más deseable que ahorrar ancho de banda, esto debería establecerse en un valor bajo (en kB)

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

Sitios sin caché

En algún momento el proxy no puede manejar correctamente algunos sitios mal diseñados. Para excluir uno o varios dominios de la caché, utilice la propiedad `NoCache`.

Ejemplo:

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

4.12.6 Puertos seguros

Los puertos seguros son una lista de puertos accesibles mediante el proxy. Si un puerto no está dentro de la lista de puertos seguros, el proxy se negará a ponerse en contacto con el servidor. Por ejemplo, dado un servicio HTTP que se ejecuta en el puerto 1234, no se puede acceder al servidor mediante el proxy.

La propiedad `SafePorts` es una lista de puertos separados por comas. Los puertos listados se agregarán a la lista predeterminada de puertos seguros.

P.ej. Acceda a puertos adicionales 446 y 1234:

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

4.13 Filtro de contenido web

El filtro de contenido analiza todo el tráfico web y bloquea sitios web seleccionados o sitios que contienen virus. Los sitios prohibidos se seleccionan de una lista de categorías, que a su vez deben ser descargadas desde fuentes externas y almacenadas en el sistema.

El sistema permite crear un número infinito de perfiles. Un perfil se compone de tres partes:

- **Quién**: el cliente asociado con el perfil. Puede ser un usuario, un grupo de usuarios, un host, un grupo de hosts, una zona o una función de interfaz (como verde, azul, etc.).
- **Qué**: qué sitios pueden ser explorados por el cliente perfilado. Es un filtro creado dentro de la sección *Filtros*.
- **Cuando**: el filtro siempre se puede activar o validar sólo durante cierto período de tiempo. Los intervalos de tiempo se pueden crear dentro de la sección *Tiempos*.

Este es el orden recomendado para la configuración del filtro de contenido:

1. Seleccione una lista de categorías de la página *Listas negras* e inicie la descarga
2. Crear una o más condiciones de tiempo (opcional)
3. Crear categorías personalizadas (opcional)
4. Cree un filtro nuevo o modifique el predeterminado
5. Cree un nuevo perfil asociado a un usuario u host, luego seleccione un filtro y un marco de tiempo (si está habilitado)

Si no hay coincidencias de perfiles, el sistema proporciona un perfil predeterminado que se aplica a todos los clientes.

4.13.1 Filtros

Un filtro puede:

- Bloquear el acceso a categorías de sitios
- Bloquear el acceso a los sitios a los que se accede mediante la dirección IP (recomendado)
- Filtrar URL con expresiones regulares
- Bloquear archivos con extensiones específicas
- Habilitar lista negra y lista blanca global

Un filtro puede funcionar en dos modos diferentes:

- Permitir todo: permitir el acceso a todos los sitios, excepto los explícitamente bloqueados
- Bloquear todos: bloquea el acceso a todos los sitios, excepto los explícitamente permitidos

---

Nota: La lista de categorías se mostrará sólo después de la descarga de la lista seleccionada de la página *Blacklist*.

Bloquando Google Translate

Los servicios de traducción en línea, como Google Translate, se pueden utilizar para evitar el filtro de contenido porque las páginas visitadas a través del traductor siempre se refieren a un dominio de Google a pesar de tener contenido de servidores externos.

Es posible bloquear todas las solicitudes a Google translate, creando una URL bloqueada dentro de la página *General*. El contenido de la URL bloqueada debe ser: `translate.google`.

4.13.2 Users from Active Directory

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

Nota: Groups from Active Directory are not supported.

4.13.3 Antivirus

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

4.13.4 Solución de problemas

Si no se bloquea una página incorrecta, compruebe:

- El cliente está navegando usando el proxy
- El cliente no tiene un bypass configurado dentro la sección *Hosts sin proxy*
- El cliente no está navegando por un sitio con un bypass configurado dentro de la sección *Sitios sin proxy*
- El cliente está realmente asociado con un perfil no permitido para visitar la página
- El cliente está navegando dentro de un marco de tiempo cuando el filtro es permisivo

4.14 Firewall y gateway / Cortafuego y Puerta de enlace

NethServer Puede actuar como: index:*cortafuego* y puerta de enlace dentro de la red donde está instalado. Todo el tráfico entre computadoras de la red local e Internet pasa a través del servidor que decide cómo enrutar paquetes y qué reglas aplicar.

Principales características:

- Configuración de red avanzada (puente, enlaces, alias, etc.)
- Soporte multi WAN (hasta 15)
- Gestión de reglas de firewall
- Conformación del tráfico (QoS)
- Reenvío de puertos
- Reglas de enrutamiento para desviar tráfico en una WAN específica
- Sistema de prevención de intrusiones (IPS, Intrusion Prevention System)

Los modos de firewall y gateway sólo están habilitados si:

- El paquete *nethserver-firewall-base* está instalado
- Al menos hay una interfaz de red configurada con rol rojo

4.14.1 Política

Cada interfaz se identifica con un color que indica su función dentro del sistema. Véase red-sección.

Cuando un paquete de red pasa a través de una zona de cortafuegos, el sistema evalúa una lista de reglas para decidir si el tráfico debe ser bloqueado o permitido. *Políticas* son las reglas predeterminadas que se aplicarán cuando el tráfico de red no coincide con los criterios existentes.

El cortafuego implementa dos políticas predeterminadas editables desde la página *Reglas de firewall* -> :guilabel:‘ Configurar‘:

- *Allowed*: all traffic from green to red is allowed
- *Bloqueado*: todo el tráfico de la red verde a la red roja está bloqueado. Se debe permitir tráfico específico con reglas personalizadas.

Las políticas de firewall permiten el tráfico entre zonas según este esquema:

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

El tráfico se permite de izquierda a derecha, bloqueado de derecha a izquierda.

Puede crear reglas entre zonas para cambiar las políticas predeterminadas de la página *Reglas de firewall*.

Nota: El tráfico desde la red local al servidor en el puerto SSH (predeterminado 22) y el puerto del Administrador del servidor (predeterminado 980) es **siempre** permitido.

4.14.2 Reglas

Las Reglas se aplican a todo el tráfico que pasa a través del cortafuego. Cuando un paquete de red se desplaza de una zona a otra, el sistema busca entre las reglas configuradas. Si el paquete coincide con una regla, se aplica la regla.

Nota: El orden de la regla es muy importante. El sistema siempre aplica la primera regla que coincide.

Una regla consta de cuatro partes principales:

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

Las acciones disponibles son:

- *ACCEPT*: acepta el tráfico de red
- *REJECT*: bloquea el tráfico y notifica al host remitente
- *DROP*: bloquea el tráfico, los paquetes se eliminan y no se envía ninguna notificación al host del remitente
- *ROUTE*: enruta el tráfico al proveedor de WAN especificado. Véase *Multi WAN*.

Nota: El cortafuego no generará reglas para las zonas azul y naranja, si al menos una interfaz roja está configurada.

REJECT vs DROP

Como regla general, debe utilizar: index: *REJECT* cuando desea informar al host de origen de que el puerto al que está intentando acceder está cerrado. Por lo general, las reglas en el lado de LAN pueden usar REJECT.

Para conexiones desde Internet, se recomienda utilizar: index:*DROP*, con el fin de minimizar la divulgación de información a cualquier atacante.

Registro

Cuando una regla coincide con el tráfico en curso, es posible registrar el evento en un archivo de registro marcando la opción de la interfaz web. El registro de firewall se guarda en `/var/log/firewall.log`.

Ejemplos

A continuación hay algunos ejemplos de reglas.

Bloquear todo el tráfico de DNS de la LAN a Internet:

- Acción: REJECT
- Fuente: verde
- Destino: rojo
- Servicio: DNS (puerto UDP 53)

Permitir que la red de invitados tenga acceso a todos los servicios que escuchan en Servidor1

- Acción: ACCEPT
- Fuente: azul
- Destino: Servidor1
- Servicio: -

4.14.3 Multi WAN

El término *WAN* (Wide Area Network) se refiere a una red pública fuera del servidor, generalmente conectada a Internet. Un *proveedor* es la empresa que realmente gestiona el enlace WAN.

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

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

El sistema puede utilizar conexiones WAN en dos modos (botón *Configurar* en la página *Multi WAN*):

- *Balance*: todos los proveedores se utilizan simultáneamente según su peso
- *Activar copia de seguridad*: los proveedores se utilizan uno a uno al vuelo con el que tiene el peso más alto. Si el proveedor que está utilizando pierde su conexión, todo el tráfico se desviará al proveedor siguiente.

Para determinar el estado de un proveedor, el sistema envía un paquete ICMP (ping) a intervalos regulares. Si el número de paquetes perdidos excede un determinado umbral, el proveedor está deshabilitado.

El administrador puede configurar la sensibilidad de la supervisión mediante los siguientes parámetros:

- Porcentaje de paquetes perdidos

- Número de paquetes perdidos consecutivos
- Intervalo en segundos entre paquetes enviados

La página *Reglas de firewall* permite enrutar paquetes de red a un proveedor de WAN determinado, si se cumplen algunos criterios. Véase *Reglas*.

Ejemplo

Dados dos proveedores configurados:

- Proveedor1: interfaz de red eth1, peso 100
- Proveedor2: interfaz de red eth0, peso 50

Si se selecciona el modo equilibrado, el servidor encaminará un número doble de conexiones en Proveedor1 sobre Proveedor2.

Si se selecciona el modo de copia de seguridad activa, el servidor enrutará todas las conexiones en Proveedor1; Sólo si Proveedor1 se vuelve inasequible las conexiones se redirigirán a Proveedor2.

4.14.4 Reenviar puerto

El cortafuego bloquea las solicitudes de las redes públicas a las privadas. Por ejemplo, si el servidor web se ejecuta dentro de la LAN, sólo los equipos de la red local pueden acceder al servicio en la zona verde. Cualquier solicitud hecha por un usuario fuera de la red local está bloqueada.

Para permitir que cualquier usuario externo acceda al servidor web, debe crear una *remisión de puerto*. Una remisión de puerto es una regla que permite un acceso limitado a los recursos desde fuera de la LAN.

Al configurar el servidor, debe elegir los puertos de escucha. El tráfico de las interfaces rojas se redireccionará a los puertos seleccionados. En el caso de un servidor web, los puertos de escucha son generalmente el puerto 80 (HTTP) y 443 (HTTPS).

Cuando cree un puerto hacia adelante, debe especificar al menos los siguientes parámetros:

- El puerto fuente
- El puerto de destino, que puede ser diferente del puerto de origen
- La dirección del host interno al que se debe redirigir el tráfico
- Es posible especificar un rango de puertos usando dos puntos como separador en el campo de puerto de origen (eX: 1000: 2000), en este caso el puerto de destino de campo se debe dejar vacío

Ejemplo

Dado el siguiente escenario:

- Servidor interno con IP 192.168.1.10, denominado Servidor1
- Servidor Web escuchando en el puerto 80 en Servidor1
- Servidor SSH escuchando en el puerto 22 en Servidor1
- Otros servicios en el rango de puerto entre 5000 y 6000 en Servidor1

Si desea que el servidor web esté disponible directamente desde redes públicas, debe crear una regla como esta:

- puerto de origen: 80
- puerto de destino: 80

- Dirección del host: 192.168.1.10

Todo el tráfico entrante en las interfaces rojas del firewall en el puerto 80, será redirigido al puerto 80 en Servidor1.

En caso de que quiera hacer accesible desde fuera del servidor SSH en el puerto 2222, tendrá que crear un puerto hacia adelante de esta manera:

- puerto de origen: 2222
- puerto de destino: 22
- Dirección del host: 192.168.1.10

Todo el tráfico entrante en las interfaces rojas del firewall en el puerto 2222, será redirigido al puerto 22 en Servidor1.

En caso de que quiera hacer accesible desde fuera del servidor en toda la gama de puertos entre 5000 y 6000, tendrá que crear un puerto como este:

- Puerto de origen: 5000:6000
- puerto de destino:
- Dirección del host: 192.168.1.10

Todo el tráfico entrante en las interfaces de firewall rojo en el rango de puerto entre 5000 y 6000 será redirigido a los mismos puertos en Servidor1.

Limitar el acceso

Puede restringir el acceso al puerto sólo desde algunas direcciones IP o redes utilizando el campo *Permitir sólo de*.

Esta configuración es útil cuando los servicios deben estar disponibles sólo de IP o redes de confianza. Algunos valores posibles:

- `10.2.10.4`: habilitar el puerto hacia adelante para el tráfico procedente de la IP 10.2.10.4
- `10.2.10.4,10.2.10.5`: habilitar el puerto hacia adelante para el tráfico procedente de las IPs 10.2.10.4 y 10.2.10.5
- `10.2.10.0/24`: habilita el reenvío del puerto sólo para el tráfico procedente de la red 10.2.10.0/24
- `!10.2.10.4`: habilita el reenvío de puertos para todas las IP excepto 10.2.10.4
- `192.168.1.0/24!192.168.1.3,192.168.1.9`: habilita el reenvío de puertos para la red 192.168.1.0/24, excepto los hosts 192.168.1.3 y 192.168.1.9

4.14.5 NAT 1:1

NAT uno a uno es una forma de hacer que los sistemas detrás de un cortafuegos y configurado con direcciones IP privadas parecieran tener direcciones IP públicas.

Si tiene un montón de direcciones IP públicas y si desea asociar una de ellas a un host de red específico, NAT 1:1 es el camino.

Ejemplo

En nuestra red tenemos un host llamado `example_host` con IP `192.168.5.122`. También hemos asociado una dirección IP pública `89.95.145.226` como un alias de la interfaz `eth0` (`ROJA`).

Queremos mapear nuestro host interno (`example_host` - `192.168.5.122`) con IP pública `89.95.145.226`.

En el panel *NAT 1:1*, elegimos para el IP‘‘89.95.145.226‘‘ (campo de sólo lectura) el host específico (`example_host`) del cuadro combinado. Hemos configurado correctamente el NAT de uno a uno para nuestro host.

4.14.6 Conformación del tráfico

La Modulación del tráfico permite aplicar reglas de prioridad sobre el tráfico de red a través del cortafuego. De esta forma es posible optimizar la transmisión, comprobar la latencia y afinar el ancho de banda disponible.

Para habilitar la modulación del tráfico es necesario conocer la cantidad de ancho de banda disponible en ambas direcciones y rellenar los campos que indican la velocidad del enlace de Internet. Tenga en cuenta que en caso de congestión por el proveedor no hay nada que hacer para mejorar el rendimiento.

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

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

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

Nota: Be sure to specify an accurate estimate of the bandwidth on network interfaces.

4.14.7 Objetos del cortafuego

Los Objetos del cortafuego son representaciones de componentes de red y son útiles para simplificar la creación de reglas.

Hay 6 tipos de objetos, 5 de ellos representan fuentes y destinos:

- Host: representa los ordenadores locales y remotos. Ejemplo: web_server, pc_boss
- Grupos de hosts: representación de grupos homogéneos de ordenadores. Los hosts de un grupo siempre deben ser accesibles utilizando la misma interfaz. Ejemplo: servidores, pc_secretaria
- Redes CIDR: Puede expresar una red CIDR para simplificar las reglas del firewall.

  Ejemplo 1 : los últimos 14 direcciones IP de la red se asignan a servidores (192.168.0.240/28).

  Ejemplo 2 : tiene varias interfaces verdes pero desea crear reglas de firewall sólo para una verde (192.168.2.0/24).
- *Zona*: representa redes de hosts, deben expresarse en notación CIDR. Su uso es para definir una parte de una red con diferentes reglas de firewall de las de la interfaz nominal. Se utilizan para necesidades muy específicas.

Nota: De forma predeterminada, todos los hosts pertenecientes a una zona no pueden realizar ningún tipo de tráfico. Es necesario crear todas las reglas en el cortafuegos para obtener el comportamiento deseado.

El último tipo de objeto se utiliza para especificar el tipo de tráfico:

- Servicios: un servicio de escucha en un host con al menos un puerto y protocolo. Ejemplo: ssh, https

Al crear reglas, puede utilizar los registros definidos en *DNS* y *Servidor DHCP y PXE* como objetos host. Además, cada interfaz de red con un rol asociado se lista automáticamente entre las zonas disponibles.

4.14.8 Enlace IP/MAC

Cuando el sistema actúa como servidor DHCP, el cortafuego puede utilizar la lista de reservas de DHCP para verificar estrictamente todo el tráfico generado desde los hosts dentro de las redes locales. Cuando Enlace IP/MAC está habilitado, el administrador elegirá qué política se aplicará a los hosts sin una reserva de DHCP. El uso común es permitir el tráfico solamente desde los anfitriones conocidos y bloquear todo el otro tráfico. En este caso, los hosts sin reserva no podrán acceder al cortafuego ni a la red externa.

Para habilitar el tráfico sólo desde hosts bien conocidos, siga estos pasos:

1. Crear una reserva DHCP para un host
2. Vaya a la página *Reglas firewall* y seleccione *Configurar* en el menú de botones
3. Seleccione *Validación MAC (enlace IP/MAC)*
4. Elija *Bloquear tráfico* como directiva para aplicar a hosts no registrados

---

Nota: Recuerde crear al menos una reserva DHCP antes de habilitar el enlace IP/MAC, de lo contrario ningún host será capaz de administrar el servidor utilizando la interfaz web o SSH.

4.15 Cloud content filter

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

4.15.1 Preliminary operations

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

4.15.2 Configuration

The configuration is composed of two parts:

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

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

Manual or transparent proxy

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

Steps:

- Create a host group
- Open the tab *IP profiles* and click on *Create new*
- Select a host group and enter a description

- To select the blacklist associated with the profile, click on *Configure* and access the FlashStart

Authenticated proxy

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

Steps:

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

---

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

4.16 Proxy pass

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

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

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

Scenario:

- NethServer es el cortafuegos de su LAN
- Usted tiene un dominio http://mydomain.com
- You would like http://mydomain.com/mysite to forward to the internal server (internal IP: 192.168.2.100)

Commands for this example:

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

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

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

4.16.1 Configuración manual

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

Ejemplo

Crear archivo `/etc/httpd/conf.d/myproxypass.conf` con este contenido:

```
<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>
```

Consulte la documentación oficial de Apache para obtener más información: http://httpd.apache.org/docs/2.2/mod/mod_proxy.html

4.17 IPS (Snort)

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

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

A special widget inside the dashboard summarizes all detected attacks.

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

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

---

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

4.18 Bandwidth monitor (ntopng)

ntopng es una potente herramienta que le permite analizar el tráfico de red en tiempo real. Le permite evaluar el ancho de banda utilizado por los hosts individuales e identificar los protocolos de red más utilizados.

Habilitar ntopng Enabling ntopng, all traffic passing through the network interfaces will be analyzed. It can cause a slowdown of the network and increase system load.

Puerto El puerto donde ver la interfaz web ntopng.

Contraseña para el usuario "admin" Contraseña del usuario administrador. Esta contraseña no está relacionada con la clave de administrador de NethServer .

Interfaces Interfaces on which ntopng will listen to.

4.19 Estadísticas (collectd)

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

- Panel de gráficos Collectd (CGP), paquete *nethserver-cgp*

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

Después de la instalación, el sistema reunirá las siguientes estadísticas:

- uso de CPU
- carga del sistema
- número de procesos
- Uso de la memoria RAM
- uso de memoria virtual (swap)
- tiempo de actividad del sistema
- uso del espacio en disco
- operaciones de lectura y escritura de disco
- interfaces de red
- latencia de la red

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

4.19.1 Latencia de conexion

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

Los hosts adicionales podrían ser monitoreados (es decir, un servidor web) usando una lista de hosts separados por comas dentro de la propiedad `PingHosts`.

Ejemplo:

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

4.20 DNS

NethServer puede configurarse como servidor *DNS* (Domain Name System/Sistema de nombres de dominio) dentro de la red. Un servidor DNS es responsable de la resolución de nombres de dominio (ej. *www.example.com*) a sus direcciones numéricas correspondientes (por ejemplo, 10.11.12.13) y viceversa.

El servidor realiza solicitudes de resolución de nombres DNS en nombre de clientes locales y sólo es accesible desde la red LAN (verde) y la red de invitados (azul).

Durante una búsqueda de nombres el servidor será:

- Busque el nombre entre los hosts configurados localmente
- Realizar una consulta en dns externo: las solicitudes se almacenan en el caché para acelerar las consultas posteriores

Si NethServer es también el servidor DHCP en la red, todas las máquinas se configuran para utilizar el propio servidor para la resolución de nombres.

Nota: Tienes que especificar al menos un servidor DNS externo, en la página *DNS server*.

4.20.1 Hosts

La página *Hosts* le permite asignar nombres de host a direcciones IP, ya sean locales o remotas.

Por ejemplo, si tiene un servidor web interno, puede asociar el nombre *www.mysite.com* a la dirección IP del servidor web. Entonces todos los clientes pueden llegar al sitio web escribiendo el nombre elegido.

Los nombres configurados localmente siempre tienen prioridad sobre los registros DNS de servidores externos. De hecho, si el proveedor inserta *www.mydomain.com* con una dirección IP correspondiente al servidor web oficial, pero dentro de NethServer el IP de *www.mydomain.com* está configurado con otra dirección, los hosts dentro de la LAN no podrán ver el sitio.

4.20.2 Alias

Un *alias* es un nombre alternativo usado para llegar al servidor local. Por ejemplo, si el servidor se llama *mail.example.com*, puede crear un Alias de DNS *myname.example.com*. A continuación, el servidor será accesible desde los clientes de la LAN incluso con el nombre que acaba de definir.

Los alias sólo son válidos para la LAN interna. Si desea que el servidor sea accesible desde el exterior con el mismo nombre, deberá solicitar al proveedor que asocie la dirección pública del servidor al nombre deseado.

4.21 Servidor DHCP y PXE

El servidor *Dynamic Host Configuration Protocol* (DHCP)[1] centraliza la gestión de la configuración de red local para cualquier dispositivo conectado a ella. Cuando un ordenador (o un dispositivo como una impresora, un teléfono inteligente, etc.) se conecta a la red local, puede solicitar los parámetros de configuración de red mediante el protocolo DHCP. El servidor DHCP responde, proporcionando el IP, DNS y otros parámetros de red relevantes.

Nota: En la mayoría de los casos, los dispositivos ya están configurados para utilizar el protocolo DHCP al iniciar.

La especificación de *Preboot eXecution Environment* (PXE) [#PXE] _ permite a un dispositivo de red recuperar el sistema operativo desde una ubicación de red centralizada mientras se inicia, a través de los protocolos DHCP y TFTP. Véase *Arranque desde la configuración de red* para un ejemplo sobre cómo configurar un caso similar.

4.21.1 Configuración DHCP

El servidor DHCP se puede habilitar en todas las interfaces *verde * y *azul * (ver *Red*). NethServer asignará una dirección IP libre dentro de la configuración *rango DHCP* en la página *DHCP > Servidor DHCP*.

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

El rango DHCP debe definirse dentro de la red de la interfaz asociada. Por ejemplo, si la interfaz verde tiene IP/netmask `192.168.1.1/255.255.255.0` el rango debe ser `192.168.1.2 - 192.168.1.254`.

4.21.2 Reserva IP del host

El servidor DHCP concede una dirección IP a un dispositivo durante un período de tiempo limitado. Si un dispositivo requiere tener siempre la misma dirección IP, se le puede otorgar una *reserva IP* asociada a su dirección MAC.

La página *DHCP> IP reservation* lista las direcciones IP actualmente asignadas:

- Una línea con botón *IP reservation* identifica un host con un arriendo temporal (color gris);
- Una línea con el botón *Edit* identifica un host con una IP reservada (color negro). Un pequeño icono de dos flechas junto al nombre del host indica que la concesión DHCP ha caducado: es una condición normal para los hosts con configuración IP estática, ya que nunca se ponen en contacto con el servidor DHCP.

4.21.3 Arranque desde la configuración de red

Para permitir a los clientes arrancar desde la red, se requieren los siguientes componentes:

- the *DHCP* server, as we have seen in the previous sections,
- the *TFTP* server[2],
- the software for the client, served through TFTP.

TFTP es un protocolo de transferencia de archivos muy simple y por lo general se utiliza para la transferencia automatizada de archivos de configuración y arranque.

En NethServer la implementación TFTP viene con el módulo DHCP y está habilitada de forma predeterminada. Para permitir el acceso a un archivo a través de TFTP, basta con ponerlo en `/var/lib/tftpboot`.

Nota: Para deshabilitar TFTP, escriba los siguientes comandos en una consola como root:

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

Por ejemplo, ahora configuramos un cliente para iniciar CentOS desde la red. En NethServer, escriba desde la consola de root:

```
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
```

A continuación, cree el archivo `/var/lib/tftpboot/pxelinux.cfg/default` con el siguiente contenido:

```
default menu.c32
prompt 0
timeout 300

MENU TITLE PXE Menu
```

(continué en la próxima página)

[2] Protocolo Trivial de transferencia de archivos https://es.wikipedia.org/wiki/TFTP

(proviene de la página anterior)

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

Crear un directorio CentOS:

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

Copie dentro del directorio `vmlinuz` y `initrd.img`. Estos archivos son públicos y se pueden encontrar en la imagen ISO, en el directorio `/images/pxeboot` o descargados desde un espejo de CentOS.

Por último, encienda el host del cliente, seleccionando el arranque PXE (o arranque desde la red) desde la pantalla de inicio.

Referencias

4.22 VPN

Una VPN (Virtual Private Network, Red Privada Virtual) le permite establecer una conexión segura y encriptada entre dos o más sistemas usando una red pública, como la Internet.

El sistema admite dos tipos de VPN:

1. roadwarrior: o modo guerrero, conecta un cliente remoto a la red interna
2. net2net o tunel: conecta dos redes remotas

4.22.1 OpenVPN

OpenVPN le permite crear fácilmente conexiones VPN, que trae con numerosas ventajas, incluyendo:

- Disponibilidad de clientes para varios sistemas operativos: Windows, Linux, Apple, Android, iOS
- Múltiple NAT traversal, no necesita una IP estática dedicada en el firewall
- Alta estabilidad
- Configuración sencilla

Roadwarrior / guerrero

El servidor OpenVPN en modo roadwarrior - o modo guerrero - permite la conexión de varios clientes.

Los métodos de autenticación admitidos son:

- Usuario y contraseña del sistema
- Certificado
- Usuario del sistema, contraseña y certificado

El servidor puede funcionar en dos modos: enrutado o puenteado. Usted debe elegir el modo puente solo si el túnel debe llevar tráfico no-IP.

Para permitir que un cliente establezca una VPN:

1. Crear una nueva cuenta: se recomienda utilizar una cuenta VPN dedicada con certificado, evitando la necesidad de crear un usuario del sistema.

   Por otro lado, es obligatorio elegir una cuenta de sistema si desea utilizar la autenticación con nombre de usuario y contraseña.

2. Descargue el archivo que contiene la configuración y los certificados.
3. Importe el archivo en el cliente e inicie la VPN.

Túnel (net2net)

Al crear una conexión OpenVPN net2net, debe elegir un maestro entre los servidores implicados. Todos los demás servidores se consideran como esclavos (clientes).

Pasos a realizar en el servidor maestro:

- Habilitar servidor roadwarrior
- Cree una cuenta VPN solo para cada esclavo
- Durante la creación de la cuenta, recuerde especificar la red remota configurada detrás del esclavo

Pasos a realizar en el esclavo:

- Crear un cliente desde la página: guilabel: *Cliente*, especificando los datos de conexión al servidor maestro.
- Copie y pegue el contenido de los certificados descargados desde la página de configuración principal.

4.22.2 IPsec

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

Roadwarrior (L2TP)

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

Los métodos de autenticación admitidos son:

- Usuario del sistema, contraseña y certificado
- Secret shared key (PSK)

Para permitir que un cliente establezca una VPN:

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

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

Túnel (net2net)

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

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

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

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

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

4.23 FTP

Nota: El protocolo FTP es inseguro: la contraseña se envía en texto claro.

El servidor FTP permite transferir archivos entre cliente y servidor.

Un usuario FTP puede ser *virtual* o un sistema de usuarios. Los usuarios virtuales sólo pueden acceder al servidor FTP. Esta es la configuración recomendada. La interfaz web sólo permite la configuración de usuarios virtuales.

Al acceder al servidor FTP, un usuario puede explorar todo el sistema de archivos según sus propios privilegios. Para evitar la divulgación de información, el usuario FTP puede configurarse en una jaula mediante la opción *chroot*: el usuario no podrá salir del directorio de la jaula.

Este comportamiento puede ser útil en caso de que una carpeta compartida se utilice como parte de un simple alojamiento web. Inserte la ruta de la carpeta compartida dentro del campo personalizado. Por ejemplo, dada una carpeta compartida llamada *mysite*, rellene el campo con:

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

El usuario FTP virtual sólo podrá acceder al directorio especificado.

4.23.1 Usuarios del sistema

Advertencia: Esta configuración es sumamente desalentadora

Después de habilitar los usuarios del sistema, todos los usuarios virtuales se desactivarán. Toda la configuración debe hacerse utilizando la línea de comandos.

Habilitar usuarios del sistema:

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

Dado un nombre de usuario *goofy*, primero asegúrate de que el usuario tenga acceso remoto al shell. Ver: ref: *users_services-section*. Luego, habilita el acceso FTP:

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

Para deshabilitar un usuario ya habilitado:

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

Si no se deshabilita explícitamente, todos los usuarios del sistema son chrooted. Para deshabilitar un chroot por un usuario del sistema:

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

4.24 ownCloud

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

Key features:

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

4.24.1 Installation

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

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

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

4.24.2 LDAP Configuration

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

1. Copy the LDAP password using the following command:

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

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

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

7. Fill «User filter» tab with:

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

8. Fill «Access filter» tab with:

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

9. Fill «Group filter» tab with:

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

10. Configure «Advanced» tab with:

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

Special Attributes
    Email field: email
```

11. Configure «Expert» tab with:

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

12. Click the «Save» button

4.24.3 LDAP Note

User list

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

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

1. login to ownCloud as administrator

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

4.24.4 Trusted Domains

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

- domain name
- ip address

To add a new one use:

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

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

4.25 Phone Home

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

4.25.1 Visión de conjunto

The tool is *disabled* by default.

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

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

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

All the infos are used to populate the map.

4.25.2 Configuration

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

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

4.26 WebVirtMgr

Esta herramienta se utiliza para gestionar: index:*máquina virtual* a través de una sencilla interfaz web

- Crear y destruir nuevas máquinas (KVM)
- Crear plantilla personalizada de máquinas virtuales
- Acceso remoto a shell fácil
- Increíble interfaz de usuario

4.26.1 Configuración

La aplicación web escucha en el puerto **8000** de su máquina host, por ejemplo: `http://HOST_IP:8000/`.

El servidor está deshabilitado de manera predeterminada

Desde la página *Máquinas virtuales* puede:

- habilitar el administrador de máquinas virtuales
- habilitar el acceso a la consola de máquinas virtuales desde el navegador web

Para acceder a la interfaz web, debe iniciar sesión con credenciales que se pueden encontrar en la misma página:

- *Usuario:* admin
- *Contraseña*: aleatoria alfanumérica (editable)

Advertencia: No cree puentes de red utilizando la interfaz WebVirtManager. Basta con crear el puente dentro de la página *Red* y usarla en WebVirtManager.

Para obtener más información, consulte la documentación oficial:

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

4.27 SNMP

El protocolo SNMP (Simple Network Management Protocol) permite administrar y monitorizar dispositivos conectados a la red. El servidor SNMP puede responder a consultas específicas sobre el estado actual del sistema.

El servidor está deshabilitado de manera predeterminada

Durante la primera configuración. Debe establecer tres opciones principales:

- el nombre de la comunidad SNMP
- El nombre de la ubicación donde se encuentra el servidor
- El nombre y la dirección de correo del administrador del sistema

4.28 WebTop 4

WebTop es un groupware completo que implementa el protocolo ActiveSync.

El acceso a la interfaz web es: `https://<server_name>/webtop`.

4.28.1 Autenticación

Interfaz web

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

Ejemplo

- Nombre del servidor: mymail.mightydomain.com
- Dominio de correo alternativo: baddomain.net
- Usuario: goofy
- Ingresar: goofy

Sincronización activa

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

Ejemplo

- Nombre del servidor: mymail.mightydomain.com
- Dominio de correo alternativo: baddomain.net
- Usuario: goofy
- Nombre de usuario: goofy@mightydomain.com

Al configurar una cuenta de Active Sync, asegúrese de especificar la dirección del servidor y de dejar el campo de dominio vacío.

Nota: El protocolo Active Sync sólo se admite en dispositivos Android e iOS. Outlook no es compatible. La sincronización de correo no es compatible actualmente.

Usuario administrador

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

Las credenciales predeterminadas son:

- Usuario: admin
- Contraseña: admin

Admin user password must be changed from WebTop interface.

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

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

Ejemplo

- Nombre del servidor: mymail.mightydomain.com
- Usuario: admin
- Nombre de usuario: admin@mightydomain.com

4.28.2 WebTop vs SOGo

WebTop y SOGo se pueden instalar en la misma máquina.

ActiveSync está habilitada de forma predeterminada en SOGo y WebTop, pero si ambos paquetes están instalados, SOGo tendrá prioridad.

Para deshabilitar ActiveSync en SOGo:

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

Para deshabilitar ActiveSync en WebTop:

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

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

4.28.3 Active Directory authentication

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

Edit the following fields:

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

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

4.28.4 Importando desde SOGo

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

- Calendarios: `/usr/share/webtop/doc/sogo2webtop_cal.php`
- Libretas de direcciones: `/usr/share/webtop/doc/sogo2webtop_card.php`

Antes de utilizar las secuencias de comandos, debe instalar este paquete:

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

Al iniciar los scripts, indique el nombre de usuario que desea importar desde SOGo:

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

Donde `usuario` puede ser un nombre de usuario o `todos`.

Ejemplos

Import all address books from SOGo:

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

Import the calendar of user «foo»:

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

Nota: Si la secuencia de comandos se ejecuta varias veces, tanto los calendarios como las libretas de direcciones se importarán varias veces. Actualmente, no se admite la importación de listas de distribución y eventos recurrentes.

4.28.5 Importación desde Outlook PST

Puede importar correo electrónico, calendarios y libretas de direcciones desde un archivo Outlook PST.

Antes de usar los scripts siguientes, necesitará instalar el paquete *libpst*:

```
yum install libpst -y
```

Correo

Script inicial para importar mensajes de correo: `/usr/share/webtop/doc/pst2webtop.sh`

Para iniciar la importación, ejecute el script especificando el archivo PST y el usuario del sistema:

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

Se importarán todos los mensajes de correo. Los contactos y los calendarios se guardarán dentro de los archivos temporales para su posterior importación. El script mostrará todos los archivos temporales creados.

Contactos

Script para importar contactos: `/usr/share/webtop/doc/pst2webtop_card.php`.

El script utilizará los archivos generados desde la fase de importación de correo:

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

Ejemplo

Supongamos que el script pst2webtop.sh ha generado la siguiente salida de la importación de correo:

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

Para importar la libreta de direcciones predeterminada (WebTop) de *foo usuario:

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

Calendarios

Script para importar calendarios: `/usr/share/webtop/doc/pst2webtop_cal.php`

El script utilizará los archivos generados desde la fase de importación de correo:

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

Ejemplo

Supongamos que el script pst2webtop.sh ha generado la siguiente salida de la importación de correo:

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

Para importar el calendario predeterminado (WebTop) de *foo* usuario:

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

Nota: El script importará todos los eventos utilizando la zona horaria seleccionada por el usuario dentro de WebTop, si se establece. De lo contrario se utilizará la zona horaria del sistema.

4.28.6 Integración de Google y Dropbox

Los usuarios pueden agregar sus propias cuentas de Google Drive y Dropbox dentro de WebTop. Antes de continuar, el administrador debe crear un par de credenciales de acceso a la API.

API de Google

- Acceder a https://console.developers.google.com/project y crear un nuevo proyecto
- Cree nuevas credenciales seleccionando el tipo «OAuth 2.0 clientID» y recuerde compilar la sección «Pantalla de consentimiento de OAuth»
- Inserte nuevas credenciales (Client ID e Client Secret) dentro de la configuración de WebTop

  Desde shell, accede a la base de datos webtop:

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

Ejecute las consultas, utilizando el valor correspondiente en lugar de la variable `__value__`:

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

API de Dropbox

- Acceder a https://www.dropbox.com/developers/apps y crear una nueva aplicación
- Inserte el nuevo par de claves de credencial (App key e App secret) dentro de la configuración de WebTop

  Desde shell, accede a la base de datos webtop:

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

  Ejecute las consultas, utilizando el valor correspondiente en lugar de la variable `__value__`:

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

Si necesita aumentar el límite de usuario, lea la documentación oficial de Dropbox.

Nota: La versión Enterprise ya está integrada con Google y Dropbox.

4.29 Adagios

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

Key features:

- full view/edit of hosts,services, etc
- tons of pre-bundled plugins and configuration templates
- network scan
- remote installation of linux/windows agents
- modern Status view as an alternative to default nagios web interface
- backup Adagios data with NethServer backup data tool
- rest interface for status of hosts/services and for for viewing and modifying configuration
- full audit of any changes made

4.29.1 Installation

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

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

For more information, see official documentation:

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

4.30 OCS Inventory NG

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

Key features:

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

4.30.1 Installation

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

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

For more information, see official documentation:

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

4.31 HA (High Availability)

NethServer supports High Availability only for some specific scenarios.

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

This configuration supports:

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

Example

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

4.31.1 Limitations

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

4.31.2 Hardware requirements

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

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

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

Fence device

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

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

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

External links:

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

4.31.3 Installation

Before install:

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

Primary node

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

Configuring DRBD storage

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

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

- Create a physical volume:

```
pvcreate /dev/vdb1
```

- Extend the volume group:

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

- Create a logic volume for DRBD:

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

Software

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

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

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

```
yum install nethserver-ha
```

- Install extra software, like MySQL:

```
yum install nethserver-mysql
```

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

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

- Apply the configuration and start services on master node:

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

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

```
pcs status
```

Service configuration

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

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

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

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

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

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

Check cluster and service status:

```
pcs status
```

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

Secondary node

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

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

Final steps

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

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

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

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

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

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

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

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

Fencing with IPMI

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

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

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

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

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

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

Fencing with IF-MIB switch

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

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

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

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

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

4.31.4 Failure and recovery

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

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

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

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

Failed nodes

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

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

```
pcs cluster start
```

Disconnected fence devices

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

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

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

DRBD Split Brain

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

```
pcs status
```

DRBD state will be:

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

instead of:

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

Solution:

On the node with valid data launch the following command

```
drbdadm invalidate-remote drbd00
```

On the node with wrong storage data, run

```
drbdadm invalidate drbd00
```

On both nodes, launch

```
drbdadm connect drbd00
```

Check drbd synchronization with

```
cat /proc/drbd
```

Disaster recovery

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

Just follow these steps:

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

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

4.31.5 Backup

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

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

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

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

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

Example:

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

4.32 Upgrade tool

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

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

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

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

4.32.1 Preparation step

Estimated time: 1 hour

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

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

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

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

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

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

4.32.2 Upgrade step

Estimated time: 30 minutes

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

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

---

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

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

4.32.3 Post-upgrade step

Estimated time: 15 minutes

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

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

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

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

4.32.4 Post-upgrade checklist

Advertencia:

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

Upgrade completed check

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

```
Startup finished
```

Upgrade errors check

To check if any error occurred, run

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

Installed modules check

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

Let's Encrypt certificate check

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

4.32.5 Upgrade to Active Directory

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

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

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

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

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

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

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

4.32.6 Upgrade risks and how to reduce them

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

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

CAPÍTULO 5

Mejores prácticas

5.1 Software de terceros

Puede instalar cualquier certificado CentOS/RHEL software de terceros en NethServer.

Si el software es de 32 bits solamente, debe instalar las bibliotecas de compatibilidad antes de instalar el software. Las bibliotecas relevantes deben ser:

- glibc
- glib
- libstdc++
- zlib

Por ejemplo, para instalar los paquetes mencionados anteriormente:

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

5.1.1 Instalación

Si el software es un paquete RPM, utilice **yum** para instalarlo: el sistema se encargará de resolver todas las dependencias necesarias.

En caso de que una instalación de yum no sea posible, el mejor directorio de destino para software adicional está en `/opt`. Por ejemplo, dado un software llamado *mysoftware*, instálelo en `/opt/mysoftware`.

5.1.2 Copia de seguridad

El directorio que contiene datos relevantes debe incluirse dentro de la copia de seguridad añadiendo una línea a `/etc/backup-data.d/custom.include`. Véase *Personalización de la copia de seguridad de datos*.

5.1.3 Firewall

Si el software necesita algunos puertos abiertos en el firewall, cree un nuevo servicio llamado `fw_<softwarename>`.

Por ejemplo, dado el software *mysoftware* que necesita los puertos 3344 y 5566 en LAN, utilice los siguientes comandos:

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

5.1.4 Inicio y detención

NethServer utiliza el estándar nivel de ejecución 3.

El software instalado con yum ya debería estar configurado para comenzar en el arranque en el nivel de ejecución 3. Para verificar la configuración, ejecuta el comando **`chkconfig`**. El comando mostrará una lista de servicios con su propio estado.

Para habilitar un servicio en boot:

```
chkconfig mysoftware on
```

Para deshabilitar un servicio en boot:

```
chkconfig mysoftware off
```

CAPÍTULO 6

Apéndice

6.1 Migración del servidor NethService/SME

La migración es el proceso para convertir una máquina SME Server/NethService (*source*) en un NethServer (*destination*).

1. En el host de origen, cree un archivo de copia de seguridad completo y muévalo al host de destino.
2. En el host de destino, instale todos los paquetes que cubran las mismas características del origen.
3. Descargar el archivo de copia de seguridad completo en algún directorio; Por ejemplo, cree el directorio `/var/lib/migration`.
4. In NethServer, signal the event `migration-import`:

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

   Este paso requerirá algún tiempo.
5. Compruebe si hay algún mensaje de error en `/var/log/messages`:

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

Nota: No se migra ninguna plantilla personalizada durante el proceso de migración. Compruebe los archivos de la plantilla nueva antes de copiar cualquier fragmento personalizado de la copia de seguridad antigua.

6.1.1 Correo electrónico

Antes de ejecutar el NethServer en producción, se requieren algunas consideraciones sobre la red y las configuraciones de cliente de correo existentes: qué puertos están en uso, si SMTPAUTH y TLS están habilitados. Consulte las secciones *Configuración del cliente* y *Políticas especiales de acceso SMTP* para obtener más información.

En una migración de servidor de correo, el servidor de correo de origen podría estar en producción incluso después de que se haya realizado la copia de seguridad y los mensajes de correo electrónico continúan siendo entregados hasta que se borran permanentemente.

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

```
Usage:
  ./sync_maildirs.sh [-h] [-n] [-p] -s IPADDR
      -h          help message
      -n          dry run
      -p PORT     ssh port on source host (default 22)
      -s IPADDR   rsync from source host IPADDR
```

El host de origen en `IPADDR` debe ser accesible por el usuario `root`, a través de `ssh` con autenticación de clave pública.

6.2 Documentación de la licencia

Esta documentación se distribuye bajo los términos de la licencia **Creative Commons - Attribution-NonCommercial-ShareAlike 4.0 Internacional (CC BY-NC-SA 4.0)**.

Usted es libre de:

- **Compartir** - copiar y redistribuir el material en cualquier medio o formato
- **Adaptar** - combinar, transformar y construir sobre el material

El licenciante no puede revocar estas libertades siempre y cuando siga los términos de la licencia.

Bajo los siguientes términos:

- **Atribución** - Debe dar un crédito apropiado, proporcionar un enlace a la licencia e indicar si se realizaron cambios. Puede hacerlo de cualquier manera razonable, pero no de ninguna manera que sugiera que el licenciante lo respalda o su uso.
- **No comercial** - No puede utilizar el material con fines comerciales.
- **Compartir igual** - Si combinas, transformas o construyes el material, debes distribuir tus contribuciones bajo la misma licencia que el original.

No hay restricciones adicionales - No puede aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros de hacer cualquier cosa que la licencia permita.

Este es un resumen legible (y no un sustituto) de la licencia completa disponible en: http://creativecommons.org/licenses/by-nc-sa/4.0/

La documentación de la arquitectura es del proyecto SME Server y se autoriza bajo la licencia GNU de documentación libre 1.3 (http://www.gnu.org/copyleft/fdl.html). Consulte la documentación original en http://wiki.contribs.org/.

CAPÍTULO 7

Índices

- Índice general
- Buscar

Índice

Q

R

S

T

U

V

W

X

Z