NethServer Documentation

Release 7 Final

Nethesis

20 mag 2019

Indice

See also

- Sito web
- Community
- Wiki
- Manuale sviluppatore

CAPITOLO 1

Note di rilascio 7

1.1 Note di rilascio 7

NethServer versione 7

- La ISO release 7.6.1810 «final» sostituisce la precedente ISO 7.6.1810
- Questa versione è basata su CentOS 7 (1810)
- CentOS 7 riceverà aggiornamenti di sicurezza fino al 30/06/2024
- *List of NethServer 7 ISO releases*
- Lista delle principali modifiche
- Lista di bug noti
- Analisi dei possibili bug

1.1.1 Cambiamenti principali al 27/12/2018

- La ISO release 7.6.1810 «final» sostituisce la precedente ISO 7.6.1804
- PHP 5.6 da SCL è giunto a fine vita (endo-of-life) ed è perciò deprecato. Vedi *PHP 5.6 SCL*
- La policy TLS adottata di default è la `2018-10-01`
- La politica di conservazione dei log di sistema è stata aumentata a 52 settimane
- Il protocollo di rete Zeroconf è ora disabilitato di deafult
- Per impostazione predefinita, gli eventi Evebox vengono conservati per 30 giorni. Il nuovo valore predefinito viene applicato ai sistemi aggiornati come correzione di un bug
- Il modulo NDPI è stato aggiornato alla versione 2.4 ed alcuni vecchi protocolli non vengono più riconosciuti. Vedi *NDPI 2.4* per una lista completa dei protocolli rimossi
- Il server SMTP può essere utilizzato direttamente dalle reti fidate

- Le connessioni PPPoE utilizzano di default il plugin rp-pppoe per migliorare la velocità di rete
- Per i repository che supportano la firma dei metadati GPG, YUM esegue ora un controllo di integrità (`repo_gpgcheck = 1`) per maggiore sicurezza. Questa nuova impostazione predefinita viene applicata automaticamente a meno che un file `.repo` sia stato modificato localmente. In tal caso viene creato un file `.rpmnew` invece di sovrascrivere le modifiche locali. Rinominare il file `.rpmnew` in `.repo` per applicare i nuovi valori di default. Questa è la lista dei file da controllare:
  - `/etc/nethserver/yum-update.d/NsReleaseLock.repo`
  - `/etc/yum.repos.d/NethServer.repo`
  - `/etc/yum.repos.d/NsReleaseLock.repo`

1.1.2 Cambiamenti principali al 11/06/2018

- ISO release 7.5.1804 «final» sostituisce le precedenti ISO 7.5.1804 «rc» e «beta»
- Il modulo *Email* ora è basato su Rspamd
- La sovrascrittura dei record DNS MX per gli host LAN è stata rimossa. Rimossa la prop `postfix / MxRecordStatus`
- Gli alias dei nomi host sono convertiti in record DB «hosts». Vedi *Host alias addizionali*
- `/etc/fstab` non è più un template espanso. Fare riferimento a *Requisiti* e *Cartelle home dell'utente* per maggiori dettagli
- Autorizzazioni predefinite per *Cartelle condivise* is *Concedi il pieno controllo al creatore*
- Default *TLS policy* è `2018-03-30`
- il valore di default della *session idle timeout* del Server Manager è di 60 minute, la session life time è di 8 ore
- L'implementazione QoS (Quality of Service) ora utilizza FireQOS, la configurazione corrente viene migrata automaticamente. Vedi *Gestione banda*
- La voce *Aggiornamenti automatici* è stata rimossa dal Server Manager. Gli aggiornamenti automatici sono ora configurati da *Software center* > *Configura*. Vedi *Aggiornamenti software*
- Il modulo *NethServer subscription* è disponibile di default nelle nuove installazioni. Eseguire il comando seguente per aggiornare il modulo di base impostato su installazioni esistenti: `yum update @nethserver-iso`
- Il progetto WebVirtMgr non viene più mantenuto ed il modulo corrispondente è stato rimosso insieme al pacchetto nethserver-libvirt. Vedi *Macchine virtuali* per dettagli su come usare la virtualizzazione

1.1.3 Cambiamenti principali al 26/10/2017

- Rilascio della ISO 7.4.1708 «final» che sostituisce le precedenti ISO 7.4.1708 «beta1» e 7.3.1611 «update 1»
- Il provider di account AD locale applica automaticamente gli aggiornamenti all'istanza Samba DC (#5356) La versione più recente di Samba DC è la 4.6.8
- La pagina del Softeware center avvisa quando una nuova upstream release è disponibile (#5355)
- Aggiunto il modulo FreePBX 14
- Squid è stato patchato per una migliore esperienza di navigazione web in caso di utilizzo del proxy trasparente SSL

- Ntopng 3 sostituisce Bandwidthd, il Server Manager contiene una nuova pagina «top talkers» che traccia l'utilizzo della banda da parte degli host
- Suricata può essere configurato con molteplici categorie di regole
- EveBox può segnalare anomalie di traffico rilevate da Suricata
- Nextcloud 12.0.3
- Web antivirus basato su ICAP invece che su ECAP
- Filtri web: ufdbGuard aggiornato alla versione 1.33.4, apportati piccoli miglioramenti UI all'interfaccia web
- Strumenti di diagnostica: aggiunto speedtest
- ufdbGuard aggiornato alla versione 1.33.4
- WebTop4 è stato rimosso

1.1.4 Cambiamenti principali al 31/07/2017

- Rilascio della ISO 7.3.1611 «update 1» che sostituisce la precedente ISO 7.3.1611 «Final»
- Miglioramento della pagina di backup della configurazione
- Miglioramento della pagina degli Account provider
- Procedure di migrazione da sme8 e di aggiornamento da ns6
- OpenVPN: migliorati tunnel net2net
- WebTop 5.0.7
- Backup dati: supporto base per backup su WebDAV e statistiche storage
- Ritocchi UI per tunnel IPSec
- Proxy web: supporto instradamenti e regole di priorità
- NextCloud 12
- Pagina strumenti diagnostici di rete

1.1.5 Cambiamenti principali al 30/01/2017

- Rilascio della ISO 7.3.1611 «Final» che sostituisce la precedente ISO 7.3.1611 «RC4»
- Installatore: aggiunta modalità di installazione manuale
- Account provider: il gruppo "administrators" è stato sostituito dal gruppo "domain admins" (*Accesso al Server Manager*)
- Mail server: sistemata l'espansione di pseudonimi per i gruppi
- Mail server: le caselle di posta condivise sono ora abilitate per default (*Caselle di posta condivise*)
- Mail server: gli pseudonimi specifici per dominio hanno ora la precedenza su quelli generici
- OpenVPN: abilitato l'avvio automatico dei client VPN al boot
- Filtro web: corretti i profili basati su gruppi
- Firewall: corretta la selezione delle condizioni temporali
- IPS: configurazione aggiornata per l'ultima release di pulledpork

1.1.6 Funzionalità e pacchetti obsoleti

PHP 5.6 SCL

PHP 5.6 del repository SCL ha raggiunto il fine vita (EOL)[1][2].

Per evitare problemi con le applicazioni legacy esistenti, i pacchetti PHP 5.6 SCL di CentOS 7.5.1804 saranno ancora disponibili nei repository di NethServer per tutto il ciclo di vita della versione 7.6.1810.

Avvertimento: I pacchetti PHP 5.6 SCL **non** riceveranno alcun aggiornamento di sicurezza. Verrà garantito un minimo supporto limitatamente a quanto possibile

Il pacchetto `nethserver-rh-php56-php-fpm` sarà rimosso dalla prossima release di NethServer.

Gli sviluppatori sono invitati ad aggiornare i loro moduli, sostituendo `nethserver-rh-php56-php-fpm` con `nethserver-rh-php71-php-fpm` il prima possibile.

NDPI 2.4

I seguenti protocolli sono stati rimossi:

- tds
- winmx
- imesh
- http_app_veohtv
- quake
- meebo
- skyfile_prepaid
- skyfile_rudics
- skyfile_postpaid
- socks4
- timmeu
- torcedor
- tim
- simet
- opensignal
- 99taxi
- easytaxi
- globotv
- timsomdechamada
- timmenu

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

- timportasabertas
- timrecarga
- timbeta

Le regole che utilizzano i protocolli di cui sopra, verranno automaticamente disabilitate.

1.1.7 Aggiornare NethServer 6 a NethServer 7

È possibile aggiornare la precedente *major release* di NethServer a 7 con la strategia backup/restore. Vedere *Aggiornamento da NethServer 6* per dettagli.

Accesso al Server Manager

Se si desidera abilitare l'accesso *Server Manager access to other users than root*, aggiungere gli utenti al gruppo "domain admins" ed eseguire:

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

Caselle di posta condivise

Se si desidera abilitare le caselle di posta condivise dagli utenti, eseguire:

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

Pacchetti rimossi

I seguenti pacchetti erano disponibili nella precedente release 6 e sono stati rimossi nella 7:

- nethserver-collectd-web: sostituito con nethserver-cgp
- nethserver-password: integrato in nethserver-sssd
- nethserver-faxweb2: vedere la discussione faxweb2 vs avantfax.
- nethserver-fetchmail: sostituito con getmail
- nethserver-ocsinventory, nethserver-adagios: a causa di problemi di compatibilità con Nagios, questi moduli verranno supportati solo su NethServer 6
- nethserver-ipsec: i tunnel IPSec sono ora implementati in nethserver-ipsec-tunnels, la funzione L2TP è stata eliminata
- nethserver-webvirtmgr

Riferimenti

CAPITOLO 2

Installazione

2.1 Installazione

2.1.1 Requisiti minimi

I requisiti minimi sono:

- CPU a 64 bit (x86_64)
- 1 GB di RAM
- 10 GB di spazio disco

Suggerimento: Si consiglia l'uso di almeno 2 hard disk in modo che venga garantita l'integrità dei dati attraverso il supporto automatico RAID 1.

Compatibilità hardware

NethServer è compatibile con tutto l'hardware certificato per Red Hat® Enterprise Linux® (RHEL®), elencato sul sito Web del fornitore di hardware o nel Red Hat Customer Portal.

2.1.2 Tipi di installazione

Sono supportati due modi per installare NethServer. In breve:

Installazione da ISO

- Scaricare l'immagine ISO
- Preparare un DVD o una chiavetta USB
- Seguire la procedura guidata

Installazione da YUM

- Installare CentOS Minimal
- Configurare la rete
- Eseguire l'installazione da rete

2.1.3 Installazione da ISO

Avvertimento: L'installazione eliminerà tutti i dati esistenti sui dischi rigidi!

Creazione sorgente d'installazione

Scaricare **il file ISO più recente disponibile** dal sito ufficiale www.nethserver.org. Il file ISO scaricato può essere utilizzato per **creare un supporto avviabile**, come un DVD o una chiavetta USB.

Chiavetta USB

Su una macchina Linux, aprire il terminale ed eseguire:

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

Dove *NethServer.iso* è il nome del file della ISO scaricata, e */dev/sdc* è la destinazione che corrisponde all'intera chiavetta USB, non una partizione (come /dev/sdc1).

Su una macchina Windows, formattare la chiavetta USB e smontarla. Quindi usare uno dei seguenti tool per scrivere i dati:

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

DVD

La creazione di un disco avviabile è diversa dalla semplice scrittura di un file su DVD e richiede l'uso di una funzione dedicata, di solito presente nei programmi per la creazione di DVD (es. *scrivi* immagine oppure *masterizza ISO*). Le istruzioni su come creare un DVD avviabile a partire dall'immagine ISO sono facilmente reperibili su Internet o nella documentazione del proprio sistema operativo.

Modalità di installazione

Avviare la macchina utilizzando il supporto appena creato. Se non viene riconosciuto, fare riferimento alla documentazione del BIOS della scheda madre. Una problematica tipica è impostare la priorità dei dispositivi all'avvio. Il primo dispositivo di avvio dovrebbe essere il lettore DVD o la chiavetta USB.

All'avvio verrà mostrato un menù con i diversi tipi di installazione:

NethServer *interactive installation*

Verrà richiesto di selezionare soltanto il layout della tastiera e la time zone. Le schede di rete verranno automaticamente configurate in DHCP e i primi due hard disk saranno utilizzati in RAID-1.

Altre modalità di installazione di NethServer

- *Unattended installation* – Verranno automaticamente selezionati tutti i parametri di configurazione senza intervento dell'utente.
- *Manual installation* – L'opposto di *unattended*: non verranno utilizzati default, è necessario selezionare tutte le opzioni di configurazione (rete, dischi, time zone, tastiera, etc).

Installazione standard di CentOS

Utilizza la procedura d'installazione standard di CentOS. Si configurerà NethServer in seguito seguendo le istruzioni nella sezione *Installazione su CentOS*

Tools

Avvia in modalità *rescue* (recupero), esecuzione del memory test e strumenti di rilevazione dell'hardware.

Avvio da disco locale

Tenta l'avvio di un sistema già installato sul disco rigido.

Alla fine della procedura di installazione verrà chiesto di effettuare il riavvio della macchina. **Rimuovere il media di installazione**, prima di riavviare.

Parametri di avvio opzionali

E" possibile aggiungere parametri all'installazione automatica, premendo `TAB` e modificando la linea di comando. Utile per la modalità *unattended*.

Per disabilitare la creazione di un set RAID, aggiungere questa opzione:

```
raid=none
```

Se si desidera selezionare i dischi su cui installare, usare:

```
disks=sdx,sdy
```

Per abilitare la *cifratura del filesystem*, usare:

```
fspassword=s3cr3t
```

Abilitando il file system cifrato, tutti i dati scritti sul disco verranno cifrati usando la crittografia simmetrica. In caso di furto, un malintenzionato non sarà in grado di leggere i dati a meno di non possedere la chiave crittografica.

Nota: Sarà necessario inserire la password scelta ad ogni avvio del sistema.

Altre opzioni disponibili (solo modalità *unattended*):

- `Tastiera`, layout della tastiera, di default è `keyboard=us`
- `Fuso orario`, di default è `timezone=UTC`

Indirizzo IP di default

Nel caso in cui non sia possibile ottenere un indirizzo IP via DHCP, al primo avvio la **prima** interfaccia di rete verrà configurata come segue:

- IP 192.168.1.1
- netmask 255.255.255.0

Password amministratore di sistema

È altamente consigliato scegliere una password sicura per l'utente `root` durante la prima configurazione. Una buona password deve:

- essere lunga almeno 8 caratteri
- contenere lettere maiuscole e minuscole
- contenere simboli e numeri

La password di default nella modalità *unattended* è `Nethesis,1234`.

Lingua

La lingua di installazione di NethServer è *Inglese (Stati Uniti)*. Ulteriori lingue possono essere installate in seguito. Vedi *Prossimi passi*.

Modalità interattiva e Manuale

La modalità **interattiva** consente di effettuare poche e semplici scelte sulla configurazione del sistema.

Le scelte richieste sono:

- Lingua
- Layout della tastiera
- Password dell'utente root

Tutte le altre opzioni vengono configurate in base all'hardware utilizzato (vedi la sezione *Modalità unattended* per i dettagli), ma rimane comunque possibile modificare manualmente ogni configurazione disponibile.

Al contrario, la modalità **manuale** avvia l'installazione senza alcun default. Dovranno essere configurati anche la rete e i dischi.

> **Avvertimento:** Nella sezione *Network* > *General*, soltanto le interfacce marcate come *Automatically connect to this network when it is available* saranno abilitate all'avvio del sistema appena installato. Per maggiori informazioni, fare riferimento alla Guida di installazione di RHEL 7.

Problemi noti

- Quando si installa su macchine con firmware UEFI, Anaconda potrebbe fallire nel partizionamento automatico. Per aggirare il problema, passare a *Manual installation*, o *Standard CentOS installation* quindi seguire *Installazione su CentOS*. In caso di installazione con software RAID, assicurarsi di creare manualmente partizioni UEFI su tutti i dischi di avvio.

Modalità unattended

La modalità *unattended* non richiede nulla durante l'installazione. Il sistema verrà installato automaticamente e riavviato con la seguente configurazione:

- Layout tastiera: `us`
- Time zone: `UTC`
- Password di `root`: `Nethesis,1234`
- DHCP abilitato su tutte le interfacce; se non vengono ricevuti indirizzi IP verrà applicata la *configurazione di default*
- Se sono presenti due o più dischi, verrà creato un set RAID 1 sui primi due dischi e dei volumi LVM sul set RAID 1
- Le partizioni *swap* e *root* sono allocate automaticamente; la dimensione di *boot* è di 1GB

2.1.4 Installazione su CentOS

È possibile installare NethServer su una nuova installazione di CentOS minimal utilizzando un paio di comandi. Questo metodo di installazione è progettato per i server virtuali virtuali (VPS) in cui CentOS viene già installato dal provider VPS.

Abilitare i repository NethServer specifici con il comando:

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

Per installare il sistema di base eseguire:

```
nethserver-install
```

Oppure, per installare contestualmente del software addizionale, passare il nome dei moduli desiderati come parametro allo script di installazione. Esempio:

```
nethserver-install nethserver-mail nethserver-nextcloud
```

2.1.5 Passi successivi

Al termine dell'installazione, *accedere al Server Manager* per *installare il software addizionale*.

2.2 Accesso al Server Manager

NethServer può essere configurato utilizzando l'interfaccia web *Server Manager*. Per accedere all'interfaccia web è necessario un browser come Mozilla Firefox o Google Chorme puntando all'indirizzo (URL) `https://a.b.c.d:980` oppure `https://server_name:980`, sostituendo *a.b.c.d* e *server_name* rispettivamente con l'indirizzo IP del server e il nome del server utilizzato durante l'installazione.

Se il modulo web server è installato, l'interfaccia web è raggiungibile anche all'indirizzo `https://server_name/server-manager`.

Il Server Manager utilizza certificati SSL auto-firmati, sarà quindi necessario accettare esplicitamente tali certificati la prima volta che si accede al server. La connessione è comunque sicura e cifrata.

2.2.1 Login

La pagina di accesso consente di selezionare una lingua alternativa tra quelle già installate sul sistema. Dopo aver effettuato l'accesso, spostarsi alla pagina: ref:*software-center-section* per installare altre lingue.

La pagina di accesso fornirà un accesso affidabile all'interfaccia web. Accedere come **root** digitando la password scelta durante l'installazione di NethServer.

Nota: La procedura di installazione *unattended* imposta la password di root al valore predefinito `Nethesis,1234`.

2.2.2 Wizard di prima configurazione

La prima volta che viene eseguito l'accesso con l'utente **root**, viene visualizzato il *Wizard di prima configurazione*.

Se la password di root è ancora quella predefinita, è necessario modificarla.

Il Wizard di prima configurazione consente di ripristinare un *backup della configurazione*. Fare rifermento alla sezione *Disaster recovery* per maggiori dettagli.

In alternativa il Wizard consente di configurare:

- Nome host
- *Data e fuso orario*
- Porta SSH
- *Configurazione smarthost*
- *Statistiche d'utilizzo*

2.2.3 Cambiare la password attuale

Si può modificare la password di root dall'interfaccia web andando sull'etichetta *root@host.domain.com*, nell'angolo in alto a destra dello schermo, e cliccando su *Profilo*.

2.2.4 Logout

Per terminare la sessione corrente del Server Manager andare sull'etichetta *root@host.domain.com* nell'angolo in alto a destra dello schermo e cliccare su *Logout*.

2.2.5 Timeout della sessione

Di default (a partire da NethServer 7.5.1804), una sessione Server Manager viene terminata dopo **60 minuti di inattività** (idle timeout) e **scade 8 ore dopo il login** (session life time).

Il seguente comando imposta una idle timeout di 2 ore e una life time massima per una sessione a 16 ore. Il tempo è espresso in secondi:

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

Per disabilitare i timeout

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

I nuovi valori di timeout saranno effettivi sulle nuove sessioni. Invece non alterano le sessione attive.

2.3 NethServer subscription

Una installazione di NethServer può essere registrata su un'istanza pubblica o privata Dartagnan[1], ottenendo l'accesso al portale di monitoraggio ed ai repository di aggiornamento stabili.

Suggerimento: La NethServer Subscription di Nethesis[2] consente l'accesso a un'istanza Dartagnan pubblica pronta all'uso, insieme a servizi di supporto professionale immediati per le proprie implementazioni di NethServer. Per piu informazioni https://my.nethserver.com

---

L'attivazione di un abbonamento abiliterà i repository YUM stabili, ma disabiliterà qualsiasi altro repository eventualmente aggiunto. Puoi riattivare qualsiasi altro repository creando un «template-custom» per: file: */ etc / nethserver / eorepo.conf*.

Il fornitore dell'abbonamento potrebbe non accettare richieste di supporto per i contenuti dei repository personalizzati.

2.3.1 Registrando il sistema

1. Accedere alla pagina *Sottoscrizione* del Server Manager
2. Cliccare su *Sottoscrivi*
3. Accedere o registrarsi su https://my.nethserver.com per ottenere un codice di registrazione
4. Copiare e incollare il codice all'interno del campo *Registrazione token*
5. Cliccare su bottone *Registra ora*

Al termine della procedura, il nome e la validità del piano di abbonamento sottoscritto saranno riportati all'interno della pagina. Il monitoraggio e l'accesso ai repository stabili saranno automaticamente abilitati.

2.3.2 Rimozione di una subscription

Alla scadenza dell'abbonamento o alla fine di un periodo di prova, utilizzare il seguente comando per annullare qualsiasi modifica ai repository e accedere a quelli della community:

```
config setprop subscription Secret '' SystemId ''
signal-event nethserver-subscription-save
```

Se è stato installato il *nuovo server manager*, noto anche come *cockpit*, è possibile rimuovere la licenza della macchina dalla pagina *Subscription*. cliccando sul pulsante **Unsubscribe**.

Fare riferimento a *Aggiornamenti software* per ulteriori informazioni sull'origine degli aggiornamenti della community.

[1] Documentazione Dartagnan: https://nethesis.github.io/dartagnan/
[2] Sito ufficiale Nethesis: http://www.nethesis.it

CAPITOLO 3

Configurazione

3.1 Software center

NethServer è altamente modulare: al termine dell'installazione il sistema contiene solo i moduli di base *configurazione di rete*, *visualizzazione log*. La pagina del *Software center* consente all'amministratore di selezionare e **installare** dei *moduli* aggiuntivi, e anche di elencare e **aggiornare** i *pacchetti* software già installati.

Un *modulo* è solitamente costituito da più *pacchetti*. Estende le funzionalità del sistema. Ad esempio un modulo può trasformare NethServer in un server di posta elettronica o un proxy Web.

Un *pacchetto* software è un'unità indivisibile. Viene reso pubblico da un repository software. NethServer i pacchetti sono sotto forma di file RPM[1] . Dunque in questo preciso contesto, i termini *pacchetto* e *RPM* possono essere usati come sinonimi.

3.1.1 Aggiornamenti software

Un sistema NethServer 7 riceve aggiornamenti da diversi progetti software:

- il progetto NethServer stesso[2]
- il progetto CentOS[3]
- repository EPEL[4]

Ogni progetto software rilascia aggiornamenti in base alle sue regole specifiche e al ciclo di sviluppo, ma tutti preferiscono la stabilità del software rispetto a nuove funzionalità.

Fare riferimento al forum della community[5] e *Note di rilascio 7* per ulteriori informazioni sugli aggiornamenti di NethServer.

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

Gli aggiornamenti rilasciati dal progetto CentOS sono immediatamente resi disponibili per NethServer, attingendo direttamente dai mirror CentOS. Vengono presi in considerazione solo gli aggiornamenti per la versione corrente del sistema (ad esempio «7.6.1804»), fino aggiornamento alla successiva versione di sistema, procedura che va avviata manualmente.

Maggiori informazioni sugli aggiornamenti CentOS:

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

Gli aggiornamenti rilasciati da EPEL sono resi immediatamente disponibili dai mirror EPEL ufficiali. Poiché EPEL non è legato al numero di versione del sistema corrente, il *Software center* installa sempre le versioni software più recenti disponibili su EPEL.

Maggiori informazioni sugli aggiornamenti EPEL:

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

Suggerimento: Anche se i progetti in questione mirano alla stabilità del software, è necessario prestare attenzione per verificare se gli aggiornamenti si adattano bene. Ogni volta che il sistema verrà aggiornato, **create a backup of the data and review the updates changelog** per capire cosa sta per succedere. Se possibile, prova gli aggiornamenti in un macchina non in produzione. Per qualsiasi dubbio chiedi al forum della community di NethServer![5]

Procedura di aggiornamento manuale

Quando gli aggiornamenti sono disponibili, viene visualizzato un messaggio di avviso nella pagina *Software center*.

Gli aggiornamenti per il software installato sono elencati nella scheda *Updates*. Ulteriori dettagli su i pacchetti installati sono disponibili in *Updates CHANGELOG*.

Per avviare l'aggiornamento del sistema, fai clic sul pulsante *Scarica e installa*.

Suggerimento: Aggiorna regolarmente il software installato per correggere bug, problemi di sicurezza e ricevere nuove funzionalità

Procedura di aggiornamento automatico

È possibile eseguire alcune azioni automatiche quando sono disponibili nuovi aggiornamenti software.

- Scarica e (facoltativamente) installa gli aggiornamenti
- Invia una e-mail all'amministratore di sistema (root) e ad un ulteriore elenco di destinatari

La disponibilità degli aggiornamenti è controllata da un'attività che viene eseguita in un momento casuale durante la notte.

Suggerimento: Se l'e-mail di notifica non viene consegnata o è contrassegnata come spam, è possibile configurare un *smarthost*

3.1.2 Installazione dei moduli

La scheda *Available* elenca tutti i moduli che possono essere installati. Questo elenco può essere filtrato per categoria. Vedi anche *Lingue aggiuntive*.

Per **install a module**, selezionare la casella corrispondente e fare clic su *Add*. Alcuni moduli suggeriscono pacchetti opzionali che possono essere installati anche in un secondo momento.

Una volta che un modulo è stato installato, è elencato nella scheda *Installed*.

Per **installare i pacchetti opzionali** in seguito, selezionare il tab *Installati* e premere il pulsante *Modifica* di una voce della lista.

Per **remove a module**, vai alla scheda *Installed* e premi il pulsante *Remove* corrispondente.

> **Avvertimento:** In fase di rimozione, alcuni moduli collegati potrebbe essere rimossi indirettamente! Leggere attentamente la lista dei pacchetti in rimozione per evitare di rimuovere delle funzionalità necessarie.

Lista dei pacchetti installati

La lista completa dei pacchetti RPM installati è disponibile nel tab *Installati*.

La sezione *Installed software* mostra tutti i pacchetti installati con la versione completa del pacchetto.

Lingue aggiuntive

Il Server Manager permette di selezionare la lingue dell'interfaccia al momento del login. Sono elencate solo le lingue installate.

Nel tab *Disponibili*, selezionare la categoria *Lingue* e installare le lingue desiderate.

Riferimenti

3.2 Sistema base

Questo capitolo descrive tutti i moduli disponibili al termine dell'installazione. Tutti i moduli al di fuori di questa sezione devono essere installati dalla pagina *Software center*, inclusi il *Backup* e il supporto per gli utenti.

3.2.1 Dashboard

La pagina mostrata di default dopo il login è la Dashboard; qui viene visualizzato un riepilogo dello stato del sistema e delle sue impostazioni.

Analizzatore disco

Questo strumento è usato per visualizzare l'"utilizzo del disco in un semplice grafico in cui è possibile interagire con click e doppio click per navigare nelle cartelle.

Dopo l'installazione andare nella pagina *Dashboard* e poi nella scheda *Utilizzo disco*, quindi cliccare su *Aggiorna* per indicizzare la directory root e mostrare il grafico. Questo processo può durare diversi minuti in base allo spazio occupato su disco.

Alcune cartelle note sono:

- Cartelle condivise: `/var/lib/nethserver/ibay`
- Home degli utenti: `/var/lib/nethserver/home`
- Mail: `/var/lib/nethserver/vmail`
- Fax: `/var/lib/nethserver/fax`
- Database MySQL: `/var/lib/mysql`

3.2.2 Rete

La pagina *Rete* consente di stabilire in quale modo il server è collegato alla rete locale (LAN) oppure alle reti pubbliche (Internet).

Se il server svolge la funzionalità di firewall e gateway, sarà in grado di gestire reti aggiuntive con funzionalità speciali come DMZ (DeMilitarized Zone) o rete ospiti.

NethServer supporta un numero illimitato di schede di rete. Le reti gestite devono sottostare alle regole seguenti:

- le reti devono essere fisicamente separate (non possono essere collegate allo stesso switch/hub)
- le reti devono essere logicamente separate (essere configurate su sotto-reti differenti)
- le reti private (es. LAN) devono rispettare le regole per gli indirizzi specificate nel documento RFC1918. Vedi *Numerazione delle reti private (RFC1918)*

Ogni interfaccia di rete ha un ruolo specifico che ne determina l'utilizzo e il comportamento. I ruoli sono indicati tramite colori. Ogni colore indica la zona di appartenenza della scheda di rete e le regole ad essa applicate:

- green: rete locale. I computer su questa rete possono accedere a qualsiasi altra rete configurata sul server
- blue: rete ospiti. I computer su questa rete possono accedere alle reti orange e red, ma non possono accedere alla zona green
- orange: rete DMZ. I computer su questa rete possono accedere alle reti red, ma non possono accedere alle zone blue e green
- red: rete pubblica. I computer in questa rete possono accedere solo al server stesso

Si veda *Policy* per maggiori informazioni sull'uso dei ruoli nelle regole del firewall.

Nota: Il server deve avere almeno un'interfaccia di rete. Quando il server ha una sola scheda di rete, tale scheda deve avere il ruolo green.

In caso di installazione su VPS (Virtual Private Server) pubblico, il server deve essere configurato con una schede di rete green. Si consiglia quindi di chiudere le porte dei servizi critici usando il pannello *Servizi di rete*.

Alias IP

Per assegnare più indirizzi IP alla stessa scheda è possibile utilizzare gli alias IP.

In tal modo è possibile ad esempio associare alla stessa red più indirizzi IP della stessa classe e gestirli in modo indipendente (ad esempio con dei port forward che discriminano in base allo specifico IP di destinazione).

L'alias è configurabile cliccando nel menu a tendina della specifica scheda di rete e avrà lo stesso ruolo della scheda fisica associata.

Nota: L'alias IP su interfaccia PPPoE in alcuni casi potrebbe non funzionare correttamente a causa di differenze nella fornitura del servizio tra i vari provider internet.

Interfacce logiche

Nella pagina *Network* premere il pulsante *Nuova interfaccia* per creare una interfaccia logica. I tipi di interfacce logiche supportate sono:

- bond: combina due o più interfacce, garantisce bilanciamento del traffico e tolleranza ai guasti
- bridge: collega due reti distinte, è spesso utilizzata per le VPN in bridge e le macchine virtuali
- VLAN (Virtual Local Area Network): crea due o più reti fisicamente separate usando una singola interfaccia fisica
- PPPoE (Point-to-Point Protocol over Ethernet): collegamento a Internet attraverso un modem DSL

I bond consentono di aggregare banda o tollerare guasti. I bond posso essere configurati in varie modalità.

Modalità che supportano aggregazione di banda e tolleranza ai guasti:

- Balance Round Robin (raccomandato)
- Balance XOR
- 802.3ad (LACP): richiede il supporto nel driver della scheda di rete ed uno switch in cui sia abilitata la modalità IEEE 802.3ad Dynamic link
- Balance TLB: richiede il supporto nel driver della scheda di rete
- Balance ALB

Modalità che supportano solo tolleranza ai guasti:

- Active backup (raccomandato)
- Broadcast policy

I bridge hanno la funzione di collegare segmenti di rete differenti, per esempio consentendo ai client collegati in VPN o macchine virtuali di accedere alla rete locale (green).

Quando non è possibile separare fisicamente due reti diverse, è possibile utilizzare le VLAN con tag. Il traffico delle due reti può essere trasmesso sullo stesso cavo ma sarà trattato come se fosse inviato e ricevuto da due schede separate. L'utilizzo delle VLAN necessita di switch adeguatamente configurati.

Avvertimento: All'interfaccia logica **PPPoE** deve essere assegnato il ruolo di red, quindi richiede la funzionalità di gateway. Vedi *Firewall e gateway* per i dettagli.

Numerazione delle reti private (RFC1918)

Per reti private TCP/IP indirettamente connesse a Internet dovrebbero utilizzare indirizzi speciali selezionati dall'Internet Assigned Numbers Authority (IANA)

ID rete privata	Subnet mask	Intervallo di indirizzi 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

3.2.3 Servizi di rete

Un servizio di rete è un servizio che viene eseguito sul firewall stesso.

Ogni servizio ha una lista di porte «aperte» su cui risponde alle connessioni. Le connessioni possono essere accettate da zone selezionate. Un controllo più fine sull'accesso ai servizi di rete può essere configurato utilizzando le regole del firewall.

3.2.4 Reti fidate

Le reti fidate sono reti speciali (locali, VPN o remote) a cui è garantito l'accesso a servizi speciali del server.

Ad esempio, i computer sulle reti fidate possono accedere a:

- Server Manager
- Cartelle condivise (SAMBA)

Se la rete remota è raggiungibile attraverso un router, ricordarsi di creare la rotta statica corrispondente nel pannello *Rotte statiche*.

3.2.5 Rotte statiche

Il pannello consente di specificare instradamenti particolari (rotte statiche) che non facciano uso del default gateway (ad esempio per raggiungere reti private collegate tramite linee dedicate o simili).

Ricordarsi di aggiungere la rete a *Reti fidate*, se si desidera consentire agli host remoti di accedere ai servizi locali.

3.2.6 Indirizzo dell'organizzazione

I campi della pagina *Indirizzo dell'organizzazione* sono utilizzati come valori di default nella creazione degli utenti. Inoltre il nome dell'organizzazione e l'indirizzo sono mostrati nella pagina di login del Server Manager.

3.2.7 Certificato del server

La pagina *Certificato del server* mostra i certificati X.509 attualmente installati e il certificato di default fornito dal sistema per cifrare le comunicazioni TLS/SSL.

NethServer controlla la validità del certificato e invia una email all'utente root se il certificato sta per scadere.

Il pulsante *Imposta default* consente di scegliere il certificato di default. Quando viene scelto un nuovo certificato, tutti i servizi che utilizzano TLS/SSL vengono riavviati e i client di rete devono accettare il nuovo certificato.

Quando NethServer è installato viene automaticamente generato un certificato RSA auto-firmato. Dovrebbe essere modificato inserendo dei valori appropriati prima di utilizzarlo dai client di rete. Quando il certificato auto-firmato sta per scadere ne viene creato automaticamente uno nuovo con la stessa chiave RSA e gli stessi attributi.

La pagina *Certificato del server* permette anche di:

- caricare un certificato esistente e la chiave privata RSA/ECC. In aggiunta può essere specificato anche un chain file. Tutti i file devono essere codificati nel formato PEM.
- richiedere un nuovo certificato di *Let's Encrypt*[1]. Questo è possibile se sono rispettati i seguenti requisiti:

[1] Sito web di Let's Encrypt https://letsencrypt.org/

1. il server deve essere raggiungibile dall'esterno alla porta 80. Assicurarsi che la porta 80 è aperta alle connessioni da Internet (si può effettuare un test da siti come[2]);
2. i domini che si vogliono associare al certificato devono essere domini pubblici, associati all'indirizzo IP pubblico del server. Assicurarsi di avere un nome registrato nel DNS pubblico che punta correttamente al proprio server (si può effettuare un test da siti come[3]).

   I certificati wildcard (es. `*.nethserver.org`) non sono supportati.

Il campo *Invia notifiche a* verrà usato da Let's Encrypt per inviare notifiche sul certificato.

Il certificato Let's Encrypt viene automaticamente rinnovato 30 giorni prima della scadenza.

Nota: Per evitare problemi di importazione certificato con Internet Explorer, si consiglia di configurare il campo CN (Common Name) o Nome Comune in modo che corrisponda al FQDN del server.

Disattivare Let's Encrypt

Il certificato Let's Encrypt può essere disabilitato seguendo questi passi:

1. Accedere alla pagina *Server certificate*, impostare come predefinito il certificato autofirmato o uno caricato
2. Aprire la shell ed eseguire i seguenti comandi:

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

3.2.8 Arresto

La macchina su cui è installato NethServer può essere riavviata o spenta dalla pagina *Arresto*. Selezionare l'opzione Riavvia oppure Spegni e fare click su *Arresta il sistema*.

Al fine di evitare danni al sistema, utilizzare sempre questo modulo per effettuare una corretta procedura di riavvio o spegnimento del server.

3.2.9 Visualizza Log

Tutti i servizi registrano le operazioni svolte all'interno di file detti *log*. L'analisi dei log è lo strumento principale per individuare malfunzionamenti e problemi. Per visualizzare i file di log fare clic su *Visualizza Log*.

Questo modulo consente di:

- effettuare ricerche all'interno di tutti i log del server
- visualizzare un singolo log
- seguire in tempo reale il contenuto di un log

[2] Sito web http://www.canyouseeme.org/
[3] Sito web http://viewdns.info/

3.2.10 Data e ora

Al termine dell'installazione, assicurarsi che il server sia configurato con il corretto fuso orario. L'orologio della macchina può essere configurato manualmente o automaticamente usando server NTP pubblici (consigliato).

La corretta configurazione dell'orologio è importante per il funzionamento di molti protocolli. Per evitare problemi, tutti gli host della LAN possono essere configurati per usare il server stesso come server NTP.

3.2.11 Aiuto in linea

Tutti i pacchetti che sono configurabili attraverso il Server Manager contengono un manuale in linea che spiega l'utilizzo base e tutti i campi contenuti nella pagina.

Il manuale in linea è consultabile in tutte le lingue in cui è tradotto il Server Manager.

Una lista di tutti i manuali installati nel sistema è disponibile all'indirizzo:

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

Esempio

Se il server ha indirizzo 192.168.1.2 e si desidera visualizzare la lista dei manuali in italiano, usare il seguente indirizzo:

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

3.3 Utenti e gruppi

3.3.1 Account provider

NethServer supporta autenticazione e autorizzazione da un *account provider* **locale** o **remoto**.

I tipi di account provider supportati sono:

- OpenLDAP locale in funzione sullo stesso NethServer
- Server LDAP remoto con schema RFC2307
- Samba 4 Active Directory Domain Controller locale
- Active Directory remoto (sia Microsoft che Samba)

L'utente root può configurare ogni tipo di account provider dalla pagina *Accounts provider*.

Prestare attenzione alla seguente nota relativa agli account provider:

> Dopo che NethServer è stato collegato ad un account provider remoto, la pagina *Utenti e gruppi* visualizza gli account di dominio in sola lettura.

Provider remoto Dopo che NethServer è stato collegato ad un account provider remoto, la pagina *Utenti e gruppi* visualizza gli account di dominio in sola lettura.

Provider locale Dopo aver installato un provider locale (sia Samba 4 che OpenLDAP), l'amministratore può creare, modificare ed eliminare gli utenti e i gruppi.

Avvertimento: La scelta del tipo di account provider da adottare va fatta con estrema accuratezza perché **non è reversibile**. Inoltre il sistema impedirà qualsiasi modifica all'FQDN una volta che l'account provider sarà configurato.

Scegliere l'account provider giusto

L'amministratore dovrà decidere quale backend adottare secondo le necessità contingenti scegliendo l'attestazione ad un provider remoto o l'installazione di un provider locale.

Il modulo *File server* di NethServer, che abilita la pagina *Cartelle condivise*, può autenticare i client SMB/CIFS solo se NethServer è collegato ad un dominio Active Directory. I provider LDAP consentono l'accesso alle *Cartelle condivise* solo in modalità *guest*. Vedere inoltre *Cartelle condivise*.

D'altra parte il provider OpenLDAP locale è più semplice da installare e configurare.

In pratica, se il protocollo di condivisione file SMB non è richiesto, il provider LDAP è la scelta migliore.

Installazione del provider locale OpenLDAP

Per installare e configurare un account provider locale OpenLDAP, spostarsi nella pagina *Accounts provider* > *LDAP* > *Installa localmente*. Il sistema necessita una connessione internet funzionante per poter scaricare gli opportuni pacchetti aggiuntivi.

Al termine dell'installazione il pacchetto sarà automaticamente configurato e l'amministratore potrà gestire utenti e gruppi dalla pagina *User and groups*.

Fare riferimento alla sezione *Account admin* per maggiori informazioni in merito all'utente ed al gruppo amministrativo di default.

Avvertimento: L'account provider OpenLDAP locale disponibile NethServer non supporta completamente la scadenza password dell'utente. Fare riferimento alla sezione *Effetti della password scaduta* per maggiori dettagli

Installazione del provider locale Samba Active Directory

Per installare Samba Active Directory come account provider locale, il sistema necessita un **indirizzo IP addizionale** ed una **connessione ad internet funzionante**.

L'indirizzo IP addizionale è assegnato ad un Linux Container che esegue le funzioni di un controllore di dominio Active Directory e deve essere accessibile dalla LAN (rete green).

Pertanto l'indirizzo IP aggiuntivo deve soddisfare tre condizioni:

1. l'indirizzo IP deve essere **libero**; non può essere usato da alcun dispositivo
2. l'indirizzo IP deve appartenere alla stessa subnet di una rete green
3. la rete green deve essere assegnata ad una interfaccia bridge sulla quale il Container Linux possa attaccare la sua interfaccia virtuale; la procedura di installazione è in grado di creare l'interfaccia bridge automaticamente se non presente.

Per installare un account provider Active Directory locale, spostarsi nella pagina *Account provider* > *Active Directory* > *Crea un nuovo dominio*.

Il *Nome dominio DNS* definisce il suffisso DNS del nuovo dominio. NethServer svolge il ruolo di server DNS autoritativo per quel dominio. Per approfondimenti fare riferimento a *DNS e dominio AD*.

Il *Nome dominio NetBIOS* (noto anche come «nome corto di dominio» o «nome dominio NT») è l'identificativo alternativo per domini Active Directory, compatibile con i client più datati. Per approfondimenti fare riferimento a *Accesso alla rete*.

Il campo *Indirizzo IP Controller di Dominio* deve essere valorizzato con **l'indirizzo IP aggiuntivo** di cui sopra.

Una volta valorizzati tutti i campi, premere il bottone *Crea dominio*.

Avvertimento: Il *Nome dominio DNS* ed il *Nome dominio NetBIOS* di Active Directory non possono essere modificati una volta che il dominio è stato creato

La procedura di configurazione di Active Directory può richiedere un po" di tempo per completarsi, perché crea il *chroot* per il Linux Container, scaricando da internet dei pacchetti aggiuntivi.

La directory radice del Linux Container è `/var/lib/machines/nsdc/` e richiede un filesystem con supporto alle ACL Posix. Il filesystem di default XFS include il supporto alle ACL Posix e non richiede ulteriori configurazioni. Per altri filesystem (es. EXT4) abilitare le ACL come spiegato nei *Requisiti per le cartelle condivise*.

Al termine della procedura di configurazione, la macchina host NethServer è automaticamente inserita nel dominio di Active Directory. Andare alla pagina *Utenti e gruppi* per modificare gli account predefiniti.

L'indirizzo IP assegnato in precedenza può essere modificato dal menu *Account provider* > *Modifica IP*

Avvertimento: La modifica dell'indirizzo IP del Controller di Dominio può causare problemi ai client di Active Directory. Se utilizzano un server DNS esterno, aggiornarlo perché venga utilizzato il nuovo indirizzo IP.

Dopo aver installato Samba Active Directory, la pagina *Utenti e gruppi* contiene due elementi predefiniti; entrambi sono disabilitati: *administrator* e *admin*. «Administrator» è l'account privilegiato predefinito di Active Directory e non è necessario in NethServer; va bene tenerlo disabilitato. «admin» in NethServer è l'account amministrativo predefinito. E" membro del gruppo AD «Domain admins». Vedere *Account admin* per maggiori informazioni.

DNS e dominio AD

Un dominio di Active Directory richiede un dominio DNS riservato per funzionare. È buona pratica assegnare un sottodominio del dominio DNS pubblico per questa funzione. Il sottodominio AD può essere accessibile solo dalle reti LAN (green).

Esempio:

- dominio pubblico (*esterno*): `nethserver.org`
- FQDN del server: `mail.nethserver.org`
- dominio Active Directory (*interno* solo LAN): `ad.nethserver.org`
- FQDN domain controller (assegnato di default): `nsdc-mail.ad.nethserver.org`

Suggerimento: Quando si sceglie un dominio per Active Directory utilizzare un dominio *interno* che sia un sottodominio del dominio *esterno*[1]

Installazione su macchina virtuale

Samba Active Directory viene eseguito all'interno di un container Linux che utilizza un'interfaccia di rete virtuale in bridge con l'interfaccia di rete del sistema. L'interfaccia di rete virtuale deve essere visibile all'interno della rete fisica, ma spesso i software di virtualizzazione bloccano il traffico ARP e questo preclude la visibilità del container Samba Active Directory dalla LAN.

È quindi necessario assicurarsi che il virtualizzatore abiliti il traffico di rete con la *modalità promiscua*.

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

VirtualBox

Per configurare la modalità promiscua, selezionare «Permetti tutto» dal menù a discesa presente nella sezione di configurazione di rete.

VMWare

Entrare nella sezione di configurazione di rete del nodo da virtualizzare e abilitare lo switch virtuale in modalità promiscua.

KVM

Assicurarsi che la macchina virtuale sia in bridge con un bridge reale (per esempio br0) e che sia configurato in modalità promiscua.

È possibile forzare un bridge (per esempio, `br0`) in modalità promiscua usando il seguente comando:

```
ifconfig br0 promisc
```

Hyper-V

Configurare il MAC Address Spoofing per gli adattatori di rete virtuali[2]

Rimozione account provider locale

Sia l'account provider locale LDAP che quello AD possono essere rimossi dalla pagina *Account provider* > *Disinstalla*.

Quando il DB di account locale è disinstallato, tutti gli account utente, gruppi e computer vengono cancellati.

- Un elenco di utenti e gruppi in formato TSV viene scaricato in `/var/lib/nethserver/backup/users.tsv` e `/var/lib/nethserver/backup/groups.tsv`. Fare riferimento alla sezione *Importazione ed eliminazione account da file plain-text*.
- I file esistenti di proprietà di utenti e gruppi devono essere rimossi manualmente. Questa è l'elenco delle directory di sistema contenenti dati di utenti e gruppi:

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

Join ad un dominio Active Directory esistente

In questo scenario NethServer è collegato ad un account provider Active Directory remoto. Può essere una implementazione Samba o Microsoft. NethServer diventa quindi un server membro di un dominio Active Directory esistente. Quando si accede ad una risorsa su NethServer da una workstation del dominio, le credenziali dell'utente sono verificate da uno dei controllori di dominio e l'accesso alla risorsa viene consentito.

Per l'attestazione a un dominio di Active Directory è necessario siano soddisfatti i seguenti requisiti:

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

Il protocollo Kerberos richiede che la differenza tra gli orologi dei dispositivi del dominio sia meno di 5 minuti. Sincronizzare gli orologi dei client di rete con una sorgente di orario comune. Per NethServer andare alla pagina *Data e ora*.

Soddisfatti i prerequisiti, spostarsi alla pagina *Account provider* > *Active Directory* > *Join a un dominio*.

- Immettere il *Nome dominio DNS* del dominio AD. Il nome di dominio NetBIOS (nome breve di dominio) viene verificato automaticamente.
- Compilare il campo *Server DNS AD*. Solitamente è l'indirizzo IP di un controller di dominio AD.
- Fornire il *Nome utente* e la *Password* di un account AD avente i necessari privilegi per attestare un computer al dominio. Attenzione, l'account *amministratore* predefinito potrebbe essere disattivato!

Avvertimento: Alcuni moduli aggiuntivi, come *Nextcloud*, *WebTop*, *Roundcube*, *Ejabberd*, richiedono un accesso in sola lettura ai servizi LDAP di AD. Per renderli pienamente operativi, è necessario fornire un account di dominio **aggiuntivo** per eseguire semplici bind LDAP.

Creare un **account dedicato** in AD impostandogli una password complessa *priva di scadenza*.

Una volta completata l'attestazione ad AD di NethServer, specificare le credenziali dell'**account dedicato** nel campo *Accounts provider* > *Credenziali di autenticazione per le applicazioni LDAP*.

Collegamento ad un server LDAP remoto

Per configurare un provider di account LDAP remoto, spostarsi nella pagina *Account provider* > *LDAP* > *Collega remotamente*.

Digitare l'indirizzo IP del server LDAP nel campo *Nome host o IP*. Se il servizio LDAP viene eseguito su una porta TCP non standard, specificarla nel campo *Porta TCP*.

Quindi una query LDAP *rootDSE* verrà inviata all'host specificato e il form verrà valorizzato con i dati restituiti. Controllare che i valori siano corretti e premere il tasto *Salva* per confermare.

Se il server LDAP richiede l'autenticazione, compilare i campi sotto *Binding autenticato*. Abilitare `ldaps://` o STARTTLS per crittografare la connessione.

Suggerimento: Se il server LDAP remoto è un NethServer e si trova nella rete LAN (green), selezionare *Bind anonimo*

3.3.2 Utenti

Un nuovo utente rimane bloccato finché non gli viene assegnata una password. Agli utenti bloccati è negato l'accesso ai servizi del sistema.

I seguenti campi sono obbligatori per la creazione di un utente:

- Nome utente
- Nome completo (nome e cognome)

Un utente può essere aggiunto ad uno o più gruppi usando la pagina *Utenti* o *Gruppi*.

In alcuni casi potrebbe essere necessario bloccare l'accesso ai servizi a degli utenti senza eliminarne l'account. L'approccio più sicuro è

- bloccare l'utente utilizzando l'azione *Blocca*
- (opzionale) modificare la password dell'utente con una casuale

Nota: Quando un utente viene eliminarto, anche la home directory e la sua casella di posta verranno eliminate.

Modifica della password

Se durante la creazione dell'utente non è stata impostata una password, l'account utente è disabilitato. Per abilitarlo, impostare una password con il pulsante *Cambia password* .

Quando un utente è abilitato, può accedere al Server Manager e cambiare la propria password dalla voce *Profilo* nel menù *user@domain.com* in alto a destra.

Se il sistema è collegato ad un account provider di tipo Active Directory, gli utenti possono cambiare la propria password anche utilizzando gli strumenti appositi di Windows. In questo caso, non è possibile impostare password più corte di 6 *caratteri*, indipendentemente dalla policy selezionata. Windows esegue dei controlli prima di inviare la password al server,dove viene valutata in base alla *policy configurata*.

Credenziali per i servizi

Le credenziali dell'utente sono lo **username** e la **password**. Le credenziali sono richieste per accedere ai servizi installati sul sistema.

Lo username può essere utilizzato in due forme: *lungo* (default) e *breve*. La forma lunga è sempre accettata dai servizi. La forma breve potrebbe non essere valida in qualche servizio.

Per esempio se il dominio è *example.com* e l'utente è *goofy*:

Forma lunga username *goofy@example.com*

Forma breve username *goofy*

Per accedere ad una cartella condivisa, vedere anche *Accesso alla rete*.

Cartelle home dell'utente

Le directory home degli utenti sono memorizzate all'interno della directory :file: /var/lib/ nethserver/home‘, al fine di semplificare la distribuzione di un sistema di partizione a crescita singola.

L'amministratore può comunque ripristinare il noto `/home` usando il bind mount:

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

3.3.3 Gruppi

Un gruppo di utenti può essere usato per assegnare permessi speciali ad alcuni utenti, come autorizzare l'accesso alle *cartelle condivise*.

Si possono creare due gruppi speciali. Gli utenti che appartengono a questi gruppi ottengono l'accesso alle pagine del Server Manager.

- *domain admins*: gli utenti di questo gruppo hanno gli stessi permessi di root nel Server Manager.

- *managers*: gli utenti di questo gruppo hanno l'accesso alle pagine della sezione Gestione.

3.3.4 Account admin

Se è installato un account provider locale LDAP o AD, l'utente admin, membro del gruppo domain admins è creato automaticamente. Questo account consente di accedere a tutte le pagine di configurazione del Server Manager. Inizialmente è bloccato e non ha accesso alla console.

Suggerimento: Per abilitare l'account admin impostargli la password.

Dove possibile, l'account admin riceve dei permessi speciali da parte di servizi specifici, come poter aggiungere una workstation al dominio di Active Directory.

Se NethServer è collegato ad un account provider remoto, l'utente admin e il gruppo domain admins possono essere creati, se non esistono già.

Se un utente o un gruppo con una funzione simile è già presente nella base dati dell'account provider remoto, ma si chiama diversamente, può essere designato come admin usando questi comandi:

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

3.3.5 Gestione password

Il sistema prevede la possibilità di impostare dei vincoli sulla *complessità* e la *scadenza* delle password.

Le politiche di gestione password possono essere cambiate usando l'interfaccia web.

Complessità

La complessità password è un insieme di condizioni minime che devono essere soddisfatte affinché la password venga accettata dal sistema: è possibile scegliere tra due differenti policy di gestione complessità delle password:

- *none*: non viene fatto alcun controllo sulla password immessa se non sulla lunghezza di almeno 7 caratteri
- *strong*

La policy strong impone che la password debba rispettare le seguenti regole:

- lunghezza minima 7 caratteri
- contenere almeno 1 numero
- contenere almeno 1 carattere maiuscolo
- contenere almeno 1 carattere minuscolo
- contenere almeno 1 carattere speciale
- contenere almeno 5 caratteri diversi
- non deve essere presente nei dizionari di parole comuni
- deve essere diversa dallo username
- non può avere ripetizioni di pattern formati da più 3 caratteri (ad esempio la password As1.$As1.$ non è valida)
- se è installato Samba Active Directory, sarà abilitato anche lo storico delle password

La policy di default è *strong*.

Avvertimento: Cambiare le politiche predefinite è altamente sconsigliato. L'utilizzo di password deboli è la prima causa di compromissione dei server da parte di attaccanti esterni.

Scadenza

La scadenza password **NON** è abilitata di default.

Ogni volta che un utente cambia la sua password, la data della modifica della password viene registrata e, se l'opzione *Abilita scadenza password* viene attivata, la password viene considerata scaduta quando è trascorso il tempo di *Durata massima password*.

Per esempio, supponendo che

- l'ultimo cambio password sia stato effettuato in gennaio,
- in ottobre la *Durata massima password* venga impostata a '' 180 giorni'' ed *Abilita scadenza password* sia attivato

la password sarà **immediatamente considerata scaduta** (gennaio + 180 giorni = giugno!).

Effetti della password scaduta

Avvertimento: il server **non invia alcuna notifica relativa alla scadenza della password**!

Gli effetti di una password scaduta dipendono dall" account provider configurato.

Quando una password è scaduta

- con `Active Directory` (sia locale che remoto) un utente **non è più in grado di autenticarsi ad alcun servizio**;
- con l'account provider `LDAP` di NethServer (sia locale che remoto) **alcuni servizi ignorano la scadenza password**, consentendo l'accesso all'utente in ogni caso.

Un esempio di servizi che non supportano completamente la scadenza password in caso di utilizzo dell'account provider LDAP di NethServer sono:

- NextCloud
- WebTop (sono disponibili unicamente rubriche e calendari)
- SOGo

. . . ed ogni altro servizio che autentichi direttamente con LDAP

3.3.6 Importazione ed eliminazione account da file plain-text

Importazione utenti

È possibile creare utenti a partire da un file TSV (Tab Separated Values) con il seguente formato:

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

Esempio:

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

quindi eseguire:

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

Per esempio, se il file è /root/users.tsv, eseguire:

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

Per utilizzare un carattere separatore alternativo:

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

Importazione email

E" possibile creare indirizzi mail da un file TSV (Tab Separated Values) con il seguente formato:

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

Poi si può usare lo script *import_emails'*. Vedi *Importazione ed eliminazione account da file plain-text* per un esempio di invocazione del comando.

Importazione gruppi

La gestione dei gruppi è disponibile da linea di comando usando gli eventi group-create e group-modify

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

Eliminazione utenti

È possibile eliminare gli account utente a partire da un file con il seguente formato:

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

Esempio:

```
mario <NEWLINE>
```

quindi eseguire:

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

Suggerimento: È inoltre possibile utilizzare lo stesso file utilizzato per l'importazione degli utenti per effettuare la loro eliminazione.

Per esempio, se il file è /root/users.tsv, eseguire:

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

Per utilizzare un carattere separatore alternativo:

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

3.4 DNS

NethServer può essere configurato come server *DNS* (Domain Name System) della rete. Un server DNS si occupa della risoluzione dei nomi di dominio (es. *www.esempio.com*) nei loro corrispettivi indirizzi numerici (es. 10.11.12.13) e viceversa.

Il server DNS esegue le richieste di risoluzione nomi per conto dei client locali, ed è accessibile solo dalla LAN (rete green) e dalla rete ospiti (blue).

Quando si effettua una risoluzione nomi, il server potrà:

- ricercare il nome all'interno degli host configurati localmente
- effettuare una query sui dns esterni: le richieste vengono salvate in cache per velocizzare le successive query

---

Nota: E' obbligatorio specificare almeno un DNS esterno all'interno della scheda *Network* > *Server DNS*

Se NethServer è anche il server DHCP della rete, tutte le macchine saranno configurare per utilizzare il server stesso anche per la risoluzione nomi.

3.4.1 Hosts

La pagina *Hosts* consente di associare i nomi host ad indirizzi IP, siano essi locali o remoti.

Ad esempio, se si possiede un server web interno, è possibile associare il nome host *www.miosito.com* con l'IP del server web stesso. Tutti i client potranno quindi raggiungere il sito web digitando il nome scelto.

I nomi configurati localmente hanno sempre la precedenza sui record DNS dei server esterni. Infatti se il provider inserisce *www.dominio.it* con IP corrispondente al server web ufficiale, ma in NethServer *www.dominio.it* è configurato un ip diverso, i pc della LAN non saranno in grado di vedere il sito in questione.

3.4.2 Alias

Un *alias* è un nome alternativo usato per raggiungere il server stesso. Ad esempio, se il server si chiama *mail.example.com*, è possibile creare un alias DNS *myname.example.com*. Il server sarà quindi raggiungibile dai client della LAN anche usando il nome appena definito.

Gli alias valgono solo per la LAN interna. Se si desidera che il server sia raggiungibile con lo stesso nome anche dall'esterno è necessario chiedere al provider di associare l'indirizzo pubblico del nostro server al nome desiderato.

3.5 Server DHCP e PXE

Il server DHCP (*Dynamic Host Configuration Protocol*[1]) permette di controllare la configurazione di rete di tutti i computer o dispositivi collegati alla LAN. Quando un computer (o un dispositivo come una stampante, smartphone, etc.) si connette alla rete il DHCP gli assegna automaticamente un indirizzo IP valido e effettua la configurazione di DNS e gateway.

Nota: Nella maggior parte dei casi i dispositivi sono già configurati per utilizzare il protocollo DHCP.

La specifica PXE (*Preboot eXecution Environment*[3]) consente ad un dispositivo di scaricare da rete il sistema operativo all'avvio da una postazione di rete centralizzata, mediante i protocolli DHCP e TFTP. Vedere *Configurazione per l'avvio da rete* per un esempio su come configurare un caso simile.

3.5.1 Configurazione DHCP

Il server DHCP può essere abilitato su tutte le interfacce *green* e *blue* (vedi *Rete*). NethServer sceglierà un indirizzo IP libero all'interno dell'*intervallo DHCP* configurato nella pagina *DHCP > Server DHCP*.

L'intervallo DHCP deve appartenere alla rete dell'interfaccia associata. Per esempio, se l'interfaccia green ha IP 192.168.1.1 e maschera di rete 255.255.255.0, allora l'intervallo DHCP può andare da 192.168.1.2 a 192.168.1.254.

Opzioni avanzate

Il DHCP ha sette opzioni avanzate. Possono essere utilizzate indistintamente, da 0 a tutte 7.

Per i campi server – DNS, NTP, WINS and TFTP – è possible assegnare zero, uno o più server; in caso di più di uno, separare i valori con una virgola, senza lasciare spazi.

3.5.2 IP riservato a un host

Il server DHCP rilascia un indirizzo IP per un periodo di tempo limitato. Se un dispositivo necessita di avere sempre lo stesso IP, è possibile assegnarli un *IP Riservato* associato all'indirizzo MAC.

Nella pagina *Riserva IP* sono elencati tutti gli indirizzi IP correntemente assegnati:

- una riga con il pulsante *Riserva IP* identifica un host con un lease temporaneo (colore grigio);
- una riga con il pulsante *Modifica* identifica un host con un IP riservato (colore nero). Una piccola icona con due frecce indica che il lease DHCP è scaduto: questa è una condizione normale per gli host con configurazione IP statica, poiché non comunicano mai col server DHCP.

3.5.3 Configurazione per l'avvio da rete

Per consentire ai client di avviarsi dalla rete, sono richiesti i seguenti componenti:

- il server *DHCP*, come visto nelle sezioni precedenti
- il server *TFTP*[2]
- il software per il client, servito mediante TFTP

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

TFTP è un protocollo di trasferimento file molto semplice e generalmente utilizzato per il trasferimento automatico di file di configurazione o di boot.

In NethServer l'implementazione di TFTP è contenuta nel modulo DHCP ed è abilitata per default. Per consentire l'accesso a un file mediante TFTP è sufficiente mettere il file nella directory `/var/lib/tftproot`.

Nota: Per disabilitare TFTP digitare i seguenti comandi in una console di root:

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

Per esempio, ora configuriamo un client per avviarsi da rete con CentOS. In NethServer, digitare in una console di 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
```

Quindi, creare il file `/var/lib/tftpboot/pxelinux.cfg/default` con il seguente contenuto:

```
default menu.c32
prompt 0
timeout 300

MENU TITLE PXE Menu

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

Creare una directory CentOS:

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

Copiare dentro la directory appena creata i file `vmlinuz` e `initrd.img`. Questi file sono pubblici e possono essere trovati nella immagine ISO, sotto la directory `/images/pxeboot`, oppure scaricati da un mirror di CentOS.

Per finire, avviare il client, selezionando dalla schermata di avvio la modalità «PXE boot» o «boot from network», o simile.

Riferimenti

3.6 TLS policy

La pagina *TLS policy* controlla come i singoli servizi configurano il protocollo TLS (Transport Layer Security), selezionando un *identificativo di policy*.

Se non diversamente specificato, le impostazioni TLS delle policy sono sempre *cumulative*: **le nuove policy estendono quelle più vecchie**.

Ogni implementazione di modulo decide come implementare uno specifico identificatore di policy, fornendo un compromesso tra sicurezza e compatibilità con il client. Le politiche più recenti sono più orientate alla sicurezza, mentre quelle più vecchie offrono una migliore compatibilità con i vecchi client.

Le seguenti sezioni descrivono ciascun identificatore di policy.

3.6.1 Policy 2018-10-01

Questo criterio limita le impostazioni TLS della configurazione predefinita di Ejabberd. Si applica solo a Ejabberd versione 18 e successivi.

Ejabberd (XMPP)

- Vedi https://bettercrypto.org/static/applied-crypto-hardening.pdf category B
- Disabilitati SSLv3 e TLSv1.0
- Priorità di cifratura del server
- Certificato ECC
- Cifrari supportati:

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

3.6.2 Policy 2018-06-21

Questa policy estende la `2018-03-30` aggiungendo il supporto per i certificati ECC a

- Apache
- Dovecot
- OpenSSH
- Postfix

Slapd (openldap-servers)

- Riferimento https://access.redhat.com/articles/1474813
- Disabilitati SSLv3 e TLSv1.0
- Cipher suite

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

3.6.3 Policy 2018-03-30

L'obiettivo di questa politica è di rafforzare il set di cifratura di default fornito da upstream . Non è compatibile con IE 8 XP e Java 6u45 e 7u25 client. Non supporta i certificati ECC.

Apache

- Vedi https://bettercrypto.org/static/applied-crypto-hardening.pdf category B

- Cipher suite

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

- Disabilita SSLv2 e SSLv3
- Ignora le impostazioni di `httpd/SSLCipherSuite` (vedi :ref:‘:ref:‘tlspolicy-default”)

Dovecot

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

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

- Disabilita SSLv2 e SSLv3

OpenSSH

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

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

Postfix

- Vedi https://bettercrypto.org/static/applied-crypto-hardening.pdf category B
- Utilizza TLS per le connessioni in uscita, se il server remoto lo supporta
- Disabilita SSLv2 e SSLv3 sulle porte di submission
- Cipher suite

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

- Exclude ciphers

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

3.6.4 Politica upstream predefinita

L’obiettivo di questa policy è mantenere le impostazioni upstream. Questo è l’obiettivo principale dall’avvento di NethServer 7.

Questa politica consente di personalizzare `httpd` (Apache) con una determinata lista di cifrature, eseguendo i seguenti comandi:

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

CAPITOLO 4

Moduli

4.1 Backup

Il backup è l'unica procedura che consenta di ripristinare una macchina in caso di disastro. Il sistema gestisce due tipi di backup:

- backup della configurazione
- backup dei dati

Il backup della configurazione contiene solo i file di configurazione del sistema. Lo scopo di questo tipo di backup è ripristinare rapidamente una macchina in caso di *disaster recovery*. Quando la macchina è funzionate, è possibile eseguire un ripristino completo dei dati anche se la macchina è già in produzione.

Il backup dei dati si abilita installando il modulo «Backup» e, per impostazione predefinita, contiene tutti i dati memorizzati nel sistema (home dell'utente, cartelle condivise, e-mail, ecc.). Il *backup singolo* viene eseguito una volta al giorno e può essere completo od incrementale su base settimanale. Questo backup contiene anche l'archivio del backup di configurazione. È possibile configurare più backup per salvare dati diversi a intervalli diversi.

4.1.1 Backup configurazione

Dalla pagina *Backup (configurazione)* è possibile salvare, scaricare, eseguire l'upload o ripristinare la configurazione del sistema

Inoltre, un'attività automatizzata viene eseguita ogni notte alle 00.15 e crea un nuovo archivio, `/var/lib/nethserver/backup/backup-config.tar.xz`, se la configurazione è stata modificata nelle ultime 24 ore. E" possibile specificare il numero di *Backup automatici da mantenere* dal pannello *Backup (configurazione)*> *Configura*.

L'elenco dei moduli installati è incluso nell'archivio di backup. La procedura di ripristino consente di scaricare e installare automaticamente i moduli elencati.

Personalizzazione backup configurazione

Nella maggior parte dei casi non è necessario modificare il backup della configurazione. Ma può essere utile, ad esempio, se si è aggiunta una configurazione custom per httpd. In questo caso è possibile aggiungere il percorso del file che contiene la personalizzazione al backup della configurazione.

Inclusione

Se si desidera includere una directory o un file nel backup della configurazione, aggiungere una linea al file `/etc/backup-config.d/custom.include`.

Ad esempio, per eseguire il backup del file `/etc/httpd/conf.d/mycustom.conf`, aggiungere la riga:

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

Non aggiungere mai directory e file voluminosi al backup della configurazione.

Esclusione

Se si desidera escludere una directory o un file dal backup della configurazione, aggiungere una riga al file `/etc/backup-config.d/custom.exclude`.

Avvertimento: Assicurarsi di non lasciare linee vuote nei file modificati. La sintassi del backup della configurazione supporta solo percorsi file e directory semplici.

4.1.2 Backup dati

Il backup dei dati può essere eseguito utilizzando diversi engine:

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

Quando si seleziona un engine, l'amministratore di sistema deve valutare attentamente molteplici aspetti:

- Compressione: i dati vengono compressi sulla destinazione, l'utilizzo del disco può variare in funzione dell'efficienza della compressione, che dipende anche dal set di dati
- Deduplicazione: invece di comprimere i file, i dati vengono suddivisi in blocchi e viene conservata solo una copia di ciascun blocco. L'efficienza dipende molto dal set di dati
- Crittografia: i dati salvati nella memoria di destinazione sono crittografati. Di solito i dati vengono crittografati prima del trasferimento
- Dimensione: lo spazio utilizzato nella destinazione per ciascun backup può essere inferiore o uguale al set di dati originale. Quando si utilizzano engine senza supporto per la compressione, lo spazio sulla destinazione dovrebbe sempre essere più grande rispetto a quello occupato nella sorgente
- Conservazione: la politica che fissa la quantità di tempo in cui un set di dati rimarrà disponibile per il ripristino
- Integrità: è la capacità dell'engine di verificare se il backup eseguito è valido in caso di ripristino
- Tipo: un backup può essere completo, incrementale o basato su snapshot (sempre incrementale):
  - completo: tutti i file vengono copiati nella destinazione ogni volta
  - incrementale: confronta i dati con l'ultimo backup completo e copia solo gli elementi modificati o aggiunti. Il backup completo e tutti gli incrementali intermedi sono necessari per il processo di ripristino. È richiesto che venga eseguito regolarmente un backup completo.

  - snapshot: crea un backup completo solo la prima volta, successivamente crea solo backup differenziali. Le istantanee possono essere eliminate e consolidate ed è necessario un solo backup completo

Engine	Compressione	Deduplicazione	Crittografia	Integrità	Tipo
duplicity	Sì	No	No	Sì	completo / incrementale
restic	No	Sì	Sì	Sì	snapshot
rsync	No	Parziale	No	No	snapshot

L'amministratore può pianificare più backup utilizzando diversi engine e destinazioni. Una buona politica potrebbe essere quella di creare un backup settimanale su una destinazione locale utilizzando Duplicity e pianificare un ulteriore backup giornaliero su uno storage cloud usando Restic.

Quando si configurano più backup è opportuno rammentare due regole d'oro:

- utilizzare sempre destinazioni diverse per ciascun engine
- evitare la pianificazione di backup simultanei, ogni backup deve essere eseguito quando il precedente è stato completato

---

Nota: Mentre un backup singolo può essere configurato e ripristinato attraverso il Server Manager, i backup multipli devono essere configurati utilizzando il nuovo Server Manager (Cockpit).

Backend di archiviazione

Supportati da tutti gli engine:

- CIFS: cartella condivisa Windows, disponibile su tutti i NAS (Network Attached Storage). Utilizza credenziali di accesso come: MioUtente,domain=miodominio.com
- NFS: cartella condivisa Linux, disponibile su tutti i NAS, solitamente più veloce di CIFS
- WebDAV: disponibile su molti server NAS e remoti (utilizzare come destinazione WebDAV un server con un certificato SSL valido, altrimenti il sistema non riuscirà a montare il filesystem)
- USB: disco collegato ad una porta USB/SATA locale

Supportati da restic ed rsync

- SFTP: SSH File Transfer Protocol

Supportati solo da restic

- Amazon S3 (o altro server compatibile come Minio)
- Backblaze B2

Engine

Duplicity

Duplicity è l'engine di backup predefinito per NethServer. Ha un buon algoritmo di compressione che riduce in modo apprezzabile l'utilizzo della spazio sulla destinazione. Duplicity richiede un backup completo una volta alla settimana, quando il set di dati è molto grande il processo potrebbe richiedere più di 24 ore per essere completato. NethServer non implementa la crittografia per il backup se l'engine è Duplicity.

Backend di archiviazione supportati:

- CIFS
- NFS
- USB
- WebDAV (solo quando usato come *backup singolo*)

Nota: Il nome della directory di destinazione è basato sul nome host del server: in caso di modifica dell'FQDN, l'amministratore dovrà occuparsi di copiare/spostare i dati di backup dalla vecchia directory a quella nuova.

Restic

Restic implementa un backup basato su snapshot e sempre crittografato. Supporta la deduplicazione e può eseguire il backup sui servizi cloud. Poiché Restic richiede solo un backup completo, tutte le esecuzioni successive alla prima dovrebbero essere veloci e potrebbero essere programmate più volte al giorno.

Backend di archiviazione supportati:

- CIFS
- NFS
- USB
- WebDAV (solo quando usato come *backup singolo*)
- SFTP (SSH File Transfer Protocol)
- Amazon S3 (o altro server compatibile come Minio)
- Backblaze B2
- Restic REST server

Rsync

L'engine di backup stile Time machine utilizza: index: rsync‘. Dopo il primo backup completo, copia solo i file modificati o nuovi utilizzando un effiecente sistema di trasferimento incrementale. Sulla destinazione, la deduplicazione parziale viene ottenuta attraverso l'uso di link fisici. Se la directory di destinazione del backup è piena, i backup più vecchi vengono automaticamente eliminati per liberare spazio.

Backend di archiviazione supportati:

- CIFS
- NFS
- USB
- WebDAV (solo quando usato come *backup singolo*)
- SFTP (SSH File Transfer Protocol)

Rsync non supporta la crittografia né la compressione sulla destinazione. Durante il trasferimento dei dati, SFTP assicura la crittografia e i dati vengono compressi per ridurre al minimo l'utilizzo della banda utilizzata.

Nota: Quando si utilizza l'engine rsync, assicurarsi che il backend di destinazione supporti link simbolici e fisici. Si rammenta che NethServer non supporta collegamenti su condivisioni Samba per implicazioni di sicurezza. Inoltre i link simbolici non sono supportati su WebDAV.

Esecuzione da riga di comando

Per lanciare un backup da riga di comando, utilizzare:

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

in cui `name` è il nome del backup che si desidera lanciare.

Nota: Di default il nome del *primo* backup configurato su NethServer è `backup-data`

Personalizzazione backup dati

In caso di installazione di software aggiuntivi, potrebbe esser necessario modificare la lista delle directory e dei file inclusi (o esclusi) dal backup.

Inclusioni

Se si desidera includere una directory o un file nel backup dei dati, aggiungere una linea al file `/etc/backup-data.d/custom.include`.

Ad esempio, per eseguire il backup di un software installato nella directory `/opt`, aggiungere la linea:

```
/opt/mysoftware
```

La stessa sintassi si applica al backup della configurazione. Le modifiche dovranno essere incluse all'interno del file `/etc/backup-config.d/custom.include`.

Esclusioni

Se si desidera escludere una directory o un file dal backup dei dati, aggiungere una linea al file `/etc/backup-data.d/custom.exclude`.

Ad esempio, per escludere dal backup tutte le directory chiamate *Download*, aggiungere la linea:

```
**Download**
```

Per escludere una casella di posta *test*, aggiungere la riga:

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

La stessa sintassi si applica al backup della configurazione. Le modifiche dovrebbero essere fatte all'interno del file `/etc/backup-config.d/custom.exclude`.

Personalizzazione inclusioni ed esclusioni

Tutti i backup utilizzano la stessa configurazione, ma l'elenco dei file salvati ed esclusi può essere personalizzato utilizzando due file speciali:

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

In cui `name` è il nome del backup.

Entrambi i file sostituiranno il set di dati inclusi ed esclusi dal backup. La sintassi accettata è la stessa indicata nel paragrafo precedente.

Ad esempio, dato un backup chiamato `mybackup1` creare i seguenti file:

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

Esempio

È possibile configurare un backup che includa solo i file della posta programmato ogni ora.

1. Configurare il nuovo `mymailbackup` utilizzando l'interfaccia utente
2. Creare un file include custom contenente solo la directory delle email:

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

3. Creare un file exclude custom vuoto:

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

4. Applicare la configurazione:

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

Avvertimento: Assicurarsi di non lasciare linee vuote nei file modificati.

Nota: Questo tipo di backup non può essere utilizzato in caso di disaster recovery.

4.1.3 Ripristino selettivo dei file

Assicurarsi che la destinazione del backup sia raggiungibile (ad esempio, il disco USB deve essere collegato).

Nella sezione *Ripristino file* è possibile cercare, selezionare e ripristinare una o più directory dal backup, navigando tutti i percorsi inclusi nel backup nell'albero grafico.

Per impostazione predefinita, viene mostrato l'albero del backup più recente. Se si desidera ripristinare un file da un backup precedente, selezionare la data di backup dal selettore *Backup file*.

Sono disponibili due opzioni in fase di ripristino:

- Ripristina i file nel percorso originale, i file correnti nel filesystem vengono sovrascritti dai file ripristinati dal backup
- Ripristina i file nel percorso originale ma i file ripristinati dal backup vengono spostati in una nuova directory (i file non vengono sovrascritti) in questo percorso:

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

Per utilizzare il campo di ricerca, è sufficiente inserire almeno 3 caratteri e la ricerca inizia automaticamente evidenziando le directory corrispondenti.

È possibile ripristinare le directory facendo clic sul pulsante **Ripristina**.

Nota: E" possibile effettuare una selezione multipla mantenendo premuto il tasto `Ctrl`.

Nota: L'interfaccia utente per il ripristino selettivo è disponibile solo per il backup denominato `backup-dati`.

Procedura da riga di comando

Tutti i dati sono sono posizionati nella directory `/var/lib/nethserver/` :

- Cartelle di posta: `/var/lib/nethserver/vmail/<user>`
- Cartelle condivise: `/var/lib/nethserver/ibay/<name>`
- Home utenti: `/var/lib/nethserver/home/<user>`

Per elencare i dati all'interno di un backup, utilizzare:

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

Per ripristinare tutti i dati nella posizione originale, utilizzare:

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

Per ripristinare un file o una directory, utilizzare:

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

Esempio, ripristinare un file alla versione di 15 giorni fa:

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

L'opzione `-t` consente di specificare il numero di giorni (15 in questo scenario). Quando viene utilizzato con engine basati su snapshot, l'opzione `-t` richiede il nome dello snapshot da ripristinare.

Nota: Nel caso si utilizzi *CIFS* per accedere alla condivisione e il comando di restore non funzioni nel modo atteso, verificare che utente e password della condivisione di rete siano corretti. Se la coppia utente/password è sbagliata nel file `/var/log/messages` si troveranno degli errori di NT_STATUS_LOGON_FAILURE. Allo stesso tempo il comando backup-data-list non andrà a buon fine e uscirà immediatamente riportando degli errori.

4.1.4 Configurazione disco USB

Il miglior filesystem per dischi di backup USB è EXT3 o EXT4. Il filesystem FAT è supportato ma *non raccomandato*, mentre NTFS **non è supportato**. EXT3 o EXT4 è obbligatorio per il engine rsync.

Per eseguire la formattazione, è necessario collegare il disco e identificarlo correttamente:

```
# dmesg | tail -20

Apr 15 16:20:43 mynethserver kernel: usb-storage: device found at 4
Apr 15 16:20:43 mynethserver kernel: usb-storage: waiting for device to settle before␣
↪scanning
Apr 15 16:20:48 mynethserver kernel:   Vendor: WDC WD32  Model: 00BEVT-00ZCT0     Rev:
Apr 15 16:20:48 mynethserver kernel:   Type:   Direct-Access           ANSI SCSI␣
↪revision: 02
Apr 15 16:20:49 mynethserver kernel: SCSI device sdc: 625142448 512-byte hdwr sectors␣
↪(320073 MB)
Apr 15 16:20:49 mynethserver kernel: sdc: Write Protect is off
Apr 15 16:20:49 mynethserver kernel: sdc: Mode Sense: 34 00 00 00
Apr 15 16:20:49 mynethserver kernel: sdc: assuming drive cache: write through
Apr 15 16:20:49 mynethserver kernel: SCSI device sdc: 625142448 512-byte hdwr sectors␣
↪(320073 MB)
Apr 15 16:20:49 mynethserver kernel: sdc: Write Protect is off
Apr 15 16:20:49 mynethserver kernel: sdc: Mode Sense: 34 00 00 00
Apr 15 16:20:49 mynethserver kernel: sdc: assuming drive cache: write through
Apr 15 16:20:49 mynethserver kernel:  sdc: sdc1
Apr 15 16:20:49 mynethserver kernel: sd 7:0:0:0: Attached scsi disk sdc
Apr 15 16:20:49 mynethserver kernel: sd 7:0:0:0: Attached scsi generic sg3 type 0
Apr 15 16:20:49 mynethserver kernel: usb-storage: device scan complete
```

Un altro buon comando da utilizzare può essere:

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

In questo esempio, il disco è stato riconosciuto come device *sdc*.

- Creare una unica partizione Linux sull'intero disco sdc:

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

- Crea il filesystem sulla partizione *sdc1* con un'etichetta denominata *backup*. Il filesystem dovrebbe essere ottimizzato per l'engine di backup usato: rsync e restic richiedono molti inode, duplicity ha prestazioni migliori su file system ottimizzati per file di grandi dimensioni.

  Per duplicity usare:

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

  Per rsync e restic usare:

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

- Scollegare e ricollegare il disco USB:

  E' possibile utilizzare il comando seguente per simulare il collegamento del disco:

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

- A questo punto la voce *backup* sarà selezionabile dalla pagina *Backup (data)*.

4.1.5 Disaster recovery

Il sistema viene ripristinato in due fasi: prima la configurazione, poi i dati. Subito dopo il ripristino della configurazione, il sistema è pronto per essere utilizzato se sono installati i pacchetti corretti. È possibile installare pacchetti aggiuntivi prima o dopo il ripristino. Ad esempio, se il server di posta è installato, il sistema può inviare e ricevere posta.

Altre configurazioni ripristinate:

- Utenti e gruppi
- Certificati SSL

Avvertimento: Non ripristinare un backup di configurazione proveniente da una vecchia minor version in una versione più recente. Il backup dovrebbe provenire da un NethServer avente la stessa versione del sistema operativo della nuova installazione.

Es: evitare di ripristinare un backup della configurazione proveniente da una installazione 7.4.1708 in un più recente sistema 7.6.1810, questo potrebbe introdurre derive inattese.

I passi da eseguire sono:

1. Installa la nuova macchina. Se possibile, abilitare una connessione di rete all'avvio (fare riferimento alla sezione *Modalità interattiva e Manuale*) per reinstallare automaticamente i moduli richiesti
2. Accedere al Server Manager e seguire la procedura *Wizard di prima configurazione*
3. Allo step *Ripristino configurazione* caricare il backup della configurazione. L'opzione *Scarica automaticamente moduli* può essere abilitata.
4. Se un avviso lo richiede, riconfigurare le interfacce di rete. Vedi *Assegnamento delle interfacce di rete*
5. Verificare che la macchina sia funzionante
6. Ripristinare il backup dei dati eseguendo dalla console

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

Si noti che il disater recovery dovrebbe essere sempre eseguito da un supporto locale (ad esempio NFS o USB) per velocizzare il processo.

Nota: La password di root/admin non viene ripristinata, verrà mantenuta quella impostata nel nuovo sistema.

Assegnamento delle interfacce di rete

Se la configurazione contiene una scheda di rete assente, le pagine *Dashboard*, *Backup (configurazione)* > *Ripristino* e *Network* mostrano un avviso. Questo può accadere per esempio nei seguenti casi:

- dopo il ripristino del backup della configurazione su un nuovo hardware
- una o più schede di rete sono state sostituite
- i dischi del sistema sono stati spostati su una nuova macchina

L'avviso porta a una pagina che elenca le schede di rete fisiche presenti nel sistema, evidenziando quelle che non hanno un *ruolo* assegnato. Per ogni scheda di questo tipo, un menù a discesa mostra i ruoli da assegnare.

Per esempio, se una scheda con ruolo *orange* è stata sostituita, il menù a discesa elencherà un elemento `orange` in corrispondenza della nuova scheda di rete.

Lo stesso accade se la vecchia scheda era il componente di una interfaccia logica, come un bridge o un bond.

Selezionando un elemento dal menù a discesa, le impostazioni del ruolo sono trasferiti alla nuova scheda.

Premendo il pulsante *Salva* le modifiche vengono applicate.

Avvertimento: Assegnare con attenzione i ruoli alle nuove interfacce. Un errore può portare ad un sistema isolato dalla rete.

Nel caso in cui fosse il ruolo `green` a mancare, in fase di avvio del sistema una procedura automatica tenterà di ripristinare la configurazione di rete essenziale per consentire di accedere nuovamente al Server Manager.

4.2 Email

Il modulo Email è composto da tre parti principali:

- server SMTP per l'invio e la ricezione[1]
- server IMAP e POP3 per la lettura della posta[2], e linguaggio Sieve per organizzarla[3]
- Filtro antispam, antivirus e blocco degli allegati[4]

Vantaggi

- Completa autonomia nella gestione della posta
- Esclusione di eventuali problemi dovuti al provider
- Possibilità di ricostruire tutto il tragitto dei messaggi al fine di individuare eventuali errori
- Scansione antispam ed antivirus ottimizzata

Vedi anche gli argomenti correlati:

- Come funziona la posta elettronica[5]
- Record DNS di tipo MX[6]
- Simple Mail Transfer Protocol (SMTP)[7]
- firma DKIM[8]

Nota: Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *Proxy POP3* sono basate sul motore di filtraggio Rspamd. Le precedenti installazioni di NethServer verranno automaticamente aggiornate a Rspamd come descritto nella sezione *Aggiornamento Email a Rspamd*

[1] Postfix mail server http://www.postfix.org/
[2] (1, 2) Dovecot Secure IMAP server http://www.dovecot.org/
[3] Sieve mail filtering language https://en.wikipedia.org/wiki/Sieve_(mail_filtering_language)
[4] Rspamd: sistema di filtraggio di spam veloce, gratuito e open source. https://rspamd.com/
[5] Posta elettronica, https://it.wikipedia.org/wiki/Posta_elettronica
[6] Il record DNS MX, https://it.wikipedia.org/wiki/MX_record
[7] SMTP, https://it.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol
[8] Domain Keys Identified Mail (DKIM) è un metodo di autenticazione e-mail progettato per rilevare lo spoofing delle e-mail – *Wikipedia <https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail>* _

4.2.1 Domini

NethServer consente la gestione di un numero illimitato di domini, configurabili dalla pagina *Email* > *Domini*. Per ciascun dominio sono disponibili due modalità:

- *Consegna locale*: la posta viene consegnata agli utenti locali e salvata in formato Maildir[9]
- *Inoltra* i messaggi ad un altro server di posta.

Nota: Eliminando un dominio, non verranno eliminate e-mail, ma solo inibita la ricezione di mail indirizzate al dominio. Eventuali mail già ricevute rimarranno conservate sul server.

NethServer permette di conservare una *copia nascosta* di tutte le mail in transito, con relativo contenuto (quindi non un semplice log di mittenti e destinatari): tutti i messaggi verranno consegnati *sia* al destinatario *sia* ad un indirizzo personalizzato. Questa opzione è configurabile individualmente per ciascun dominio gestito dal server di posta.

Avvertimento: L'attivazione dell'opzione *Copia nascosta (Bcc)* va valutata attentamente, perché, in ambito aziendale, potrebbe essere equiparata ad un telecontrollo del lavoratore, pratica vietata dalla legge in diversi stati.

Se il destinatario finale non può essere raggiunto (ad esempio se l'indirizzo del destinatario non esiste), il messaggio viene normalmente rifiutato. A volte (ad esempio quando viene migrato un dominio di posta elettronica) potrebbe essere utile accettare e consegnare il messaggio ad una cassetta postale di tipo catch-all. Questo comportamento può essere ottenuto abilitando l'opzione *Accept unknown recipients*.

Aggiungere un avviso legale

Avvertimento: Dal NethServer 7.5.1804 questa funzionalità è distribuita in un pacchetto separato e opzionale: `nethserver-mail2-disclaimer`. Questo pacchetto è *deprecato* perché il progetto alterMIME[10] che provvede all'attuale implementazione, non è più sviluppato e può smettere di funzionare in qualsiasi momento.

Se il pacchetto opzionale `nethserver-mail2-disclaimer` è stato installato dal *Software center*, NethServer può automaticamente *aggiungere una nota legale ai messaggi inviati*. Questo testo è anche conosciuto come «disclaimer» e serve per ottemperare a determinati requisiti legali.

Il disclaimer può contenere codice Markdown[11] che consente la formattazione del testo.

Notare che *signature* e *disclaimer* sono concetti diversi.

In generale, il **disclaimer** è un testo statico e deve essere *allegato* (non aggiunto) ai messaggi dal server di posta. Questa tecnica aiuta a mantenere l'integrità del messaggio in caso di firma digitale.

Esempio di disclaimer:

```
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.
```

[9] The Maildir format, https://en.wikipedia.org/wiki/Maildir
[10] alterMIME è un piccolo programma che viene utilizzato per modificare il tuo mailpack con codifica mime – https://pldaniels.com/altermime/
[11] The Markdown plain text formatting syntax, https://en.wikipedia.org/wiki/Markdown

La **signature** deve essere inserita nel testo del messaggio solo dal client di posta (MUA): Outlook, Thunderbird, ecc. Di solito è un testo definito dall'utente che contiene informazioni come indirizzi mittente e numeri di telefono.

Esempio di firma:

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

Firma DKIM

DomainKeys Identified Mail (DKIM)[8] fornisce un modo per convalidare l'MTA di invio, che aggiunge una firma crittografata alle intestazioni MIME dei messaggi in uscita.

Per attivare la firma DKIM in un Dominio di posta, abilitare *Email* > *Domini* > *Firma i messaggi in uscita con DomainKeys Identified Mail (DKIM)*.

Le intestazioni delle firme DKIM vengono aggiunte solo ai messaggi inviati tramite le porte TCP 587 (submission) e 465 (smtps).

Per funzionare efficacemente, il DNS pubblico deve essere configurato correttamente. Fare riferimento alle istruzioni del proprio provider DNS per eseguire le seguenti operazioni:

1. Aggiungere un record TXT al provider DNS pubblico con la chiave «default._domainKey»
2. Copia e incolla della chiave assegnata nella sezione Dati del record DNS (RDATA)

4.2.2 Indirizzi email

Ogni utente ha un propria *casella di posta* e ogni nome utente nella forma <*username*>@<*domain*> è anche un indirizzo email valido a cui inviare messaggi.

La lista delle caselle di posta è visualizzata nella pagina *Indirizzi email* > *Caselle di posta utente*. Il pulsante *Modifica* consente di disabilitare l'*Accesso ai servizi email* (IMAP, POP3, SMTP/AUTH) per un utente specifico e i messaggi inviati a questo utente posso essere inoltrati a un indirizzo email esterno.

Avvertimento: Se il sistema è collegato a un *account provider remoto* dove viene rimosso un account utente, la mailbox associata deve essere cancellata manualmente. Il percorso in cui si trova è `/var/lib/nethserver/vmail/`.

Le caselle di posta possono essere condivise tra gruppi di utenti. La pagina *Indirizzi email* > *Caselle di posta condivise* consente la creazione di una nuova *casella di posta condivisa* e la definizione di uno o più gruppi a cui appartiene. Le caselle di posta condivise possono anche essere create da un qualunque client IMAP che supporta l'estensione del protocollo IMAP ACL (RFC 4314).

Il sistema consente la creazione di un numero illimitato di *indirizzi email* aggiuntivi, dalla pagina *Indirizzi email* > *Indirizzi email aggiuntivi*. Ogni *indirizzo email aggiuntivo* è associato a una o più destinazioni. Una *destinazione* può essere:

- casella di posta utente
- casella di posta condivisa
- indirizzo email esterno

Un indirizzo email aggiuntivo può essere associato a qualsiasi dominio di posta o ad uno specifico. Per esempio:

- Primo dominio: miodominio.it

- Secondo dominio: esempio.com
- Indirizzo email *info* valido per entrambi i domini: info@miodominio.it, info@esempio.com
- Indirizzo email *pippo* valido solo per un dominio: pippo@esempio.com

A volte le aziende proibiscono l'uso di indirizzi e-mail personali per le comunicazioni dell'organizzazione verso l'esterno. L'opzione *Solo reti locali* (o visibilità *Internal*) impedisce ad un indirizzo di ricevere e-mail dall'esterno. L'indirizzo «solo rete locale» può essere però utilizzato per scambiare messaggi con altri account del sistema.

4.2.3 Configurazione caselle di posta

La pagina *Email* > *Caselle di posta* mostra l'elenco dei protocolli disponibili per l'accesso alle caselle di posta:

- IMAP[12] (raccomandato)
- POP3[13] (sconsigliato)

Per motivi di sicurezza, tutti protocolli richiedono la connessione cifrata in modalità STARTTLS. Anche se fortemente sconsigliato, è possibile disabilitare la cifratura abilitando l'opzione *Consenti connessioni non cifrate*. In questo modo le password e i contenuti dei messaggi possono transitare in chiaro nella rete.

Avvertimento: Non consentire le connessioni in chiaro negli ambienti di produzione!

Dalla stessa pagina lo *Spazio disco* di una casella di posta può essere limitato da una *quota* prestabilita. Se alle caselle di posta è applicata una quota, la pagina *Dashboard* > *Mail quota* riassume l'utilizzo dello spazio disco di ogni utente. La quota può essere personalizzata per un utente particolare dal controllo *Indirizzi email* > *Caselle utenti* > *Modifica* > *Quota email personalizzata*.

I messaggi marcati come **spam** (vedi *Filtro*) possono essere spostati automaticamente all'interno della cartella *Junk* abilitando l'opzione *Sposta nella cartella «Junk»*. I messaggi di spam vengono automaticamente rimossi dopo che è trascorso il periodo specificato da *Conserva per*. Tale periodo può essere personalizzato per un utente particolare dal controllo *Utenti* > *Modifica* > *Servizi* > *Personalizza tempo di permanenza delle email di spam*.

L'utente `root` può impersonare un altro utente, acquisendo pieni diritti sui contenuti della casella di posta e sui permessi delle cartelle di quest'ultimo. L'opzione *Root può accedere impersonando un altro utente* controlla questa facoltà, conosciuta con il nome di *master user* in Dovecot[2].

Quando *Root può accedere impersonando un altro utente* è abilitata, le seguenti credenziali sono accettate dal server IMAP:

- nome utente al quale sia aggiunto il suffisso `*root`
- password di root

Per esempio, per accedere come `john` con la password di root `secr3t`, utilizzare le seguenti credenziali:

- nome utente: `john*root`
- password: `secr3t`

4.2.4 Messaggi

Dalla pagina *Email* > *Messaggi*, il controllo *Accetta messaggi fino a* imposta la dimensione massima dei messaggi che attraversano il sistema. Se questo limite è superato, un messaggio non entra affatto nel sistema, e viene rifiutato.

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

Quando un messaggio entra in NethServer, viene registrato nella *coda messaggi*, in attesa di essere consegnato o inoltrato altrove (relay). Quando NethServer inoltra un messaggio ad un server remoto, possono verificarsi degli errori. Per esempio:

- la connessione di rete fallisce, oppure
- l'altro server è spento, o è in sovraccarico

Questi ed altri errori sono *temporanei*: in questi casi, NethServer tenta di riconnettersi all'host remoto ad intervalli regolari, finché viene raggiunto un limite. Il controllo *Tenta l'invio per* imposta questo limite. Di default è impostato a *4 giorni*.

Mentre i messaggi sono nella coda, l'amministratore può richiedere un tentativo immediato di spedizione, premendo il pulsante *Tenta l'invio* dalla scheda *Gestione coda*. In alternativa, l'amministratore può eliminare i messaggi in coda in maniera selettiva, o svuotare completamente la coda mediante il pulsante *Elimina tutti*.

L'opzione *Spedisci sempre una copia* abilita la copia nascosta di qualsiasi messaggio attraversi il server di posta. Questa funzionalità è differente dall'opzione simile nella scheda *Email* > *Domain* perché non fa differenza tra i domini di posta e in più cattura i messaggi in uscita.

Avvertimento: L'attivazione dell'opzione *Copia nascosta (Bcc)* va valutata attentamente, perché, in ambito aziendale, potrebbe essere equiparata ad un telecontrollo del lavoratore, pratica vietata dalla legge in diversi stati.

4.2.5 Smarthost

Il menu *Email* > *Smarthost* consente di affidare l'invio di tutti i messaggi in uscita ad uno speciale server SMTP, tecnicamente denominato *smarthost*. Uno smarthost consente l'inoltro dei messaggi se sono verificate determinate condizioni. E" possibile che verifichi:

- l'indirizzo IP del client
- le credenziali SMTP AUTH

Nota: Spedire tramite uno *smarthost* è in genere sconsigliato, a meno che il server non sia temporaneamente in una blacklist[14], o il traffico SMTP sia bloccato dall'ISP.

4.2.6 Filtro

Tutta la posta in transito è sottoposta ad una serie di controlli che possono essere abilitati selettivamente dalla pagina *Email* > *Filtro*:

- Blocco allegati
- Antivirus
- Antispam

Blocco allegati

Il sistema può ispezionare le email, negando l'accesso a messaggi che contengono file in formati proibiti dalle politiche aziendali. È possibile bloccare i seguenti tipi:

[14] DNSBL https://it.wikipedia.org/wiki/DNSBL

- *file eseguibili* (es. exe, msi)
- *archivi* di file (es. zip, tar.gz, docx)
- lista personalizzata di estensioni

Il sistema riconosce il tipo del file analizzandone il contenuto, indipendentemente dal nome del file. Quindi è possibile che file MS Word (docx) e OpenOffice (odt) siano bloccati perché sono in realtà anche degli archivi zip.

Antivirus

Il componente antivirus individua i messaggi di posta elettronica contenenti virus. I messaggi infetti vengono scartati. Il database contenente le impronte dei virus è aggiornato periodicamente.

Antispam

Il filtro antispam[4] analizza i messaggi rilevando e classificando lo *spam*[15] tramite criteri euristici, regole predeterminate e valutazioni statistiche sul contenuto dei messaggi.

Il filtro può anche verificare se il server mittente è elencato in una o più black list (DNSBL [#DNSBL] _). Un punteggio è associato a ciascuna regola.

il punteggio totale raggiunto alla fine dell'analisi permette al server di decidere cosa fare di un messaggio, in accordo con tre **thresholds** che possono essere impostate in *Email* > *Filter* > *Anti spam*.

1. Se il punteggio spam è superiore a *Greylist threshold* il messaggio è **temporarily rejected**. La tecnica *greylisting*[16] presuppone che uno spammer abbia fretta e molto probabilmente non invii di nuovo la mail, mentre un MTA conforme allo standard SMTP tenterà di recapitare nuovamente il messaggio posticipato.
2. Se il punteggio spam è superiore a *Spam threshold* il messaggio viene **marcato come spam** con l'aggiunta dello speciale header `X-Spam-Flag: YES` usato per la gestione specifica dello spam, quindi viene recapitato come gli altri messaggi. In alternativa, l'opzione *Aggiungi un prefisso ai messaggi spam* rende visibile il flag di spam sull'oggetto del messaggio, anteponendo la stringa data all'intestazione `Subject`.
3. Se il punteggio di spam è sopra *Deny message spam threshold* Il messaggio è **rejected**.

I filtri statistici, chiamati *bayesiani*[17], sono regole speciali che evolvono e adattano rapidamente l'esito dell'analisi dei messaggi marcandoli come **spam** o **ham**.

I filtri statistici possono quindi essere addestrati con qualsiasi client IMAP semplicemente spostando un messaggio dentro e fuori da *Junk folder*. Come prerequisito, la cartella Junk deve essere abilitata dalla pagina *Email* > *Mailboxes* selezionando l'opzione *Move to «Junk» folder»*.

- *Spostando un messaggio dentro la cartella «junkmail»*, i filtri apprendono che il messaggio è spam e assegneranno un punteggio più alto ad altri messaggi simili.
- Al contrario, *spostando un messaggio fuori di «junkmail»*, i filtri apprendono che è *ham*: a messaggi simili sarà assegnato un punteggio più basso.

Per impostazione predefinita, tutti gli utenti possono addestrare i filtri utilizzando questa tecnica. Se esiste un gruppo chiamato `spamtrainers`, solo gli utenti di questo gruppo potranno addestrare i filtri.

L'allenamento dei filtri bayesiani si riflette su tutti gli utenti del sistema, non solo sull'utente che ha contrassegnato un'e-mail come spam o ham.

E" importante capire come funzionino i test Bayesiani:

[15] SPAM https://it.wikipedia.org/wiki/Spam

[16] Il greylisting è un metodo per proteggere gli utenti e-mail dallo spam. Un agente di trasferimento posta (MTA) che utilizza il greylisting «temporarily reject» qualsiasi e-mail da un mittente che non riconosce –Wikipedia

[17] Filtro bayesiano https://it.wikipedia.org/wiki/Filtro_bayesiano

- Non contrassegnano i messaggi come spam se questi contengono un argomento specifico od uno specifico indirizzo mittente. Si occupano di identificare le caratteristiche specifiche del messaggio.
- Un messaggio può essere contrassegnato solo una volta. Se lo stesso messaggio viene contrassegnato più volte, non avrà alcun effetto in quanto i test dinamici sono già stati addestrati da quel messaggio.
- I test Bayesiani **non sono attivi fino a quando non hanno ricevuto informazioni sufficienti. Queste prevedono un minimo di 200 mail di spam e 200 mail di ham (falsi positivi).**

Nota: È buona norma controllare costantemente la propria «junkmail» per non correre il rischio di perdere messaggi riconosciuti erroneamente come spam.

Se il sistema fallisce nel riconoscere lo spam anche dopo alcuni tentativi di allenamento, la *whitelist* e la *blacklist* possono venire in aiuto. Queste sono liste di indirizzi di posta elettronica che vengono o sempre ammessi o sempre rifiutati a spedire o ricevere un messaggio.

La sezione *Regole di accesso per indirizzi email* consente la creazione di tre tipi di regole:

- *Blocca da*: tutti i messaggi provenienti dal mittente indicato vengono sempre bloccati
- *Accetta da*: tutti i messaggi provenienti dal mittente indicato vengono sempre accettati
- *Accetta a*: tutti i messaggi destinati all'indirizzo indicato vengono sempre accettati

Benché sconsigliato, è possibile creare regole "Accetta'o "Blocca" anche per un intero dominio di posta: per farlo è sufficiente specificare solo il dominio nella regola (es: nethserver.org).

Avvertimento: **Anti-virus checks are disabled** too, in case *whitelist* settings.

Interfaccia web di Rspamd

Il modulo antispam è implementato da Rspamd[4] che è corredato della sua interfaccia web di amministrazione, disponibile all'URL

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

Per maggiori informazioni su Rspamd, fare riferimento alla sezione *Rspamd*.

Quarantena (beta)

NethServer esegue la scansione di tutti i messaggi di posta elettronica in arrivo prima che vengano recapitati alla casella postale dell'utente. I messaggi identificati come spam verranno inviati a una casella di posta utente specifica. Lo scopo di questa funzione è di verificare l'e-mail prima di eliminarla. E" possibile inviare una notifica e-mail anche al postmaster (alias di root) per ogni e-mail in quarantena abilitando una opzione dedicata.

Nota: È possibile accedere ai messaggi in quarantena tramite web mail o con un account IMAP

Avvertimento: La cassetta postale utilizzata per la quarantena deve essere in grado di accettare lo spam. Dovrebbe essere una casella di posta condivisa locale o una casella di posta dell'utente. Se si utilizza un account esterno, assicurarsi che l'account esista sul server remoto. Sincerarsi che la casella di quarantena sia stata creata solo per questo scopo specifico, altrimenti la cassetta postale sarà sovraccaricata di spam indesiderato.

La quarantena è fornita da un modulo opzionale chiamato‘‘nethserver-mail-quarantine‘‘. Una volta installato dal *Software center* sarà necessario impostare manualmente le proprietà del suo database.

Le proprietà sono disponibili sotto la chiave `rspamd` (database di configurazione):

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

- `QuarantineAccount`: L'utente o la casella di posta condivisa in cui inviare tutti i messaggi di spam (il controllo dello spam è disabilitato automaticamente su questo account). Va creato manualmente. È possibile utilizzare una casella di posta esterna, in tal caso accertarsi di disabilitare il controllo dello spam sul server remoto
- `QuarantineStatus`: abilita la quarantena, lo spam non viene più respinto. I valori ammessi sono enabled/disabled. L'impostazione predefinita è disabled
- `SpamNotificationStatus`: Abilita la notifica via email quando la posta elettronica viene messa in quarantena. I valori ammessi sono enabled/disabled. L'impostazione predefinita è disabled

Ad esempio, i seguenti comandi abilitano la quarantena e la notifica a root:

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

4.2.7 Configurazione client

NethServer supporta client per la posta elettronica aderenti agli standard che utilizzano le seguenti porte IANA:

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

L'autenticazione richiede la cifratura in modalità STARTTLS e supporta le seguenti varianti:

- LOGIN
- PLAIN
- GSSAPI (solo se NethServer è collegato con Samba/Microsoft Active Directory)

Inoltre le seguenti porte SSL sono disponibili per software datato che ancora non supporta STARTTLS:

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

Avvertimento: La porta SMTP standard 25 è riservata ai trasferimenti di posta tra server MTA. I client di posta (MUA) devono utilizzare la porta submission per l'invio.

4.2.8 Politiche SMTP di invio speciali

La configurazione predefinita di NethServer richiede che tutti i client utilizzino la porta submission (587) con cifratura e autenticazione abilitate per inviare messaggi attraverso il server SMTP.

Per semplificare la configurazione di ambienti preesistenti, la pagina *Email* > *Accesso SMTP* consente di specificare delle eccezioni ai criteri di accesso SMTP di default.

Avvertimento: Non modificare i criteri di accesso di default in nuove installazioni!

Per esempio, ci sono alcuni dispositivi (stampanti, scanner, . . .) che non supportano l'autenticazione SMTP, la cifratura o l'uso di porte personalizzate. Questi possono essere abilitati all'invio di messaggi email elencando il loro indirizzo IP nell'area di testo *Consenti relay dai seguenti indirizzi IP*.

Avvertimento: Gli indirizzi IP elencati sono esclusi da tutti i controlli di filtraggio della posta: utilizzare questa funzione solo come ultima possibile risorsa

Sotto *Opzioni avanzate* si trovano inoltre

- L'opzione *Consenti relay dalle reti fidate*, che abilita la spedizione di messaggi da qualsiasi client connesso dalle reti fidate.
- L'opzione *Abilita autenticazione sulla porta 25*, che consente l'autenticazione dei client SMTP e l'invio (relay) di messaggi anche sulla porta 25.

Corrispondenza mittente/login

Per impostazione predefinita, un client SMTP autenticato non ha particolari restrizioni sull'impostazione dell'indirizzo del mittente SMTP.

Per evitare l'uso non autorizzato degli indirizzi e-mail e lo spoofing dell'indirizzo del mittente, è possibile abilitare l'opzione *Forza corrispondenza mittente/login*, disponibile nel nuovo Server Manager, sotto *Email* > *Relay* > *Configurazione* > *Dettagli*.

Se abilitata, solo gli indirizzi associati al login SMTP corrente sono consentiti.

Relay host multipli

Il nuovo Server Manager consente di specificare il percorso di un messaggio di posta elettronica, inviandolo tramite un host di inoltro esterno, con specifiche porte, autenticazione e impostazioni TLS.

Creare una descrizione dell'host di inoltro sotto *Email* > *Relay* > *Crea relay host*.

L'host di inoltro è identificato dall'indirizzo del mittente SMTP. È possibile abbinare l'indirizzo completo del mittente o solo il suo dominio.

4.2.9 HELO personalizzato

Il primo passo di una sessione SMTP è lo scambio del comando *HELO* (o *EHLO*). Tale comando richiede un parametro obbligatorio che l'RFC 1123 definisce come il nome di dominio principale e valido del server.

NethServer ed altri server di posta, nel tentativo di ridurre lo spam, non accettano HELO con domini non registrati nel DNS pubblico.

Quando comunica con un altro server di posta, NethServer utilizza il valore del dominio principale (FQDN) come parametro del comando HELO. Se questo non è registrato nel DNS pubblico, l'HELO può essere corretto impostando una *prop* speciale. Per esempio, assumendo che `myhelo.example.com` sia il record registrato nel DNS pubblico, digitare i seguenti comandi:

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

Tale configurazione è utilizzabile anche quando non si è proprio in possesso di un dominio registrato, in questo caso è possibile registrare gratuitamente un DNS dinamico, associarlo all'IP pubblico del server ed utilizzare questo dominio come parametro HeloHost del precedente comando.

4.2.10 Posta eliminata Outlook

A differenza della quasi totalità dei client IMAP, Outlook non sposta i messaggi eliminati nel cestino, ma si limita a marcarli «cancellati».

È possibile forzare lo spostamento di tali messaggi nel cestino con questi comandi:

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

Si consiglia quindi di modificare la configurazione di Outlook in modo che nasconda i messaggi eliminati dalla posta in arrivo. La funzione è disponibile nel menu delle opzioni di visualizzazione.

4.2.11 Log

Ogni operazione eseguita dal server di posta è trascritta nei seguenti file di log:

- `/var/log/maillog`: contiene tutte le operazioni di invio e consegna
- `/var/log/imap`: contiene tutte le azioni di login/logout alle caselle di posta

Un transazione registrata nel file `maillog` di solito coinvolge diversi componenti del server di posta. Ogni riga contiene rispettivamente:

- la data e l'ora
- il nome host
- il nome del componente e l'id del processo dell'istanza
- il testo che descrive l'operazione

La configurazione di NethServer utilizza Rspamd come milter. Esegue un proxy worker Rspamd in modalità «self-scan»[19].

La chiave per tracciare l'intera transazione SMTP, incluse le decisioni di Rspamd, è l'intestazione ID messaggio o il Postfix Queue ID (QID). Entrambi sono disponibili nel sorgente del messaggio. L'intestazione `Message-ID` è generata dal mittente, mentre il QID è assegnato dal MTA ricevente. Per esempio

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

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

Qui `A785B308622AB` e il QID, mentre `5afa242e.hP5p/mry+fTNNjms%no-reply@example.com` è il ID del messagio.

Entrambe le stringhe possono essere usate con il comando ‘‘ grep‘‘ per trovare righe di log rilevanti in ‘‘/var/log/maillog* ‘‘ (notare il «*» finale per cercare anche nei file di log archiviati). Per esempio

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

Resa

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

Riferimenti

4.3 Webmail

Roundcube è il client webmail predefinito. Le caratteristiche principali di Roundcube sono:

- Semplice e veloce
- Rubrica integrata con LDAP
- Supporto per messaggi HTML
- Cartelle condivise
- Plugins

La webmail è raggiungibile ai seguenti indirizzi:

- http://_server_/webmail

- http://_server_/roundcubemail

Per esempio, dato un server con indirizzo IP *192.168.1.1* e nome *mail.miodominio.com*, gli indirizzi validi sono:

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

Nota: Se NethServer è attestato ad un account provider remoto Active Directory, un account utente AD aggiuntivo e dedicato è necessario al modulo per essere pienamente operativo! Fare riferimento alla sezione *Join ad un dominio Active Directory esistente*.

4.3.1 Plugins

Roundcube supporta molti plugin già inclusi nell'installazione.

I plugin abilitati di default sono:

- Manage sieve: gestione dei filtri sulla posta in arrivo
- Mark as junk: marca i messaggi come spam e li sposta nell'apposita cartella

Altri plugin consigliati:

- Notifica nuova mail
- Emoticon
- Supporto VCard

I plugin possono essere aggiunti o rimossi modificando la lista separata da virgole salvata nell'opzione `Plugins`. Per esempio, è possibile abilitare i plugin "mail notification", "mark as junk" e "manage sieve plugins" con il seguente comando:

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

Una lista dei plugin inclusi può essere trovata nella directory file: `/usr/share/roundcubemail/plugins`. Per recuperare la lista, eseguire:

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

4.3.2 Accesso

La configurazione di default prevede l'accesso HTTPS alla webmail da tutte le reti.

Se si desidera restringere l'accesso solo alla reti green e alle reti fidate, eseguire:

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

Se si desidera aprire l'accesso da tutte le reti:

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

4.3.3 Rimozione

Se si desidera rimuovere Roundcube, eseguire il seguente comando.

```
yum autoremove nethserver-roundcubemail
```

4.4 WebTop 5

WebTop è un groupware completo che implementa il protocollo ActiveSync.

L'indirizzo per accedere all'interfaccia web è: `https://<nome_server>/webtop`.

Nota: Se NethServer è attestato ad un account provider remoto Active Directory, un account utente AD aggiuntivo e dedicato è necessario al modulo per essere pienamente operativo! Fare riferimento alla sezione *Join ad un dominio Active Directory esistente*.

4.4.1 Autenticazione

Usa sempre il nome utente completo in formato `<user>@<domain>` per accedere all'applicazione web e via Active Sync.

Esempio

- Nome server: mymail.mightydomain.com
- Dominio di posta alternativo: baddomain.net
- Utente: goofy
- Login: goofy@mightydomain.com

Nota: Il protocollo Active Sync è supportato solo su dispositivi Android e iOS. Outlook non è supportato. La sincronizzazione della posta non è al momento supportata.

Utente admin

Dopo l'installazione, WebTop sarà accessibile utilizzando il suo utente amministrativo. L'utente amministrativo può cambiare le impostazioni globali ed effettuare login come un altro utente, ma non è un utente di sistema e non può accedere agli altri servizi come Mail, Calendario, ecc.

Le credenziali di default sono:

- Utente: admin
- Password: admin

La password del'utente admin deve essere cambiata dall'interfaccia di WebTop.

Avvertimento: E" fondamentale cambiare la password dell'amministratore subito dopo l'installazione!

E' possibile controllare la posta dell'utente admin di sistema usando questo login: admin@<dominio> dove `<dominio>` è il dominio del server che fa parte del FQDN.

Esempio

- Nome server: mymail.mightydomain.com
- Utente: admin
- Login: admin@mightydomain.com

Cambio della password di admin

Accedere a WebTop usando l'utente `admin`, quindi aprire le impostazioni utente facendo clic dal menu nell'angolo in alto a destra.

Selezionare *Impostazioni* quindi cliccare sul tasto guilabel:*Cambia password*.

Se si desidera reimpostare la password dell'amministratore da riga di comando, utilizzare i seguenti comandi:

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

Ricordarsi di sostituire `<newpassword>` con la nuova password che si vuole impostare, esempio:

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

4.4.2 Autenticazione a due fattori (2FA)

WebTop supporta l'autenticazione a due fattori. L'utente può scegliere tra:

- Google Authenticator: il codice verrà generato utilizzando l'app Google Authenticator (https://support.google.com/accounts/answer/1066447?co=GENIE.Platform%3DAndroid)
- Mail secondaria: il codice di accesso verrà inviato all'indirizzo di posta selezionato

Per abilitare 2FA:

- Fare clic sul pulsante del menu nell'angolo in alto a destra e selezionare *Impostazioni*
- Quini selezionare *Sicurezza (OTP)* e cliccare sul pulsante *Attiva*.

_static/webtop-2fa.png

4.4.3 Sincronizzazione con ActiveSync (EAS)

I dispositivi mobili possono essere sincronizzati utilizzando ActiveSync. ActiveSync può essere utilizzato solo per **contatti** e **calendari**.

Nota: Per sincronizzare le **e-mail** è necessario configurare un account IMAP.

Apple iOS

Accedere al iOS device, poi su Impostazioni e aggiungere un account Exchange seguendo la guida ufficiale: https://support.apple.com/en-us/HT201729

Compilare i campi richiesti con:

- **E-mail**: aggiungere indirizzo e-mail, es: pippo@nethserver.org
- **Server**: aggiungere il nome pubblico del server, es: mail.nethserver.org
- **Dominio**: lasciare vuoto
- **User name**: Inserire il nome utente completo, es: pippo@nethserver.org
- **Password**: inserire la password

Infine, *disabilitare* la sincronizzazione della Mail e creare un account IMAP: https://support.apple.com/en-us/HT201320

Nota: I device iOS richiedono un certificato SSL valido sul server. Vedi *Certificato del server*

Google Android

Accedere al device Android, navigare su Impostazioni, quindi selezionare *Aggiungi account* -> *Exchange* (o «Aziendale» per vecchie versioni).

Compilare i campi richiesti con:

- **User name**: Inserire il nome utente completo, es: pippo@nethserver.org
- **Password**: inserire la password

Selezionare *Configurazione manuale* e cambiare il nome del *Server* impostando il nome pubblico corretto. In fine, se si utilizza un certificato auto-firmato sul server, selezionare l'opzione *SSL/TLS (accetta ogni certificato)*.

Infine, *disabilitare* la sincronizzazione della Mail e creare un account IMAP

Nota: Su alcune versioni Android (es. Samsung), il nome utente e il dominio devono essere inseriti sulla stessa riga. In questo caso, lasciare vuoto il campo prima del carattere backslash () ed inserire il nome utente nel seguente formato: ‘‘ pippo@nethserver.org‘‘

Calendari e Rubriche multiple

Calendari e rubriche condivise con l'utente possono essere sincronizzati utilizzando il protocollo ActiveSync.

Le risorse condivise sono visualizzate con il nome e la categoria del proprietario (il numero tra parentesi quadre è l'ID interno). Gli eventi privati non vengono sincronizzati.

I device mobili basati su Apple iOS supportano integralmente le cartelle/categorie per calendario, contatti e attività (chiamati promemoria), inclusi i colori originali.

I dispositivi mobili basati su Android supportano solo calendari e contatti (le attività non sono supportate), ma utilizzando l'applicazione Google Calendar tutti gli elementi avranno lo stesso colore.

Installando e utilizzando l'applicazione CloudCal è possibile modificare i colori associati ad ogni calendario, inclusi quelli condivisi.

Sui dispositivi Android, i contatti delle rubriche condivise vengono uniti a quelli della rubrica personale e visualizzati in un'unica vista. I contatti possono essere modificati e le modifiche verranno recepite dalla sorgente originale.

Nota: Per ricevere i dati tramite EAS sui dispositivi mobili, è necessario verificare che le risorse condivise (Calendari e Contatti) abbiano la sincronizzazione abilitata (completa o di sola lettura):

_static/webtop-multiple_sync.png

È possibile abilitare o disabilitare la sincronizzazione per ogni risorsa condivisa (calendari e contatti). L'utente può personalizzare ogni risorsa condividendo con lui decidendo il tipo di sincronizzazione.

Per farlo, basta fare clic con il pulsante destro del mouse sulla risorsa condivisa → Personalizza → Sincronizza dispositivi:

_static/webtop-sync_shared_eas.png

L'impostazione predefinita è «Disattiva».

4.4.4 Sincronizzazione con CalDAV e CardDAV

Calendari e rubriche possono essere sincronizzati anche attraverso i protocolli CalDAV e CardDAV.

Per sincronizzare un calendario, copiare il suo link `URL` cliccando con il tasto destro sul calendario e selezionando *Link a questo calendario*, quindi usarlo per configurare il client di terze parti.

Per sincronizzare una rubrica, copiare il suo link URL cliccando con il tasto destro sulla rubrica e selezionando *Link a questa rubrica*, quindi usarlo per configurare il client di terze parti.

Per l'autenticazione, fornire le credenziali nel seguente formato:

- **Nome utente**: inserire il nome utente completo (es. *pippo@nethserver.org*)
- **Password**: inserire la password

Alcuni client di terze parti consentono di semplificare la configurazione tramite la funzione di *autodiscovery* che rileva automaticamente le risorse sincronizzabili, come nel caso dei client di dispositivi mobili (ad esempio dispositivi Android o iOS).

Nota: Se si utilizzano client che non supportano l'autodiscovery, è necessario utilizzare l'URL completo: `https://<server_name>/webtop-dav/server.php`

Se si utilizzano client che supportano l'autodiscovery, utilizzare l'URL: `https://<server_name>`

Google Android

Un buon client di terze parti Android gratuito è Opensync.

- installare dal market l'app suggerita;
- aggiungere un nuovo account cliccando sul tasto + e selezionare *Login with URL and username*;
- inserire l'URL (`https://<server_name>`), il nome utente completo (es. *pippo@nethserver.org*) e la password;
- cliccare sul nuovo profilo e selezionare le risorse che si vogliono sincronizzare.

Apple iOS

Il supporto CalDAV/CardDAV è integrato su iOS, quindi per configurarlo:

- spostarsi su Impostazioni -> Account e password -> Aggiungi account;
- selezionare *Altro* -> Aggiungere un account *CalDAV* o :guilabel: *CardDAV*;
- inserire il nome del server (ad esempio *server.nethserver.org*), nome utente completo (ad esempio *pippo@nethserver.org*) e password.

Per impostazione predefinita, l'URL di sincronizzazione utilizza il nome principale del server (FQDN), se fosse necessario modificarlo:

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

Client per desktop

Thunderbird

Per utilizzare CalDAV e CardDAV su Thunderbird sono necessari degli add-on di terze parti come *Cardbook* (per i contatti) e *Lightning* (per i calendari).

- L'add-on *Cardbook* funziona bene, il setup è semplice e supporta l'autodiscovery.

- Il componente aggiuntivo *Lightning* non supporta l'autodiscovery: qualsiasi calendario deve essere aggiunto manualmente.

Outlook

- Il client open source *Outlook CalDav Synchronizer* funziona bene, e supporta sia CardDAV che CalDAV.

Avvertimento: Webtop è concepito come **groupware clientless**: tutte le sue funzionalità sono unicamente disponibili **tramite l'interfaccia web**!

L'utilizzo di CalDAV/CardDAV tramite client di terze parti **non può essere considerato un'alternativa di interfaccia Web**.

4.4.5 Condividere le cartelle e-mail o l'intero account

È possibile condividere una singola cartella o l'intero account con tutte le sottocartelle incluse. Selezionare la cartella da condividere -> tasto destro -> «Gestisci condivisione»:

- selezionare l'utente a cui condividere la risorsa (1).
- selezionare se si vuole condividere anche l'identità con l'utente e se forzare la propria firma (2).
- scegliere il livello di permessi associati a questa condivisione (3).
- se è necessario modificare i livelli di autorizzazione in modo più granulare, selezionare «Avanzate» (4).
- infine, scegliere se applicare la condivisione solo alla cartella da cui si è iniziato, o solo al ramo di sottocartelle o all'intero account (5).

Nota: Se si seleziona anche «Forza firma», quando viene utilizzata questa identità, verrà automaticamente inserita la firma dell'utente da cui è stata ricevuta la posta condivisa.

In questo caso, tuttavia, è necessario che la firma personalizzata dell'Utente da cui proviene sia stata associata all'indirizzo e-mail e non all'Utente.

4.4.6 Condivisione di calendari e rubriche

Condivisione Calendario

E" possibile condividere ogni calendario personale individualmente. Selezionare il calendario da condividere -> tasto destro -> «Condivisione e permessi»:

Selezionare l'utente destinatario della condivisione (o gruppo) e attivare le autorizzazioni sia per la cartella che per i singoli elementi:

Condivisione Rubrica

Allo stesso modo, puoi sempre condividere i tuoi contatti selezionando la directory che vuoi condividere -> tasto destro -> «Condivisione e permessi». Selezionare l'utente destinatario della condivisione (o gruppo) e abilitare le autorizzazioni sia per la cartella che per i singoli elementi.

4.4.7 Etichette sulle Mail

E" possibile etichettare ogni messaggio con diverse etichette colorate. Basta selezionare un messaggio, fare clic con il tasto destro e selezionare: guilabel: *Etichetta*.

Puoi modificare i tag esistenti o aggiungerne di nuovi selezionando *Gestisci etichette*.

Le etichette possono essere utilizzate per filtrare i messaggi utilizzando la barra superiore del filtro.

4.4.8 Anteprima mail sulla riga del messaggio

Per impostazione predefinita, nella pagina della posta elettronica verrà visualizzata un'anteprima del contenuto degli ultimi messaggi ricevuti.

Questa funzione può essere abilitata o disabilitata dal menù *Impostazioni* -> *Posta Elettronica*, la casella di controllo è denominata *Mostra anteprima sulla riga del messaggio*.

4.4.9 Archiviazione mail

L'archiviazione è utile per mantenere organizzata la cartella della posta in arrivo spostando manualmente i messaggi.

Nota: Archivio mail non è un backup

Il sistema crea automaticamente una nuova cartella speciale di archivi

Se la cartella *Archivi* non viene visualizzata immediatamente al momento dell'accesso, verrà visualizzata alla prima archiviazione.

Esistono tre criteri di archiviazione in *Impostazioni -> Posta -> Archiviazione*

- **Cartella singola** una cartella principale per tutte l'email archiviate
- **Per anno** un alberatura per ogni anno
- **Per anno/mese** un alberatura per ogni anno e mese

Per mantenere la struttura originale delle cartelle è possibile attivare *Mantieni struttura cartelle*

L'operazione di archiviazione è accessibile dal menu contestuale (tasto destro). Clicca su :guilabel: *Archivia*

Il sistema elaborerà l'archiviazione in base alle ultime impostazioni scelte.

4.4.10 Sottoscrizione di cartelle IMAP

Su WebTop, per impostazione predefinita, tutte le cartelle IMAP sul server vengono automaticamente sottoscritte e sono quindi visibili dal primo accesso.

Se si vuole nascondere dalla vista alcune cartelle, che equivale a rimuovere la sottoscrizione, è possibile farlo semplicemente cliccando con il tasto destro del mouse sulla cartella per nasconderla e selezionare dal menu interattivo la voce «Nascondi dall'elenco».

Ad esempio, se si desidera nascondere la sottocartella «cartella1» da questo elenco, è sufficiente fare clic con il pulsante destro del mouse su di essa e selezionare «Nascondi dall'elenco»:

È possibile gestire la visibilità delle cartelle nascoste attraverso la funzionalità «Gestisci visibilità»:

Ad esempio, se si desidera ripristinare la sottoscrizione della «cartella1» appena nascosta, basta selezionarla dall'elenco delle cartelle nascoste e fare clic sull'icona a sinistra:

4.4.11 Esportazione eventi (CSV)

Per esportare gli eventi dei calendari nel formato CSV (Comma Separated Value), fare clic sull'icona nell'angolo in alto a destra.

Infine, seleziona un intervallo di tempo e clicca su: guilabel: *Avanti* per esportare in un file CSV.

4.4.12 Integrazione con Nextcloud

Nota: Prima di procedere, verificare che il modulo «Nextcloud» sia stato installato da: guilabel:*Software Center*

Per impostazione predefinita, l'integrazione con Nextcloud è disabilitata per tutti gli utenti. Per abilitarla, utilizzare il pannello di amministrazione a cui è possibile accedere utilizzando la password dell'amministratore di Webtop

Ad esempio, se si desidera attivare il servizio per tutti gli utenti di WebTop, procedere come segue:

1. accedi al pannello di amministrazione e seleziona «Gruppi»:

   
   _static/webtop-admin_panel_groups.png

2. modificare le proprietà del gruppo «utenti» facendo doppio clic e selezionare il pulsante relativo alle autorizzazioni:

   
   _static/webtop-admin_panel_permission.png

3. aggiungere alle autorizzazioni già presenti quelle relative sia alla risorsa `STORE_CLOUD` che a `STORE_OTHER` selezionando le voci come illustrate qui sotto:

   
   _static/webtop-admin_panel_nextcloud_auth_1.png

   
   _static/webtop-admin_panel_nextcloud_auth_2.png

   in modo da ottenere questo:

   
   _static/webtop-admin_panel_nextcloud_auth_3.png

4. salvare e chiudere.

A questo punto da qualsiasi utente sarà possibile inserire la risorsa Nextcloud (locale o remota) nel proprio Cloud personale.

Per farlo basterà selezionare il pulsante relativo al Cloud e aggiungere una nuova risorsa **«Nextcloud»** cliccando con il tasto destro su **«My resources»** e successivamente **«Add resource»** in questo modo:

Si aprirà una procedura guidata precompilata:

Nota: Ricordarsi di compilare i campi Nome utente e Password relativi all'accesso alla risorsa Nextcloud, altrimenti non sarà possibile utilizzare il link pubblico ai file condivisi

Procedere con il tasto Next fino a completamento del Wizard.

4.4.13 Usa il Cloud personale per inviare e ricevere documenti

Il modulo Cloud ti consente di inviare e ricevere documenti tramite link web.

Nota: Il server deve essere raggiungibile sulla porta HTTP 80

Come creare un link per inviare un documento

Per creare un link, selezionare il pulsante in alto a destra:

Seguire la procedura guidata per generare il collegamento, utilizzare il campo *date* per impostare la scadenza.

è possibile impostare una *password* per proteggerlo:

Il link verrà generato e verrà inserito nella nuova mail:

Il download del file genera una notifica al mittente:

Richiesta di un documento

Per creare la richiesta, inserire l'oggetto della e-mail quindi selezionare il pulsante in alto a destra:

Seguire il wizard. È possibile impostare sia una data di scadenza che una password. Il link verrà automaticamente inserito nel messaggio:

Una mail di richiesta verrà inviata per caricare il documento sul Cloud:

Il mittente riceverà una notifica per ogni file che verrà caricato:

Per scaricare i file ricevuti accedere al *Cloud* -> *Uploads* -> *Cartella* con data e nome:

4.4.14 Integrazione chat

Per default il servizio di webchat è disabilitato per tutti gli utenti.

Per abilitare l'integrazione con il server chat:

1. Installare il modulo «Messaggistica istantanea» dal *Software Center*.
2. Accedere a WebTop con l'utente admin quindi abilitare l'autorizzazione per la chat:
   - Accedere al menu *Administration*, quindi scegliere *Domains* → *NethServer* → *Groups* → *Users* → *Authorizations*
   - *Add (+)* → *Services* → *com.sonicle.webtop.core (WebTop)* → *Resource* → *WEBCHAT* → *Action* → *ACCESS*
   - Cliccare *OK* quindi salvare ed uscire

4.4.15 Chiamate WebRTC audio e video con chat (Beta)

Avvertimento: Questa funzione è attualmente rilasciata in Beta. Quando verrà rilasciata la versione finale, è probabile che le configurazioni precedentemente adottate vengano ripristinate a default.

La configurazione è disponibile unicamente dal pannello di amministrazione di Webtop. Le impostazioni da inserire sono documentate all'interno della sezione impostazioni webrtc. Oltre alle impostazioni WebRTC è anche necessario fornire l'URL pubblico **XMPP BOSH** come illustrato all'interno delle impostazioni xmpp.

Dall'interfaccia web accedendo al pannello di amministrazione -> *Proprietà (sistema)* -> *Aggiungi* -> selezionare *com.sonicle.webtop.core (WebTop)* ed inserire i dati nei campi *Chiave* e *Valore* in base alla chiave da configurare:

`webrtc.ice.servers` : definisce l'elenco dei server ICE come array JSON

`xmpp.bosh.url` : specifica l'URL XMPP a cui è possibile accedere tramite il protocollo BOSH

Per la chiave `webrtc.ice.servers` inserire come «Valore» il contenuto in formato json che mostra i valori di queste variabili:

`url` : URL ice server

`username` : nome utente server (opzionale)

`credential` : password server (opzionale)

Ad esempio:

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

Nella chiave `xmpp.bosh.url` valorizzare il campo «Value» con questo tipo di URL: `https://<public_server_name>/http-bind`

Con queste configurazioni, ogni utente autorizzato ad utilizzare il servizio **WEBCHAT** può effettuare chiamate audio e video con altri utenti disponibili sullo stesso server di chat tramite i pulsanti disponibili nella finestra di chat.

Nota: Se i pulsanti sono disattivati, i requisiti per l'attivazione della chiamata non sono soddisfatti. Ad esempio: l'URL XMPP BOSH od il server ICE potrebbero essere non raggiungibili.

4.4.16 Invio SMS dai contatti

È possibile inviare messaggi SMS a un contatto che ha il numero di cellulare nella rubrica. Per attivare l'invio di SMS, è necessario scegliere uno dei due provider supportati: SMSHOSTING o TWILIO.

Una volta registrati al servizio del provider scelto, recuperare le chiavi API (AUTH_KEY e AUTH_SECRET) da inserire nel db di configurazione di WebTop. Le impostazioni da configurare sono quelle indicate qui .

È possibile farlo dall'interfaccia web accedendo al pannello di amministrazione -> :guilabel: *Proprietà (sistema)* -> :guilabel: *Aggiungi* -> selezionando *com.sonicle.webtop.core (WebTop)* ed inserendo i dati nei campi *Chiave* e *Valore* in base alla chiave da configurare:

`sms.provider` = smshosting o twilio

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

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

`sms.sender` = (default opzionale)

La chiave `sms.sender` è facoltativa e viene utilizzata per specificare il mittente predefinito quando si invia un SMS. È possibile indicare un numero (massimo 16 caratteri) od una stringa di testo (max 11 caratteri).

Nota: Ogni utente ha sempre la possibilità di sovrascrivere il mittente personalizzandolo come desiderato attraverso il suo pannello delle impostazioni: *WebTop -> Centralino VOIP e SMS -> Servizio SMS Hosting configurato -> Mittente predefinito*

Per inviare un SMS dalla rubrica, fare clic con il tasto destro del mouse su un contatto con il campo mobile valorizzato *-> Invia SMS*

4.4.17 Pulsanti di collegamento personalizzati

Per configurare i pulsanti accedere al pannello di amministrazione di WebTop e selezionare *-> Domini -> NethServer -> Barra di avvio* :

Per ciascun pulsante, inserisci questi tre valori

`Nome` : testo descrittivo che appare con il mouseover

‘‘ URL link‘‘: URL aperto in un nuovo browser

`Icona URL` : icona immagine URL (per evitare problemi di ridimensionamento, usare immagini vettoriali)

Avvertimento: L’URL da cui recuperare l’immagine vettoriale dell’icona deve essere sempre raggiungibile pubblicamente dal browser con cui ci si connette.

Se non è possibile recuperare un link Internet per immagine dell’icona, è possibile copiare l’immagine localmente sul server in due modi diversi:

1. copiare il file (ad esempio `icon.svg`) direttamente nella directory `/var/www/html/` del server e usare questo tipo di URL per il campo “URL Icona”: `https://<public_name_server>/<icon.svg>`
2. caricare il file icona sul cloud pubblico di WebTop (dove le immagini vengono caricate per le mailcards) tramite il pannello di amministrazione ->: guilabel: *Cloud* ->: guilabel:‘ Immagini pub.‘ e inserire un URL di questo tipo nel campo “URL Icona”: `https://<public_name_server>/webtop/resources/156c0407/images/<icon.svg>`

Nota: I pulsanti di collegamento personalizzati configurati verranno mostrati a tutti gli utenti al successivo accesso.

4.4.18 Notifiche del browser

Con WebTop è stata introdotta la modalità di notifica desktop integrata con il browser.

Per attivarla, accedere semplicemente alle impostazioni generali dell’utente:

_static/webtop-desktop_notifications.png

È possibile abilitare la notifica sul desktop in due modalità:

- **Sempre**: le notifiche verranno sempre mostrate, anche con il browser aperto
- **Auto (solo in background)**: le notifiche verranno visualizzate solo quando il browser è in background

Una volta selezionata la modalità, verrà visualizzata una richiesta di autorizzazione del browser in alto a sinistra:

_static/webtop-chrome_notifications.png

Se è necessario abilitare questo consenso più tardi su un altro browser, basta fare clic sul pulsante appropriato:

_static/webtop-button_desktop_notifications.png

4.4.19 Gestione firme utenti e di dominio

Una delle caratteristiche principali della gestione delle firme su WebTop, è l'opportunità di integrare immagini o campi personalizzati profilati per utente.

Per utilizzare le immagini è necessario caricarle sul cloud pubblico attraverso l'utente admin di WebTop in questo modo:

_static/webtop-public_images.png

Per caricare una immagine è possibile usare il tasto *Carica* che si trova in basso oppure semplicemente tramite un drag & drop.

Nota: si ricorda che le immagini pubbliche inserite nella firma vengono in realtà collegate con un link pubblico. Per risultare visibili ai destinatari delle mail è necessario che il server sia raggiungibile da remoto sulla porta 80 (http) e che il suo nome FQDN sia risolvibile pubblicamente.

In alternativa, è possibile configurare un'impostazione globale per trasformare automaticamente le immagini in allegati inline anziché in collegamenti Internet pubblici

È possibile farlo dall'interfaccia web accedendo al pannello di amministrazione -> *Proprietà (sistema)* -> *Aggiungi* -> selezionando *com.sonicle.webtop.mail (Mail)* ed inserendo i dati nei campi *Chiave* e *Valore* in base alla chiave da configurare:

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

Per cambiare la propria firma, ogni utente può accedere a *Impostazioni* -> *Posta Elettronica* -> *Composizione* -> *Modifica Firma utente*:

L'immagine pubblica appena caricata sarà possibile richiamarla all'interno dell'editor HTML della firma con questo pulsante:

Nota: La firma personale può essere associata all'utente o alla sua email: associandola per email sarà anche possibile condividere la firma ad altri utenti con cui si condivide l'identità

Accedendo alle impostazioni dal pannello di amministrazione di WebTop è inoltre possibile impostare una mailcard generale per il dominio che verrà impostata automaticamente per tutti gli utenti che non hanno configurato la propria mailcard personale:

Inoltre, sarà anche possibile modificare le informazioni personali:

che potranno essere utilizzate all'interno dei campi parametrizzati all'interno dell'editor della firma di dominio:

_static/webtop-domain_mailcard.png

In questo modo è possibile creare un'unica firma che verrà automaticamente personalizzata per ogni utente che non utilizzi la propria firma.

4.4.20 Configurare più firme per un singolo utente

È possibile configurare più firme HTML per ogni singolo utente.

Accedere a *Impostazioni* -> *Posta* -> *Identità* e creare identità multiple:

_static/webtop-sig_sig1.png

Per modificare ogni singola firma selezionare *Impostazioni* -> *Posta Elettronica* -> *Identità*, quindi selezionare ogni singola firma e cliccare sul pulsante *modifica firma*

_static/webtop-sig_sig2.png

_static/webtop-sig_sig3.png

Al termine, chiudere la finestra e fai clic su SÌ:

_static/webtop-sig_sig4.png

per utilizzare più firme, creare una nuova e-mail e scegliere la firma:

_static/webtop-sig_sig5.png

4.4.21 Gestisci identità

In *Impostazioni* → *Posta Elettronica* → *Identità* cliccare su *Aggiungi* quindi compilare i campi

È possibile associare la nuova identità a una cartella del proprio account o di un account condiviso

Account Locale

Account condiviso

In alternativa le mail inviate finiranno sempre nella cartella «Posta inviata» dell'account personale.

4.4.22 Sottoscrizione di risorse remote

WebTop supporta la sottoscrizione di calendari e contatti remoti utilizzando CardDAV, CalDav e iCal.

Calendari remoti

E' possibile aggiungere e sincronizzare un Calendario Internet. Per farlo basta cliccare il tasto dx su calendari personali *Aggiungi calendario internet*. Sono supportate due tipologie di calendari remoti: Webcal (formato ics) e CalDAV.

Nota: La sincronizzazione dei calendari Webcal (ics) avviene sempre scaricando ogni evento sulla risorsa remota ogni volta, mentre solo le differenze sono sincronizzate con la modalità CalDAV

Esempio di calendario remoto Google Cal (solo Webcal - ICS)

1) Prelevare dal proprio calendario Google il link ICS (formato iCal) di accesso pubblico: *Opzioni del calendario -> Impostazioni e condivisione -> Indirizzo segreto in formato iCal*
2) Su WebTop, aggiungere un calendario Internet di tipo Webcal ed incollare l'URL copiato senza inserire le credenziali di autenticazione nel passo 1 del wizard.

3) Il wizard effettuerà la connessione al calendario, dando la possibilità di modificarne il nome e il colore, quindi effettuerà la prima sincronizzazione.

Nota: La prima sincronizzazione potrebbe fallire a causa delle impostazioni di sicurezza di Google. Se si riceve una notifica che avvisa del tentativo di accesso alle proprie risorse è necessario consentirne l'utilizzo confermando che si tratta di un tentativo legittimo.

Rubrica remota

Esempio di rubrica remota CarDAV Google

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

2) Inserire le credenziali di autenticazione (come username usare l'indirizzo completo di gmail):

3) La procedura guidata nei passaggi seguenti si collegherà alla rubrica, dando la possibilità di cambiare il nome e il colore, quindi eseguirà la prima sincronizzazione.

Nota: Per riuscire a completare la sincronizzazione è necessario abilitare sul proprio account Google, nelle impostazioni di sicurezza, l'uso di app considerate meno sicure (a questo link una guida su come fare: https://support.google.com/accounts/answer/6010255?hl=it).

La sincronizzazione delle risorse remote può essere eseguita manualmente o automaticamente.

Sincronizzazione automatica

Per la sincronizzazione automaticamente è possibile scegliere tra tre intervalli di tempo: 15, 30 e 60 minuti. La scelta dell'intervallo di tempo può essere effettuata nella fase di creazione o modificando successivamente le opzioni. Per farlo è sufficente un clic con il tasto destro sulla rubrica (o sul calendario), *Modifica categoria*, *Rubrica Internet* (o *Calendario Internet*):

Sincronizzazione manuale

Per aggiornare ad esempio una rubrica remota, fare clic su di essa con il tasto destro del mouse e selezionare la voce «Sincronizza»:

_static/webtop-sync_google.png

Per le rubriche di CardDav e per i calendari CalDAV remoti, è possibile selezionare se eseguire una sincronizzazione completa o solo per le modifiche. Per fare ciò, fare clic con il tasto destro sulla rubrica (o sul calendario), *Modifica categoria*:

_static/webtop-edit_sync_google.png

Selezionare la modalità desiderata accanto al pulsante di sincronizzazione:

_static/webtop-edit_sync_google2.png

4.4.23 Gestione impostazioni utente

La maggior parte delle impostazioni utente può essere gestita direttamente dall'utente stesso tramite il menu delle impostazioni. Le impostazioni bloccate richiedono privilegi di amministrazione.

L'amministratore può impersonare gli utenti, per verificare la correttezza e le funzionalità di un account, attraverso un login specifico:

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

Durante l'*impersonate* l'admin assume i privilegi dell'utente, potendo così di controllare esattamente ciò che l'utente può vedere. L'amministrazione completa delle impostazioni utente è disponibile direttamente nell'interfaccia di amministrazione, facendo clic con il pulsante destro del mouse su un utente: il menu delle impostazioni aprirà il pannello delle impostazioni utente completo, con tutte le opzioni sbloccate.

È anche possibile effettuare una modifica massiva del dominio di posta elettronica degli utenti selezionati: selezionare gli utenti (Clic + CTRL per selezione multipla) a cui si desidera applicare questa modifica, quindi fare clic con il pulsante destro del mouse su *Bulk update email domain*.

4.4.24 Impostazioni SMTP

La configurazione predefinita per l'invio di posta al server SMTP è anonima e senza crittografia sulla porta 587. È possibile abilitare l'invio autenticato in questo modo:

```
config setprop webtop SmtpAuth enabled
```

per abilitare anche la crittografia:

```
config setprop webtop SmtpStarttls enabled
```

Per applicare le nuove impostazioni, scatenare l'evento che riavvia anche l'applicazione:

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

4.4.25 Modifica del logo

Per modificare e personalizzare il logo iniziale visualizzato nella pagina di accesso di WebTop, è necessario caricare il file immagine personalizzato sulle immagini pubbliche dell'utente amministratore e rinominarlo con «login.png».

Procedere come segue:

1. accedere con l'utente admin di WebTop
2. selezionare il servizio cloud e le immagini pubbliche:

3. caricare l'immagine (tramite il pulsante Upload in basso a sinistra o semplicemente trascinando con un drag & drop)
4. rinominare l'immagine caricata in modo che il suo nome sia **«login.png»** (usare il tasto destro del mouse -> Rinomina):

5. il prossimo login mostrerà il nuovo logo sulla pagina di login

4.4.26 Modifica dell'URL pubblico

Per impostazione predefinita, l'URL pubblico di WebTop è configurato con il nome FQDN impostato nel server-manager.

Per cambiare URL da: `http://server.domain.local/webtop` a: `http://mail.publicdomain.com/webtop`

eseguire i seguenti comandi

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

4.4.27 Modifica il limite predefinito «Dimensione massima del file»

Esistono limiti configurati hard-coded relativi alla dimensione massima del file:

- Dimensione massima del file per upload di chat (default interno = 10 MB)
- Massima dimensione del file allegato al singolo messaggio di posta (predefinito interno = 10 MB)
- Dimensione massima del file per i caricamenti interni al cloud (default interno = 500 MB)
- Dimensione massima del file per i caricamenti pubblici (predefinito interno = 100 MB)

Per modificare questi valori predefiniti per tutti gli utenti, è possibile aggiungere le seguenti chiavi tramite l'interfaccia di amministrazione: :guilabel: *Proprietà (sistema)* -> *Aggiungi*

Dimensione massima del file per i caricamenti della chat

- Servizio: `com.sonicle.webtop.core`
- Chiave: `im.upload.maxfilesize`

Dimensione massima del file allegato per un singolo messaggio di posta

- Servizio: `com.sonicle.webtop.mail`
- Chiave: `attachment.maxfilesize`

Dimensione massima del file per i caricamenti interni al cloud

- Servizio: `com.sonicle.webtop.vfs`
- Chiave: `upload.private.maxfilesize`

Dimensione massima del file per i caricamenti pubblici su cloud

- Servizio: `com.sonicle.webtop.vfs`
- Chaive: `upload.public.maxfilesize`

Nota: Il valore deve essere espresso in Byte (Esempio 10MB = 10485760)

4.4.28 Importazione di contatti e calendari

WebTop supporta l'importazione di contatti e calendari da vari formati di file.

Contatti

Formato dei contatti supportati:

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

Per importare i contatti:

1. Fare clic con il tasto destro sulla rubrica di destinazione, quindi selezionare: *Importa contatti*

   

2. Selezionare il formato di importazione assicurandosi che i campi del file corrispondano a quelli disponibili su WebTop

   

Se stai importando una rubrica esportata da Outlook, assicurarsi di impostare: guilabel: *Qualificatore di testo* con questo valore `"`.

Calendari

Formato del calendario supportato: iCalendar (*.ics, *.ical, *.icalendar)

Per importare eventi:

1. Fare clic con il tasto destro sul calendario di destinazione, quindi selezionare *Importa eventi*

   

2. Selezionare il formato di importazione

   

3. Quindi scegliere se si desidera eliminare tutti gli eventi esistenti e importarne di nuovi o semplicemente aggiungere i dati importati agli eventi del calendario esistenti

4.4.29 Nascondi il destinatario suggerito automaticamente nelle ricerche

Per disabilitare il suggerimento di indirizzi salvati automaticamente, accedere al pannello di amministrazione ->: guilabel: *Proprietà (sistema)* ->: guilabel: *Aggiungi* -> selezionare: guilabel: *com.sonicle.webtop.core (WebTop)* e inserire i dati nei campi: guilabel: *Chiave* e: guilabel: *Valore* in base alla chiave da configurare:

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

4.4.30 Modificare l'oggetto di una mail e salvarlo

Per abilitare la modifica dell'oggetto nelle e-mail ricevute e inviate, accedere al pannello di amministrazione ->: guilabel: *Proprietà (sistema)* ->: guilabel: *Aggiungi* -> selezionare: guilabel: *com.sonicle.webtop.mail (Posta Elettronica)* e inserire i dati nei campi: guilabel: *Chiave* e: guilabel: *Valore* in base alla chiave da configurare:

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

4.4.31 Importazione da PST Outlook

E" possibile importare email, calendari e rubriche da un archivio PST di Outlook .

Prima di utilizzare lo script, è necessario installare il pacchetto *libpst*:

```
yum install libpst -y
```

Assicurarsi inoltre che la timezone di PHP corrisponda a quella del server:

```
config getprop php DateTimezone
```

La time zone di PHP può essere modificata utilizzando il comando seguente:

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

Mail

Script iniziale per l'importazione dei messaggi mail: `/usr/share/webtop/doc/pst2webtop.sh`

Per iniziare l'importazione, lanciare lo script specificando il file PST e l'utente di sistema:

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

Esempio:

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

Tutti i messaggi mail saranno importati. Contatti e calendari saranno salvati in un file temporaneo e lo script genererà a schermo gli ulteriori comandi da utilizzare per importare contatti e calendari.

Esempio:

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

...

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

Tutti i comandi saranno riportati anche nel file di log generato dallo script.

Contatti

Script importazione Contatti: `/usr/share/webtop/doc/pst2webtop_card.php`.

Lo script utilizzerà i file generati nella fase di importazione della posta:

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

Esempio

Ipotizziamo che lo script pst2webtop.sh abbia generato il seguente output a seguito dell'importazione delle mail:

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

Per importare nella Rubrica predefinita (WebTop) dell'utente *foo*:

```
/usr/share/webtop/doc/pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/
↪Contacts/contacts' WebTop
```

Calendari

Script importazione Calendari: `/usr/share/webtop/doc/pst2webtop_cal.php`

Lo script utilizzerà i file generati nella fase di importazione della posta:

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

Esempio

Ipotizziamo che lo script pst2webtop.sh abbia generato il seguente output a seguito dell'importazione delle mail:

```
Events Folder found: Personal folders/Calendar/calendar
 Import to webtop:
./pst2webtop_cal.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/Calendar/calendar'
↪<foldername>
```

Per importare gli eventi nel Calendario predefinito (WebTop) dell'utente *foo*:

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

Limitazioni note:

- verrà importata solamente la prima occorrenza di eventi ricorrenti
- I promemoria di Outlook verranno ignorati

Nota: Lo script importerà gli eventi utilizzando il fuso orario dall'utente WebTop, se configurato. Altrimenti verrà utilizzato il fuso orario del sistema.

4.4.32 Troubleshooting

Dopo l'accesso viene visualizzato un «mail account authentication error»

Se un intero account di posta è condiviso tra diversi utenti, è possibile raggiungere un limite di connessione Dovecot. Questo è l'errore visualizzato:

In `/var/log/imap` si rilevano messaggi come i seguenti:

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

Per elencare le connessioni IMAP attive per utente, eseguire:

```
doveadm who
```

Per risolvere il problema, basta aumentare il limite (es. 50 connessioni per ogni utente/IP):

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

Infine, eseguire il logout e di nuovo il login in WebTop.

Pagina vuota dopo il login

È possibile accedere a WebTop utilizzando l'utente amministratore di sistema (NethServer Administrator) utilizzando il nome di accesso completo, ad es .: *admin@nethserver.org'*.

Se l'accesso fallisce, soprattutto quando si aggiorna da WebTop 4, significa che l'utente admin non ha un indirizzo mail

Per risolvere il problema, eseguire il seguente comando:

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

Gli eventi sincronizzati mostrano una differenza di orario

Può capitare che gli eventi di calendario creati sui device mobili e sincronizzati tramite EAS vengano riportati sull'interfaccia con una differenza di orario di 1 o 2 ore.

Il problema è dovuto al Time Zone di PHP che può risultare disallineato rispetto a quello di sistema.

Con questo comando è possibile vedere l'attuale Time Zone impostato per il PHP:

```
config getprop php DateTimezone
```

Esempio di output:

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

Se il Time Zone non fosse quello desiderato (ad esempio Europe/Rome) è possibile correggere in questo modo:

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

Per mettere in produzione la modifica eseguire:

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

Elenco dei time zone supportati da PHP: http://php.net/manual/it/timezones.php

Eliminare gli indirizzi email suggeriti automaticamente

Quando si compila il destinatario di una mail, vengono suggeriti alcuni indirizzi email salvati automaticamente. Se è necessario eliminarne qualcuno perché è sbagliato, spostarsi con i tasti freccia finché non si seleziona quello che si vuole eliminare (senza fare clic su di esso), quindi eliminarlo con *Shift + Canc*

4.4.33 WebTop vs SOGo

WebTop e SOGo possono essere installati sulla stessa macchina, anche se è sconsigliato mantenere tale configurazione a lungo termine.

ActiveSync è abilitato per impostazione predefinita sia su SOGo che su WebTop, ma se entrambi i pacchetti sono installati, SOGo avrà la precedenza.

Per disabilitare ActiveSync su SOGo:

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

Per disabilitare ActiveSync su WebTop:

```
config setprop webtop ActiveSync disabled
signal-event nethserver-webtop5-update
```

Tutti i filtri di posta configurati da SOGo, devono essere ricreati manualmente all'interno dell'interfaccia di WebTop. La stessa cosa si applica se l'utente sta effettuando il passaggio inverso da WebTop a SOGo.

4.4.34 Integrazione Google

Gli utenti possono aggiungere i propri account Google Drive all'interno di WebTop. Prima di procedere, l'amministratore deve creare una coppia di credenziali di accesso API.

Google API

- Accedere a https://console.developers.google.com/project e creare un nuovo progetto
- Creare una nuova coppia di credenziali di tipo "OAuth 2.0 clientID" avendo cura di compilare la sezione "OAuth consent screen"
- Inserire la coppia di credenziali appena create (Client ID e Client Secret) nella configurazione di WebTop

È possibile farlo dall'interfaccia web accedendo al pannello di amministrazione -> :guilabel: *Proprietà (sistema)* -> :guilabel: *Aggiungi* -> selezionando *com.sonicle.webtop.core (WebTop)* ed inserendo i dati nei campi *Chiave* e *Valore* in base alla chiave da configurare:

`googledrive.clientid` = (Google API client_ID)

`googledrive.clientsecret` = (Google API client_secret)

4.5 Proxy POP3

Nota: Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *Proxy POP3* sono basate sul motore di filtraggio Rspamd. Le precedenti installazioni di NethServer verranno automaticamente aggiornate a Rspamd come descritto nella sezione *Aggiornamento Email a Rspamd*

Un utente della LAN potrebbe configurare il proprio client di posta al fine di collegarsi ad un server POP3 esterno, per scaricare i propri messaggi. La posta scaricata potrebbe però contenere virus che potrebbero infettare il computer eludendo ogni controllo da parte del server.

Il proxy POP3 intercetta le connessioni ai server esterni sulla porta 110, scansionando tutte le mail in entrata, in modo da bloccare i virus ed etichettare lo spam. Per i client di posta il processo è assolutamente trasparente: l'utente crederà di collegarsi direttamente al server POP3 del proprio provider, mentre il proxy intercetterà tutto il traffico effettuando la connessione al server esterno.

E' possibile attivare selettivamente i seguenti controlli:

- antivirus: i messaggi contenenti virus vengono rifiutati ed una mail di notifica è inviata al destinatario
- spam: i messaggi verranno marcati con gli opportuni punteggi antispam

4.5.1 POP3s

Il proxy può anche intercettare connessioni POP3s sulla porta 995. Il proxy stabilirà una connessione sicura al server esterno, ma lo scambio di dati con i client LAN avverrà in chiaro.

Nota: I client dovranno essere configurati per collegarsi alla porta 995 con la cifratura disattivata.

4.6 Connettore POP3

Nota: Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *Proxy POP3* sono basate sul motore di filtraggio Rspamd. Le precedenti installazioni di NethServer verranno automaticamente aggiornate a Rspamd come descritto nella sezione *Aggiornamento Email a Rspamd*

La pagina *Connettore POP3* permette di configurare un elenco di account di posta elettronica che il server scarica ad intervalli di tempo regolari, consegnando le email agli utenti locali.

Non è consigliabile utilizzare il connettore POP3 come metodo principale per la gestione della posta elettronica. Il recapito della posta può essere influenzato dallo spazio su disco e dai problemi di connettività del server del provider. Inoltre, il filtro antispam sarà meno efficace a causa della perdita delle informazioni contenute nell'envelope della mail originale.

Gli account POP3/IMAP sono configurabili dalla pagina *Connettore POP3* > *Indirizzi esterni*. Per ogni account possono essere specificati:

- l'indirizzo email (come identificativo univoco per l'account)
- il protocollo (IMAP/POP3/IMAP con SSL/POP3 con SSL)
- l'indirizzo del server remoto
- le credenziali dell'account
- l'utente locale a cui consegnare i messaggi
- se un messaggio vada eliminato dal server remoto dopo la consegna
- controlli antispam e antivirus

Nota: È consentito associare più account esterni ad uno locale. L'eliminazione di un account *non* cancellerà i messaggi già consegnati.

Completata la configurazione di un account, questo viene automaticamente controllato per rilevare la presenza di nuovi messaggi di posta.

L'implementazione è basata su *Getmail*[1]. Dopo aver scaricato i messaggi dal provider POP3/IMAP remoto, Getmail applica tutti i filtri attivati (spam e virus), quindi consegna il messaggio localmente. I messaggi vengono filtrati in base alle *regole configurate*.

Tutte le operazioni di download sono riportate nel file `/var/log/maillog`.

Avvertimento: Se un account scelto per la consegna venisse successivamente eliminato, la configurazione diventerebbe inconsistente. Se questo dovesse accadere la relativa configurazione esistente nella pagina *Connettore POP3* dovrà essere disabilitata o eliminata.

[1] Getmail è un programma per il download di email da remoto http://pyropus.ca/software/getmail/

Riferimenti

4.7 Chat

Il servizio di chat utilizza il protocollo standard Jabber/XMPP, supporta TLS sulla porte XMPP standard (5222 o 5223).

La principali funzionalità sono:

- messaggi fra gli utenti del sistema
- amministratori chat
- messaggi broadcast
- chat di gruppo
- messaggi offline
- trasferimenti file in LAN
- S2S
- Archiviazione dei messaggi

Tutti gli utenti di sistema possono accedere alla chat usando le proprie credenziali.

Nota: Se NethServer è attestato ad un account provider remoto Active Directory, un account utente AD aggiuntivo e dedicato è necessario al modulo per essere pienamente operativo! Fare riferimento alla sezione *Join ad un dominio Active Directory esistente*.

4.7.1 Server to server (S2S)

Il sistema XMPP è federato nativamente. Se S2S è abilitato, gli utenti con account su un server possono comunicare con gli utenti su server remoti. S2S consente ai server di comunicare tra loro, formando una rete IM globale «federata».

A tale scopo, il record DNS SRV deve essere configurato per il proprio dominio (https://wiki.xmpp.org/web/SRV_Records#XMPP_SRV_records) e il server deve disporre di un certificato SSL/TLS valido.

4.7.2 Client

I client Jabber sono disponibili per tutte le piattaforme desktop e mobile.

Fra i client più diffusi:

- Pidgin disponibile per Windows e Linux
- Adium per Mac OS X
- BeejibelIM per Android e iOS, o Xabber solo Android

Quando si configura il client, assicurarsi che sia abilitato TLS (o SSL). Inserire il nome utente e il dominio della macchina.

Se NethServer è anche il server DNS della rete, i client dovrebbero trovare automaticamente l'indirizzo del server attraverso speciali record DNS preconfigurati. In caso contrario, specificare l'indirizzo del server nelle opzioni avanzate.

Con le funzionalità TLS, server o client rigorosamente configurati potrebbero rifiutare la connessione con il server Ejabberd se nel certificato SSL/TLS non corrispondesse il nome di dominio. Inoltre, il certificato dovrebbe contenere due sottodomini `pubub.*` e `conference.*`. Un certificato con tali caratteristiche può essere generato gratuitamente con Let's Encrypt (vedi *Certificato del server*).

4.7.3 Amministratori

Tutti gli utenti all'interno del gruppo `jabberadmins` sono considerati amministratori del server di chat.

Gli amministratori possono:

- inviare messaggi broadcast
- controllare lo stato degli utenti collegati

Il gruppo `jabberadmins` è configurabile dalla pagina *Gruppi*.

4.7.4 Gestione archivio messaggi

Message Archive Management (mod_mam) implementa la gestione dell'archivio messaggi come descritto in *XEP-0313 <http://xmpp.org/extensions/xep-0313.html> _*. Se abilitato, tutti i messaggi verranno archiviati all'interno del server e i client XMPP compatibili potranno utilizzarlo per archiviare la propria cronologia chat sul server.

Il database può memorizzare fino a 2 GB di messaggi, i messaggi archiviati possono essere eliminati automaticamente. Per configurare i criteri di conservazione dei messaggi, impostare l'opzione *Elimina messaggi più vecchi di X giorni*.

Nota: Se abilitato, questo modulo memorizzerà ogni messaggio inviato tra gli utenti. Questa funzionalità impatterà sulla privacy degli utenti.

4.8 Team chat (Mattermost)

Il modulo team chat installa la piattaforma Mattermost Team Edition all'interno di NethServer.

Mattermost è un cloud privato Open Source Slack-alternative. L'eccellente documentazione ufficiale del progetto è disponibile qui: https://docs.mattermost.com/.

4.8.1 Configurazione

L'installazione di Mattermost richiede un virtual host dedicato, un FQDN come `chat.nethserver.org`.

Prima di procedere con la configurazione, assicurarsi di aver creato il record DNS corrispondente. Se NethServer svolge il ruolo di server DNS della LAN, fare riferimento alla sezione *DNS*.

Se il server utilizza il certificato Let's Encrypt come predefinito, assicurarsi anche di avere un record DNS pubblico corrispondente. Vedi *Certificato del server* per maggiori informazioni.

Come configurare:

1. Accedere alla pagina guilabel:*Team chat* del Server Manager
2. Spuntare l'opzione *Abilita Mattermost Team Edition*, quindi inserire un FQDN valido nel campo *Nome virtual host* (ad esempio `chat.nethserver.org`)

3. Accedere al nome DNS indicato attraverso il browser, ad esempio `https://chat.nethserver.org`. Al primo accesso una procedura guidata creerà l'utente amministratore

Le seguenti funzionalità sono abilitate di default:

- notifiche mail
- notifiche push per le app mobile
- redirect da HTTP ad HTTPS

4.8.2 Autenticazione

L'autenticazione per Mattermost *non* è integrata con alcun Account Provider. L'amministratore di Mattermost dovrà occuparsi della creazione di utenti e team.

Nota: L'amministratore deve sempre utilizzare la procedura guidata di Mattermost per creare l'utente amministratore, quindi inviare il link di invito del team a ciascun utente.

Importazione di utenti

Se l'amministratore di sistema ha ancora bisogno della creazione di massa degli utenti, può usare il comando `mattermost-bulk-user-create`.

Il comando provvederà a:

- creare il team di default utilizzando il nome dell'azienda definito nella sezione *Indirizzo dell'organizzazione*
- leggere tutti gli utenti dall'Account Provider locale o remoto e ri-crearli all'interno di Mattermost

Si noti che:

- gli utenti disabilitati nel Server Manager o già esistenti in Mattermost saranno omessi
- per ogni utente verrà generata una password casuale
- il primo utente importato verrà impostato come amministratore se nessun amministratore è già stato creato

Esempio di Invocazione:

```
mattermost-bulk-user-create

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

Nota: Gli utenti non vengono automaticamente sincronizzati all'interno di Mattermost. Ogni volta che un utente viene creato o rimosso, è necessario ricordarsi di eseguire il comando `mattermost-bulk-user-create` o di creare manualmente l'utente usando l'interfaccia web di amministrazione di Mattermost.

Forzare una password predefinita comune

È possibile impostare una password predefinita per ogni nuovo utente Mattermost, basta aggiungere la password predefinita in fase di esecuzione del comando.

Esempio:

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

4.9 UPS

NethServer supporta la gestione di UPS (Uninterruptible Power Supply) collegati al sistema.

Il server può essere configurato in due modalità:

- *master*: l'UPS è direttamente collegato al server, il server accetta connessioni dagli slave
- *slave*: l'UPS è collegato ad un altro server raggiungibile via rete

---

Nota: Si consiglia di consultare la lista dei modelli supportati prima dell'acquisto. Installare il pacchetto UPS da *Amministrazione* > *Software center*. In *Configurazione* appare la nuova voce di menù *UPS* dove si può trovare il dispositivo supportato inserendo il modello all'interno del campo di ricerca *Cerca driver per modello*.

Nella modalità master, l'UPS può essere collegato al server:

- su una porta seriale
- su una porta USB
- con un adattatore da USB a seriale

Nella modalità slave sarà necessario fornire l'indirizzo IP del server master.

La configurazione di default prevede uno spegnimento controllato in caso di assenza di alimentazione.

4.9.1 Device personalizzato

Se l'UPS è collegato ad una porta non elencata nell'interfaccia web, è possibile configurare un device personalizzato con i seguenti comandi:

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

4.9.2 Statistiche UPS

Se il modulo statistiche (collectd) è installato e funzionante, il modulo raccoglierà automaticamente statistiche sullo stato dell'UPS.

4.10 Server FAX

Il server fax permette di ricevere e inviare fax attraverso un modem fisico collegato direttamente al server o attraverso un modem virtuale.

L'interfaccia web consente di configurare:

- Prefisso e numero di fax
- Mittente (TSI)
- Un modem fisico specificando i parametri della linea telefonica e la modalità di invio/ricezione
- Uno o più *Modem virtuali*
- Notifiche mail per fax inviati e ricevuti, con documento allegato in formati multipli (PDF, PostScript, TIFF)
- Stampa dei fax ricevuti
- Stampante virtuale Samba
- Rapporto di invio giornaliero
- Invio fax via mail

4.10.1 Modem

Sebbene HylaFAX supporti un vasto numero di marche e modelli, si consiglia di utilizzare modem esterni seriali o USB.

Un modem interno, in caso di blocco, richiede il riavvio completo del server, mentre un modem esterno ha la possibilità di essere spento in maniera distinta. Inoltre, la maggior parte dei modem interni in commercio appartiene alla cosiddetta famiglia dei winmodem, modem "software" che necessitano di un driver, solitamente disponibile solo in ambiente Windows.

Inoltre si consiglia di fare attenzione al fatto che anche molti modem esterni USB sono winmodem.

In linea di massima sono da preferire modem funzionanti in classe 1 o 1.0, in particolare se basati su chipset Rockwell/Conexant o Lucent/Agere. Sono supportati anche modem in classi 2, 2.0 e 2.1.

4.10.2 Client

Si consiglia l'utilizzo del client fax YajHFC (http://www.yajhfc.de/) che si collega direttamente al server e consente:

- l'utilizzo di una rubrica LDAP
- possibilità di selezionare i modem per l'invio
- visualizzare la situazione dei modem fax

Autenticazione

Il sistema supporta due metodi di autenticazione per l'invio di fax:

- Host Based: utilizza l'indirizzo IP del computer che invia la richiesta
- PAM: utilizza nome utente e password, gli utenti devono appartenere al gruppo *faxmaster*. Il gruppo *faxmaster* deve essere creato espressamente.

Assicurarsi inoltre che sia abilitata l'opzione *Visualizza fax inviati dai client*.

4.10.3 Stampante virtuale Samba

Attivando l'opzione SambaFax il server mette a disposizione della rete locale una stampante virtuale, denominata "sambafax".

I singoli client dovranno configurare questa stampante usando il driver Apple LaserWriter 16/600 PS.

Il documento da inviare dovrà rispettare i seguenti prerequisiti:

- Deve contenere esattamente la stringa "Numero Fax: ", contenente il numero fax, per esempio:

```
Numero Fax: 12345678
```

- La stringa può essere presente in qualsiasi posizione del documento, ma su una riga singola.
- La stringa deve essere scritta con carattere non bitmap (ad esempio Truetype)

I fax spediti avranno come mittente l'id dell'utente specificato. Questa informazione sarà ben visibile nella coda dei fax.

4.10.4 Mail2Fax

Avvertimento: Per abilitare questa funzione, assicurarsi che sia installato il modulo ‘‘ Email‘‘.

Tutte le email inviate da rete locale all'indirizzo `sendfax@<nomedominio>` saranno trasformate in fax ed inviate al destinatario.

Il `<nomedominio>` deve corrispondere ad un dominio di posta configurato per la consegna locale.

Le mail devono rispettare questo formato:

- Il numero del destinatario deve essere specificato nel campo oggetto (o subject)
- L'email deve essere in formato solo testo
- Può contenere allegati di tipo PDF o PS che saranno convertiti e inviati insieme al fax

Nota: Questo servizio è abilitato solo per i client che inviano mail dalla rete green.

4.10.5 Modem virtuali

I modem virtuali sono modem software che comunicano con un PBX (solitamente Asterisk) utilizzando degli interni IAX.

La configurazione dei modem virtuali si compone di due parti:

1. Creazione dell'interno IAX all'interno del PBX
2. Configurazione del modem virtuale

4.11 Firewall e gateway

NethServer è in grado di svolgere il ruolo di firewall e gateway all'interno della rete in cui viene installato. Tutto il traffico fra i computer della rete locale e Internet passa attraverso il server che decide come instradare i pacchetti di rete (routing) e quali regole applicare.

Funzioni principali:

- Configurazione di rete avanzata (bridge, bond, alias, ecc. . .)
- Supporto WAN multiple (fino a 15)
- Gestione regole firewall
- Gestione banda (QoS)
- Port forwarding
- Regole per routing traffico su una specifica WAN
- Intrusion Prevention System (IPS)
- Deep packet inspection (DPI)

La modalità firewall e gateway viene attivata solo se:

- il pacchetto *nethserver-firewall-base* è installato
- è configurata almeno una scheda di rete con ruolo red

4.11.1 Policy

Ogni interfaccia di rete è identificata da un colore che ne indica il ruolo all'interno del sistema. Vedi *Rete*.

Quando un pacchetto di rete attraversa una zona del firewall, il sistema valuta una lista di regole per decidere se il traffico debba essere bloccato o permesso. Le *policy* sono le regole di default che vengono applicate se il traffico di rete non corrisponde a nessun criterio esistente.

Il firewall implementa due policy standard modificabili nella pagina *Regole firewall* -> *Configura*:

- *Permesso*: tutto il traffico dalla rete green alla red è permesso
- *Bloccato*: tutto il traffico dalla rete green alla red è bloccato. Il traffico permesso deve essere esplicitato con apposite regole

Le policy del firewall permettono il traffico fra zone seguendo lo schema qui sotto:

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

Il traffico è permesso da sinistra a destra, bloccato da destra a sinistra.

Per cambiare le policy di default è possibile creare delle regole tra zone nella pagina *Regole firewall*.

Nota: Il traffico dalla rete locale verso il server sulla porta SSH (default 22) e Server Manager (default 980) è **sempre** permesso.

4.11.2 Regole

Le regole vengono applicate a tutto il traffico di rete che attraversa il firewall. Quando un pacchetto di rete transita da una zona all'altra, il sistema cerca fra le regole configurate. Se le caratteristiche del pacchetto corrispondono a quelle descritte in una regola, tale regola viene applicata.

Nota: L'ordine delle regole è molto importante. Il sistema applica sempre la prima regola che corrisponde al traffico in transito.

Una regola si compone di tre parti principali:

- Azione: azione da intraprendere quando si applica la regola
- Origine traffico: indirizzo di origine del traffico, può essere una zona, una rete o un singolo host
- Destinazione traffico: indirizzo di destinazione del traffico, può essere una zona, una rete o un singolo host
- Servizio: porta e protocollo che individua un determinato tipo di traffico
- Condizione temporale: la regola si applica solo nell'intervallo temporale specificato

Le azioni disponibili sono:

- *ACCEPT*: accetta il traffico
- *REJECT*: blocca il traffico ed informa il mittente che la richiesta effettuata non è permessa
- *DROP*: blocca il traffico, i pacchetti vengono scartati e il mittente non viene notificato
- *ROUTE*: instrada il traffico al provider WAN specificato. Vedi anche *Multi WAN*.
- *Priority*: marca il traffico come alta/bassa priorità. Vedi *Gestione banda*.

Nota: Se non è configurata almeno un'interfaccia red, il firewall non genererà nessuna regola per le zone blue e orange.

REJECT vs DROP

Come regola generale, si consiglia di usare REJECT quando si desidera informare l'host sorgente del traffico che la porta a cui si sta provando ad accedere è chiusa. Solitamente le regole che rispondono alle richieste della LAN possono usare REJECT.

Per le connessioni provenienti da Internet si consiglia di usare DROP, al fine di minimizzare la rivelazione di informazioni ad eventuali attaccanti.

Log

Quando una regola viene applicata, è possibile registrare l'evento nel log abilitando la relativa spunta. Il log del firewall è salvato nel file `/var/log/firewall.log`.

Deep Packet Inspection (DPI)

La Deep Packet Inspection (DPI)[1] è una tecnica avanzata di filtraggio dei pacchetti di rete.

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

Attivando il modulo DPI, vengono rese disponibili delle voci aggiuntive per il campo *Servizi* disponibile nelle schermate di creazione/modifica delle regole firewall. Queste voci sono etichettate come *protocollo DPI* tra le usuali voci *servizio* e *servizio di rete*.

Il modulo DPI utilizza la libreria *nDPI <https://www.ntop.org/products/deep-packet-inspection/ndpi/>* _ in grado di identificare oltre 250 tipi di traffico di rete suddiviso in protocolli di rete (ad esempio OpenVPN, DNS) e applicazioni Web (ad esempio, Netflix, Spotify).

Le regole del firewall che utilizzano i servizi DPI vengono generate all'interno della tabella mangle, per questo motivo tali regole hanno alcune limitazioni:

- L'azione *reject* non è supportata, va utilizzata l'azione *drop* per bloccare il traffico
- non è possibile utilizzare gli oggetti *tutti (any)* e *firewall* come sorgente o destinazione
- l'azione *devia su X* non è supportata: l'identificazione del protocollo inizia spesso dopo che la connessione è già stata stabilita, quindi la policy di routing non può essere modificata

Anche se DPI può identificare il traffico da/per specifici siti web come Facebook, è più adatto per bloccare o priorizzare protocolli come VPN, FTP, ecc. L'accesso ai siti Web deve essere disciplinato utilizzando il *Proxy web*.

E" opportuno sottolineare che alcuni protocolli DPI (come Amazon) possono corrispondere a grandi CDN, quindi è opportuno non bloccare tali protocolli usando le regole DPI a meno che non si desideri impedire l'accesso a migliaia di siti.

La marcatura DPI viene applicata automaticamente anche al traffico proveniente dal firewall stesso, come il traffico HTTP dal proxy web

L'elenco completo dei protocolli DPI, insieme ai contatori per il traffico corrispondente, è disponibile nella pagina *DPI* sotto la categoria *Stato* del menu di sinistra.

Esempi

Si riportano di seguito alcuni esempi di regole.

Bloccare tutto il traffico DNS proveniente dalla LAN e diretto verso Internet:

- Azione: REJECT
- Origine: green
- Destinazione: red
- Servizio: DNS (UDP porta 53)

Permettere alla rete ospiti di accedere a tutti i servizi in ascolto sul Server1:

- Azione: ACCEPT
- Origine: blue
- Destinazione: Server1
- Servizio: -

4.11.3 Multi WAN

Con il termine *WAN* (Wide Area Network) si indica una rete pubblica esterna al server, solitamente collegata a Internet. I fornitori di collegamenti WAN sono detti *provider*.

Il sistema supporta fino ad un massimo di 15 connessioni WAN. Se sul server sono configurate due o più schede red, è obbligatorio procedere alla configurazione dei campi *Peso link*, *Banda entrante* e *Banda uscente* della pagina *Rete*.

Ogni provider configurato rappresenta una connessione WAN ed è associato ad una scheda di rete. Ciascun provider definisce un *peso*: maggiore è il peso maggiore è la priorità della scheda di rete associata al provider stesso.

Il sistema può utilizzare le connessioni WAN in due modalità (pulsante *Configura* nella pagina *Multi WAN*):

- *Balance*: tutti i provider sono utilizzati contemporaneamente in base al loro peso
- *Active backup*: i provider sono utilizzati uno alla vola a partire da quello con il peso più alto. Se il provider in uso perde la connessione, tutto il traffico verrà dirottato sul successivo provider.

Per determinare lo stato di un provider, il sistema invia un pacchetto ICMP (ping) ad intervalli regolari. Se il numero di pacchetti persi supera una determinata soglia, il provider viene disabilitato.

L'amministratore può configurare la sensibilità del monitoraggio attraverso i seguenti parametri:

- percentuale di pacchetti persi
- numero consecutivo di pacchetti persi
- intervallo di invio fra un pacchetto e l'altro

La pagina *Regole firewall* consente di instradare i pacchetti di rete verso un particolare provider WAN, a patto che siano soddisfatte alcune condizioni. Vedi anche *Regole*.

Esempio

Dati due provider così configurati:

- Provider1: interfaccia di rete eth1, peso 100
- Provider2: interfaccia di rete eth0, peso 50

Se è attiva la modalità bilanciata, il server indirizzerà il doppio delle connessioni sul Provider1 rispetto al Provider2.

Se è attiva la modalità backup, il server indirizzerà tutte le connessioni sul Provider1; solo se il Provider1 diventa inutilizzabile tutte le connessioni saranno indirizzate sul Provider2.

4.11.4 Port forward

Il firewall impedisce che richieste iniziate dall'esterno possano accedere alle reti private. Se ad esempio all'interno della rete è presente un server web, solo i computer presenti nella rete green potranno accedere al servizio. Qualsiasi richiesta fatta da un utente esterno alle reti locali viene bloccata.

Per permettere a qualsiasi utente esterno l'accesso al server web si utilizza il *port forward*. Il port forward è una regola che consente un accesso limitato alle risorse delle LAN dall'esterno.

Quando si configura il server, è necessario scegliere le porte in ricezione o in ascolto su cui verrà redirezionato il traffico in ingresso nella scheda red. Nel caso di un server web, le porte in ascolto sono solitamente la porta 80 (HTTP) e 443 (HTTPS).

Quando si crea un port forward è necessario specificare almeno i seguenti parametri:

- la porta di origine
- la porta di destinazione, che può essere diversa dalla porta di origine
- l'indirizzo dell'host a cui deve essere instradato il traffico
- è possibile specificare un range di porte utilizzando i due punti come separatore nella porta di origine (es: 1000:2000), in tale caso particolare il campo porta di destinazione dovrà rimanere vuoto

Esempio

Dato il seguente scenario:

- Server interno con IP 192.168.1.10, detto Server1
- Server web in ascolto sulla porta 80 su Server1
- Server SSH in ascolto sulla porta 22 su Server1
- Altri servizi nell'intervallo di porte tra 5000 e 6000 sul Server1

In caso si voglia rendere accessibile dall'esterno il server web direttamente sulla porta 80, si dovrà creare un port forward fatto così:

- porta origine: 80
- porta destinazione: 80
- indirizzo host: 192.168.1.10

Tutto il traffico che arriva sulle reti red del firewall sulla porta 80, verrà redirezionato alla porta 80 di Server1.

In caso si voglia rendere accessibile dall'esterno il server SSH sulla porta 2222, si dovrà creare un port forward fatto così:

- porta origine: 2222
- porta destinazione: 22
- indirizzo host: 192.168.1.10

Tutto il traffico che arriva sulle reti red del firewall sulla porta 2222, verrà redirezionato alla porta 22 di Server1.

Nel caso in cui si desideri rendere il server accessibile dall'esterno usare un intervallo di porte tra 5000 e 6000, sarà necessario creare un port forward come questo:

- porta origine: 5000:6000
- porta destinazione:
- indirizzo host: 192.168.1.10

Tutto il traffico che arriva sulle reti red del firewall per il range di porte compreso tra 5000 e 6000 verrà redirezionato alle stesse porte sul Server1.

Limitare accesso

E" possibile limitare l'accesso al port forward solo da alcuni IP o reti compilando il campo *Permetti solo da*.

Questa configurazione è utile in casi alcuni servizi debbano essere accessibili solo da IP/reti fidati. Esempi di alcuni valori possibili:

- `10.2.10.4`: abilita il port forward solo per il traffico proveniente dall'IP 10.2.10.4
- `10.2.10.4,10.2.10.5`: abilita il port forward solo per il traffico proveniente dagli IP 10.2.10.4 e 10.2.10.5
- `10.2.10.0/24`: abilita il port forward solo per il traffico proveniente dalla rete 10.2.10.0/24
- `!10.2.10.4`: abilita il port forward per tutti gli IP tranne 10.2.10.4
- `192.168.1.0/24!192.168.1.3,192.168.1.9`: abilita il port forward per tutta la rete 192.168.1.0/24 ad eccezione degli host 192.168.1.3 e 192.168.1.9

4.11.5 sNAT 1:1

Il NAT uno-a-uno consiste nell'associare un indirizzo IP privato ad un indirizzo IP pubblico per configurare, ad esempio, sistemi che si trovano dietro ad un firewall.

Se si hanno a disposizione diversi IP pubblici e si vuole associare uno di questi ad un determinato host della rete, è possibile farlo, appunto, mediante il NAT 1:1.

Questa funzionalità si applica solo per il traffico generato verso internet dall'host di rete specifico oggetto della regola.

La regola non interessa in alcun modo il traffico genareato da internet verso l'Alias IP, se dovesse essere necessario instradare traffico specifico verso l'host interno andranno definite delle normali regole di port forward.

Se dovesse essere necessario instradare tutto il traffico verso l'host interno (configurazione non raccomandata) andrà definita una regola di port forward per i protocolli TCP & UDP che abbia come porte sorgenti il range 1:65535.

Esempio

Nella nostra rete abbiamo un host di nome `host_esempio` che ha IP `192.168.5.122`. Abbiamo inoltre associato un IP pubblico di cui disponiamo `89.95.145.226` come alias dell'interfaccia `eth0` (RED).

Vogliamo quindi mappare il nostro host interno (`host_esempio - 192.168.5.122`) con l'IP pubblico `89.95.145.226`.

Dal pannello *NAT 1:1* andremo a scegliere per l'IP `89.95.145.226` (che compare come campo in sola lettura) il corrispondente host (`host_esempio`) che scegliamo dal combobox. Così facendo abbiamo configurato il NAT uno-a-uno per il nostro host.

4.11.6 Gestione banda

La gestione banda (traffic shaping) permette di applicare regole di priorità sul traffico che attraversa il firewall. In tal modo è possibile ottimizzare la trasmissione, controllare la latenza e sfruttare al meglio la banda disponibile.

Per abilitare il traffic shaping è necessario conoscere l'esatta quantità di banda disponibile in download e upload. Accedi alla pagina guilabel *Network* e imposta attentamente i valori di larghezza di banda.

Se la larghezza di banda di download e upload non è impostata per un'interfaccia red, le regole di shaping non saranno abilitate per quell'interfaccia.

Nota: Assicurati di specificare una stima accurata della larghezza di banda sulle interfacce di rete. Per scegliere un'impostazione appropriata, si prega di non fidarsi del valore nominale, ma utilizzare strumenti online per verificare la reale velocità del provider.

In caso di congestione da parte del provider, non c'è nulla da fare per migliorare le prestazioni.

La configurazione del traffic shaping è composta da 2 passaggi:

- Creazione di classi per gestione della banda
- assegnazione del traffico di rete a una classe specifica

Classi

Il traffic shaping viene ottenuto controllando il modo in cui la larghezza di banda viene allocata alle classi.

Ogni classe può avere una percentuale riservata. Una percentuale riservata è la larghezza di banda che una classe avrà a disposizione in caso di necessità. La larghezza di banda disponibile è data dalla somma della larghezza di banda non impegnata e della larghezza di banda impegnata di una classe, ma non attualmente utilizzata dalla classe stessa.

Ogni classe può avere anche una banda massima. Se impostato, la classe può superare la banda stabilita,fino al banda massima. Una classe supererà la sua banda riservata solo se è disponibile abbastanza banda.

Le classi di traffic shaping possono essere definite nella pagina *Traffic shaping*. Quando crei una nuova classe, compila i seguenti campi:

- *Class name*: un nome rappresentativo
- *Min download (%)*: Download minimo consentito, se vuoto non verrà creato alcun limite
- *Max download (%)*: Download massimo consentito, se vuoto non verrà creato alcun limite
- *Min upload (%)*: Upload minimo consentito, se vuoto non verrà creato alcun limite
- *Max upload (%)*: Upload massimo consentito, se vuoto non verrà creato alcun limite
- : guilabel: *Description*: descrizione facoltativa per la classe

Il sistema fornisce due classi preconfigurate:

- : guilabel: *high*: traffico ad alta priorità generico, può essere assegnato tipo ad SSH
- : guilabel: *low*: traffico a bassa priorità, può essere assegnato a un servizio come scambio di file peer to peer

Il sistema cerca sempre di previnire la saturazione della banda quando ci sta un carico di rete elevato.

Le classi ricevono la banda non allocata in proporzione alla loro banda minima . Per esempio, se una la classe A ha 1Mbit di banda minima e la classe B ha 2Mbit, allora la classe B riceverà il doppio della banda non allocata rispetto alla classe A. In ogni caso, tutta la banda non allocata verrà utilizzata dalle classi.

Per più info,vedere[2] .

4.11.7 Oggetti firewall

Gli oggetti firewall sono delle rappresentazioni dei componenti della rete e sono utili per semplificare la creazione di regole.

Esistono 6 tipi di oggetti, 5 di questi sono relativi a sorgenti e destinazioni e sono:

- Host: rappresentano computer locali e remoti. Esempio: server_web, pc_boss
- Gruppi di host: rappresentano gruppi omogenei di computer. Gli host all'interno di un gruppo devono essere raggiungibili attraverso la stessa interfaccia. Esempio: servers, pc_segreteria
- Reti CIDR : utilizzare una rete CIDR per semplificare e rendere più leggibili le regole.

  Esempio 1 : gli ultimi 14 IP della rete sono destinati ai server (192.168.0.240/28).

  Esempio 2 : Più interfacce green configurate ma vogliamo creare una regola di firewall valida solo per una di queste green (192.168.2.0/24).
- *Zone*: rappresentano reti di host, vanno espresse in notazione CIDR, utili se si vuole definire un segmento di rete con caratteristiche differenti dalla zona di cui fa parte. Solitamente utilizzate per esigenze molto specifiche.

Nota: Di default gli host che fanno parte di una Zona non possono fare alcun tipo di traffico, sarà necessario quindi creare tutte le regole necessarie a caratterizzarne il comportamento.

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

- Condizione temporali: possono essere associati alle regole del firewall per limitarne l'effetto ad un determinato periodo di tempo.

L'ultimo oggetto invece specifica il tipo di traffico ed è quello dei:

- Servizi: rappresentano un servizio in ascolto su un host. Esempio: ssh, https

Durante la creazione delle regole, è possibile usare i record definiti in *DNS* e *Server DHCP e PXE* come oggetti host. Inoltre ogni interfaccia di rete con un ruolo associato è automaticamente elencata fra le zone disponibili.

Nota: Le regole che hanno condizioni temporali sono applicate solo per le nuove connessioni. Esempio: se si stanno bloccando le connessioni HTTP dalle 09:00 alle 18:00, tutte le connessioni stabilite prima delle ore 09:00 saranno permesse fino a quando non termineranno. Qualsiasi nuova connessione effettuata dopo le 09:00 sarà bloccata.

4.11.8 Binding IP/MAC

Quando il sistema è configurato come server DHCP, il firewall può utilizzare la lista delle DHCP reservation per controllare il traffico generato dagli host presenti nelle reti locali. Se il binding IP/MAC è abilitato, l'amministratore può scegliere quale politica applicare agli host senza DHCP reservation. Solitamente questa funzione è utilizzata per permettere il traffico solo dagli host conosciuti e bloccare tutti gli altri. In questo caso, gli host senza una DHCP reservation non potranno accedere né al firewall né alla rete esterna.

Per abilitare il traffico solo dagli host conosciuti, seguire questi passi:

1. Creare una DHCP reservation per l'host
2. Andare sulla pagina *Regole firewall* e selezionare *Configura* dal menu
3. Selezionare *Validazione MAC (Binding IP/MAC)*
4. Spuntare *Blocca traffico* come policy per gli host senza riserva DHCP

Nota: Ricordarsi di creare almeno una DHCP reservation prima di abilitare la modalità binding IP/MAC, altrimenti nessun host sarà in grado di configurare il server usando l'interfaccia web o SSH.

4.12 Proxy web

Il proxy web è un server che si interpone fra i PC della LAN e i siti Internet. I client effettuano le richieste al proxy che comunica con i siti esterni, quindi trasmette le risposte al client.

I vantaggi del proxy web sono due:

- possibilità di filtrare i contenuti
- ridurre l'utilizzo della banda facendo cache delle pagine visitate

Il proxy può essere attivato per le zone green e blue. Le modalità supportate sono:

- Manuale: tutti i client devono essere manualmente configurati
- Autenticato: gli utenti devono inserire nome utente e password per poter navigare
- Trasparente: tutti i client sono automaticamente forzati ad usare il proxy per le connessioni HTTP
- Trasparente SSL: tutti i client sono automaticamente forzati ad usare il proxy per le connessioni HTTP e HTTPS

4.12.1 Modalità autenticata

Prima di abilitare il proxy web in modalità autenticata, assicurarsi di aver configurato un account provider locale o remoto.

Quando viene installato Samba Active Directory o il server è attestato ad un dominio remoto Active Directory, le postazioni Windows possono utilizzare l'autenticazione integrata Kerberos. Su tutti i client Windows **è necessario** configurare il proxy utilizzando l'FQDN del server.

Tutti gli altri client possono utilizzare il meccanismo di basic authentication.

Nota: L'autenticazione NTLM è deprecata e non è più supportata.

4.12.2 Configurazione client

Il proxy è sempre in ascolto sulla porta **3128**. Quando si utilizzano le modalità Manuale o Autenticato, tutti i client devono essere esplicitamente configurati per utilizzare il proxy. La configurazione è accessibile dal pannello impostazioni del browser. La maggior parte dei client verranno comunque configurati automaticamente attraverso il protocollo WPAD. In questo caso è utile attivare l'opzione *Blocca porta HTTP e HTTPS* per evitare il bypass del proxy.

Se il proxy è installato in modalità trasparente, tutto il traffico web proveniente dai client viene intercettato dal firewall e indirizzato attraverso il proxy. Nessuna configurazione è necessaria sui singoli client.

Nota: Per rendere accessibile il file WPAD dalla rete ospiti, aggiungere l'indirizzo della rete blue nel campo *Consenti host* per il servizio httpd nella pagina *Servizi di rete*.

4.12.3 Proxy SSL

In modalità trasparente SSL, il proxy implementa la cosiddetta tecnica «peek and splice»: stabilisce la connessione SSL con i siti remoti e verifica la validità dei certificati senza decifrare il traffico. Quindi il server può filtrare gli URL richiesti utilizzando il filtro web e ritornare la risposta al client.

Nota: Non è necessario installare alcun certificato sui client, è sufficiente abilitare il proxy SSL.

4.12.4 Bypass

In alcuni casi può essere necessario fare in modo che il traffico originato da specifici ip della rete o verso alcune destinazioni non passi per il proxy HTTP/HTTPS, ma sia instradato direttamente; il traffico in questione non sarà più sottoposto a proxy.

Il proxy consente di creare:

- bypass per domini
- bypass per sorgente
- bypass per destinazione

Bypass per domini

I bypass per i domini possono essere configurati dalla sezione *Domini senza proxy*. Tutti i domini elencati all'interno di questa pagina possono essere acceduti direttamente dai client LAN. Nessun filtro antivirus o dei contenuti viene applicato a questi domini.

Ogni dominio elencato sarà espanso anche per i relativi sotto-domini. Ad esempio, aggiungendo *nethserver.org* verranno bypassati anche *www.nethserver.org*, *mirror.nethserver.org*, e così via.

Nota: Tutti i client della LAN **devono** utilizzare il server stesso come DNS, direttamente o come *forwarder*.

Bypass per origine e destinazione

Un bypass per origine consente l'accesso diretto a tutti i siti HTTP/HTTPS da host selezionati, gruppi host, intervalli IP e CIDR di rete. I bypass per origine sono configurabili dalla sezione *Host senza proxy*.

Un bypass per destinazione consente l'accesso diretto da qualsiasi client della LAN a siti HTTP/HTTPS ospitati su host specifici, gruppi host o CIDR di rete. I bypass per destinazione sono configurabili dalla sezione *Siti senza proxy*.

Queste regole di bypass vengono configurate anche all'interno del file WPAD.

4.12.5 Regole di priorità e di instradamento

Le regole del firewall per il routing del traffico su un provider specifico o per la modifica della priorità del traffico vengono applicate solo al traffico di rete che attraversa il gateway. Queste regole non si applicano se il traffico passa attraverso il proxy perché il traffico viene generato dal gateway stesso.

In uno scenario in cui il proxy web è abilitato in modalità trasparente e il firewall contiene una regola per abbassare la priorità di un host specifico, la regola si applica solo ai servizi non HTTP, come SSH.

La scheda *Regole* consente la creazione di regole di priorità e di instradamento anche per il traffico intercettato dal proxy.

L'interfaccia web consente di creare regole per il traffico HTTP/S per:

- aumentare la priorità di un host o una rete
- abbassare la priorità di un host o di una rete
- Instradare la sorgente su un provider specifico con failover automatico se il provider dovesse andare fuori servizio
- forzare la sorgente su uno specifico provider senza failover automatico

4.12.6 Report

Installando il modulo `nethserver-lightsquid` il sistema genererà automaticamente i report di navigazione web.

LightSquid è un analizzatore di log per Squid leggero e veloce che ogni giorno genera un nuovo report HTML, riassumendo le abitudini di navigazione degli utenti del proxy. L'interfaccia di Lightsquid è accessibile dal tab *Applicazioni* della *Dashboard*.

4.12.7 Cache

Nel pannello *Cache* è presente un form per configurare i parametri di cache:

- La cache può essere abilitata o disabilitata (*disabilitata* di default)
- **Dimensione cache disco**: valore massimo della cache di squid sul disco (in MB)
- **Dimensione minima oggetto**: può essere lasciato a 0 per mettere in cache tutto, ma può essere alzato se gli oggetti piccoli non sono desiderati in cache (in kB)
- **Dimensione massima oggetto**: gli oggetti più grandi di questa dimensione non vengono salvati in cache. Se si preferisce la velocità al salvataggio della banda, può essere impostato ad un valore basso (in kB)

Il pulsante *Svuota cache* funziona anche se il proxy è disabilitato, potrebbe essere utile per liberare spazio su disco.

Siti senza cache

A volte il proxy non è in grado di fare cache di alcuni siti mal costruiti. Per escludere uno o più domini dalla cache, usare l'opzione `NoCache`.

Esempio:

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

4.12.8 Porte sicure

Le porte sicure sono una lista di porte accessibili attraverso il proxy. Se una porta non è all'interno della lista delle porte sicure, il proxy si rifiuterà di collegarsi al server. Per esempio, dato un servizio HTTP che gira sulla porta 1234, tale servizio non sarebbe accessibile usando il proxy.

L'opzione `SafePorts` è una lista di porte separata da virgole. Le porte elencate saranno aggiunte alla lista preconfigurata di porte sicure.

Per esempio, per aprire l'accesso alle porte 446 e 1234:

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

4.12.9 Log

I log di Squid vengono conservati in formato compresso per 5 settimane, per gestire l'utilizzo dello spazio su disco. I log del proxy Web sono molto dettagliati e sono una insostituibile risorsa per approfondire gli eventuali problemi. Le attività di navigazione Web sono registrate in formato aggregato e leggibile attraverso Lightsquid.

Negli ambienti in cui sia necessario conservare i log per più di 5 settimane, è possibile modificare manualmente la configurazione di logrotate `/etc/logrotate.d/squid`. E" inoltre necessario rammentare di aggiungere `/etc/logrotate.d/squid` al backup della configurazione usando l'inclusione personalizzata.

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

4.13 Filtro contenuti web

Il filtro contenuti analizza il traffico web ed è in grado di bloccare siti pericolosi o contenenti virus. I siti proibiti sono selezionati da una lista di categorie che è possibile anche scaricare da sorgenti esterne e salvare sul sistema.

La configurazione consente di creare un numero illimitato di profili. Ciascun profilo è composto da tre parti:

- **Chi**: il client associato al profilo. Può essere un utente, un gruppo di utenti, un host, un gruppo di host, una zona o un ruolo (es. green, blue, ecc).
- **Cosa**: quali siti può vedere il client associato al profilo E" un filtro creato nella pagina *Filtri*.
- **Quando**: il profilo può essere sempre attivo o essere valido solo in alcuni periodi. Le condizioni temporali possono essere create nella sezione *Condizioni temporali*.

Si consiglia di procedere in questo ordine:

1. Selezionare una lista di categorie dalla pagina *Blacklist* ed avviare il download
2. Creare una o più condizioni temporali (opzionale)
3. Creare eventuali categorie personalizzate (opzionale)
4. Creare un nuovo filtro o modificare quello di default
5. Creare un nuovo profilo associato ad un utente o un host, selezionare quindi un filtro e una condizione temporale (se abilitata)

Il sistema prevede un profilo di default che viene applicato a tutti i client qualora non rientrino in nessun altro profilo.

4.13.1 Filtri

Un filtro consente di:

- bloccare l'accesso a categorie di siti
- bloccare l'accesso ai siti acceduti usando indirizzi IP (consigliato)
- filtrare gli URL con espressioni regolari
- bloccare file con specifiche estensioni
- abilitare blacklist e whitelist globali

Ogni filtro può lavorare in due modalità:

- Permetti tutto: permette l'accesso a tutti i siti, ad eccezione di quelli esplicitamente bloccati
- Blocca tutto: blocca l'accesso a tutti i siti, ad eccezione di quelli esplicitamente consentiti

---

Nota: La lista delle categorie compare solo al termine del download della lista selezionata nella pagina *Blacklists*.

Blocco Google Translate

E" noto che il servizio di traduzione online di intere pagine html di Google può essere usato per riuscire a scavalcare il filtro contenuti. Infatti le pagine visitate attraverso il traduttore fanno riferimento sempre ad un dominio riconducibile a Google stesso pur avendo al loro interno contenuti provenienti da server esterni.

E" possibile bloccare tutte le richieste a Google Translate (in qualsiasi lingua), creando un URL bloccato nella pagina *Generale* con il seguente contenuto: `translate.google`.

4.13.2 Antivirus

La navigazione web può essere analizzata per rilevare contenuti malevoli, ma soltanto per il protocollo in chiaro HTTP. Se il proxy è configurato in modalità trasparente SSL (*Proxy SSL*), i contenuti scaricati via HTTPS non verranno scansionati.

4.13.3 Risoluzione problemi

Nel caso una pagina indesiderata non venga bloccata, verificare che:

- il client stia navigando attraverso il proxy
- il client non abbia un bypass configurato nella sezione *Host senza proxy*
- il sito visitato non abbia un bypass configurato nella sezione *Siti senza proxy*
- il client sia associato ad un profilo in cui la pagina non è permessa
- il client non stia navigando in un periodo di tempo in cui il filtro ha una configurazione permissiva

4.14 IPS (Suricata)

Suricata è un *IPS* (Intrusion Prevention System), un sistema per la prevenzione delle intrusioni in rete. Il software analizza tutto il traffico che attraversa il firewall alla ricerca di attacchi noti e anomalie.

Quando un attacco o un'anomalia sono stati rilevati, il sistema può decidere se bloccare il traffico o limitarsi a salvare l'evento sul log (`/var/log/suricata/fast.log`).

Suricata può essere configurato utilizzando set di regole organizzati per categorie specifiche. Ogni categoria può essere configurata come:

- Abilitata: il traffico che intercetta le regole della categoria verrà segnalato
- Bloccata: il traffico che intercetta le regole della categoria verrà rifiutato
- Disabilitata: le regole della categoria verranno ignorate

Nota: L'utilizzo di un IPS impatta su tutto il traffico che attraversa il firewall. Assicurarsi di aver compreso a fondo tutte le possibili implicazioni prima di attivare la funzionalità. In particolare, prestare attenzione alle regole di blocco che potrebbero interferire con gli aggiornamenti del sistema stesso.

4.14.1 Categorie regole

Suricata utilizza regole free scaricate da https://rules.emergingthreats.net/.[1]

Le regole dono divise nelle categorie elencate di seguito.

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

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

[1] Documentazione sulle categorie:proofpoint - ETPro Category Descriptions

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

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

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

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

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

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

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

Deleted Rules removed from the rule set.

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

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

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

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

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

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

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

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

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

Info General rules to track suspicious host network traffic.

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

Malware Malware and Spyware related, no clear criminal intent. The threshold for inclusion in this set is typically some form of tracking that stops short of obvious criminal activity. This set was originally intended to be just spyware. That's enough to several rule categories really. The line between spyware and outright malicious bad

stuff has blurred to much since we originally started this set. There is more than just spyware in here, but rest assured nothing in here is something you want running on your net or PC. There are URL hooks for known update schemed, User-Agent strings of known malware, and a load of others.

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

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

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

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

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

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

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

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

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

SMTP-events Rules that will log SMTP operations.

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

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

Stream-events Rules for matching TCP stream engine events.

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

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

TLS-Events Rules for matching on TLS events and anomal

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

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

User Agents User agent identification and detection.

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

Web Client Web client side attacks and vulnerabilities.

Web Server Rules for attacks and vulnerabilities against web servers.

Web Specific Apps Rules for very specific web applications.

WORM Traffic indicative of network based worm activity.

4.14.2 EveBox

EveBox è uno strumento web per la gestione di allarmi ed eventi generati da Suricata.

Il modulo è accessibile dal Server Manager, attraverso il link nella pagina *Applicazioni*

4.15 Reverse proxy

La funzionalità reverse proxy è utile quando si desidera accedere a siti interni dalla rete esterna.

4.15.1 Regole di virtual host e path

Una richiesta di un client Web può essere inoltrata a un altro server Web in modo trasparente, in base a due tipi di regole di corrispondenza:

- Richieste che corrispondono a un percorso URL, come «http://mydomain.com/mysite‘‘
- Richieste che corrispondono a un nome virtual host , come *http://my.secondary-domain.com‘*

Lo scenario tipico per una **URL path rule** è la seguente:

- NethServer è il firewall della LAN
- Si possiede il dominio http://mydomain.com
- Si desidera che http://mydomain.com/mysite inoltri le richieste al server interno (IP privato: 192.168.2.100)

In questo scenario creare un nuovo record nella pagina *Reverse proxy*. Impostare il *Name* dell'elemento a `mysite` e *Target URL* a `http://192.168.2.100`.

Se sono consentite solo connessioni cifrate, abilitare l'opzione *Richiedi connessione SSL cifrata*.

Si può restringere l'accesso solo ai client appartenenti ad alcune reti, specificando un elenco separato da virgola di reti in notazione CIDR nel campo *Accedi da reti CIDR*.

Una **virtual host name rule** può inoltrare richieste HTTP a un altro server Web ed è definita nella pagina *Reverse proxy* > *Virtual hosts*. Per esempio:

- NethServer è il firewall della LAN
- Hai un dominio `http://my.secondary-domain.com`
- Si desidera che `http://my.secondary-domain.com` inoltri le richieste al server web interno `192.168.2.101`, porta 9000.

In questo scenario creare un nuovo record nella pagina *Reverse proxy*. Impostare il *Name* dell'elemento a `my.secondary-domain.com` e *Target URL* a `http://192.168.2.101:9000`.

Fare riferimento anche a *the UI description of Reverse Proxy* per ulteriori informazioni sulle funzionalità avanzate, come *Forward HTTP «Host» header to target* e :guilabel‘Accept invalid SSL certificate from target‘.

4.15.2 Configurazione manuale

Se la pagina *Reverse proxy* non è abbastanza, è sempre possibile configurare Apache manualmente, creando un nuovo file nella directory `/etc/httpd/conf.d/`.

Esempio

Creare il file `/etc/httpd/conf.d/myproxypass.conf` con il seguente contenuto:

```
<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>
```

Per ulteriori informazioni, consultare la documentazione ufficiale di Apache: https://httpd.apache.org/docs/2.4/mod/mod_proxy.html

4.16 Virtual hosts

Il virtual hosting consente di ospitare nomi di dominio multipli su un singolo server. Su NethServer, dalla pagina *Virtual hosts*, è possibile configurare i siti web come virtual host Apache.

4.16.1 Nomi dei virtual host (FQDN)

È la lista dei nomi di dominio FQDN che sono associati al virtual host. I valori devono essere separati con «,» (virgola). Per raggiungere il virtual host sarà anche necessario un record DNS. Se abilitata l'opzione nella sezione «Azioni aggiuntive», un alias per ogni FQDN verrà automaticamente creato su «DNS > Alias Server», ma è utile solo per i client che usano il server come DNS.

4.16.2 Configurare un'applicazione web

Quando si crea un virtual host, viene creata automaticamente una cartella /var/lib/nethserver/vhost/*NOME*. Se è stato abilitato l'accesso FTP, sarà possibile caricare file sul virtual host usando un client FTP e il nome del virtual host come username.

Avvertimento: L'FTP è disabilitato di default, bisogna anche abilitarlo dalla pagina di configurazione FTP

La password di autenticazione HTTP dovrebbe essere diversa da quella dell'FTP, in quanto l'FTP è usato per caricare contenuti, la password HTTP per limitare l'accesso alla lettura dei contenuti.

4.16.3 Permessi Apache

I file caricati via FTP sono di proprietà del gruppo «apache». Se è necessario consentire il permesso di scrittura o esecuzione ad apache, è possibile cambiare i permessi del gruppo usando il client FTP.

Avvertimento: Se un virtual host contiene del codice eseguibile, come script PHP, i permessi utente e le implicazioni di sicurezza vanno valutati attentamente

4.17 Cartelle condivise

Una *cartella condivisa* è un posto dove i file sono accessibili da un gruppo di persone tramite Samba (SMB/CIFS).

Per creare, modificare e rimuovere una cartella condivisa andare alla pagina *Cartelle condivise*.

4.17.1 Requisiti

Le cartelle condivise utilizzano ACL (Access Control List) per fornire permessi flessibili su file e directory.

Per abilitare le ACL, il filesystem deve essere montato con l'opzione `acl`. L'opzione `acl` è già abilitata su `XFS`, il filesystem CentOS predefinito, e di solito anche su filesystem `Ext3` e `Ext4`.

Abilitazione ACL

Sui filesystem Ext2/3/4, è possibile usare il comando `tune2fs` per verificare se l'opzione `acl` è già abilitata:

```
tune2fs -l /dev/sdXY | grep "Default mount options:"
```

In cui `sdXY` è il nome della partizione, l'output dovrebbe essere simile a questo:

```
Default mount options:    user_xattr acl
```

Se l'opzione `acl` non è abilitata, aggiungere l'opzione all'interno di `/etc/fstab`:

```
/dev/mapper/VolGroup-lv_root /                       ext4     defaults,acl        0
```

Oppure utilizzare `tune2fs` per abilitare la feature come opzione di mount predefinita:

```
tune2fs -o acl /dev/sdXY
```

4.17.2 Permessi di accesso

Se si è selezionato **Active Directory** come account provider, una cartella condivisa appartiene a un gruppo di utenti (*Owning group*). Ogni membro del gruppo è autorizzato a leggere il contenuto della cartella. Facoltativamente, il gruppo può avere il diritto di modificare il contenuto della cartella e l'autorizzazione di lettura può essere estesa a chiunque acceda al sistema. Questo semplice modello di autorizzazione si basa sulle tradizionali autorizzazioni del file system UNIX.

I permessi di accesso possono essere ulteriormente raffinati utilizzando le *ACL*, consentendo a singoli utenti o ad altri gruppi i permessi di lettura o scrittura.

Le ACL possono anche essere impostate su singoli file e directory da un client Windows, se l'utente dispone delle sufficienti autorizzazioni – fare riferimento alla sezione *Modifica autorizzazioni delle risorse dai client Windows* per i dettagli.

Avvertimento: Alcune impostazioni ACL supportate dai client Windows non possono essere convertite in ACL POSIX supportate da NethServer, quindi andranno perse in fase di propagazione

In qualsiasi momento, il pulsante *Reimposta permessi* propaga le autorizzazioni UNIX e le ACL POSIX alla cartella condivisa ai suoi contenuti.

Se è attiva l'opzione *Accesso guest*, sono considerate valide qualsiasi credenziali vengano presentate.

Se non è stato scelto alcun account provider o si è scelto LDAP, qualsiasi accesso alle cartelle condivise viene considerato come *Accesso ospite* in modo che a tutti sia consentito leggerne e scriverne il contenuto.

4.17.3 Accesso alla rete

SMB/CIFS è un protocollo molto diffuso che consente di condividere file in una rete di computer. Il nome della cartella condivisa diventa il nome della condivisione SMB.

Per esempio, l'indirizzo di rete SMB per la condivisione `docs` potrebbe essere

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

Avvertimento: L'accesso autenticato alle cartelle condivise è disponibile con un account provider Active Directory. Il provider LDAP consente solo l'accesso come guest.

Quando si accede ad una condivisione SMB, alcune interfacce utente forniscono un unico campo per indicare lo username. In questi casi fornire lo **user short name** anteposto dal **nome di dominio NetBIOS**. Ad esempio, se il nome di dominio NetBIOS fosse «DOMAIN» ed il nome utente fosse «john.smith», la stringa da utilizzare per accedere alla condivisione SMB sarebbe:

```
DOMAIN\john.smith
```

Al contrario, altre applicazioni mostrano dei campi di input separati per il nome di dominio NetBIOS e per il nome utente; in tal caso riempire i campi separatamente.

4.17.4 Cestino di rete

Se l'opzione *Cestino di rete* è abilitata, i file rimossi da una cartella condivisa vengono in realtà spostati in una directory «cestino» speciale. L'opzione *Mantieni più copie dei file con lo stesso nome* assicura che i file nel cestino abbiano sempre nomi distinti, impedendone la sovrascrittura.

4.17.5 Nascondere una cartella condivisa

Se è attiva l'opzione *Visibile*, la cartella condivisa sarà elencata fra le cartelle disponibili. Questa opzione non influisce sui permessi di accesso della cartella.

4.17.6 Share home

Ciascun utente di NethServer ha una condivisione personale mappata sulla sua home directory Unix. Il nome SMB della share corrisponde allo **user short name**. Ad esempio:

- user short name `john.smith`
- nome server `MYSERVER`
- indirizzo server `192.168.1.2`

L'indirizzo di rete SMB è:

```
\\MYSERVER\john.smith
\\192.168.1.2\john.smith
```

Fornire le credenziali dell'utente John come spiegato nella sezione *Accesso alla rete*.

Suggerimento: La directory home Unix viene creata al primo accesso dell'utente tramite SMB o via SFTP/SSH.

4.17.7 Modifica autorizzazioni delle risorse dai client Windows

Quando un utente si connette a una cartella condivisa con un client Windows, può modificare le autorizzazioni su singoli file e directory. Le autorizzazioni sono espresse dagli elenchi di controllo di accesso (ACL).

Avvertimento: Alcune impostazioni ACL supportate dai client Windows non possono essere convertite in ACL POSIX implementate da NethServer, quindi andranno perse in fase di propagazione

Solo il proprietario di una risorsa (che sia file o directory) ha il pieno controllo su di essa (lettura, scrittura, modifica delle autorizzazioni). L'autorizzazione per eliminare una risorsa è concessa agli utenti con permessi di scrittura sulla directory principale. L'unica eccezione a questa regola è descritta nella sezione *Accesso amministrativo*.

Quando viene creata una nuova risorsa, il proprietario può essere definito da una delle seguenti regole:

- il proprietario è l'utente che crea la risorsa
- il proprietario viene ereditato dalla directory padre

Per applicare una di queste regole, spostarsi nel menu *Windows file server* e selezionare l'opzione corrispondente nella sezione *Quando viene creato un nuovo file o directory in una cartella condivisa*.

Avvertimento: L'impostazione *Owning group* di una cartella condivisa non influisce sul proprietario di una risorsa. Vedi anche la sezione *Permessi di accesso* qui sopra

4.17.8 Accesso amministrativo

La pagina *Windows file server* consente di concedere privilegi speciali ai membri del gruppo `Domain Admins`:

- estendere l'autorizzazione del proprietario abilitando il *Assegna il controllo completo sulle cartelle condivise al gruppo Domain Admins*

- accedere alle home directory degli altri utenti abilitando *Concedi il pieno controllo sulle home directory al gruppo Domain Admins (home $ share)*. Per accedere alle home directory, è sufficiente connettersi alla condivisione nascosta `home $`. Ad esempio, l'indirizzo di rete SMB è:

```
\\MYSERVER\home$
\\192.168.1.2\home$
```

4.17.9 Auditing

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

Actions are logged to a file during the the day and are moved to a browseable database overnight.

The report web interface is available from the old Server Manager from the *Applications* page, while the new Server Manager (Cockpit) integrates a new interface inside the *File server* application.

4.18 Monitor banda

4.18.1 ntopng

ntopng è un potente strumento che permette di analizzare in tempo reale il traffico di rete. Consente di valutare la banda utilizzata dai singoli host e di individuare i protocolli di rete maggiormente usati.

Abilita ntopng Abilitando ntopng, tutto il traffico passante per le interfacce di rete verrà analizzato. Può causare un rallentamento della rete e un aumento del carico di sistema.

Porta Porta su cui raggiungere l'interfaccia web di ntopng.

Password per l'utente "admin" Password dell'utente amministratore. Questa password non è legata inalcun modo alla password di admin di NethServer.

Interfacce Interfacce su cui ntopng sarà in ascolto per eventuali richieste.

4.19 Statistiche (collectd)

Collectd è un software che raccoglie periodicamente statistiche sulle performance del sistema e le salva in speciali file RRD. Le statistiche sono quindi consultabili attraverso un'interfaccia web.

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

L'interfaccia web è accessibile dalla pagina *Grafici*.

Al termine dell'installazione, il sistema collezionerà le seguenti informazioni:

- utilizzo CPU
- carico di sistema
- numero di processi
- utilizzo memoria RAM
- utilizzo memoria virtuale (swap)
- tempo di accensione

- utilizzo spazio su disco
- operazioni di lettura e scrittura su disco
- interfacce di rete
- latenza di rete

Per ciascun controllo, l'interfaccia mostra un grafico che contiene sia l'ultimo valore raccolto, sia i valori minimi, massimi e medi.

4.19.1 Latenza di rete

Il plugin ping misura la latenza di rete. Ad intervalli regolari, collectd invia un ping al DNS configurato. Se la multi WAN è attiva, anche tutti i provider abilitati verranno controllati.

Host aggiuntivi possono essere monitorati (es. server web) usando una lista separata da virgole all'interno della proprietà `PingHosts`.

Esempio:

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

4.20 VPN

Una VPN (Virtual Private Network) consente di instaurare un collegamento sicuro e cifrato fra due o più sistemi utilizzando una rete pubblica come Internet.

Il sistema supporta due tipi di VPN:

1. roadwarrior: collegamento di un terminale remoto alla rete interna
2. net2net o tunnel: collegamento di due reti remote

4.20.1 OpenVPN

OpenVPN consente di creare facilmente collegamenti VPN, porta con sé numerosi vantaggi tra cui:

- Disponibilità di client per vari sistemi operativi: Windows, Linux, Apple, Android, iOS
- Attraversamento NAT multipli, ovvero non è necessario un IP statico dedicato al firewall
- Elevata robustezza
- Semplicità di configurazione

Roadwarrior

Il server OpenVPN in modalità roadwarrior consente il collegamento di client multipli.

I metodi di autenticazione supportati sono:

- utente di sistema e password
- certificato
- utente di sistema, password e certificato

Il server può operare in due modalità: routed o bridged. Si consiglia di scegliere la modalità bridged solo se il tunnel deve trasportare traffico non-IP.

Per consentire ad un client di stabilire una VPN:

1. Creare un nuovo account: è consigliato creare un account VPN dedicato che utilizzi un certificato. In questo modo non è necessario creare un utente di sistema per garantire l'accesso VPN.

   È invece obbligatorio scegliere un account di sistema se si desidera utilizzare l'autenticazione basata su nome utente e password.

2. Scaricare il file che contiene la configurazione e i certificati.

3. Importare il file all'interno del client ed avviare la VPN.

Tunnel (net2net)

Quando si crea una connessione OpenVPN net2net, un server ricopre il ruolo di master. Tutti gli altri server sono considerati slave (client).

Un client può essere collegato ad un altro NethServer od ad un qualsiasi altro firewall che utilizzi OpenVPN.

Tutti i tunnel utilizzano OpenVPN in modalità routed, ma esistono due tipi di topologie: *subnet* e *p2p* (Point to Point)

Topologia: subnet

Questa è la topologia consigliata. Nella topologia subnet, il server accetterà le connessioni e agirà come server DHCP per ogni client connesso.

In questo scenario

- il server gestisce l'autenticazione dei client utilizzando certificati TLS
- il server può eseguire il push delle rotte locali verso i client remoti
- il client si possono autenticare con certificati TLS o tramite nome utente e password

Topologia: P2P

Nella topologia p2p, l'amministratore deve configurare un server per ciascun client.

In questo scenario:

- l'unico metodo di autenticazione supportato è la PSK (Pre-Shared Key). Si consiglia di utilizzare un canale sicuro (come SSH o HTTPS) per scambiare la PSK
- l'amministratore deve selezionare un IP per entrambi gli end point
- le rotte per le reti remote devono essere configurate su ogni end point

Per configurare un tunnel procedere come segue:

1. Accedere al server del tunnel e aprire la pagina *OpenVPN tunnels*, spostarsi nella scheda *Tunnel servers* e cliccare sul bottone *Create new*

2. Valorizzare i campi richiesti ponendo attenzione al fatto che:

   - guilabel:*Public IPs and/or public FQDN* è una lista di IP pubblici o di nomi host che verranno usati dai client per collegarsi al server attraverso Internet
   - *Local networks* è una lista di reti locali che saranno accessibili dai server remoti. Se la topologia è di tipo p2p, la stessa lista sarà utilizzata per valorizzare il campo *Remote networks* del client
   - *Remote networks* è una lista di reti remote che si trovano dietro al server remoto e che saranno accessibili dagli host della rete locale

3. Dopo aver salvato la configurazione, cliccare sull'azione *Download* e selezionare *Configurazione client*
4. Accedere al client del tunnel, aprire la pagina *OpenVPN tunnels*, spostarsi sulla scheda *Tunnel clients* e cliccare sul bottone *Upload*

Funzionalità avanzate

L'interfaccia web consente di configurare funzionalità avanzate quali:

- lato client, nel campo *Remote hosts* possono essere specificati indirizzi multipli per ridondanza; il client OpenVPN tenterà di connettersi a ciascun host rispettando l'ordine di inserimento
- WAN priority: se il client ha più WAN (interfacce red), l'opzione consente di selezionare l'ordine in cui le WAN saranno utilizzate per connettersi al server remoto.
- Protocollo: è importante rammentare che OpenVPN è progettata per funzionare in modo ottimale in UDP, ma è possibile utilizzare TCP nelle situazioni in cui non è possibile fare ricorso ad UDP
- cifratura: l'algoritmo crittografico utilizzato per crittografare tutto il traffico. Se non viene selezionato in modo esplicito, il server e il client cercheranno di negoziare la migliore cifratura disponibile su entrambi i lati
- compressione LZO: abilitata di default, può essere disabilitata quando si utilizzano server or client legacy

Modalità legacy

I tunnel possono ancora essere creati utilzzando gli account roadwarrior.

I passi da eseguire sul server master sono:

- Abilitare il server roadwarrior
- Creare un account solo VPN per ciascun slave che dovrà collegarsi
- Durante la creazione dell'account ricordarsi di specificare la rete remota configurata dietro allo slave

I passi da eseguire sullo slave sono:

- Creare un client dalla pagina *Client* specificando i dati di collegamento al server master
- Copiare e incollare il contenuto dei certificati scaricati dalla pagina di configurazione del master

4.20.2 IPsec

Il protocollo IPsec (IP Security) è lo standard «de facto» nei tunnel VPN, utilizzato tipicamente per creare tunnel di tipo net to net ed è supportato da tutti i produttori. È possibile utilizzare questo protocollo per creare tunnel VPN tra un NethServer ed un dispositivo di un altro produttore nonché tunnel VPN tra 2 NethServer.

Nota: IPSec non è progettato per collegare singoli host ma per la configurazione net2net, questo implica due gateway su entrambe le estremità (almeno un'interfaccia RED e una GREEN).

Tunnel (net2net)

IPsec è estremamente affidabile e compatibile con molti dispositivi. Infatti, è una scelta ovvia quando è necessario creare collegamenti net2net tra firewall di diversi produttori.

A differenza della configurazione OpenVPN, in un tunnel IPsec, i firewall sono considerati nodi pari livello.

Se si sta creando un tunnel tra due NethServer, dati A e B i firewall:

1. Configurare il server A e specificare l'indirizzo remoto e la LAN del server B. Se il campo *Remote IP* è valorizzato con `% any`, il server rimane in attesa della connessione dell'altro endpoint.
2. Configurare il secondo firewall B replicando la configurazione da A all'interno della sezione remota. Il valore speciale `%any` è consentito in un solo lato!

Se un endpoint è dietro un NAT, i valori per *Local identifier* e *Remote identifier* devono essere impostati con nomi univoci personalizzati preceduti da `@`. I nomi comuni sono le posizioni geografiche dei server, ad esempio il nome di stato o città.

4.21 Nextcloud

Nextcloud è una soluzione flessibile per la sincronizzazione dei file e la loro condivisione. È possibile avere i propri file sempre a portata di mano su ogni dispositivo, utilizzando un dispositivo mobile, un personal computer, una workstation o un accesso web. La condivisione viene realizzata in maniera semplice, sicura e privata che significa avere il pieno controllo dei propri dati.

Funzionalità:

- configurazione automatica di Nextcloud con database MariaDB con credenziali di default
- integrazione automatica con gli utenti e gruppi di sistema di NethServer
- backup dei dati automatico tramite nethserver-backup-data
- personalizzare l'URL di accesso https (host virtuale personalizzato)

4.21.1 Installazione

È possibile installare NethServer tramite l'interfaccia web di NethServer. Dopo l'installazione:

- collegarsi all'url https://your_nethserver_ip/nextcloud
- usare le credenziali di default **admin/Nethesis,1234**
- cambiare la password di default

Ciascun utente presente nel sistema può accedere automaticamente tramite le sue credenziali, indipendentemente dal provider utenti utilizzato (vedi *Utenti e gruppi*). Dopo l'installazione sarà presente anche un nuovo widget applicazioni nella dashboard di NethServer.

Nota: La procedura di aggiornamento/cambio di versione di Nextcloud disabilita le app per evitare problemi di compatibilità. I registri del server tengono traccia di quali app sono state disabilitate. Dopo una corretta procedura di aggiornamento / cambio di versione è possibile utilizzare la pagina Applicazioni per aggiornare e riattivare le app.

Nota: La versione 13 di Nextcloud utilizza il nuovo PHP 7.1 (*nethserver-rh-php71-php-fpm*) mentre la versione precedente utilizza PHP 5.6 (*nethserver-rh-php56-php-fpm*). È possibile rimuovere php56 (se non ci sono problemi di dipendenze) con il comando «yum remove nethserver-rh-php56-php-fpm».

Lista utenti

Tutti gli utenti vengono elencati nel pannello dell'amministratore di NextCloud utilizzando un identificativo alfanumerico univoco. In questo modo il sistema garantisce l'assenza di duplicati nei nomi utente interni, come spiegato nella sezione *Internal Username* della Documentazione ufficiale di NextCloud.

Nota: Se NethServer è attestato ad un account provider remoto Active Directory, un account utente AD aggiuntivo e dedicato è necessario al modulo per essere pienamente operativo! Fare riferimento alla sezione *Join ad un dominio Active Directory esistente*.

4.21.2 Host virtuale personalizzato

Per personalizzare l'url web di Nextcloud:

```
config setprop nextcloud VirtualHost mynextcloud.domain.com
config setprop nextcloud TrustedDomains mynextcloud.domain.com
signal-event nethserver-nextcloud-update
```

Se si utilizza *let's encrypt* ricordarsi di aggiungere il nome di dominio all'elenco dedicato.

4.21.3 Trusted Domains

I Trusted domains sono una lista di domini su cui l'utente può effettuare il login. Quelli presenti di default sono:

- nome dominio
- indirizzo ip

Per aggiungerne uno nuovo eseguire:

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

Per aggiungerne più di uno è sufficiente concatenare i nomi con una virgola.

4.21.4 CalDAV e CardDAV

Alcuni client CalDAV e CardDAV possono avere problemi nel trovare l'URL di sincronizzazione appropriato e richiedono il rilevamento automatico dei servizi. L'individuazione del servizio è abilitata per impostazione predefinita se è stato configurato un host virtuale personalizzato per Nexcloud.

Per abilitare il rilevamento automatico dei servizi anche se Nextcloud è in esecuzione sul FQDN principale, nella sottocartella `nextcloud`, assicurarsi che WebTop o SOGo non siano installati. Quindi eseguire:

```
config setprop nextcloud Wellknown enabled
signal-event nethserver-nextcloud-update
```

4.22 FTP

Nota: Il protocollo FTP è insicuro: le password sono inviate in chiaro.

Il server FTP consente di trasferire file fra client e server.

Un utente FTP può essere *virtuale* oppure un utente di sistema. Gli utenti virtuali possono accedere solo al server FTP: questa è la configurazione consigliata. L'interfaccia web consente la configurazione solo degli utenti virtuali.

Quando accede al server FTP, un utente può esplorare l'intero filesystem a seconda dei suoi privilegi. Per evitare di esporre involontariamente informazioni, l'utente può essere confinato in una directory usando l'opzione *chroot* : l'utente non potrà uscire dalla directory in cui è stato confinato.

Questa configurazione può essere usata in caso le cartelle condivise siano usate come un semplice web hosting. Aggiungere il percorso della cartella condivisa nel campo chroot personalizzato. Ad esempio, data una cartella condivisa chiamata *miosito*, inserire questo percorso:

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

L'utente FTP virtuale potrà accedere solo alla directory specificata.

4.22.1 Utenti di sistema

Avvertimento: Questa configurazione è altamente sconsigliata.

Dopo aver abilitato gli utenti di sistema, gli utenti virtuali saranno disabilitati. Tutta la configurazione deve essere eseguita da linea di comando.

Abilitare gli utenti di sistema:

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

Dato l'utente *goofy*, per prima cosa assicurarsi che sia abilitato per l'accesso remoto da shell. Vedi Accesso ai servizi. Quindi, abilitare l'accesso:

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

Per disabilitare l'accesso ad un utente precedentemente abilitato:

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

Se non esplicitamente disabilitato, tutti gli utenti di sistema hanno l'opzione di chroot all'interno della propria home. Per disabilitare il chroot di un utente di sistema:

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

4.23 Phone Home

Nel wizard di prima configurazione, si può decidere di non contribuire alle statistiche di utilizzo. Il phone home viene usato per tenere traccia di tutte le installazioni di NethServer nel mondo. Ogni volta che si installa un nuovo NethServer, questa applicazione invia alcuni dettagli sull'installazione a un server centrale. Le informazioni vengono memorizzate in un database e utilizzate per mostrare dei marcatori in una mappa Google contenente il numero di installazioni attive raggruppate per paese e versione.

4.23.1 Panoramica

Questa applicazione è *abilitata* di default.

Per disabilitarlo in seguito, eseguire: `config setprop phone-home status disabled`

Se il phone home è *abilitato* le informazioni inviate sono:

- UUID: che si trova in `/var/lib/yum/uuid`
- RELEASE: ottenuto da `/sbin/e-smith/config getprop sysconfig Version`

Tutte le informazioni sono usate per popolare la mappa.

4.24 SNMP

Il protocollo SNMP (Simple Network Management Protocol) consente la gestione e il monitoraggio di apparati collegati in rete. Il server SNMP è in grado di rispondere a richieste specifiche riportando lo stato in tempo reale del sistema.

Il server è disabilitato di default.

Per abilitarlo è necessario configurare tre parametri principali:

- il nome della comunità SNMP
- il nome del luogo in cui risiede il server
- il nome e l'indirizzo mail dell'amministratore di sistema

L'implementazione si basa sul progetto Net-SNMP. Per ulteriori informazioni, consultare la pagina ufficiale del progetto:

http://www.net-snmp.org/

Riferimenti

4.25 Hotspot (Dedalo)

L'obiettivo principale di un hotspot è fornire connettività internet via wi-fi agli utenti occasionali. Gli utenti vengono inviati a un captive portal attraverso il quale possono accedere alla rete autenticandosi tramite social, sms o email. Il servizio di hotspot consente la regolamentazione, la responsabilità e il prezzo dell'accesso a internet in luoghi pubblici, come punti internet, hotel e fiere.

Funzioni principali:

- Separazione rete aziendale e rete ospiti

- gli ospiti possono autenticarsi utilizzando l'accesso social (Facebook, Instagram, Linkedin) così come gli sms od una e-mail
- servizio a pagamento basato su voucher
- hotspot manager con livelli di accesso diversi (amministratore, cliente, desk)
- limitazione di banda per ciascun utente
- Esportazione elenco account e report delle connessioni (non ancora implementato)

4.25.1 Come funziona?

L'implementazione è basata su 2 componenti:

- un hotspot manager remoto con una Web GUI in esecuzione su un server cloud che consente di:
  - creare un'istanza hotspot: in genere ogni istanza viene indirizzata a una posizione specifica (ad esempio Art Cafè, Ritz Hotel e così via)
  - modificare la pagina del captive portal
  - scegliere il tipo di login da utilizzare
  - vedere le sessioni e gli utenti collegati
- una parte client (dedalo) installata su un NethServer fisicamente connesso alla rete di access point: consente di assegnare gli indirizzi IP ai client della rete Wi-Fi e li reindirizza al captive portal per l'autenticazione.

Per informazioni più dettagliate, consultare https://nethesis.github.io/icaro/docs/components/.

4.25.2 Installazione

- installare il componente server: https://nethesis.github.io/icaro/docs/provisioning/ Questa procedura utilizza Vagrant per fornire un droplet Digital Ocean (DO). Se si preferisse utilizzare un altro provider cloud, il file Vagrant andrà modificato di conseguenza.
- configurare il server in modo da rendere possibile l'accesso: https://nethesis.github.io/icaro/docs/configuration/
- installare il componente client nel proprio NethServer: https://nethesis.github.io/icaro/docs/client_installation/
- è importante ricordare che per l'installazione sono necessarie almeno 3 interfacce Ethernet:
  - 1 per i client LAN, contrassegnata con il ruolo green (necessaria anche se non utilizzata, può essere una VLAN)
  - 1 (o più) per la connessione Internet, contrassegnato con il ruolo red
  - 1 per Dedalo, con il ruolo hotspot

4.25.3 Configurazione

Interfaccia hotspot manager

- accedere all'hotspot manager
- spostarsi nella sezione *Manager* e creare un nuovo *Manager* di tipo *Rivenditore* o *Cliente*. Maggiori informazioni su possibili *Ruoli* sono disponibili qui: https://nethesis.github.io/icaro/docs/manager/.
- eseguire il logout e accedere con il nuovo manager appena creato

- spostarsi nella sezione *Hotspot* e creare una nuova istanza hotspot
- fare clic sul nome dell'hotspot e configurare il captive portal

Unità Hotspot su NethServer

- spostarsi nella sezione *Unità Hotspot* su NethServer
- modificare i parametri nella pagina *Registrazione unità hotspot*:
  - `Nome host`: nome pubblico dell'Hotspot Manager
  - `Nome utente`: account utente funzionante (rivenditore o cliente)
  - `Password` : password

Successivamente, scegliere l'interfaccia ethernet su cui l'hotspot sarà attivato.

Se il proxy web è attivo, un flag specifico nella pagina dell'unità hotspot consentirà di inoltrare tutto il traffico hotspot (protocolli http e http) al proxy web per scopi di registrazione (attenzione alle implicazioni sulla privacy!).

- connettere un AP all'interfaccia hotspot.

Configurazione Access Point

L "Access Point (AP) deve svolgere la sola funzione di abilitare la connessione con il firewall, dove comportarsi come un normale switch di rete. E" necessario ricordare di:

- configurare l'access point senza autenticazione e senza DHCP
- disabilitare qualsiasi servizio (servizi di sicurezza, ecc.) per evitare interferenze con il comportamento dell'hotspot
- se si usano più AP configurali con SSID diversi (es: 1-SCUOLA / SCUOLA-2 / . . .) per identificare facilmente eventuali AP malfunzionanti
- configurare l'AP con un indirizzo IP statico su un segmento di rete (rfc-1918) diverso da quello utilizzato dall'hotspot
- se possibile, abilitare la «client isolation», per evitare il traffico tra i client connessi all'access point
- configurare l'AP per lavorare su diversi canali per ridurre al minimo le interferenze, un buon AP consente di gestire i canali automaticamente o di selezionarli manualmente
- non utilizzare prodotti troppo scadenti, AP di bassa qualità possono provocare frequenti disconnessioni che poi impattano sulla qualità del servizio generale, la raccomandazione è ancora più importante nel caso si utilizzino dei repeater

A scopo di test, è possibile collegare un laptop o un PC tramite cavo ethernet all'interfaccia hotspot invece di una rete Wi-Fi. Questo può essere molto utile se si verificano problemi e si desidera verificare se siano causati dal servizio hotspot o dalla rete AP.

Modalità Free e Modalità Voucher

La modalità Free (predefinita) consente di effettuare il login in autonomia senza la necessità di alcun codice, cliccando sul social desiderato (o tramite sms od e-mail).

La modalità Voucher obbliga a creare un voucher (in pratica «un codice») che andrà utilizzato da tutti gli utenti, solo gli utenti con il voucher potranno effettuare il login.

4.26 FreePBX

FreePBX è una applicazione web open source che controlla e gestisce Asterisk (PBX), un software di comunicazione open source (https://www.freepbx.org/).

4.26.1 Installazione

E" possibile installare FreePBX dal gestore pacchetti di NethServer, il modulo si chiama «FreePBX».

Tutte le configurazioni e i dati di FreePBX sono salvati nei backup configurazione e dati.

4.26.2 Accesso Web

Dopo l'installazione, FreePBX è accessibile all'indirizzo `https://ip_address/freepbx` dalle interfacce green. E" anche possibile configurare l'accesso da interfaccia red della pagina «Accesso PBX» nel Server Manager di NethServer.

4.26.3 FwConsole

La fwconsole è uno strumento che consente all'utente di compiere alcune azioni amministrative su FreePBX (vedi il wiki di FreePBX <https://wiki.freepbx.org/pages/viewpage.action?pageId=37912685>‘_). Per poterla usare con NethServer è necessario utilizzare scl:

```
/usr/bin/scl enable rh-php56 "/usr/sbin/fwconsole"
```

4.26.4 Documentazione avanzata

Per ulteriori informazioni è possibile consultare la documentazione di FreePBX all'indirizzo: https://wiki.freepbx.org

4.27 HotSync

Avvertimento: Il moduflo HotSync è da considerarsi una release beta. Pertanto è opportuno provarla in ambienti di test prima di procedere in produzione.

HotSync mira a ridurre i tempi di inattività in caso di problemi, sincronizzando il NethServer con un altro sistema gemello, che verrà attivato manualmente in caso di guasto del server master.

Normalmente, quando si verifica un problema hardware, il tempo necessario per ripristinare il servizio è:

1. riparazione/approvvigionamento nuovo server: da 4h a 2 giorni
2. installazione sistema operativo: 30 minuti
3. ripristino backup: da 10 minuti a 8 ore

In sintesi, gli utenti possono ricominciare a lavorare con i dati della notte precedente al guasto dopo alcune ore/giorni. Utilizzando hotsync, il tempo per le fasi 1 e 3 è praticamente 0, per la fase 2 è ridotto a 5 minuti (tempo per attivare il server di riserva). Gli utenti possono ricominciare a lavorare in pochi minuti, utilizzando i dati di alcuni minuti prima del crash.

Per impostazione predefinita, tutti i dati inclusi nel backup vengono sincronizzati ogni 15 minuti. Anche i database MariaDB sono sincronizzati, a meno che la sincronizzazione dei database non sia disabilitata. Le applicazioni che utilizzano PostgreSQL sono sincronizzate (Mattermost, Webtop5) a meno che la sincronizzazione dei database non sia disabilitata.

4.27.1 Terminologia

- MASTER è il sistema di produzione SLAVE è il server di riserva
- SLAVE è acceso, con un indirizzo IP diverso da MASTER
- Ogni 15 minuti, MASTER esegue un backup su SLAVE
- Un'e-mail viene inviata a root (admin se è installato il server di posta)

4.27.2 Installazione

Per installare nethserver-hotsync su MASTER e SLAVE, esegure dalla riga di comando:

```
yum install nethserver-hotsync
```

4.27.3 Configurazione

Master

```
[root@master]# config setprop rsyncd password <PASSWORD>
[root@master]# config setprop hotsync role master
[root@master]# config setprop hotsync SlaveHost <SLAVE_IP>
[root@master]# signal-event nethserver-hotsync-save
```

Slave

```
[root@slave]# config setprop rsyncd password <PASSWORD>
[root@slave]# config setprop hotsync role slave
[root@slave]# config setprop hotsync MasterHost <MASTER_IP>
[root@slave]# signal-event nethserver-hotsync-save
```

La `<PASSWORD>` deve essere la stessa sul master e sullo slave.

Se mysql o postgresql sono installati, saranno sincronizzati per impostazione predefinita. Per disabilitare la sincronizzazione dei database

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

Abilitazione/Disabilitazione

Hotsync è abilitato di default. Per disabilitarlo:

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

e per riabilitarlo:

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

4.27.4 Ripristino: promuovere lo SLAVE in produzione

La seguente procedura mette in produzione lo SLAVE in caso di arrewsto anomalo del master.

1. spegnere il MASTER
2. se lo SLAVE deve funzionare come gateway di rete, collegarlo al router/modem con un cavo di rete
3. sullo SLAVE, se si è connessi tramite una console ssh, lanciare il comando `screen`, per fare in modo che la sessione sopravviva in caso di interruzioni di rete:

   ```
   [root@slave]# screen
   ```

4. lanciare sullo SLAVE il seguente comando e leggere attentamente l'output generato

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

5. spostarsi nella pagina `Rete` del Server Manager e riassegnare i ruoli alle interfacce di rete secondo necessità
6. lanciare il comando

   ```
   [root@slave]# /sbin/e-smith/signal-event post-restore-data
   ```

7. aggiorna il sistema alla versione più recente dei pacchetti

   ```
   [root@slave]# yum clean all && yum -y update
   ```

8. se sul MASTER era configurato un backup su USB, collegare il disco di backup allo SLAVE

4.27.5 Pacchetti supportati

- nethserver-nextcloud
- nethserver-mysql
- nethserver-dnsmasq
- nethserver-squidguard
- nethserver-pulledpork
- nethserver-antivirus
- nethserver-samba-audit
- nethserver-freepbx > 14.0.3
- nethserver-webtop5 (lo stato di z-push non è sincronizzato)
- nethserver-collectd
- nethserver-cups
- nethserver-dc
- nethserver-letsencrypt

- nethserver-nextcloud
- nethserver-sssd
- nethserver-directory
- nethserver-ibays
- nethserver-mail-server

4.28 Macchine virtuali

NethServer è in grado di eseguire macchine virtuali attraverso un modulo basato su KVM e libvirt, ma non una interfaccia web per la loro gestione.

Il software per la virtualizzazione può essere installato e avviato utilizzando la linea di comando, eseguendo:

```
yum install --setopt=base.enablegroups=1 @virtualization-hypervisor @virtualization-
↪tools @virtualization-platform
systemctl enable libvirtd
systemctl start libvirtd
```

Se NethServer svolge il ruolo di server DHCP, l'istanza di Dnsmasq avviata da libvirtd provocherà un conflitto con principale. Per evitare il problema è necessario rimuovere la rete NAT `default` di libvirt:

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

Successivamente il sistema sarà pronto per essere gestito attraverso Virtual Machine Manager (virt-manager), un'interfaccia utente per desktop Linux per la gestione di macchine virtuali tramite libvirt.

Lanciato virt.-manager sul proprio desktop Linux, sarà sufficiente creare una nuova connessione verso NethServer utilizzando il protocollo SSH.

4.28.1 Risorse esterne

Per maggiori informazioni fare riferimento a:

- Sito ufficiale Virtual Machine Manager
- Virtual Machine Manager on RHEL
- Introduction to virtualization
- FAQ KVM/Libvirt

4.29 Fail2ban

Fail2ban esegue la scansione dei file di log (ad esempio `/var/log/apache/error_log`) e blocca gli IP che manifestano comportamenti potenzialmente dannosi: troppi errori di password, ricerca di exploit, ecc. In generale Fail2Ban viene quindi utilizzato per aggiornare le regole del firewall per rifiutare le richieste da questi indirizzi IP per un determinato periodo di tempo, sebbene sia possibile configurare qualsiasi altra azione arbitraria (ad esempio l'invio di un'e-mail). Fail2Ban viene fornito con a bordo una serie filtri per vari servizi (Apache, Dovecot, Ssh, Postfix, ecc.).

Fail2Ban è in grado di ridurre il tasso di tentativi di autenticazione errati, tuttavia non può eliminare il rischio che presenta un'autenticazione debole. Per migliorare la sicurezza, aprire l'accesso ai servizi alle sole reti conosciute e protette utilizzando il firewall.

4.29.1 Installazione

Installare il modulo dal Software Center o usando la riga di comando:

```
yum install nethserver-fail2ban
```

4.29.2 Impostazioni

Fail2ban è configurabile tramite una apposita voce presente nella categoria sicurezza del server-manager. La maggior parte delle impostazioni possono essere modificate nella scheda *Configurazione*, solo le impostazioni più avanzate devono essere configurate dal terminale.

Jail

Le jail vengono abilitate e iniziano a proteggere i vari servizi non appena si installa un nuovo modulo, la jail relativa ad un servizio (se esistente) viene automaticamente attivata dopo l'installazione del pacchetto.

Ogni jail può essere individualmente disabilitata dalle impostazioni Jail

Numero di tentativi Numero di corrispondenze (vale a dire il valore del contatore) che attiva l'azione di divieto sull'IP.

Arco di tempo Il contatore viene impostato a zero se non viene trovata nei log alcuna corrispondenza entro i secondi di «ricerca» configurati.

Tempo di ban Periodo di permanenza in ban di un IP.

La jail recidivo è permanente Quando un IP passa più volte in una jail, la jail recidiva vieta l'IP per un tempo molto più lungo. Se abilitata l'opzione, il ban è perpetuo.

Consenti ban sulla LAN

Consente i ban sulla LAN Per impostazione predefinita, i tentativi falliti dalla rete locale vengono ignorati, tranne quando è stata attivata l'opzione.

IP7reti in whitelist Gli IP elencati nell'area di testo non verranno mai bannato da fail2ban (va indicato un IP per riga). E" possibile consentire intere reti inserendole nel pannello Reti fidate.

Email

Invia notifiche email Abilitando l'opzione verranno inviate email agli amministratori.

Email amministratori Elenco di indirizzi email degli amministratori (un indirizzo per riga).

Notifica eventi di abilitazione/disabilitazione di una jail Invia notifiche via email all'avvio o all'arresto di una jail.

4.29.3 Unban IP

Gli IP sono oggetto di ban quando vengono trovati più volte nei log, in uno specifico arco di tempo. Vengono archiviati in un database per essere nuovamente bannati ogni volta che si riavvia il server o il servizio. Per sbloccare un IP è possibile utilizzare la scheda *unban IP* disponibile nella categoria stato del server-manager.

4.29.4 Statistiche

La scheda *Ban statistics*, disponibile nella categoria stato del server-manager, fornisce il numero di ban per jail e totale.

4.29.5 Strumenti

Fail2ban-client

Fail2ban-client fa parte dell'rpm di fail2ban, fornisce lo stato di fail2ban e tutte le jail disponibili:

```
fail2ban-client status
```

Per ispezionare una jail specifica:

```
fail2ban-client status sshd
```

Per verificare quali file di log siano monitorati da una jail:

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

Fail2ban-listban

Fail2ban-listban permette di contare gli IP attualmente bannati nelle varie jail attivate e mostra anche gli IP che risultano bannati da shorewall.

```
fail2ban-listban
```

Fail2ban-regex

Fail2ban-regex è uno strumento che viene utilizzato per testare le regex sui log, è una parte del software fail2ban. È consentito un solo filtro per jail, ma è possibile specificare diverse azioni, su righe separate.

La documentazione è **'consultabile sul sito del progetto fail2ban<http://fail2ban.readthedocs.io/en/latest/filters.html>'_**.

```
fail2ban-regex /var/log/YOUR_LOG /etc/fail2ban/filter.d/YOUR_JAIL.conf --print-all-
↪matched
```

E" possibile anche testare direttamente una regex personalizzata:

```
fail2ban-regex /var/log/secure '^%(__prefix_line)s(?:error: PAM: )?[aA]uthentication␣
↪(?:failure|error) for .* from <HOST>( via \S+)?\s*$'
```

Fail2ban-unban

Fail2ban-unban è utilizzabile per sbloccare un IP nel caso in cui il ban debba essere rimosso manualmente.

```
fail2ban-unban <IP>
```

È possibile utilizzare anche il comando integrato con fail2ban-client:

```
fail2ban-client set <JAIL> unbanip <IP>
```

4.29.6 Whois

Se si desidera ottenere informazioni sull'origine dell'IP bannato via e-mail, è possibile utilizzare il database `whois` installando l'rpm `whois`.

4.30 Rspamd

Rspamd è il nuovo motore antispam di NethServer, sostituisce SpamAssassin e Amavisd-new.

La documentazione ufficiale di Rspamd è disponibile all'indirizzo https://rspamd.com

Rspamd viene installato dal modulo *Email*, disponibile nel *Software center*. Il menu attraverso cui attivarlo e modificarne le impostazioni si trova nella pagina *Email* > *Filtro*. Per maggiori informazioni fare riferimento alla sezione *Email filter*.

4.30.1 Interfaccia web di Rspamd

Il componente antispam è implementato tramite Rspamd che fornisce una sua interfaccia web amministrativa all'url:

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

L'URL è disponibile anche nella pagina *Applicazioni* del *server-manager*. Di default, l'accesso all'interfaccia è concesso ai membri del gruppo `domain admins` ed all'utente `admin` (vedi anche *Account admin*). Esiste anche un account speciale aggiuntivo `rspamd` che può essere usato per accedervi. Le sue credenziali sono disponibili da *Email> Filtro> Interfaccia utente Rspamd (URL Web)*: è sufficiente seguire il link indicato.

Interfaccia utente Web di Rspamd

- visualizza messaggi e contatori delle azioni,
- mostra la configurazione del server,
- tiene traccia della cronologia dei messaggi recenti,
- consente di addestrare i filtri Bayesiani inviando un messaggio attraverso una interfaccia web.

Status

È il menu principale, le statistiche globali sono relative al servizio Rspamd.

Troughput

I grafici visualizzati in questo menu illustrano l'attività del software antispam. È possibile regolare la scala temporale (oraria, giornaliera, settimanale, mensile) e modificare alcune altre impostazioni per adattare i grafici alle proprie necessità

Configuration

Il menu *Configuration* > *Lists* consente di modificare la lista di IP/domini/mime autorizzati per i vari moduli. Quelli disponibili sono:

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

Volendo creare una lista di eccezioni per un modulo, sarà sufficiente utilizzare il percorso `/var/lib/rspamd/`, la lista sarà modificabile direttamente dall'interfaccia web di Rspamd.

Symbols

Rspamd usa il concetto di simbolo per aumentare o diminuire il punteggio di spam quando le relative regole vengono intercettate. Il peso del simbolo è modificabile, il punteggio negativo è relativo a messaggi di posta elettronica validi, quello positivo a messaggio di spam.

Individuare le corrispondenze dei simboli

Il metodo più comodo è quello offerto dall'interfaccia web, menu *History* > *History*.

Modificare il peso di un simbolo

Il modo più semplice per cambiare il peso del simbolo è utilizzare l'interfaccia utente di Rspamd: *Symbols* > *Symbols*. Per rintracciare un simbolo e modificarne il peso è disponibile una campo di ricerca.

- Il punteggio di spam associato ad un simbolo è indicato in rosso (punteggio positivo)
- Il punteggio di ham associato ad un simbolo è indicato in verde (punteggio negativo)

Se si desidera rimuovere le impostazioni personalizzate, è possibile modificare il file `/var/lib/rspamd/rspamd_dynamic` o rimuoverli tramite l'interfaccia Web di Rspamd: *Configuration* > *Lists* > *rspamd_dynamic*

È possibile modificare manualmente i punteggi dei simboli attraverso i file `/etc/rspamd/scores.d/*_group.conf` in cui i simboli sono raccolti per gruppi. Come per i moduli, è possibile sovrascrivere le impostazione riportate nei file `/etc/rspamd/local.d/*_group.conf` e :file:'/etc/rspamd/override.d/*_group.conf.

Ordine di priorità

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

Learning

Lo scopo del menu *Learning* è di addestrare il filtro Bayes, attraverso cui è possibile far apprendere a rspamd se una e-mail è uno spam o un ham utilizzando direttamente la sorgente della email attraverso l'area di testo dedicata.

Scan

Il menu *Scan* può essere usato per scansionare direttamente un'e-mail e controllarne il punteggio e i simboli corrispondenti.

History

L'interfaccia web di Rspamd può essere utilizzata per visualizzare il punteggio di spam totalizzato da un'email e la eventuale azione intrapresa dal sistema, vedi *History* > *History*

Si può visualizzare l'elenco di simboli facendo clic sul campo dell'email, aiuterà a capire l'azione eseguita (reject, add_header, no_action, rewrite_subject, greylist) e raccogliere informazioni utili come:

- il mittente
- il destinatario
- l'oggetto
- il punteggio totale

4.30.2 Moduli

Rspamd ha un approccio modulare, non tutti i moduli sono abilitati di default e sono personalizzabili dall'amministratore di sistema. Le impostazioni di default di ogni modulo sono contenute nel file `/etc/rspamd/modules.d/MODULE_NAME.conf`, il cui il nome è relativo al modulo.

Per esigenze particolari fare riferimento alla documentazione con la lista completa dei moduli.

Disabilitare un modulo

La disabilitare un modulo andrebbe fatta solo se strettamente necessario. Ad esempio, se un mittente avesse il suo IP in una blacklist, il modulo ip_score potrebbe fornire un punteggio alto di spam.

In questo caso si potrebbe disabilitare il modulo ma molti moduli (come ip_score) implementano una whitelist per evitare di controllare un IP o un dominio contro il filtro spam.

Creare un file (con il nome inerente al relativo modulo) `/etc/rspamd/override.d/MODULE_NAME.conf` che contenga

```
enabled = false;
```

Riavviare Rspamd

```
systemctl restart rspamd
```

Modificare la configurazione di un modulo

Tutte le configurazioni predefinite di un modulo sono contenute nel file `/etc/rspamd/modules.d/MODULE_NAME.conf`, NethServer utilizza il file `/etc/rspamd/local.d/MODULE_NAME.conf` per modificare i parametri predefiniti. Quindi il metodo più indicato per effettuare delle modifiche ai valori di default di Rspamd e di NethServer. Il file override usa i nuovi parametro con una priorità più alta, tutte le precedenti impostazioni vengono mantenute.

Ordine di priorità

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

In questo esempio si vuole implementare un elenco di IP da mettere in whitelist per il modulo ip_score.

Creare un file `/etc/rspamd/override.d/ip_score.conf` con il seguente contenuto

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

Riavviare rspamd

```
systemctl restart rspamd
```

La whitelist è modificabile dall'interfaccia web di Rspamd, dal menu guilabel:*Configuration* > *Lists* > *ip_score_whitelist*

Nota: Il percorso `/var/lib/rspamd` è di proprietà di Rspamd, tutti i file contenuti sono modificabili dal software

4.30.3 Domande frequenti

Le FAQ ufficiali per Rspamd sono disponibili al link https://rspamd.com/doc/faq.html

4.31 Aggiornamento Email a Rspamd

Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *Proxy POP3* sono basate sul motore di filtraggio Rspamd[1].

- Installazioni precedenti di NethServer verranno automaticamente aggiornate con Rspamd come descritto in in questa sezione.
- Le nuove funzionalità di configurazione, specifiche dell'implementazione basata su Rspamd, sono documentate nella sezione *Email*. Ecco una breve lista:
  - Firma DKIM
  - Interfaccia web di Rspamd
  - Soglia Greylist[3]

[1] Rspamd – Fast, free and open-source spam filtering system. https://rspamd.com/

[3] Greylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using greylisting will «temporarily reject» any email from a sender it does not recognize – Wikipedia

4.31.1 Funzionalità modificate

Aggiungere un avviso legale

La funzionalità *Email> Domini> Aggiungi una nota legale ai messaggi inviati* (nota anche come» Disclaimer «) è stata divisa in un pacchetto opzionale separato:‘ *nethserver-mail2-disclaimer*‘. Le nuove installazioni dovrebbero evitarne l’uso, poiché si basa su un vecchio pacchetto [#ALTERMIME] _ che potrebbe venire rimosso nelle versioni future.

Blocco porta 25

Il blocco della porta 25 può prevenire l’abuso da parte dei PC in LAN. Se il sistema è il gateway della rete, l’amministratore può creare una regola di firewall in *Regole*.

Host alias addizionali

I seguenti nomi di host erano automaticamente registrati nel servizio DNS, se `postfix/MxRecordStatus` era `enabled`:

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

In caso di aggiornamento dal vecchio modulo Email basato su Amavisd, il record `postfix/MxRecordStatus` viene rimosso e gli alias spostati come record di tipo `self` nel DB `hosts`. Possono essere modificati dalla pagina *DNS > Alias server*.

Record MX per i client della LAN

Il nuovo modulo Email basato su Rspamd non implementa più l’override del record MX per gli host della LAN. Assicurarsi che i client email della LAN siano configurati prt usare l’SMTP/AUTH o siano elencati in *Email > Accesso SMTP > Consenti relay dai seguenti indirizzi IP* prima di aggiornare.

4.31.2 Procedure di aggiornamento manuale

Le procedure di aggiornamento manuale non sono più necessarie: l’aggiornamento avviene automaticamente.

Dopo l’aggiornamento, i servizi del vecchio motore antispam forniti da amavisd e spamassassin vengono disabilitati e i loro pacchetti possono essere rimossi.

Per rimuovere gli rpm del vecchio antispam eseguire

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

Riferimenti

CAPITOLO 5

Moduli NethForge

5.1 Collabora Online

Nota: Questo pacchetto non è supportato in NethServer Enterprise

Collabora Online Collabora Online è una potente suite office online basata su LibreOffice che supporta tutti i principali formati di documenti, fogli elettronici e file di presentazione, e può essere integrata nella propria infrastruttura. Per ulterirori informazioni fare riferimento al sito web ufficiale.

5.1.1 Installazione

Installare il modulo dal Software Center o usando la riga di comando:

```
yum install nethserver-collabora
```

Configurazione virtual host

Collabora Online richiede un virtual host dedicato ed è accessibile solo da HTTPS con un certificato valido.

Nota: Collabora Online **non sarà abilitato** senza un virtual host dedicato

Per configurare Collabora Online, eseguire:

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

Dopo la configurazione del virtual host, andrà richiesto un certificato HTTPS valido tramite Let's Encrypt dalla sezione `Certificato server` dell'interfaccia Server Manager.

Utilizzo

Collabora Online verrà automaticamente abilitato per Nextcloud se il pacchetto `nethserver-nextcloud` è presente nel momento in cui viene configurato il virtual host virtuale, altrimenti è possibile abilitarlo successivamente con:

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

Se l'istanza di Nextcloud non è installata nello stesso server di Collabora Online, è necessario impostare il nome host di Nextcloud nella prop `AllowWopiHost`:

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

E configurare manualmente l'applicazione di Nextcloud richdocuments.

5.1.2 Utente admin

Al termine dell'installazione, la dashboard di amministrazione può essere abilitata con `loolconfig set-admin-password` e accessibile al url:

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

5.2 SOGo

Nota: This package is not supported in NethServer Enterprise

SOGo is a fully supported and trusted groupware server with a focus on scalability and open standards. SOGo is released under the GNU GPL/LGPL v2 and above. SOGo provides a rich AJAX-based Web interface and supports multiple native clients through the use of standard protocols such as CalDAV, CardDAV and GroupDAV, as well as Microsoft ActiveSync. SOGo is the missing component of your infrastructure; it sits in the middle of your servers to offer your users a uniform and complete interface to access their information. It has been deployed in production environments where thousands of users are involved.

Nota: SOGo provides EAS (Exchange ActiveSync) support, but not EWS (Exchange Web Service). Outlook 2013, 2016 for Windows works well with EAS. Mainstream mobile devices (iOS, Android, BlackBerry 10) work well with EAS, they can sync mails, calendars, contacts, tasks. Apple Mail.app, and Outlook for Mac support EWS. But not EAS. **Clients work very well with POP3/IMAP account, caldav/carddav account**

Avvertimento: `nethserver-sogo` doesn't integrate OpenChange and Samba4 for native MAPI support, so SOGo groupware doesn't provide full support for Microsoft Outlook clients, Mac OS X Mail.app and all iOS devices, don't try to add your mail account as an Exchange account in these mail clients. You have to add account as POP3/IMAP account, caldav/carddav account instead.

5.2.1 Installation

Nota: You need first to set an account provider which can be local (nethserver-directory for openldap or nethserver-dc for Samba AD) or remote (whatever openldap or samba AD choice). You cannot mix your choice by openldap and Samba AD, preferably if you plan to host samba shares with user authentication, you need samba AD (nethserver-dc)

Then install from the Software Center or use the command line:

```
yum install nethserver-sogo
```

5.2.2 Official documentation

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

5.2.3 Usage

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

5.2.4 Esmith database

You can modify the available properties of SOGo:

```
sogod=service
  ActiveSync=enabled
  AdminUsers=admin
  BackupTime=30 0
  Certificate=
  Dav=enabled
  DraftsFolder=Drafts
  IMAPLoginFieldName=userPrincipalName
  MailAuxiliaryUserAccountsEnabled=YES
  Notifications=Appointment,EMail               #'Folder'/'ACLs'/'Appointment'
  SOGoInternalSyncInterval=10
  SOGoMaximumPingInterval=10
  SOGoMaximumSyncInterval=30
  SOGoMaximumSyncResponseSize=2048
  SOGoMaximumSyncWindowSize=100
  SentFolder=Sent
  SxVMemLimit=512
  TrashFolder=Trash
  VirtualHost=
  WOWatchDogRequestTimeout=10
  WOWorkersCount=10
  status=enabled
```

Properties:

- AdminUsers: Parameter used to set which usernames require administrative privileges over all the users tables.
- BackupTime: Time to launch the backup, by default ("30 0")each day at 00h30, you can change it if you set a cron compatible value `* *`

- DraftsFolder: name of draft folder, default is 'Drafts'
- IMAPLoginFieldName: adjust the imap login field to your good trusted value in your ldap (see https://community.nethserver.org/t/sogo-and-ad-brainstorming/8024/31)
- SentFolder: name of the sent folder, default is 'Sent'
- TrashFolder: name of the trash folder, default is 'Trash'
- WOWorkersCount: The amount of instances of SOGo that will be spawned to handle multiple requests simultaneously
- MailAuxiliaryUserAccountsEnabled: Parameter used to activate the auxiliary IMAP accounts in SOGo. When set to YES, users can add other IMAP accounts that will be visible from the SOGo Webmail interface.
- Notifications: enabled notifications. The value is a comma separated list. Default value is "Appointment, EMail"

Notes

Terms highlighted in **bold** are documented in SOGo installation and configuration guide.

- `AdminUsers` comma separated list of accounts allowed to bypass SOGo ACLs. See **SOGoSuperUsernames** key
- Notifications comma separated list of values (no spaces between commas). Known item names are `ACLs`, `Folders`, `Appointments`. See **SOGoSendEMailNotifications**
- `{Drafts,Sent,Trash}Folder` See respective **SOGoFolderName** parameters
- `VirtualHosts` SOGo is reachable from the default host name plus the host (FQDN) listed here. The host key is generated/removed in `hosts` DB, with `type=self` automatically.

5.2.5 Access SOGo on an exclusive hostname

To make SOGo accessible with an exclusive DNS hostname:

- In "DNS and DHCP" UI module (Hosts), create the DNS host name as a server alias (i.e. webmail.example.com)
- Add the host name to sogod/VirtualHost prop list:

```
config setprop sogod VirtualHost webmail.example.com
signal-event nethserver-sogo-update
```

Same rule applies if SOGo must be accessible using server IP address. For example:

```
config setprop sogod VirtualHost 192.168.1.1
signal-event nethserver-sogo-update
```

If the VirtualHost prop is set, requests to the root (i.e. webmail.example.com) are redirected to the (mandatory) /SOGo subfolder (webmail.example.com/SOGo).

It is also possible to use a custom certificate for this virtualhost:

```
config setprop sogod Certificate example.crt
signal-event nethserver-sogo-update
```

5.2.6 Maximum IMAP command

Maximum IMAP command line length in kilo bytes. Some clients generate very long command lines with huge mailboxes, so you may need to raise this if you get «Too long argument» or «IMAP command line too large» errors often.

Set by default to 2048KB:

```
config setprop dovecot ImapMaxLineLenght 2048
signal-event nethserver-sogo-update
```

5.2.7 ActiveSync

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

ActiveSync is enabled by default on SOGo and WebTop. At installation of SOGo, Webtop-ActiveSync is disabled and SOGo will take precedence.

SOGo-ActiveSync can be disabled in the server-manager at the SOGo-panel or with:

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

To enable ActiveSync on WebTop:

```
config setprop webtop ActiveSync enabled
signal-event nethserver-webtop5-update
```

To enable ActiveSync on SOGo again:

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

5.2.8 Backup

Each night (by default) a cron run to backup user data (filter rules, specific settings, events, contacts) and save it to `/var/lib/sogo/backups` you can restore the data with a tool `sogo-restore-user`, for example:

```
sogo-restore-user /var/lib/sogo/backups/sogo-2017-12-10_0030/ stephane
```

or for all users

```
sogo-restore-user /var/lib/sogo/backups/sogo-2017-12-10_0030/ -A
```

if you want to change the time of your backup for example (in this example, run at 4h01 AM):

```
config setprop sogod BackupTime '1 4'
signal-event nethserver-sogo-update
```

5.2.9 Fine tuning

Adjust Setting

SOGo must be tuned following the number of users, some settings can be tested.

Nota: Keep in mind to set one worker per user for the activesync connection.

100 users, 10 EAS devices:

```
config setprop sogod WOWorkersCount 15
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 30
signal-event nethserver-sogo-update
```

100 users, 20 EAS devices:

```
config setprop sogod WOWorkersCount 25
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 40
signal-event nethserver-sogo-update
```

1000 users, 100 EAS devices:

```
config setprop sogod WOWorkersCount 120
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 60
signal-event nethserver-sogo-update
```

Increase sogod log verbosity

Read the SOGo FAQ for other debugging features.

SOGo floods /var/log/messages

You can see this log noise in `/var/log/message`:

```
Dec  4 12:36:01 ns7ad1 systemd: Created slice User Slice of sogo.
Dec  4 12:36:01 ns7ad1 systemd: Starting User Slice of sogo.
Dec  4 12:36:01 ns7ad1 systemd: Started Session 163 of user sogo.
Dec  4 12:36:01 ns7ad1 systemd: Starting Session 163 of user sogo.
Dec  4 12:36:01 ns7ad1 systemd: Removed slice User Slice of sogo.
Dec  4 12:36:01 ns7ad1 systemd: Stopping User Slice of sogo.
```

These messages are normal and expected – they will be seen any time a user logs in. To suppress these log entries in `/var/log/messages`, create a discard filter with rsyslog, e.g., run the following command:

```
echo 'if $programname == "systemd" and ($msg contains "Starting Session" or $msg␣
↪contains "Started Session" or $msg contains "Created slice" or $msg contains
↪"Starting User" or $msg contains "Removed slice User" or $msg contains "Stopping␣
↪User") then stop' > /etc/rsyslog.d/ignore-systemd-session-slice-sogo.conf
```

and restart rsyslog

```
systemctl restart rsyslog
```

this solution comes from RedHat solution

5.2.10 Clients

Android

Currently you have 2 ways to integrate your Android device with Sogo.

Integration via Caldav /Cardav/imap

Nota: The drawback is that you need to set all settings (Url/Username/Password) in each application.

- Email

Imaps(over ssl) is a good choice, you can use the K9-mail software to retrieve your email or the default email application

- Contacts and calendars

There are various working clients, including DAVdroid (open-source) and CalDAV-Sync/CardDav-Sync. Advantages Full integration into Android, so that almost all calendar and contacts apps can access synchronized data.

Integration via ExchangeActiveSync

Nota: The advantage is that you set the Url/Username/Password only in one location

Step-by-step configuration

- Open the account menu, choose add an exchange account
- Fill your full email address and password in Account Setup page:
- If it asks you to choose Account Type, please choose Exchange:
- In detailed account setup page, fill up the form with your server address and email account credential
  - DomainUsername: your full email address
  - Password: password of your email account
  - Server: your server name or IP address
  - Port: 443

Nota: Please also check Use secure connection (SSL) and Accept all SSL certificates

- In Account Settings page, you can choose Push. it's all up to you.
- Choose a name for your Exchange account.
- Click Next to finish account setup. That's all.

Mozilla Thunderbird and Lightning

Alternatively, you can access SOGo with a GroupDAV and a CalDAV client. A typical well-integrated setup is to use Mozilla Thunderbird and Mozilla Lightning along with Inverse's SOGo Connector plug in to synchronize your address books and the Inverse's SOGo Integrator plug in to provide a complete integration of the features of SOGo into Thunderbird and Lightning. Refer to the documentation of Thunderbird to configure an initial IMAP account pointing to your SOGo server and using the user name and password mentioned above.

With the SOGo Integrator plug in, your calendars and address books will be automatically discovered when you login in Thunderbird. This plug in can also propagate specific extensions and default user settings among your site. However, be aware that in order to use the SOGo Integrator plug in, you will need to repackage it with specific modifications. Please refer to the documentation published online.

If you only use the SOGo Connector plug in, you can still easily access your data.

- To access your personal address book:
- Choose Go > Address Book.
- Choose File > New > Remote Address Book.
- Enter a significant name for your calendar in the Name field.
- Type the following URL in the URL field: http://localhost/SOGo/dav/jdoe/Contacts/personal/
- Click on OK.

To access your personal calendar:

- Choose Go > Calendar.
- Choose Calendar > New Calendar.
- Select On the Network and click on Continue.
- Select CalDAV.
- Type the following URL in the URL field: http://localhost/SOGo/dav/jdoe/Calendar/personal/
- Click on Continue.

Windows Mobile

The following steps are required to configure Microsoft Exchange ActiveSync on a Windows Phone:

Locate the Settings options from within your application menu.

- Select Email + Accounts.
- Select Add an Account.
- Select the option for Advanced Setup.
- Enter your full email address and password for your account. Then press the sign in button.
- Select Exchange ActiveSync.
- Ensure your email address remains correct.
- Leave the Domain field blank.
- Enter the address for Server (domain name or IP)
- Select the sign in button.
- You might need to accept all certificats, if you are not able to sync

Once connected, you will see a new icon within your settings menu with the name of your new email account.

Outlook

You can use it with

- IMAP + commercial plugin as cfos or outlookdav for calendars/contacts
- ActiveSync since Outlook 2013

There is no support for Openchange/OutlookMAPI.

5.2.11 Nightly build

SOGo is built by the community, if you look to the last version, then you must use the nightly built. This version is not considered as stable, but bugs are fixed quicker than in stable version. You are the QA testers :)

NethServer 7 - SOGo 3

Execute:

```
sudo rpm --import 'http://pgp.mit.edu/pks/lookup?op=get&search=0xCB2D3A2AA0030E2C'
sudo rpm -ivh http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
sudo cat >/etc/yum.repos.d/SOGo.repo <<EOF
[sogo3]
name=SOGo Repository
baseurl=https://packages.inverse.ca/SOGo/nightly/3/rhel/7/\$basearch
gpgcheck=1
EOF
```

Then to install:

```
yum install nethserver-sogo --enablerepo=sogo3
```

5.2.12 Issues

Please raise issues on community.nethserver.org.

5.2.13 Sources

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

Developer manual on github.

5.3 PhpVirtualBox

Nota: This package is not supported in NethServer Enterprise

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

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

5.3.1 Installation

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

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

Install from the Software Center or use the command line:

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

Usage

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

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

More information are available at the Authentication section

Network access

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

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

Access on an exclusive hostname

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

- In "DNS and DHCP" UI module (Hosts), create the DNS host name as a server alias (i.e. webmail.example.com)
- Add the host name to `DomainName` prop list (default is ""):

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

Advanced settings

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

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

VM ownership and quota

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

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

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

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

5.3.2 User permissions

phpVirtualBox essentially has two access levels. `admin` and `non-admin` users. The administrator users have access to the Users section of phpVirtualBox and can add, edit, remove other users (only for the internal method). They can also perform actions that change VM group memberships and manipulate VM groups (Rename, Group, Ungroup). The administrator users are also not limited with the virtual machine quota and can manage VM of other users. The VMs are visible only by the owner, as long as the property `VMOwnerShip` is set to true.

5.3.3 Authentication

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

Example:

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

internal

The default credentials are :

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

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

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

LDAP (openldap)

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

AD (active directory)

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

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

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

5.3.4 Uploading ISOs

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

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

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

5.3.5 Oracle VM VirtualBox Extension Pack

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

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

5.3.6 The RDP console

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

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

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

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

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

5.3.7 VM networking

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

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

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

Example script

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

5.3.8 Esmith database

You can modify the available properties of phpvirtualhost:

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

Example:

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

5.3.9 Documentation

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

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

CAPITOLO 6

Best practice

6.1 Third-party software

È possibile installare su NethServer qualsiasi software di terze parti certificato per CentOS/RHEL.

Se il software è disponibile solo a 32 bit, è necessario installare le librerie di compatibilità prima del software stesso. Alcune librerie possibili:

- glibc
- glib
- libstdc++
- zlib

Ad esempio, per installare questi pacchetti usare il comando:

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

6.1.1 Installazione

Se il software è distribuito con un pacchetto RPM, si consiglia di usare il comando **yum** per l'installazione: il sistema si occuperà di risolvere e installare tutte le dipendenze necessarie.

Nel caso in cui l'installazione con yum non sia possibile, la directory più corretta in cui installare il software è `/opt`. Per esempio, dato il software chiamato *mysoftware*, installare nella directory `/opt/mysoftware`.

6.1.2 Backup

Le directory che contengono dati rilevanti devono essere incluse nel backup aggiungendo una linea al file `/etc/backup-data.d/custom.include`. Vedi *Personalizzazione backup dati*.

6.1.3 Firewall

Se il software necessita di porte aperte sul firewall, creare un servizio chiamato `fw_<softwarename>`.

Ad esempio, dato il software *mysoftware* che necessita la porta 3344 e 5566 aperta sulla LAN, usare questi comandi:

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

6.1.4 Avvio e arresto

NethServer usa il target standard multi utente di systemd.

Il software installato con yum dovrebbe già essere configurato per partire al boot del sistema. Per controllare la configurazione, eseguire il comando **`systemctl`**. Il comando mostra una lista di servizi con il relativo stato.

Per abilitare un servizio al boot:

```
systemctl enable mysoftware
```

Per disabilitare un servizio al boot:

```
systemctl disable mysoftware
```

CAPITOLO 7

Appendice

7.1 Migrazione da NethService/SME Server

La migrazione è il processo che consente di convertire una macchina per SME Server/NethService (*sorgente*) in un NethServer (*destinazione*). Il processo può essere tramite *backup* o *utilizzando rsync*.

Nota: Nessun template custom sarà migrato durante il processo di migrazione. Controllare i nuovi template prima di copiare frammenti personalizzati dal vecchio backup.

Avvertimento: Prima di eseguire la procedura di migrazione, leggere attentamente tutte le sezioni di questo capitolo.

7.1.1 Account provider

E" necessario configurare un *provider account* prima di avviare la procedura di migrazione.

- Se il sistema originale era collegato ad un dominio Active Directory (il ruolo Samba era ADS), configurare un *Active Directory remoto* come account provider.
- Se il sistema originale era un Controller di dominio NT (Samba con ruole PDC), installare un *Active Directory locale* come provider account.
- Se l'accesso alle Cartelle Condivise nella destinazione richiede l'autenticazione utente, utilizzare un *Active Directory locale* come provider account.
- In ogni altro caso, installare un *LDAP locale* come provider account.

Se si sceglie un account provider di tipo *Active Directory* locale, ricordarsi di configurare completamente ed avviare il DC prima di eseguire l'evento `migration-import`. Vedi account-provider.

Inoltre i seguenti account vengono ignorati dalla procedura di migrazione perché sono già forniti da Active Directory:

- administrator
- guest
- krbtgt

7.1.2 Email

Prima di mettere in produzione NethServer, è necessario fare qualche valutazione relativa alla rete ed alla configurazione dei client mail esistenti: quali porte siano utilizzate, se SMTPAUTH e TLS siano abilitati. Fare riferimento alle sezioni email_clients e *Politiche SMTP di invio speciali* per ulteriori informazioni.

Nella migrazione di un server di posta, il server di origine può rimanere in produzione anche dopo che il backup è stato eseguito e nuovi messaggi di posta continuano ad essere consegnati finché non viene spento definitivamente.

Uno script `rsync` di aiuto è fornito dal pacchetto `nethserver-mail-server`. Va eseguito sulla destinazione e serve a sincronizzare le caselle di posta di destinazione con il server di origine:

```
Usage:
    /usr/share/doc/nethserver-mail-server-<VERSION>/sync_maildirs.sh [-h] [-n] [-p] -
↪s IPADDR
        -h          help message
        -n          dry run
        -p PORT     ssh port on source host (default 22)
        -s IPADDR   rsync from source host IPADDR
        -t TYPE     source type: sme8 (default), ns6
```

Il server di origine con indirizzo `IPADDR` deve essere accessibile dall'utente `root`, mediante `ssh` con autenticazione a chiave pubblica.

7.1.3 Apache

La configurazione di cifratura SSL non verrà migrata automaticamente perché il sistema sorgete adotta di default un sistema di cifrature debole. Per effettuare manualmente la migrazione di tale configurazione andranno eseguiti i seguenti comandi:

```
MIGRATION_PATH=/var/lib/migration
config setprop httpd SSLCipherSuite $(db $MIGRATION_PATH/home/e-smith/db/
↪configuration getprop modSSL CipherSuite)
signal-event nethserver-httpd-update
```

7.1.4 Ibay

Le *ibay* sono state sostituite dalle *Cartelle condivise*. I protocolli supportati per accedere alle Cartelle condivise sono:

- SFTP, messo a disposizione dal demone `sshd`
- il protocollo di condivisione file SMB, tipico delle infrastrutture Windows, implementato attraverso Samba

Avvertimento: Leggere attentamente la sezione *Cartelle condivise* del capitolo *Aggiornamento da NethServer 6*, le credenziali per la connessione potrebbero variare a seguito dell'upgrade a NethServer 7.

A partire da NethServer 7, le Cartelle condivise non possono più essere esposte via HTTP. Successivamente all'evento `migration-import` le vecchie ibay potranno essere migrate rispettando le seguenti regole generali:

1. Se l'ibay aveva un **virtual host** associato, si dovrà installare il modulo «Web server» dalla pagina *Software center*. Sarà poi necessario copiare il contenuto della ibay nella directory root del virtual host. Fare riferimento a *Virtual hosts*.
2. Se l'accesso alla ibay era limitato da una **password** (ad esempio per condividere i contenuti con un gruppo di persone attraverso internet), sarà possibile replicare questa configurazione dalla pagina *Virtual hosts* . E" anche possibile pensare di sostituire la ibay utilizzata in questa configurazione con il modulo *Nextcloud*.
3. Se il contenuto della ibay era accessibile attraverso un URL come `http://<IP>/ibayname` il modo più semplice per mantenere la funzionalità sarà quello di spostare il percorso nella radice di Apache:

```
mv -iv /var/lib/nethserver/ibay/ibayname /var/www/html/ibayname
chmod -c -R o+rX /var/www/html/ibayname
db accounts delete ibayname
signal-event nethserver-samba-update
```

Dopo la migrazione, le ibay manterranno un profilo retro-compatibile. Per sfruttare le nuove funzionalità, incluso Samba Audit, la configurazione delle ibay deve essere passata al nuovo profilo. Da riga di comando eseguire:

```
db accounts setprop ibay_name SmbProfileType default
signal-event ibay-mody ibay_name
```

In cui `ibay_name` è il nome della ibay da configurare.

7.1.5 Migrazione da backup

1. Sulla macchina origine, effettuare un backup completo e spostarlo sul server destinazione.
2. Sul server destinazione, installare NethServer 7 **utilizzando la ISO più recente disponibile** e tutti i moduli che implementano i servizi presenti sulla macchina origine.
3. Estrarre il backup in una directory; per esempio, creare la directory `/var/lib/migration`.
4. Scatenare l'evento `migration-import` nell'host di destinazione:

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

   Questa operazione potrebbe richiedere molti minuti.
5. Consultare il log di sistema file:*/var/log/messages* ed assicurarsi che non si siano verificati errori:

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

7.1.6 Migrazione con rsync

Questa procedura è più rapida rispetto a quella effettuata a partire da un backup.

Prima di iniziare assicurarsi di avere:

- una installazione NethService/SME attiva, che chiameremo server origine o server sorgente
- una installazione di NethServer 7 attiva con **tutti gli update più recenti installati** e con a disposizione lo stesso spazio su disco del server sorgente, che chiameremo server destinazione
- una connessione di rete attiva tra i due server

Assicurarsi che il server sorgente consenta il login all'utente root con password ed attraverso una chiave SSH.

Sincronizzazione dei file

Lo script di sincronizzazione copia tutti i dati utilizzando rsync su SSH. I file vengono salvati nel percorso `/var/lib/migration`. Se il server di destinazione non dispone di chiavi SSH, lo script creerà anche una coppia di chiavi RSA e ne copierà la chiave pubblica nel server di origine. Tutte le directory escluse dai dati di backup non verranno sincronizzate.

Nella macchina di destinazione, eseguire il seguente comando:

```
screen rsync-migrate <source_server_name> [ssh_port]
```

In cui

- `source_server_name` è il nome host o IP del server origine
- `ssh_port` è la porta SSH del server origine (la porta di default è la 22)

Esempio:

```
screen rsync-migrate mail.nethserver.org 2222
```

Quando richiesto, inserire la password di root del server origine quindi prepararsi un caffè e aspettare con pazienza.

Lo script non eseguirà alcuna azione sulla macchina di origine e può essere rilanciato più volte.

Sincronizzazione e migrazione

Se impartito con l'opzione `-m`, `rsync-migrate` eseguirà una sincronizzazione finale e l'aggiornamento della macchina destinazione.

Prima di eseguire lo step finale di migrazione, verificare di avere installato tutti i pacchetti che coprono le stesse funzionalità del server d'origine.

Esempio:

```
screen rsync-migrate -m mail.nethserver.org 2222
```

Lo script si incaricherà di:

- fermare ogni servizio sulla macchina origine (ad eccetto di SSH)
- eseguire l'evento di `pre-backup` sulla macchina origine
- sincronizzare tutti i dati rimanenti
- eseguire l'evento `migration-import` sulla macchina destinazione

Al termine della procedura verificare la presenza di eventuali errori in `/var/log/messages`:

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

7.2 Aggiornamento da NethServer 6

L'aggiornamento da NethServer 6 a NethServer 7 può essere eseguito utilizzando uno dei tre seguenti metodi:

- *backup* (vedere anche *Disaster recovery*)
- *rsync*
- *upgrade-tool* (beta)

Avvertimento: Prima di procedere con l'aggiornamento, leggere attentamente tutte le sezioni di questo documento. Si prega di fare riferimento anche alla sezione *Pacchetti rimossi*.

Nota: Per l'intera durata del processo di upgrade tutti i servizi di rete saranno inaccessibili.

7.2.1 Account provider

Esistono differenti scenari di aggiornamento, a seconda di come è configurata la macchina di origine.

- In caso di sistema di origine Primary Domain Controller NT (ruolo del server Samba *Primary Domain Controller* – PDC) o di file server standalone (ruolo *Workstation* – WS), fare riferimento alla sezione *Aggiornamento Primary Domain Controller e Workstation*.
- In caso di sistema origine attestato ad un dominio Active Directory (ruolo server Samba *Active Directory member* – ADS), fare riferimento alla sezione *Aggiornamento membro Active Directory*.
- In tutti gli altri casi il server LDAP viene automaticamente aggiornato a «Account provider LDAP locale», preservando utenti, password e gruppi preesistenti.

Aggiornamento Primary Domain Controller e Workstation

Successivamente alla procedura di ripristino, spostarsi nella pagina *Accounts provider* e selezionare la procedura *Upgrade to Active Directory*. Il bottone sarà disponibile unicamente se la configurazione di rete sarà stata adattata al nuovo hardware.

I seguenti account vengono ignorati dalla procedura di aggiornamento perché sono già forniti da Samba Active Directory:

- `administrator`
- `guest`
- `krbtgt`

E" necessario fornire un indirizzo IP, aggiuntivo e libero, della rete *green* al container Linux per attivare l'account provider Active Directory locale.

Ad esempio:

- IP server (green): `192.168.98.252`
- IP aggiuntivo e libero della rete green: *192.168.98.7*‘

Assicurarsi che sia attiva una connessione internet:

```
# curl -I http://packages.nethserver.org/nethserver/
HTTP/1.1 200 OK
```

Per maggiori informazioni relative all'account provider Active Directory locale, fare riferimento alla sezione *Installazione del provider locale Samba Active Directory*.

Le connessioni alle cartelle condivise potrebbero richiedere delle modifiche.

Avvertimento: Leggere attentamente la sezione *Cartelle condivise*, le credenziali per la connessione potrebbero variare a seguito dell'upgrade a NethServer 7.

La procedura di upgrade preserva utenti, gruppi e account dei computer.

Avvertimento: Gli utenti non abilitati per Samba in NethServer 6 saranno migrati come utenti bloccati. Per abilitare questi utenti bloccati, l'amministratore dovrà semplicemente impostargli una nuova password.

Aggiornamento membro Active Directory

Successivamente al **ripristino della configurazione**, attestare il server ad un dominio Active Directory esistente tramite l'interfaccia web. Per ulteriori informazioni consultare la sezione *Join ad un dominio Active Directory esistente*.

Al termine, procedere con il **ripristino dei dati**.

Avvertimento: Gli alias e-mail non vengono importati automaticamente da AD!

7.2.2 Cartelle condivise

Le cartelle condivise sono state separate in due pacchetti:

- La pagina «Cartelle condivise» permette di configurare solamente delle condivisioni SMB; fornisce l'accesso ai dati utilizzando il protocollo CIFS/SMB e può essere utilizzata per condividere file tra workstation Windows e Linux
- Il pannello «Virtual host» fornisce l'accesso via HTTP ed FTP ed è stato concepito per ospitare siti ed applicazioni web

Accesso SMB

Il modello di protezione SMB adottato da NethServer 7 si basa su Active Directory. Di conseguenza, quando si esegue l'aggiornamento (o la migrazione) di un file server nel ruolo del controller di dominio primario (PDC) o di standalone workstation (WS), si applica la seguente regola:

> Quando ci si connette a una cartella condivisa, il nome di dominio NetBIOS deve essere anteposto al nome utente (ad esempio `MYDOMAIN\username`) o inserito nel campo specifico del modulo di autenticazione.

La procedura di upgrade abilita l'obsoleto metodo di autenticazione NTLM[1] al fine di preservare la compatibilità con i client della rete più vecchi, come stampanti e scanner.

Avvertimento: Si consiglia caldamente di correggere la configurazione dei client SMB più vecchi quindi di disattivare l'autenticazione NTLM.

- Modificare `/var/lib/machines/nsdc/etc/samba/smb.conf`
- Rimuovere la riga `ntlm auth = yes`
- Riavviare il DC samba con il comando `systemctl -M nsdc restart samba`

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

Accesso HTTP

Ogni cartella condivisa con accesso web configurata in NethServer 6 può essere migrata a virtual host direttamente dall'interfaccia web selezionando l'azione *Migra a virtual host*. Dopo la migrazione, i dati contenuti nel nuovo virtual host saranno accessibili solamente tramite i protocolli FTP ed HTTP.

Fare riferimento alla sezione *Virtual hosts* per ulteriori informazioni relative alla pagina *Virtual hosts*

7.2.3 Server mail

Tutte le opzioni delle cassette postali come la SPAM retention e la quota, così come le ACL, le cassette postali condivise dall'utente e le sottoscrizioni vengono conservate.

Le mailbox associate a gruppi con l'opzione *Consegna il messaggio in una cartella condivisa* abilitata, verranno convertite in cassette postali pubbliche condivise. La cartella pubblica condivisa verrà automaticamente sottoscritta da tutti i membri del gruppo, ma tutti i messaggi verranno contrassegnati come non letti.

7.2.4 TLS policy

La configurazione dei servizi di NethServer 7 può aderire a diverse *TLS policy*. Prima dell'aggiornamento, è necessario verificare la compatibilità dei client di rete con le caratteristiche delle policy disponibili.

> **Avvertimento:** Un client di rete datato potrebbe fallire la connessione se i cifrari TLS da esso supportati sono considerati non validi

La versione della policy selezionata dalla procedura di aggiornamento dipende dal versione di NethServer come documentato in *Note di rilascio 7*.

7.2.5 Let's Encrypt

I certificati Let's Encrypt vengono ripristinati durante il processo, ma non verranno automaticamente rinnovati.

Dopo aver completato il processo di aggiornamento, accedere all'interfaccia web e riconfigurare Let's Encrypt dalla pagina *Certificato del server*.

7.2.6 Owncloud e Nextcloud

In NethServer 7, Owncloud è stato ufficialmente sostituito da Nextcloud.

Tuttavia Owncloud 7 è ancora disponibile per evitare interruzioni del servizio dopo l'aggiornamento.

Nota: In caso di *upgrade da LDAP locale ad Samba AD*, i dati utente all'interno di Owncloud non saranno accessibili né dall'interfaccia web né dai client desktop/mobile. In tal caso, installare e migrare a Nextcloud dopo che è stato completato l'aggiornamento a Samba Active Directory.

Da Nextcloud 13, la migrazione da Owncloud a Nextcloud non è più supportata.

Gli utenti dovranno sostituire i client per Owncloud con quelli per Nextcloud[2], assicurandosi di impostare il nuovo URL dell'applicazione: `https://<your_server_address>/nextcloud`.

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

7.2.7 Librerie Perl

In NethServer 7, la libreria perl `NethServer::Directory` è stata sostituita da `NethServer::Password`. Gli script personalizzati andranno adattati di conseguenza.

Esempio del vecchio codice:

```
use NethServer::Directory;
NethServer::Directory::getUserPassword('myservice', 0);
```

Nuovo codice:

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

La documentazione è disponibile attraverso il comando perldoc:

```
perldoc NethServer::Password
```

7.2.8 Upgrade da backup

1. Assicurarsi di avere un backup recente del sistema di origine.
2. Installare NethServer 7 **utilizzando la ISO più recente disponibile** e completare gli step iniziali utilizzando il wizard di prima configurazione. La nuova macchina deve avere lo stesso hostname della vecchia per poter accedere correttamente al set di backup. Installare e configurare il modulo del backup.
3. Ripristinare il backup della configurazione utilizzando l'interfaccia web. Anche la configurazione della rete verrà ripristinata! Se dovesse verificarsi qualche problema, controllare il file di log `/var/log/messages` per informazioni più approfondite:

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

4. Se necessario, spostarsi nel menu *Network* e correggere la configurazione di rete conformemente al nuovo hardware. Se la macchina era attestata ad un dominio Active Directory esistente, leggere *Aggiornamento membro Active Directory*.
5. Completare la procedura di ripristino con i seguenti comandi:

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

   in cui *name* è il nome del backup configurato.

   Nota: Di default il nome del *backup-data* configurato su NethServer 6 è `backup-data`

6. Verificare i log del ripristino:

   ```
   /var/log/restore-data.log
   /var/log/messages
   ```

7. La compatibilità con la versione 7 di ciascun file contenuto nel percorso `/etc/e-smith/templates-custom/` dovrà essere verificata manualmente.

Avvertimento: La macchina non va riavviata prima di aver eseguito la procedura di restore-data.

7.2.9 Upgrade tramite rsync

Il processo tramite rsync è più rapido rispetto ad un tradizionale backup e ripristino e consenti di minimizzare il fermo servizi per gli utenti.

Prima di iniziare assicurarsi di avere:

- una installazione di NethServer 6 in produzione, che chiameremo server origine o server sorgente
- una installazione di NethServer 7 con almeno lo stesso spazio su disco del server di origine e **gli ultimi aggiornamenti installati**, che chiameremo server di destinazione
- una connessione di rete attiva tra i due server

Assicurarsi che il server sorgente consenta il login all'utente root tramite password ed attraverso una chiave SSH.

Sincronizzazione dei file

Lo script di sincronizzazione copia tutti i dati utilizzando rsync su SSH. Se il server di destinazione non dispone di chiavi SSH, lo script genererà una coppia di chiavi RSA per il server destinazione e copierà la chiave pubblica nel server di origine. Tutte le directory escluse dai dati di backup non verranno sincronizzate.

Nella macchina di destinazione, eseguire il seguente comando:

```
screen rsync-upgrade <source_server_name> [ssh_port]
```

In cui

- `source_server_name` è il nome host o l'IP del server origine
- `ssh_port` è la porta SSH del server origine (la porta di default è la 22)

Esempio:

```
screen rsync-upgrade mail.nethserver.org 2222
```

Quando richiesto, inserire la password di root del server origine quindi prepararsi un caffè e aspettare con pazienza.

Lo script non eseguirà alcuna azione sulla macchina di origine e può essere rilanciato più volte.

Sincronizzazione e migrazione

Se impartito con l'opzione `-u`, `rsync-upgrade` eseguirà una sincronizzazione finale e l'upgrade della macchina destinazione.

Esempio:

```
screen rsync-upgrade -u mail.nethserver.org 2222
```

Lo script si incaricherà di:

- chiudere l'accesso ad ogni servizio di rete della macchina sorgente (ad eccezione di SSH ed httpd-admin)
- eseguire gli eventi `pre-backup-config` e `pre-backup-data` nella macchina sorgente
- sincronizzare tutti i dati rimanenti
- eseguire il comando `restore-config` sulla macchina destinazione

Se l'`rsync-upgrade` termina senza perdita della connessione di rete,

1. Disconnettere il ns6 origine dalla rete, per evitare conflitti IP con il server di destinazione

2. Accedere all'interfaccia Server Manager e correggere la configurazione di rete dalla pagina *Rete*

Altrimenti, se durante l'`rsync-upgrade` **la connessione di rete viene persa**, è probabile che i server di origine e di destinazione abbiano un **conflitto IP**:

1. Disconnettere il ns6 origine dalla rete,
2. Da una console di root del ns7 lanciare il comando:

```
systemctl restart network
```

3. Quindi accedere nuovamente alla screen:

```
screen -r -D
```

Al termine dell'`rsync-upgrade` seguire i seguenti passi:

1. In caso di sistema di origine Primary Domain Controller NT (ruolo del server Samba *Primary Domain Controller* – PDC) o di file server standalone (ruolo *Workstation* – WS), fare riferimento alla sezione *Aggiornamento Primary Domain Controller e Workstation*.
2. In caso di sistema origine attestato ad un dominio Active Directory (ruolo server Samba *Active Directory member* – ADS), fare riferimento alla sezione *Aggiornamento membro Active Directory*.
3. Tornare alla CLI e scatenare l'evento `post-restore-data` sulla macchina di destinazione:

```
signal-event post-restore-data
```

4. Controllare nei log di ripristino eventuali occorrenze di messaggi di `ERROR` o di `FAIL`:

```
/var/log/restore-data.log
/var/log/messages
```

5. La compatibilità con la versione 7 di ciascun file contenuto nel percorso `/etc/e-smith/templates-custom/` dovrà essere verificata manualmente.

Avvertimento: La macchina non va riavviata prima di aver scatenato la evento post-restore-data.

7.2.10 Upgrade tramite Upgrade tool (beta)

Il modulo Upgrade tool consente di eseguire un **aggiornamento in-place** di NethServer dalla versione 6 alla versione 7 tramite una procedura automatica.

Fare riferimento alla pagina Upgrade tool del Manuale Amministratore di NethServer 6.

7.3 Licenza della documentazione

La documentazione è distribuita sotto i termini di licenza **Creative Commons - Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)**

Sei libero di:

- **Condividere** — riprodurre, distribuire questo materiale con qualsiasi mezzo e formato
- **Modificare** — remixare, trasformare il materiale e basarti su di esso per le tue opere

Il licenziante non può revocare questi diritti fintanto che tu rispetti i termini della licenza.

Alle seguenti condizioni:

- **Attribuzione** — Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma non con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.
- **NonCommerciale** — Non puoi utilizzare il materiale per scopi commerciali.
- **StessaLicenza** — Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

Divieto di restrizioni aggiuntive — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare.

Questo è un riassunto in linguaggio accessibile a tutti (e non un sostituto) della licenza. La licenza completa è accessibile a: http://creativecommons.org/licenses/by-nc-sa/4.0/

La documentazione sull'architettura deriva dal progetto SME Server e concessa con licenza GNU Free Documentation 1.3 (http://www.gnu.org/copyleft/fdl.html). Si veda http://wiki.contribs.org/ per la documentazione originale.

7.4 List of NethServer 7 ISO releases

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

7.4.1 7.6.1810

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

7.4.2 7.5.1804

- 2018-06-11 final
- 2018-05-31 rc
- 2018-05-21 beta

7.4.3 7.4.1708

- 2017-10-26 final - GA 2017-10-30
- 2017-09-21 beta1

7.4.4 7.3.1611

- 2017-07-31 update 1
- 2017-01-30 final - GA 2017-02-08

- 2017-01-18 rc4
- 2016-12-16 rc3

7.4.5 7.2.1511

- 2016-11-09 rc2
- 2016-10-18 rc1
- 2016-09-02 beta2
- 2016-07-12 beta1
- 2016-05-23 alpha3
- 2016-02-12 alpha2

7.5 Public issue trackers

List of public issue trackers related to NethServer.

- NethServer 7: https://github.com/NethServer/dev/issues
- NethServer 6: http://dev.nethserver.org/projects/nethserver/issues
- NethServer Enterprise: https://github.com/nethesis/dev/issues
- CentOS: https://bugs.centos.org/
- Red Hat: https://bugzilla.redhat.com

7.6 Chat

Il servizio chat utilizza il protocollo standard Jabber/XMPP. Vedi anche *Chat*.

Interfaccia web di amministrazione Il server Jabber è dotato di un'interfaccia web amministrativa il cui accesso è consentito ai membri del gruppo jabberadmins.

Federation (S2S) XMPP consente ai server di intercomunicare tra loro, formando una rete IM globale «federata».

Massima velocità trasferimento file Limita la massima velocità per il trasferimento file al valore in Byte/secondo

Velocità standard di trasferimento file Limita la velocità standard per il trasferimento file al valore in Byte/secondo

7.7 Windows file server

Vedere anche *Cartelle condivise*

Workgroup/Nome dominio NetBIOS Il valore può essere modificato solo con se il provider account è LDAP e definisce il nome del gruppo di lavoro di Windows visibile dal pannello Risorse di rete nei sistemi Windows. Con l'account provider Active Directory il valore è determinato dal dominio a cui il server è attestato

Quando un nuovo file o directory viene creato in una cartella condivisa Stabilisce chi possiede un file o una directory appena creati: il creatore della risorsa o il proprietario della directory che contiene la nuova risorsa (nota anche come directory principale)

Concedere il controllo completo sulle home directory al gruppo Domain Admins (home$ share) Permetti ai membri del gruppo `Domain Admins` di collegare la condivisione nascosta `home$` e concede loro l'accesso amministrativo a qualsiasi cartella home

Concede il pieno controllo sulle cartelle condivise al gruppo Domain Admins Consente ai membri del gruppo `Domain Admins` di connettere qualsiasi cartella condivisa e concedere loro l'accesso amministrativo sul suo contenuto

7.8 Reverse proxy

Questa pagina configura determinati paths e nomi di Virtual Host in Apache per essere offerti inoltrando la richiesta Web originale a un altro URL. Vedi anche *Reverse proxy*.

7.8.1 Creare /Modificare

Nome L'URL **path name** o il **virtual host name** (FQDN di un host). Un nome di percorso corrisponderà a URL come `http://somehost /<path name>/ ... ``, mentre un nome di un virtual host corrisponderà a un URL come ``http: //<virtual host name>/ ....` Gli URL corrispondenti vengono inoltrati a *Target URL*.

Accesso dalle reti CIDR Limita l'accesso dall'elenco fornito di reti CIDR. Gli elementi devono essere separati con una «,» (virgola).

Certificato SSL / TLS Seleziona un certificato compatibile con il nome dell virtual host

Richiede una connessione crittografata SSL Se abilitato, è possibile accedere al percorso dell'URL o al nome dell" virtual host solo con una connessione SSL/TLS.

URL di destinazione L'URL in cui è inoltrata la richiesta originale. L'URL è formato come `<scheme>://<hostname>:<port>/<path>`.

Accetta il certificato SSL non valido dalla destinazione Se il *Target URL* ha lo schema `https`, accetta il suo certificato anche se non è valido.

Forward HTTP «Host» intestazione a destinazione Se abilitata, questa opzione passerà l'header «Host» HTTP dalla richiesta in entrata all'host proxy, invece del «hostname» specificato nel campo *Target URL* field.

7.8.2 Eliminare

Rimuove la voce selezionata.

7.9 Groupware SOGo

Vedere anche *SOGo*.

Abilitazione CalDAV e CardDAV CalDAV consente agli utenti di accedere e condividere i dati del calendario presenti su un server. CardDAV consente agli utenti di accedere e condividere i contatti presenti su un server.

Abilitazione Microsoft ActiveSync ActiveSync è un'app per la sincronizzazione di dati mobili (e-mail, calendario, attività, contatti) sviluppata da Microsoft.

Consente agli utenti di aggiungere altri account IMAP Consente agli utenti di aggiungere altri account IMAP che saranno visibili dall'interfaccia di SOGo Webmail.

Amministratori Elenco degli utenti con privilegi amministrativi su tutti i dati utente.

Notifiche Sono disponibili diversi tipi di notifiche (basate su email). E" possibile attivarle in base alle proprie esigenze.

Rende raggiungibile SOGO solo da questo dominio (FQDN) SOGo è accessibile per impostazione predefinita da tutti i virtualhost del server, se si specifica qui un nome di dominio, SOGo sarà utilizzabile solo da questo nome di dominio.

Numero dei processi Questo parametro specifica il numero di istanze di SOGo che verranno generate per gestire più richieste contemporaneamente. E" consigliato almeno un worker per dispositivo activesync connesso.

Tempo massimo in secondi Parametro utilizzato per impostare la quantità massima di tempo, in secondi, che SOGo attenderà prima di eseguire un controllo interno per le modifiche dei dati (aggiunta, eliminazione e aggiornamento).

7.10 TLS policy

Livello di sicurezza applicato Configura i servizi di sistema come descritto nella sezione *TLS policy*

CAPITOLO 8

Indici

- Indice generale

Indice

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z