NethServer Documentation

Release 6.10 Final

Nethesis

06 mar 2019

Indice

Sito ufficiale: www.nethserver.org

CAPITOLO 1

Note di rilascio 6.10

1.1 Note di rilascio

NethServer versione 6.10 Final

- Note di rilascio upstream da CentOS 6.10 e RHEL 6.10
- CentOS 6 riceverà gli aggiornamenti di sicurezza fino al 2020-11-30
- Lista degli aggiornamenti della 6.10
- Tutti gli aggiornamenti della 6.9

1.1.1 Cambiamenti principali al 2018-07-23

- Di default il tempo di inattività di una sessione del Server Manager è di 60 minuti, mentre la durata massima di una sessione è di 8 ore. Questa nuova regola è applicata anche alle installazioni aggiornate. Vedere *Timeout della sessione*.

1.1.2 Aggiornamento dalla versione 6.9 alla 6.10

Eseguire il normale aggiornamento dei pacchetti dalla pagina del *Software Center*. Si consiglia un riavvio del sistema al termine della procedura di aggiornamento.

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
- 8 GB di spazio su hard disk

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 ®). Vedi: hardware.redhat.com

2.1.2 Tipi di installazione

Sono supportati due modi per installare NethServer. In breve:

Installazione da ISO

- Scaricare l'immagine ISO
- Preparare un CD/DVD
- 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!

Scaricare il file ISO dal sito ufficiale www.nethserver.org. Una volta scaricato, il file ISO può essere utilizzato per creare un **supporto avviabile**, come un CD o un DVD. La creazione di un disco avviabile è diversa dalla semplice scrittura di un file su CD/DVD, e richiede l'uso di una funzione dedicata, di solito presente nei programmi per la creazione di CD/DVD (es. *scrivi immagine* oppure *masterizza ISO*). Le istruzioni su come creare un CD/DVD avviabile a partire dall'immagine ISO sono facilmente reperibili su Internet o nella documentazione del proprio sistema operativo.

Avviare la macchina utilizzando il supporto appena creato. Se la macchina non eseguisse il boot da CD/DVD, fare riferimento alla documentazione del BIOS della scheda madre. Una problematica tipica è la configurazione della priorità del dispositivo di avvio. Il primo dispositivo di avvio deve essere il lettore CD/DVD.

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

NethServer interactive install

Consente di selezionare la lingua, configurare il supporto RAID, la rete, e il file system criptato. Sarà descritta più nel dettaglio nel prossimo paragrafo.

Other / NethServer unattended install

Questo metodo di installazione non richiede alcun tipo di intervento ed applica dove necessario i parametri predefiniti.

Installazione Standard CentOS

Utilizza le procedure di installazione standard di 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.

Modalità unattended

Al termine dell'installazione, il sistema sarà così configurato:

- Nome utente: `root`
- Password di default: `Nethesis,1234`
- Rete: DHCP abilitato su tutte le interfacce
- Tastiera: `en`

- Fuso orario: `Greenwich`
- Lingua: Inglese
- Dischi: se sono presenti due o più dischi, verrà creato un RAID1 sui primi due dischi

Opzioni installazione

E" possibile aggiungere parametri all'installazione automatica, premendo TAB e modificando la linea di comando.

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
```

Altre opzioni disponibili:

- lang: lingua del sistema, default è `en_US`
- keyboard: layout tastiera, default è `us`
- timezone: fuso orario, default è `UTC Greenwich`
- fspassword: abilita la crittografia del file system usando la password immessa Questa opzione può essere usata anche in Modalità interattiva

Modalità interattiva

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

- Lingua
- RAID software
- Configurazione di rete

Lingua

Selezionare in quale lingua si desidera utilizzare la modalità interattiva. Il layout della tastiera e il fuso orario saranno cambiati in base alla lingua selezionata. Entrambe le configurazioni saranno modificabili al primo login nell'interfaccia web.

La lingua del sistema è sempre l'inglese.

RAID software

Il RAID (Redundant Array of Independent Disks) consente di combinare tutti i dischi installati nel sistema, al fine di ottenere tolleranza ai guasti ed un incremento delle performance.

Questa schermata viene visualizzata se in fase di avvio sono stati rilevati due o più dischi.

Livelli disponibili:

- RAID 1: crea una copia esatta (mirror) di tutti i dati su due o più dischi. Numero minimo di dischi: 2

- RAID 5: usa una suddivisione dei dati a livello di blocco, distribuendo i dati di parità uniformemente tra tutti i dischi. Numero minimo di dischi: 3

Disco di spare

E" possibile creare un disco di spare se il numero dei dischi è maggiore del numero minimo richiesto dal livello raid selezionato. Un disco di spare è un disco che viene aggiunto al RAID qualora si verifichi un guasto.

Password amministratore di sistema

E" possibile cambiare la password dell'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 è `Nethesis,1234`.

File system cifrato

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.

E" possibile scegliere una password per la cifratura, altrimenti verrà utilizzata la password dell'amministratore.

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

Avvertimento: I seguenti caratteri non sono supportato all'interno della password: `#`, = e `$`.

Interfacce di rete

Selezionare l'interfaccia di rete che sarà utilizzata per accedere alla LAN. Questa interfaccia è detta anche rete *green*.

Configurazione di rete

Nome host e dominio (FQDN)

Digitare il nome host e dominio con il quale opererà il server (es. `server.mycompany.com`).

***NB*: I nomi di dominio posso contenere solo lettere, numeri e il** trattino

Indirizzo IP

Digitare un indirizzo IP privato (da RFC1918) da assegnare al server; nel caso si voglia installare la macchina in una rete già esistente occorrerà fornire un indirizzo IP libero, valido per per quella rete (in genere si tende ad usare il primo o l'ultimo host, per esempio 192.168.7.1 o .254).

Netmask

Digitare la subnet mask di rete. Generalmente si lascia invariata quella suggerita dal sistema.

Gateway

Digitare l'indirizzo IP del gateway della rete su cui si sta installando il server.

DNS

Digitare un DNS valido. Esempio: 8.8.8.8

Termine procedura installazione

Immessi i parametri la procedura avvierà l'installazione. Fare riferimento a *Passi successivi*.

2.1.4 Installazione su CentOS

È possibile installare NethServer su una nuova installazione di CentOS usando il comando **yum** per scaricare via rete i pacchetti software. Questo è il metodo di installazione racccomandato se si ha

- un server virtuale privato (VPS), oppure
- una chiavetta USB

Per esempio, per installare NethServer 6.10 si comincerà installando CentOS 6.10 sul sistema (molti fornitori di VPS offrono CentOS già pre-installato) e poi si eseguiranno alcuni comandi per trasformare CentOS in NethServer.

Abilitare repository specifici di YUM con questo comando:

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

2.1.5 Passi successivi

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

2.2 Accedere 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

Prima di accedere, è necessario autenticarsi attraverso nome utente e password. Compilare i campi come segue:

- Nome utente di default: **root**
- Password di default: Nethesis,1234

Avvertimento: Cambiare la password di root appena possibile, scegliendone una sicura, che sia composta da una sequenza casuale di lettere maiuscole, minuscole e da numeri e simboli.

In caso di installazione tramite software Center del File server, del server Mail o di un qualunque altro modulo che preveda l'utilizzo di Utenti e Gruppi, sarà possibile abilitare l'utente `admin` ed utilizzarlo per accedere all'interfaccia web con gli stessi privilegi dell'utente root. Vedi *Account admin*.

2.2.2 Timeout della sessione

Di default (a partire da NethServer 6.10), una sessione del Server Manager termina dopo **60 minuti di inattività** (idle timeout) e **scade dopo 8 ore dal login** (session life time).

I seguenti comandi impostano l'idle timeout a 2 ore e la session life time a 16 ore. Il tempo (Time) 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.

CAPITOLO 3

Configurazione

3.1 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 *Software center*, inclusi il backup e il supporto per gli utenti.

3.1.1 Dashboard

La pagina mostrata di default dopo il login è la Dashboard; qui viene visualizzato un riepilogo dello status 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`
- Profili roaming Windows: `/var/lib/nethserver/profile`
- Mail: `/var/lib/nethserver/vmail`
- Fax: `/var/lib/nethserver/fax`
- Database MySQL: `/var/lib/mysql`

3.1.2 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, ed esempio le 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

3.1.3 Servizi di rete

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

Tali servizi sono sempre accessibili da tutti i computer nella rete green (rete locale). E" possibile cambiare le politiche di accesso dalla pagina *Servizi di rete*.

Le politiche di accesso disponibili sono:

- Accesso solo dalle reti green (private): comprende tutti gli host sulla rete green e tutti i computer collegati in VPN

- Accesso dalle reti green e red (public): tutti gli host dalle reti green, VPN e reti esterne. Ma non dalla rete ospiti (blue) e dalla DMZ (orange)
- Accesso solo dal server stesso (none): nessun host può collegarsi al servizio selezionato

Accesso personalizzato

Se la politica selezionata è private o public, è possibile specificare una lista di host e reti che sono sempre consentiti (o bloccati) usando i campi *Consenti host* e *Blocca host*. La regola di applica anche per le reti orange e blue.

Esempio

Data la seguente configurazione:

- Rete orange: 192.168.2.0/24
- Server NTP con politica di accesso private

Se gli host dalla DMZ devono accedere al server NTP, aggiungere la rete 192.168.2.0/24 nel campo *Consenti host*.

3.1.4 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*.

3.1.5 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.

3.1.6 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.

3.1.7 Certificato del server

La pagina *Certificato del server* mostra il certificato SSL attualmente installato e che viene presentato da tutti i servizi presenti nel sistema.

Il pulsante *Nuovo certificato* consente di generare un nuovo certificato SSL auto-firmato. Se si genera un nuovo certificato, tutti i servizi SSL verranno riavviati e ai client di rete sarà richiesto di accettare il nuovo certificato.

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.

Installare un certificato personalizzato

I certificati personalizzati devono essere salvati all'interno delle seguenti directory:

- `/etc/pki/tls/certs`: chiave pubblica
- `/etc/pki/tls/private`: chiave privata

Configurare i percorsi della chiave pubblica e privata:

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

E" possibile anche configurare il file di chain SSL:

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

Segnalare il cambio di certificato a tutti i demoni:

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

Backup certificato personalizzato

Ricordarsi sempre di aggiungere i certificati personalizzati al backup della configurazione. E" sufficiente aggiungere i percorsi nel file `/etc/backup-config.d/custom.include`.

Per esempio, se il certificato è `/etc/pki/tls/certs/mycert.crt`, eseguire semplicemente:

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

Certificato Let's Encrypt

Let's Encrypt è una certification authority gratuita e aperta, gestita dall'associazione non-profit Internet Security Research Group (ISRG). Può creare certificati SSL validi utilizzabili sul sistema.

Da https://letsencrypt.readthedocs.org:

> Il Client Let's Encrypt è un client estremamente funzionale e estensibile per la CA Let's Encrypt (o qualsiasi altra CA che parli il protocollo ACME) che consente di automatizzare le attività per ottenere certificati e configurare i server web per utilizzarli.

Prerequisiti

1. Il server deve essere raggiungibile dall'esterno sulla porta 80.

   Assicurarsi che la porta 80 sia aperta al pubblico da Internet, è possibile controllarlo usando questo sito: http://www.canyouseeme.org/.

2. Il fully qualified name (FQDN) del server deve essere pubblico, associato all'indirizzo IP pubblico del server.

   Assicurarsi di avere un record DNS pubblico che punti al server, è possibile controllarlo con questo sito: http://viewdns.info/.

Come funziona

Il sistema crea un singolo certificato per l'FQDN (Fully Qualified Domain Name) del server.

Quando si desidera accedere al server, è necessario usare l'FQDN. Se si desidera accedere al server usando alias multipli. Let's Encrypt può aggiungere altri nomi FQDN validi al certificato per consentire l'accesso al server con altri nomi.

Esempio

L'FQDN del server: “”server.nethserver.org”” con IP pubblico ““1.2.3.4””. Si desidera accedere al server usando anche gli altri nomi associati (alias): “”mail.nethserver.org”” e “”www.nethserver.org””.

Il server deve:

- avere la porta 80 aperta su internet: accededendo all'indirizzo http://1.2.3.4 da un sito remoto, deve essere visibile la pagina di NethServer
- avere un record DNS pubblico per “”server.nethserver.org””, “”mail.nethserver.org”” e “”www.nethserver.org””. Tutti i record DNS devono puntare allo stesso server (il server può avere anche indirizzi IP multipli).

Installazione

Installare il pacchetto da linea di comando:

```
yum install nethserver-letsencrypt
```

Configurazione

La configurazione di Let's Encrypt deve essere fatta da linea di comando dall'utente root. Accedere al server usando un monitor o collegandosi via SSH.

Certificato per FQDN

Abilitare Let's Encrypt globalmente, questa operazione abilita la generazione del certificato per l'FQDN. Eseguire:

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

Certificato per alias (opzionale)

Il certificato FQDN può essere esteso per domini extra configurati come alias server. Questa funziona si chiama SubjectAltName (SAN): https://en.wikipedia.org/wiki/SubjectAltName

Creare un alias per il server all'interno della pagina DNS, quindi abilitare Let's Encrypt sul record appena creato.

Esempio per l'alias “”alias.mydomain.com””:

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

Opzioni

E" possibile personalizzare le seguenti opzioni utilizzando il comando config:

- `LetsEncryptMail`: se impostato, Let's Encrypt invierà una mail di notifica all'indirizzo specificato quando il certificato è in scadenza (deve essere attivato prima di eseguire lo script letsencrypt-certs per la prima volta!)
- LetsEncryptRenewDays: minimo numero di giorni entro i quali il certificato sarà rinnovato (default: 30)

Esempio:

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

Test di generazione del certificato

Dal momento che è possibile richiedere un certificato al massimo 5 volte in una settimana, assicurarsi che la configurazione sia corretta prima di procedere. Eseguire:

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

Questo comando genera un certificato di test usando Let's Encrypt. Se tutto è configurato correttamente, l'output dovrebbe essere simile al seguente:

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

Verificare la presenza del certificato rilasciato da Let's Encrypt CA per tutti i servizi che utilizzano SSL: se qualcosa dovesse andare storto, verificare che i prerequisiti siano soddisfatti.

Ottenere un certificato valido

Se la configurazione è stata validata con il test precedente, il sistema è pronto per richiedere un certificato valido. Eseguire il seguente script verso il server di Let's Encrypt:

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

Accedere al server http e verificare che il certificato sia valido.

3.1.8 Cambio password utente

Ogni utente può collegarsi al Server Manager utilizzando le proprie credenziali ed accedere al profilo utente.

Dopo l'accesso, l'utente potrà cambiare la propria password e le informazioni associate al proprio account:

- Nome e Cognome
- Indirizzo email esterno

L'utente può anche sovrascrivere i seguenti campi già impostati dall'amministratore:

- Società
- Ufficio
- Indirizzo
- Città

3.1.9 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.

3.1.10 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

3.1.11 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.

3.1.12 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
```

3.2 Software center

NethServer è altamente modulare: al termine dell'installazione il sistema contiene solo i moduli di base. La configurazione base include moduli come configurazione di rete e la visualizzazione log. L'amministratore può quindi decidere quali componenti installare in base alle proprie esigenze come *Email*, *Server DHCP e PXE* o *Firewall e gateway*.

La vista principale mostra una lista di componenti software disponibili ed installati (con segno di spunta). Si può filtrare la lista per categoria.

Per installare un componente software, aggiungere il segno di spunta, quindi premere il pulsante *Applica*. La schermata successiva riepiloga cosa sarà installato. Inoltre, viene mostrata la lista di pacchetti opzionali, da selezionare per l'installazione.

Nota: I pacchetti opzionali possono essere installati anche *dopo* l'installazione del componente relativo: cliccare di nuovo sul bottone *Applica* e selezionarli dalla schermata di riepilogo.

La sezione *Software installato* elenca i pacchetti installati sul sistema.

CAPITOLO 4

Moduli

4.1 Backup

Avere un Backup è l'unico modo per ripristinare una macchina in caso di calamità. Il sistema gestisce due tipi di backup:

- backup della configurazione
- backup dei dati

Il backup della configurazione contiene solo le configurazioni di sistema. Viene eseguito automaticamente ogni notte e genera un nuovo archivio, `/var/lib/nethserver/backup/backup-config.tar.xz`, solo in caso la configurazione sia cambiata nelle ultime 24 ore. Il backup della configurazione salva anche la lista dei moduli installati. Tutti i moduli saranno reinstallati durante il processo di ripristino. Lo scopo del backup della configurazione è quello di consentire un rapido ripristino della macchina in caso di disaster recovery. Dopo aver ripristinato la configurazione, la macchina può già essere messa in produzione mentre i dati vengono ripristinati in background.

Il backup dei dati è abilitato installando il modulo "Backup" e comprende i dati degli utenti come caselle di posta e cartelle condivise. Viene eseguito ogni notte e può essere completo o incrementale su base settimanale. Questo backup contiene anche il backup della configurazione.

Il backup dei dati può essere fatto su tre tipi di destinazione:

- USB: disco collegato via USB, utile in caso di molti dati, ma limitato dalla velocità dell'USB (Vedi: *Configurazione disco USB*)
- CIFS: cartella condivisa Windows, disponibile su tutti i NAS (Network Attached Storage)
- NFS: cartella condivisa Linux, disponibile su tutti i NAS, solitamente più veloce di CIFS

L'esito del backup può essere notificato all'amministratore o ad un indirizzo mail esterno.

Nota: La directory di destinazione è basta sul nome host del server: in caso di cambio FQDN, l'amministratore dovrà occuparsi di spostare manualmente i dati del backup dalla vecchia alla nuova directory.

4.1.1 Ripristino dati

Assicurarsi che la destinazione contenente il backup sia raggiungibile (es. disco USB collegato).

Linea di comando

Elenco contenuti

E' possibile elencare i file presenti nell'ultimo backup con il comando:

```
backup-data-list
```

Il comando può richiedere del tempo in base alla dimensione del backup.

File e directory

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>`

Dopo aver individuato il file da ripristinare, usare il comando:

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

Esempio, ripristinare nella directory `/tmp` la cartella di posta *test*:

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

Esempio, ripristinare la cartella di posta *test* nella posizione originale:

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

Il sistema supporta la possibilità di ripristinare directory (o file) ad una versione precedente rispetto all'ultimo backup.

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

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

L'opzione `-t` consente di specificare il numero di giorni (in questo caso 15).

Interfaccia grafica

Nel menu *Restore Data* è possibile cercare, selezionare e ripristinare una o più cartelle dal backup, navigando l'albero grafico con tutti i percorsi inclusi nel backup.

Ci sono due opzioni di ripristino:

- Ripristinare i dati nel percorso originale, i file correnti del filesystem sono sovrascritti con quelli ripristinati dal backup.
- Ripristinare i dati nel percorso originale ma i file ripristinati dal backup sono spostati in una nuova directory (i file non sono sovrascritti) in questo percorso:

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

Per usare il campo di ricerca, inserire almeno 3 caratteri e la ricerca partirà automaticamente, evidenziando le cartelle corrispondenti alla ricerca

Il ripristino delle cartelle avviene cliccando sul bottone **Ripristino**.

Nota: Tenendo premuto il tasto Ctrl è possibile effettuare la selezione multipla di cartelle.

4.1.2 Disaster recovery

Il sistema è ripristinato in due fasi: prima la configurazione, poi i dati. Al termine del ripristino, il sistema è pronto all'uso se i moduli sono già installati. E' possibile installare i moduli opzionali sia prima che dopo il ripristino. Ad esempio, se il server di posta è installato, il sistema è già in grado di inviare e ricevere mail.

Altre configurazioni ripristinate:

- Utenti e gruppi
- Certificati SSL

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

I passi da eseguire sono:

1. Installare una nuova macchina e configurarla con lo stesso nome host della vecchia
2. Installare e configurare il backup dei dati
3. Se la vecchia macchina era il gateway della rete, ricordarsi di reinstallare il modulo firewall
4. Eseguire il ripristino della configurazione dalla pagina *Backup (configurazione)* > *Ripristino* nel Server Manager, oppure eseguendo il comando **`restore-config`**
5. Se un avviso lo richiede, riconfigurare le interfacce di rete. Vedi *Assegnamento delle interfacce di rete*
6. Verificare che la macchina sia funzionante
7. Ripristinare i dati eseguendo il comando **`restore-data`**

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.

Se il ruolo mancante è `green` una procedura interattiva chiede di aggiustare la configurazione all'avvio del sistema, per assicurare una connettività di rete minima e accedere di nuovo al Server Manager.

Ripristino moduli installati

Il processo di ripristino della configurazione reinstalla tutti i moduli presenti precedentemente.

Per evitare che i moduli vengano reinstallati, eseguire questo comando prima del ripristino:

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

4.1.3 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.

Includere

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
```

Escludere

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`.

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

4.1.4 Personalizzazione backup configurazione

Nella maggior parte dei casi non è necessario modificare il beackup della configurazione. Può essere utile, ad esempio, se è stato installato un certificato SSL personalizzato. In questo caso è possibile aggiungere il percorso del file che contiene il certificato al backup della configurazione.

Includere

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/pki/mycert.pem`, aggiungere la linea:

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

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

Escludere

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

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

4.1.5 Configurazione disco USB

Si consiglia di formattare i dischi USB in formato EXT3 per le migliori prestazioni. Generalmente i dischi utilizzano il filesystem NTFS, che **non è supportato**. Il filesystem FAT è invece supportato ma *sconsigliato*.

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
```

(continues on next page)

(continua dalla pagina precedente)

```
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
  ```

- Creare il filesystem sulla partizione *sdc1* assegnando una label, ad esempio *backup*:

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

- 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)*.

4.2 Utenti e gruppi

4.2.1 Utenti

L'utente di sistema è necessario per accedere a molti servizi erogati da NethServer (email, cartelle condivise etc.).

Ogni utente è caratterizzato da una coppia di credenziali (utente e password). Un nuovo account utente rimane bloccato finché non viene impostata una password. Un utente bloccato non può utilizzare i servizi di server che richiedono l'autenticazione.

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

- Nome utente
- Nome
- Cognome

Campi opzionali:

- Società
- Ufficio
- Indirizzo
- Città
- Telefono

Al termine della creazione, l'utente risulta disabilitato fino a quando non viene settata una password usando il pulsante *Cambia password*. Quando un utente è abilitato, l'utente può accedere al Server Manager e cambiare la propria password: *Cambio password utente*.

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

A volte può essere necessario bloccare l'accesso ai servizi di un utente senza eliminare l'account. E" possibile farlo usando i pulsanti *Blocca* e *Sblocca*.

Nota: Quando l'utente viene eliminato, verranno eliminati anche tutti i dati dell'utente.

Accesso ai servizi

Dopo la creazione, un utente può essere abilito ad alcuni (o tutti) i servizi. La configurazione può essere fatta dalla sezione *Servizi*.

4.2.2 Gruppi

Un gruppo di utenti può essere usato per assegnare permessi speciali o per creare liste di distribuzione email.

Come gli utenti, un gruppo può essere abilitato ad alcuni (o tutti) i servizi.

Suggerimento: Per delegare l'accesso al Server Manager è possibile utilizzare i gruppi `managers` o `administrators`.

Si possono creare due gruppi speciali, gli utenti che appartengono a questi gruppi ottengono dei permessi aggiuntivi alle pagine del Server Manager.

- *administrators*: Gli utenti di questo gruppo hanno gli stessi permessi di root e admin.
- *managers*: Gli utenti di questo gruppo hanno l'accesso alle pagine della sezione Gestione.

4.2.3 Account admin

La pagina *Utenti* ha un elemento di default: *admin*. Questo account consente di accedere al Server Manager con gli stessi permessi dell'utente *root*. Inizialmente è *disabilitato* e non ha accesso dalla console.

Suggerimento: Per abilitare l'account `admin` impostare la sua password.

Dove possibile, l'utente `admin` ha dei privilegi speciali su alcuni servizi specifici, come *aggiungere una workstation al dominio Samba*.

4.2.4 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 dopo aver installato il modulo `nethserver-password`.

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)

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.

Per cambiare l'impostazione a none:

```
config setprop passwordstrength Users none
```

Per cambiare l'impostazione a strong:

```
config setprop passwordstrength Users strong
```

Verificare la policy attualmente in uso sul server:

```
config getprop passwordstrength Users
```

Scadenza

La scadenza delle password viene attivata di default a 6 mesi a partire dal momento in cui la password viene impostata. Il sistema invierà una mail informativa all'utente quando la sua password è in scadenza.

Nota: Al momento dell'attivazione il sistema farà riferimento alla data dell'ultimo cambio password, se tale data è precedente più di 6 mesi, il server invierà una mail per segnalare che la password è scaduta. In tal caso è necessario cambiare la password dell'utente. Ad esempio: se l'ultimo cambio password è stato fatto in gennaio, e l'attivazione della scadenza in ottobre, il sistema riterrà la password cambiata in gennaio come scaduta, e lo segnalerà all'utente.

Per ignorare la scadenza password globalmente (consentire l'accesso anche ad utenti con password scaduta):

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

Per disabilitare la scadenza password su un utente (sostituire username con l'utente):

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

Di seguito sono riportati i comandi per visualizzare le policy in uso.

Numero massimo di giorni per cui è possibile tenere la stessa password (default:180):

```
config getprop passwordstrength MaxPassAge
```

Numero minimo di giorni per cui si è costretti a tenere la stessa password (default 0):

```
config getprop passwordstrength MinPassAge
```

Numero di giorni in cui viene inviato il warning per email (default:7):

```
config getprop passwordstrength PassWarning
```

Per modificare i parametri sostituire al comando **`getprop`** il comando **`setprop`** e specificare in fondo alla riga il valore desiderato del parametro, infine dare il comando:

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

Ad esempio per modificare a 5 il «Numero di giorni in cui viene inviato il warning per email»:

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

Effetti password scaduta

Allo scadere della password l'utente sarà in grado di scaricare ed inviare regolarmente la posta ma non potrà più accedere alle cartelle e stampanti condivise sul server (Samba) o da altri pc in caso il pc faccia parte del dominio.

Password di dominio

In caso il sistema sia configurato come controller di dominio, l'utente potrà cambiare la propria password usando gli strumenti di Windows.

In quest'ultimo caso non è possibile impostare password più corte di 6 *caratteri* indipendentemente dalla configurazione delle policy sul server. Infatti Windows esegue dei controlli preliminari e invia le password al server dove vengono poi valutate con le policy in uso.

4.2.5 Lingua di notifica

La lingua di default per le notifiche è l'inglese. Se si desidera cambiarla, usare il seguente comando:

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

Esempio per l'italiano:

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

4.2.6 Importazione utenti

E" possibile importare una lista di utenti a partire da un file CSV. Il file deve contenere una linea per utente, ogni linea deve avere i campi separati da TAB, rispettando il seguente formato:

```
username    firstName    lastName    email    password
```

Esempio:

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

Assicurarsi che il modulo server di posta sia installato, quindi eseguire il comando:

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

Per esempio, se il file che contiene gli utenti si chiama `/root/users.csv`, eseguire:

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

Il comando può essere eseguito più volte: gli utenti esistenti saranno saltati.

Nota: Il comando fallisce se il modulo del server di posta non è installato.

4.3 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 anti-spam, anti-virus e blocco 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 anti-spam ed anti-virus ottimizzata

Vedi anche gli argomenti correlati:

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

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

4.3.1 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[8]
- *Passa ad un altro server* (*relay*): la posta ricevuta viene inoltrata 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 dirette ad uno specifico dominio: tutti i messaggi verranno consegnati sia al destinatario sia ad un utente (o gruppo) locale. Questa opzione è attivabile attraverso la check box *Spedisci sempre una copia (Bcc)*

Avvertimento: L'attivazione della «copia nascosta» va valutata attentamente, perché, in ambito aziendale, potrebbe essere equiparata ad un telecontrollo del lavoratore, vietato dalla legge in alcuni stati.

La funzionalità *Aggiungi una nota legale in calce ai messaggi inviati* aggiunge automaticamente alle email in spedizione un testo predefinito, detto disclaimer, utilizzabile per esempio, per soddisfare possibili requisiti di legge. Si noti che *firma* e disclaimer sono concetti molto diversi.

La firma dovrebbe essere inserita nel testo della email solo dal client di posta (il MUA): Outlook, Thunderbird, ecc.. È un testo personalizzabile contente ad esempio i dati del mittente, contatti, indirizzi, numeri di telefono.

Esempio di firma:

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

Il «disclaimer» invece, è un testo fisso e può essere soltanto «allegato» dal server. Il disclaimer viene allegato alla mail in uscita, non aggiunto al messaggio.

Questa tecnica permette di non alterarne la validità in caso di utilizzo 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.
```

Il disclaimer può contenere codice Markdown[9] che consente la formattazione del testo.

4.3.2 Indirizzi email

Il sistema consente la creazione di un numero illimitato di *indirizzi email* detti anche pseudonimi dalla pagina *Indirizzi email*. Ciascun indirizzo è associato ad un utente o un gruppo di sistema a cui è associata una *mailbox* (see *Caselle di posta di utenti e gruppi*). Può funzionare con tutti i domini configurati oppure solo su domini specifici. Per esempio:

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

- 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, un'azienda preferisce che le comunicazioni aziendali tramite email utilizzino degli indirizzi email «ufficiali» (amministrazione@dominio.it o supporto@dominio.it) piuttosto che indirizzi nominativi (nome.cognome@dominio.it), perché il destinatario potrebbe essere assente ed in questo caso non si corre il rischio di lasciarsi sfuggire eventuali risposte.

Quando si crea un nuovo account dalle pagine *Utenti* o *Gruppi*, il sistema suggerisce un indirizzo email di default per ogni dominio di posta configurato.

Per esempio, creando un nuovo profilo per l'utente *Donald Duck*:

- Nome utente: donald.duck
- Domini: ducks.net, ducks.com
- Indirizzi suggeriti: donald.duck@ducks.net, donald.duck@ducks.comjavascript:;

4.3.3 Caselle di posta di utenti e gruppi

I messaggi di posta elettronica consegnati ad un utente o gruppo, così come configurato dalla pagina *Indirizzi email*, sono scritti in una posizione del disco chiamata *casella di posta*.

Quando viene installato il modulo Email, eventuali utenti e gruppi già esistenti non hanno una casella di posta associata. Essa deve essere abilitata in maniera esplicita dalla scheda *Utenti* > *Servizi* o *Gruppi* > *Servizi*. Al contrario, i nuovi account hanno questa opzione abilitata di default.

Dalla stessa scheda *Servizi* delle pagine *Utenti* e *Gruppi* può essere impostato un indirizzo email esterno dove saranno inoltrati i messaggi. Una copia di ogni singolo messaggio può essere mantenuta sul server stesso.

Quando un indirizzo è associato ad un gruppo, il server può essere configurato per consegnare i messaggi di posta in due modi, dalla scheda *Gruppi* > *Servizi*:

- inviare una copia del messaggio a ciascun membro del gruppo
- depositare il messaggio in una *cartella condivisa*. Questa opzione è raccomandata per gruppi con tanti membri che ricevono allegati molto grandi.

Avvertimento: L'eliminazione di un gruppo o di un utente rimuove la casella di posta associata!

Dal pannello *Email* > *Caselle di posta* è possibile scegliere quali protocolli utilizzare per consentire l'access alle mailbox di utenti e gruppi:

- IMAP[10] (raccomandato)
- POP3[11] (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.

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

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 *Utenti* > *Modifica* > *Servizi* > *Quota email personalizzata*.

I messaggi marcati come spam (vedi *Filtro*) possono essere spostati automaticamente all'interno della cartella *junkmail* abilitando l'opzione *Sposta nella cartella «junkmail»*. 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 admin può impersonare un altro utente, acquisendo pieni diritti sui contenuti della casella di posta e sui permessi delle cartelle di quest'ultimo. L'opzione *Admin può accedere impersonando un altro utente* controlla questa facoltà, conosciuta con il nome di *master user* in[2].

Quando *Admin può accedere impersonando un altro utente* è abilitata, il server IMAP accetta qualsiasi nome utente al quale sia aggiunto il suffisso `*admin`, e la password di admin come credenziali valide.

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

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

4.3.4 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.

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 della «copia nascosta» va valutata attentamente, perché, in ambito aziendale, potrebbe essere equiparata ad un telecontrollo del lavoratore, vietato dalla legge in alcuni stati.

L'opzione *Invia tramite smarthost* obbliga tutti i messaggi in uscita ad essere diretti verso un server SMTP speciale, detto in gergo *smarthost*. Uno smarthost accetta d'inoltrare i messaggi sotto certe restrizioni. Potrebbe controllare:

- 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[12], o il traffico SMTP sia bloccato dall'ISP.

4.3.5 Filtro

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

- Blocco allegati
- Anti-virus
- Anti-spam

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:

- *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.

Anti-virus

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

Anti-spam

Il filtro *anti-spam*[14] analizza la posta elettronica rilevando e classificando un messaggio come *spam*[13] utilizzando criteri euristici, regole predeterminate e valutazioni statistiche sul contenuto del messaggio. Le regole sono pubbliche e aggiornate periodicamente. Il filtro inoltre può controllare se il server mittente è presente in una o più blacklist (DNSBL). Un punteggio è associato ad ognuna di queste regole.

Il punteggio totale raccolto alla fine dell'analisi consente al server di decidere se rifiutare il messaggio o marcarlo come spam e consegnarlo lo stesso. Le soglie dei punteggi sono controllate mediante i cursori *Soglia spam* e *Soglia rifiuto messaggio*, nella pagina *Email* > *Filtro*.

I messaggi marcati come spam hanno uno speciale header `X-Spam-Flag: YES`. L'opzione *Aggiungi un prefisso all'oggetto dei messaggi spam* evidenzia i messaggi marcati come spam, modificandone con la stringa data l'oggetto (header `Subject`).

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

I filtri statistici, chiamati *bayesiani*[15], sono regole speciali che evolvono e adattano rapidamente l'esito dell'analisi dei messaggi marcandoli come **spam** o **ham**.

I filtri bayesiani possono essere addestrati mediante un qualsiasi client IMAP, semplicemente spostando un messaggio dentro o fuori della *cartella «junkmail»*. Come prerequisito, la cartella junkmail deve essere abilitata dalla pagina *Email* > *Caselle di posta*, abilitando l'opzione *Sposta nella cartella «junkmail»*.

- *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.

Normalmente qualsiasi utente può addestrare i filtri con questa tecnica. Se un gruppo chiamato `spamtrainers` esiste, solo gli utenti di questo gruppo saranno invece autorizzati ad addestrare i filtri.

Nota: E" 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

Benchè sconsigliato è possibile creare regole non solo sul singolo indirizzo email, ma su un intero dominio di posta, per farlo è sufficiente specificare solo il dominio nella regola (es: nethserver.org).

Nota: Il controllo anti-virus è eseguito indipendentemente dalle impostazioni di *whitelist*.

4.3.6 Blocco porta 25

Se il sistema è anche il gateway della rete, le zone blue e green non potranno inviare mail a server esterni usando la porta 25 (SMTP). Il blocco della porta 25 evita che macchine nella LAN siano utilizzate da remoto per l'invio di SPAM.

L'amministratore può cambiare questa politica creando un'apposita regola del firewall nella pagina *Regole*.

4.3.7 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

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

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

- LOGIN
- PLAIN

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 per i trasferimenti di messaggi tra server MTA. Nei client utilizzare solo le porte summenzionate.

Se NethServer agisce anche come server DNS nella LAN, registra il suo nome come record MX insieme ai seguenti alias:

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

Esempio:

- Dominio: `miosito.com`
- Hostname: `mail.miosito.com`
- MX record: `mail.miosito.com`
- Alias disponibili: `smtp.miosito.com`, `imap.miosito.com`, `pop.miosito.com`, `pop3.miosito.com`.

Nota: Alcuni client email (es.: Mozilla Thunderbird) sono in grado di usare gli alias DNS e il record MX per configurare automaticamente gli account di posta, digitando soltanto l'indirizzo email.

Per disabilitare il record MX e gli alias, accedere alla console di root e digitare:

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

4.3.8 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 ambienti nuovi!

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*.

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.

4.3.9 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.

4.3.10 Email in Active Directory

Il modulo Email si integra in un ambiente Active Directory (AD) se il ruolo *Active Directory member* è abilitato nella pagina *Rete Windows*.

Assicurarsi che il valore del campo *Ramo LDAP degli account* nella pagina *Rete Windows* sia correttamente impostato al ramo LDAP sotto cui gli utenti e i gruppi per cui attivare l'email sono posizionati.

Questo è l'esempio di un nodo LDAP corrispondente ad un utente di AD (alcuni attributi sono stati omessi):

```
dn: CN=John Smith,OU=Sviluppo,OU=Nethesis,DC=adnethesis,DC=it
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: John Smith
sn: Smith
givenName: John
distinguishedName: CN=John Smith,OU=Sviluppo,OU=Nethesis,DC=adnethesis,DC
 =it
instanceType: 4
displayName: John Smith
memberOf: CN=sviluppo,OU=Nethesis,DC=adnethesis,DC=it
memberOf: CN=secgroup,OU=Nethesis,DC=adnethesis,DC=it
memberOf: CN=tecnici,OU=Nethesis,DC=adnethesis,DC=it
```

(continues on next page)

(continua dalla pagina precedente)

```
name: John Smith
primaryGroupID: 513
sAMAccountName: john.smith
sAMAccountType: 805306368
userAccountControl: 66048
userPrincipalName: john.smith@adnethesis.it
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=adnethesis,DC=it
mail: john@adnethesis.it
otherMailbox: smtp:js@adnethesis.it
proxyAddresses: smtp:j.smith@adnethesis.it
```

Per far funzionare NethServer con il database LDAP esterno di Active Directory vengono applicate le seguenti regole:

1. Sono considerati solo gli account abilitati (attributo `userAccountControl`).
2. Il nome di login per IMAP e SMTP è preso dall'attributo `sAMAccountName`.
3. Gli indirizzi email associati ad un utente provengono dagli attributi `mail`, `otherMailbox` e `proxyAddresses`. Gli ultimi due si aspettano il prefisso `smtp:` prima del valore vero e proprio. Inoltre `userPrincipalName` è di default considerato anche come indirizzo email, ma può essere disabilitato (vedi *i comandi qui sotto*).
4. L'indirizzo email di un gruppo è preso dal suo attributo `mail`. Per default ogni gruppo è trattato come una *lista di distribuzione*: una copia del messaggio è consegnata ai suoi membri.
5. Il suffisso di dominio degli indirizzi email specificati dagli attributi suddetti deve corrispondere ad uno dei *domini configurati*, altrimenti viene ignorato.

Per configurare globalmente i gruppi di sicurezza per ricevere i messaggi in una *cartella condivisa*, digitare i seguenti comandi nella console di root:

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

Avvertimento: Evitare le lettere maiuscole nel nome dei gruppi di AD con cartella condivisa: le ACL IMAP non funzionano come atteso. Vedere BUG#2744.

Per evitare che l'attributo `userPrincipalName` sia considerato un indirizzo email valido, digitare i seguenti comandi nella console di root:

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

4.3.11 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.

4.3.12 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

Di seguito una breve descrizione dei nomi dei componenti e delle azioni tipiche che eseguono:

`transfer/smtpd`

Identifica il demone SMTP in ascolto sulla porta 25 pubblica. Una riga di log di questo componente segnala un'attività che coinvolge un altro server di posta (MTA).

`submission/smtpd`

Identifica il demone SMTP in ascolto sulla porta 587 o 465 pubblica. Una riga di log di questo componente segnala un'attività che coinvolge un client di posta (MUA) che spedisce un messaggio.

`amavis`

Il demone SMTP Amavis applica tutte le regole di filtraggio della posta elettronica. Le righe di log di questo componente dettagliano le decisioni prese dal filtro.

`queue/smtpd`

Identifica un demone SMTP interno, accessibile unicamente dal sistema locale. Si occupa di ricevere e mettere in coda i messaggi buoni provenienti da Amavis.

`relay/smtp`

Questo è il client SMTP connesso ad un server remoto: prende un messaggio dalla coda e lo trasferisce al server remoto, così come specificato dalla configurazione dei domini di posta.

`delivery/lmtp`

I messaggi diretti agli account locali sono presi dalla coda e trasferiti all'istanza di Dovecot locale.

`dovecot`

Il demone Dovecot consegna i messaggi nelle caselle di posta degli utenti, eventualmente applicando i filtri Sieve.

Un quadro di tutto il sistema è disponibile dal sito workaround.org[16].

Riferimenti

4.4 Webmail

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

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

- 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

4.4.1 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
```

4.4.2 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
```

4.5 Connettore POP3

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 o gruppi locali.

Si sconsiglia di utilizzare il connettore POP3 come metodo primario di gestione della posta elettronica, perché vincola al provider, con i relativi problemi di spazio sulla casella, disservizi dell'accesso POP3. Inoltre l'efficacia dei filtri antispam viene ridotta perché non sono più disponibili le informazioni sulla provenienza diretta della mail.

Gli account POP3/IMAP sono configurati dalla pagina *POP3 connector* > *Indirizzi esterni*. Per ogni account possono essere specificati:

- l'indirizzo email (come identificativo per l'account),
- il protocollo (IMAP/POP3),
- l'indirizzo del server remoto,
- le credenziali dell'account,
- l'utente o il gruppo locale dove consegnare i messaggi,
- se SSL va disabilitato (sconsigliato),
- se un messaggio va eliminato dal server remoto dopo la consegna.

Nota: È possibile creare un numero illimitato di account esterni associati ad un gruppo o un utente di sistema. L'eliminazione di un account *non* comporta l'eliminazione dei messaggi già consegnati.

Dopo aver completato la configurazione degli account, il modulo Connettore POP3 va attivato esplicitamente dalla pagina *Connettore POP3* > *Generale*. Nella stessa pagina si può impostare ogni quanto controllare la presenza di messaggi nel server remoto, dal menù *Controlla ogni*.

L'implementazione sottostante è basata su *Fetchmail*[1]. Dopo aver scaricato i messaggi dal provider POP3/IMAP, Fetchmail li consegna localmente connetendosi direttamente al filtro di posta locale. I messaggi vengono filtrati in base alle *regole configurate*.

Tutte le operazioni di download sono riportate nei seguenti file:

- `/var/log/fetchmail.log`
- `/var/log/maillog`

Avvertimento: Se un account di *Active Directory* scelto per la consegna viene eliminato in un secondo momento, la configurazione diventa inconsistente. La configurazione dell'account esistente nella pagina *Connettore POP3* deve essere disabilitata o eliminata.

[1] Fetchmail è una programma per ricevere e inoltrare la posta remota http://www.fetchmail.info/

Riferimenti

4.6 Proxy POP3

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
- antispam: i messaggi verranno marcati con gli opportuni punteggi antispam

4.6.1 POP3s

Il proxy può anche intercettare connessioni POP3s sulla posrta 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 ma dovranno disattivare la cifratura.

4.7 Cartelle condivise

Una *cartella condivisa* è un posto dove i file sono accessibili da un gruppo di persone, utilizzando diversi metodi, o *protocolli*. Poiché NethServer è un sistema modulare, i metodi disponibili dipendono da quali moduli sono stati installati.

I metodi/protocolli disponibili sono:

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

4.7.1 Permessi di accesso

Una cartella condivisa appartiene sempre ad un gruppo di utenti (*Gruppo proprietario*). Ogni membro del gruppo può leggere i contenuti della cartella. Opzionalmente, al gruppo può essere concesso di modificare il contenuto della cartella e i permessi di lettura possono essere estesi a chiunque abbia accesso al sistema. Questo semplice modello di permessi è basato sui tradizionali permessi del filesystem di UNIX.

I permessi di accesso possono essere ulteriormente raffinati dalla scheda *ACL*, consentendo a singoli utenti o ad altri gruppi i permessi di lettura o scrittura. Questo modello di permessi esteso è basato sulla specifica POSIX ACL.

4.7.2 Accesso web

Il metodo *Accesso web* consente la connessione di un browser web ad una cartella condivisa mediante il protocollo HTTP. Le risorse web sono identificate da una stringa, detta Uniform Resource Locator, o URL.

Per esempio, se il nome della cartella condivisa è `docs` gli URL per accedervi potrebbero essere:

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

Ogni URL ha tre componenti:

- protocollo (`http://` or `https://`),
- nome host (`192.168.1.1`, `myserver`, `www.domain.com`),
- percorso (`docs`).

Il gruppo *Indirizzo web* definisce il componente «percorso».

- *Nome cartella* è il default, lo stesso della cartella condivisa, come `docs` nell'esempio precedente.
- *Radice del sito web* significa nessun percorso. Per esempio `http://docs.domain.com`.
- *Personalizzato* significa un nome alternativo, da specificare.

Il selettore *Host virtuale* elenca tutti gli *Alias server* definiti nella pagina *DNS*. «Tutti» significa che il nome host non è considerato nell'associare l'URL alla cartella condivisa.

L'accesso web è anonimo è in sola lettura. Ci sono alcune opzioni con cui restringere ulteriormente il permesso di accesso.

- *Consenti l'accesso solo dalle reti fidate*, restringe l'accesso in base all'indirizzo IP del client,
- *Richiedi la password*, limita l'accesso a chi conosce la password condivisa (da specificare).
- *Richiedi connessione SSL cifrata*.

4.7.3 Configurare un'applicazione web

La casella *Consenti override di .htaccess e dei permessi di scrittura* attiva una speciale configurazione di Apache pensata per ospitare una semplice applicazione web in una cartella condivisa. Consente di modificare la configurazione di default di Apache e di concedere i permessi di scrittura per specifice sub-directory.

Avvertimento: Se una cartella condivisa contiene condice eseguibile, come ad esempio script PHP, i permessi degli utenti e le possibili implicazioni di sicurezza devono essere vaultati attentamente.

Se la casella è abilitata

- i file con nome `.htaccess` sono caricati come configurazione di Apache <http://httpd.apache.org/docs/2.2/howto/htaccess.html>‘_.
- un file di testo con nome `.htwritable` posizionato nella radice della cartella condivisa può contenere una lista di sotto-directory dove Apache ottiene i permessi di scrittura. La sintassi del file è una sotto-directory per ogni riga. Le righe che iniziano con # sono commenti. Quando il contenuto del file `.htwritable` cambia il pulsante *Reimposta permessi* deve essere premuto di nuovo per propagare i permessi al file system.

Nota: Le cartelle condivise sono uno strumento potente ma non vanno intese come una soluzione completa per il web hosting! Per configurare Apache e i virtual host in maniera più avanzata aggiungere un file `.conf` sotto la directory `/etc/httpd/conf.d/`. Fare riferimento alla documentazione di Apache per questo.

4.7.4 Samba

SMB/CIFS è un protocollo molto diffuso che consente di condividere file in una rete di computer. In un modo simile agli URL Web visti sopra, 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
```

I client compatibili con SMB possono essere utilizzati per impostare le ACL su specifici file o sotto-directory. In ogni momento, il pulsante *Reimposta permessi* ripristina i permessi UNIX e POSIX secondo quanto definito nelle schede *Generale* e *ACL*.

Se l'opzione *Cestino di rete* è abilitata, i file rimossi da una cartella condivisa sono in realtà spostati in una directory «cestino» speciale. L'opzione *Mantieni file omonimi* assicura che i file nel cestino abbiano sempre nomi distinti, impedendo la sovrascrittura.

Se è attiva l'opzione *Accesso guest*, sono considerate valide qualsiasi credenziali vengano presentate.

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.

4.8 Windows network

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

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

Currently the following roles are available:

- Workstation
- Primary Domain Controller
- Active Directory Member

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

Workstation

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

Primary Domain Controller

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

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

Active Directory member

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

4.8.1 Workstation

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

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

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

4.8.2 Primary domain controller

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

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

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

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

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

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

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

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

4.8.3 Active Directory member

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

Joining an Active Directory domain has some pre-requisites:

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

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

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

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

4.9 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
- possibilità di suddividere gli utenti in gruppi, in base all'azienda o al dipartimento/ufficio
- amministratori chat
- messaggi broadcast
- chat di gruppo
- messaggi offline
- trasferimenti file in LAN

Tutti gli utenti di sistema possono accedere alla chat usando le proprie credenziali.

4.9.1 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.

4.9.2 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*.

4.10 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 attraverso il *Software center*. Dalla pagina *UPS* sarà possibile verificare i modelli supportati digitandone il nome nel campo *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.

4.10.1 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
```

4.10.2 Statistiche UPS

Se il modulo statistiche (collectd) è installato e funzionante, il modulo raccoglierà automaticamente statistiche sullo stato dell'UPS.

4.11 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

4.11.1 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.

4.11.2 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*

Assicurarsi inoltre che sia abilitata l'opzione *Visualizza fax inviati dai client*.

4.11.3 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 «Fax Number: «, contente il numero fax, per esempio:

```
Fax Number: 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.

4.11.4 Mail2Fax

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.

4.11.5 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

4.12 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

Nota: Assicurarsi di avere installato il modulo Utenti (pacchetto nethserver-directory), se si desidera utilizzare la modalità autenticata.

4.12.1 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.

Il certificato del server è posizionato in `/etc/pki/tls/certs/NSRV.crt`, può essere scaricato dai client all'indirizzo `http://<ip_server>/proxy.crt`.

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*.

4.12.2 Proxy SSL

Avvertimento: Decifrare connessioni SSL senza il consenso dell'utente è illegale in molti stati.

In modalità trasparente SSL, il server è in grado di filtrare anche il traffico cifrato in HTTPS. Il proxy stabilisce il collegamento SSL con i siti remoti, verifica la validità dei certificati, e decifra il traffico. Infine genera un nuovo certificato firmato con la Certification Authority (CA) del server stesso.

Il traffico fra il client e il proxy è sempre cifrato, ma sarà necessario installare su tutti i client (browser) il certificato CA del server.

Il certificato server si trova nel percorso `/etc/pki/tls/certs/NSRV.crt`. È consigliabile trasferire il file utilizzando un client SSH (ad es. FileZilla).

4.12.3 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 sorgente, configurabili nella sezione *Host senza proxy*
- bypass per destinazione, configurabili nella sezione *Siti senza proxy*

Le regole di bypass create sono configurate anche all'interno del file WPAD.

4.12.4 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 generare un nuovo report HTML. Il collegamento all'interfaccia web è disponibile nella scheda *Applicazioni* all'interno della *Dashboard*.

4.12.5 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 squid 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
```

4.12.6 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
```

4.13 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 Utenti da Active Directory

Se il server è stato configurato per fare il join ad un dominio Active Directory (*Active Directory member*), è possibile creare profili collegati ad utenti appartenenti al dominio.

Nota: I gruppi residenti nell'Active Directory non sono supportati.

4.13.3 Antivirus

Si consiglia di abilitare sempre la scansione antivirus sul contenuto delle pagine. Se il proxy è configurato in modalità trasparente SSL (*Proxy SSL*), la scansione funziona anche sui contenuti scaricati via HTTPS.

4.13.4 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 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)

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

4.14.1 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.

4.14.2 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
- Sorgente:
- Destinazione:
- Servizio:

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*.

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`.

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: -

4.14.3 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 configurare due o più schede red, è obbligatorio procedere alla configurazione dei provider dalla pagina *Multi WAN*.

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.

4.14.4 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 in ascolto sul range di porte compreso tra 5000 e 6000

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.

In caso si voglia rendere accessibile dall'esterno il server sull'intero range di porte compreso tra 5000 e 6000 si dovrà creare un port forward fatto così:

- 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

4.14.5 NAT 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.

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.

4.14.6 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 attivare il traffic shaping è necessario conoscere la quantità di banda disponibile nelle due direzioni e compilare i campi indicando la velocità nominale del link Internet, consapevoli del fatto che in caso di congestione da parte del provider non c'è nulla da fare per poter migliorare le prestazioni.

La configurazione della banda può essere effettuata nella pagina *Gestione banda -> Regole interfacce*.

Il sistema prevede tre livelli di priorità, alta, media e bassa: di default tutto il traffico ha priorità media, ma è possibile assegnare priorità alta o bassa a determinati servizi in base alla porta utilizzata (per esempio bassa al traffico peer to peer).

Da evidenziare il fatto che il sistema funziona anche senza che vengano specificati servizi a priorità alta o bassa, perché, di default, il traffico interattivo viene automaticamente gestito ad alta priorità (significa che, per esempio, non è necessario specificare porte per il traffico VoIP o SSH). Anche al traffico di tipo PING è garantita alta priorità.

Nota: Assicurarsi di specificare una stima accurata della banda disponibile.

4.14.7 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.

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.

4.14.8 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.

4.15 Cloud content filter

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

4.15.1 Preliminary operations

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

4.15.2 Configuration

The configuration is composed of two parts:

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

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

Manual or transparent proxy

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

Steps:

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

Authenticated proxy

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

Steps:

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

---

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

4.16 Proxy pass

La funzionalità proxy pass è utile quando si desidera accedere a siti interni dall rete esterna.

La configurazione del proxy pass deve essere effettuata da linea di comando. Prima di procedere, assicurarsi che il pacchetto `nethserver-httpd` sia installato:

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

Scenario:

- NethServer è il firewall della LAN
- Si possiede il dominio http://mydomain.com
- Si desidera inoltrare le richieste per http://mydomain.com/mysite ad un server interno (IP interno: 192.168.2.100)

Comandi per questo esempio:

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

E" possibile restringere l'accesso ad una lista di IP:

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

4.16.1 Configurazione manuale

Se questa configurazione non è abbastanza, è sempre possibile creare manualmente il proprio proxy pass 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>
```

Far riferimento alla documentazione ufficiale di Apache per maggiori informazioni: http://httpd.apache.org/docs/2.2/mod/mod_proxy.html

4.17 IPS (Snort)

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

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

A special widget inside the dashboard summarizes all detected attacks.

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

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

---

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

4.18 Monitor banda (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 è in ascolto

4.19 Statistiche (collectd)

Collectd è un demone che si occupa di raccogliere periodicamente le statistiche di performance del sistema e li salva in file RRD. Le statistiche saranno visibili all'interno dell'interfaccia web chiamata

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

L'interfaccia web creerà un URL casuale accessibile dalla scheda *Applicazioni* all'interno della *Dashboard*. E" possibile condividere l'URL casuale per consentire la visualizzazione dei grafici agli utenti non autenticati. L'accesso è consentito unicamente dalle zone e dagli indirizzi IP del servizio http-admin (vedi Servizi di rete).

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 ogni metrica, l'interfaccia web visualizzerà un grafico che contiene l'ultimo valore raccolto ed anche i valori minimi, massimi e medi.

4.19.1 Latenza di rete

Il plugin ping misura la latenza di rete. Ad intervalli regolari, invia un ping ICMP al DNS configurato a monte. Se il modulo multi WAN è configurato, viene anche verificato ciascuno dei provider abilitati.

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 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

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

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

4.20.1 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.

4.20.2 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.

4.21 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.

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

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.

4.21.1 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.

4.21.2 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.

4.21.3 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.

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:

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

```
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

4.22 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

4.22.1 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)

Il collegamento OpenVPN net2net prevede che uno dei server coinvolti venga eletto come master, mentre tutti gli altri sono considerati slave (client).

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

4.22.2 IPsec

Il protocollo IPsec (IP Security) viene di norma utilizzato per realizzare dei tunnel con dispositivi di altri produttori

Roadwarrior (L2TP)

L2TP è considerato il sostituto di PPTP ormai ritenuto insicuro. Molti dispositivi includono il supporto nativo per questo protocollo ma non tutte le implementazioni sono compatibili fra loro.

I metodi di autenticazione supportati sono:

- utente di sistema, password e certificato
- chiave condivisa segreta (PSK)

Per consentire ad un client di stabilire una VPN:

1. Configurare il server come PDC (Primary Domain Controller) dalla pagina *Rete Windows*.
2. Creare un nuovo account di sistema.
3. Scaricare il file che contiene i certificati.
4. Importare i certificati del client e della CA (Certification Authority) all'interno del client.
5. Procedere alla configurazione con i dati di collegamento al server ed avviare la VPN.

Nota: Si consiglia di utilizzare L2TP se e solo se sul dispositivo da collegare non è possibile installare il client OpenVPN.

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.

4.23 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.

4.23.1 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
```

4.24 ownCloud

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

Key features:

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

4.24.1 Installation

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

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

- change the default password

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

4.24.2 LDAP Configuration

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

1. Copy the LDAP password using the following command:

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

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

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

7. Fill «User filter» tab with:

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

8. Fill «Access filter» tab with:

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

9. Fill «Group filter» tab with:

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

10. Configure «Advanced» tab with:

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

Special Attributes
    Email field: email
```

11. Configure «Expert» tab with:

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

12. Click the «Save» button

4.24.3 LDAP Note

User list

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

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

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

4.24.4 Trusted Domains

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

- domain name
- ip address

To add a new one use:

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

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

4.25 Phone Home

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 per mezzo di specifiche API. 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.

4.25.1 Panoramica

Questa applicazione è *disabilitata* di default.

Per abilitarla, eseguire: `config set phone-home configuration status enabled`

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.

4.25.2 Configurazione

Se si utilizza un proxy, modificare opportunamente i relativi segnaposto che si trovano nel file `phone-home` disponibile nel percorso `/etc/sysconfig/` :

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

4.26 WebVirtMgr

Queto tool è usato per la gestione di macchine virtuali attraverso una semplice interfaccia web:

- Creazione e rimozione di macchine virtuali (KVM)
- Creazione di template per la creazione di macchine
- Accesso remoto tramite shell
- Interfaccia grafica accattivante

4.26.1 Configurazione

L'applicazione web è in ascolto sulla porta **8000** del server, per esempio: `http://HOST_IP:8000/`.

Il servizio è disabilitato di default.

Dalla pagina *Macchine virtuali* è possibile:

- abilitare il gestore delle macchine virtuali
- abilitare l'accesso alla console delle macchine virtuali direttamente dal browser

Per accedere all'interfaccia web, effettuare il login con le credenziali disponibili nella pagina stessa:

- *Utente*: admin
- *Password*: casuale, alfanumerica (modificabile)

Avvertimento: Non creare bridge di rete usando l'interfaccia di WebVirtManager. È sufficiente creare il bridge dalla pagina *Rete* ed utilizzarlo all'interno di WebVirtManager.

Per maggiori informazioni si rimanda alla documentazione ufficiale:

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

4.27 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 presentando lo stato attuale del sistema.

Il server è disabilitato di default.

Alla prima configurazione, si consiglia di configurare i 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

4.28 WebTop 4

WebTop è un groupware completo che implementa il protocollo ActiveSync.

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

4.28.1 Autenticazione

Interfaccia web

Il login all'applicazione web è sempre effettuato usando utente semplice e password, a prescindere da quanti domini di posta siano configurati.

Esempio

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

Active Sync

Il login ad Active Sync è invece <utente>@<dominio> dove `<dominio>` è il dominio del server che fa parte del FQDN.

Esempio

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

Quando si configura un account Active Sync, assicurarsi di specificare l'indirizzo del server e lasciare vuoto il campo dominio.

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, NethTop è accessibile con un 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 NethTop.

Avvertimento: E" fortemente consigliato cambiare la password di admin 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

4.28.2 WebTop vs SOGo

WebTop e SOGo possono essere installati sulla stessa macchina.

ActiveSync è abilitato di default sia su SOGo che su WebTop, ma se sono entrambi 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-webtop4-update
```

Tutti i filtri di posta configurati da SOGo, devono essere ricreati manualmente all'interno dell'interfaccia di NethTop. La stessa cosa si applica se l'utente sta effettuando il passaggio inverso da NethTop a SOGo.

4.28.3 Autenticazione Active Directory

Dopo aver eseguito il join al dominio Active Directory, accedere alla pagina di amministrazione di WebTop, dall'albero di sinistra selezionare *Domini -> NethServer*.

Modificare i campi nella pagina come segue:

- Authentication Uri: selezionare la modalità `ldapAD` e indicare il nome FQDN completo del server e la porta 389. Esempio: w2k8.nethserver.org:389
- Admin LDAP: nome dell'utente amministratore del dominio AD
- Password LDAP: password dell'utente amministratore del dominio AD

Dopo il salvataggio, nella pagina *Utenti* saranno visualizzati gli utenti di Active Directory.

4.28.4 Importazione da SOGo

E" possibile migrare alcuni dati da SOGo a WebTop utilizzando i seguenti script:

- Calendari: `/usr/share/webtop/doc/sogo2webtop_cal.php`
- Rubriche: `/usr/share/webtop/doc/sogo2webtop_card.php`

Prima di utilizzare gli script è necessario installare questo pacchetto:

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

Entrambi gli script vanno eseguiti indicando il nome utente di cui si vuole eseguire l'importazione da SOGo: :.

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

Dove `user` può essere un nome utente oppure `all`.

Esempi

Importare tutte le rubriche presenti su SOGo:

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

Importare il calendario dell'utente «foo»:

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

Nota: Se lo script viene eseguito più volte verranno importati più volte sia calendari che rubriche. Attualmente non è supportata l'importazione sia delle liste di distribuzione dalle rubriche che degli eventi ricorrenti dai calendari.

4.28.5 Importazione da Outlook PST

E' possibile importare email, calendari e rubriche da un archivio PST Outlook .

Prima di utilizzare lo script installare il pacchetto *libpst*:

```
yum install libpst -y
```

Mail

Script per importare i messaggi di posta: `/usr/share/webtop/doc/pst2webtop.sh`

Per iniziare l'importazione eseguire lo script indicando il file PST e l'utente di sistema:

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

Verranno importati tutti i messaggi di posta. Contatti e calendari verranno salvati all'interno di file temporanei per successiva importazione. Lo script elencherà tutti i file temporanei creati.

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 precedente pst2webtop.sh abbia generato il seguente output a seguito dell'importazione delle mail:

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

Per importare nella Rubrica predefinita (WebTop) dell'utente *foo*:

```
/usr/share/webtop/doc/pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Cartelle personali/
↪Contatti/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 precedente pst2webtop.sh abbia generato il seguente output a seguito dell'importazione delle mail:

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

Per importare nel Calendario predefinito (WebTop) dell'utente *foo*:

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

Nota: Lo script importa gli eventi utilizzando il fuso orario dall'utente WebTop, se configurato. Altrimenti verrà utilizzato il fuso orario del sistema.

4.28.6 Integrazione Google e Dropbox

Ogni utente può integrare i propri account Google Drive e Dropbox all'interno di WebTop. Prima di procedere, l'amministratore deve creare una coppia di credenziali per l'accesso alle 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

  Da shell accedere al database webtop:

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

  Eseguire le query, sostituendo al campo `__value__` il valore corrispondente:

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

Dropbox API

- Accedere a https://www.dropbox.com/developers/apps e creare una nuova app
- Inserire la coppia di credenziali appena create (App key e App secret) nella configurazione di WebTop.

  Da shell accedere al database webtop:

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

  Eseguire le query, sostituendo al campo `__value__` il valore corrispondente:

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

Se si desidera cambiare il limite massimo di utenti, verificare la procedura corretta nella documentazione ufficiale di Dropbox.

Nota: La versione Enteprise è già integrata con Google e Dropbox.

4.29 Adagios

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

Key features:

- full view/edit of hosts,services, etc
- tons of pre-bundled plugins and configuration templates
- network scan
- remote installation of linux/windows agents
- modern Status view as an alternative to default nagios web interface
- backup Adagios data with NethServer backup data tool
- rest interface for status of hosts/services and for for viewing and modifying configuration
- full audit of any changes made

4.29.1 Installation

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

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

For more information, see official documentation:

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

4.30 OCS Inventory NG

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

Key features:

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

4.30.1 Installation

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

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

For more information, see official documentation:

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

4.31 HA (High Availability)

NethServer supports High Availability only for some specific scenarios.

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

This configuration supports:

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

Example

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

4.31.1 Limitations

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

4.31.2 Hardware requirements

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

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

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

Fence device

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

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

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

External links:

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

4.31.3 Installation

Before install:

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

Primary node

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

Configuring DRBD storage

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

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

- Create a physical volume:

```
pvcreate /dev/vdb1
```

- Extend the volume group:

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

- Create a logic volume for DRBD:

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

Software

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

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

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

```
yum install nethserver-ha
```

- Install extra software, like MySQL:

```
yum install nethserver-mysql
```

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

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

- Apply the configuration and start services on master node:

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

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

```
pcs status
```

Service configuration

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

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

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

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

(continues on next page)

(continua dalla pagina precedente)

```
/usr/sbin/pcs -f /tmp/mycluster resource create sym_root_.my.cnf␣
↪ocf:heartbeat:symlink params target="/mnt/drbd/root/.my.cnf" link="/root/.my.cnf"␣
↪backup_suffix=.active

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

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

Check cluster and service status:

```
pcs status
```

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

Secondary node

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

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

Final steps

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

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

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

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

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

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

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

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

Fencing with IPMI

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

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

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

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

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

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

Fencing with IF-MIB switch

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

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

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

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

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

(continues on next page)

(continua dalla pagina precedente)

```
pcs constraint location ns2sw1 prefers <HOST_1>=INFINITY
pcs constraint location ns2sw2 prefers <HOST_1>=INFINITY
```

4.31.4 Failure and recovery

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

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

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

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

Failed nodes

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

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

```
pcs cluster start
```

Disconnected fence devices

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

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

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

DRBD Split Brain

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

```
pcs status
```

DRBD state will be:

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

instead of:

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

Solution:

On the node with valid data launch the following command

```
drbdadm invalidate-remote drbd00
```

On the node with wrong storage data, run

```
drbdadm invalidate drbd00
```

On both nodes, launch

```
drbdadm connect drbd00
```

Check drbd synchronization with

```
cat /proc/drbd
```

Disaster recovery

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

Just follow these steps:

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

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

4.31.5 Backup

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

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

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

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

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

Example:

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

4.32 Upgrade tool (beta)

Il modulo *Upgrade tool* consente di aggiornare NethServer dalla versione 6 alla versione 7 attraverso una procedura automatica che agisce in tre passaggi:

1. **preparazione**: scarica tutti i pacchetti richiesti dai repository software configurati
2. **aggiornamento**: al successivo riavvio esegue la transazione di aggiornamento dei pacchetti, le attività di aggiornamento, quindi si riavvia automaticamente
3. **post-aggiornamento**: esegue la riconfigurazione completa del sistema

Ogni passaggio è descritto nelle sezioni seguenti. Le stime temporali dipendono dal numero di pacchetti, dalla connessione Internet, dalla CPU e dalla velocità dei dischi.

Avvertimento: Leggere attentamente *Rischi legati all'upgrade e come ridurne l'impatto*

4.32.1 Fase di preparazione

Tempo stimato: 1 ora

La fase di (1) **preparazione** può essere avviata dalla pagina *Upgrade tool* del Server Manager.

Se il modulo File server è presente e il ruolo del server Samba è *Domain Controller Primario* o *Workstation* il sistema deve essere configurato con un account provider Active Directory locale. Vedi *Aggiornamento ad Active Directory*.

L'upgrade tool non può essere utilizzato se il ruolo del server Samba è impostato su *Membro Active Directory*.

Durante la fase di preparazione il sistema è ancora completamente operativo. Il download dei pacchetti viene eseguito in background. L'operazione può richiedere del tempo, anche in virtù della banda di rete disponibile.

Lo spazio disponibile sul disco viene controllato due volte, prima e dopo la fase di preparazione, per garantire che i passaggi successivi non vengano eseguiti nel caso in cui lo spazio su disco fosse insufficiente.

Terminato il download, dalla pagina Web è possibile interrompere la procedura o continuare con il riavvio del sistema per lanciare la successiva fase di aggiornamento.

4.32.2 Fase di aggiornamento

Tempo stimato: 30 minuti

La fase (2) **aggiornamento** inizia al successivo riavvio del sistema. La procedura di aggiornamento avvia il kernel Linux della versione 7 per impostazione predefinita. Se il controller del disco a bordo della macchina non dovesse essere compatibile con esso, la procedura fallirà.

Suggerimento: È possibile selezionare il vecchio kernel per avviare il sistema nello stato precedente, interrompendo così l'aggiornamento

Se la macchina si avvia con il nuovo kernel e monta correttamente i dischi, il sistema viene **disconnesso dalla rete** ed inizia l'aggiornamento dei pacchetti. Da questo punto non si può tornare indietro. Durante la fase di aggiornamento è possibile accedere al sistema solo dalla console di sistema.

L'aggiornamento può richiedere del tempo, a seconda della velocità del sistema e del numero dei pacchetti. Alla fine della fase di aggiornamento il sistema viene automaticamente riavviato.

4.32.3 Fase di post-aggiornamento

Tempo stimato: 15 minuti

La fase di (3) **post-aggiornamento** viene lanciata al secondo riavvio.

Il sistema di base è stato completamente aggiornato nel passaggio precedente; la fase post-aggiornamento rinomina le interfacce di rete in base alle nuove regole di denominazione della NIC e riconfigura i moduli installati.

Durante questo ultimo passaggio un eventuale problema può essere ripristinato in modo sicuro attraverso la console di sistema. Al termine del passaggio post-aggironamento SSH, Server Manager e gli altri servizi saranno nuovamente disponibili.

Ogni cron job giornaliero, settimanale e mensile verrà riavviato entro un'ora dall'avvio del sistema.

4.32.4 Checklist post-aggiornamento

Avvertimento:

1. Alcuni moduli, come ownCloud, devono essere aggiornati o sostituiti manualmente. Fare riferimento alla documentazione di aggiornamento di NethServer 7
2. Una volta tornato accessibile ilServer Manager, sarà necessario rammentare di aggiornare la cache del browser con la combinazione di tasti `Ctrl + Shift + R` per correggere eventuali problemi di visualizzazione causati dai fogli di stile aggiornati (CSS)

Verifica procedura completata

Per verificare che la procedura di aggiornamento abbia effettivamente terminato la sua esecuzione è possibile utilizzare il comando `systemd-analyze`. L'output dovrebbe essere simile a questo:

```
Startup finished
```

Verifica errori aggiornamento

Per verificare se si siano riscontrati errori, eseguire

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

Verifica moduli installati

Controllare tramite il *Software center* se i moduli installati in precedenza siano ancora contrassegnati come installati sul sistema aggiornato. Ogni modulo è composto da alcuni pacchetti: poiché le composizioni dei moduli sono cambiate dalla versione 6 alla 7, alcuni di essi potrebbero apparire come non installati. Per risolvere il problema, dovrebbe essere sufficiente installarli di nuovo con il pulsante *aggiungi*.

Verifica certificato Let's Encrypt

Il certificato Let's Encrypt, se presente, dovrà essere richiesto nuovamente attraverso la pagina *Certificato del server*. Andrà poi impostato dalla stessa pagina come certificato di sistema predefinito. Per ulteriori informazioni, consultare la pagina di manuale «Certificato server» di NethServer 7.

4.32.5 Aggiornamento ad Active Directory

Se il sistema necessita di un account provider di tipo Active Directory (AD) locale, l'Upgrade tool prevede l'inserimento di alcuni parametri aggiuntivi:

- *Nome dominio DNS* di AD
- *Nome dominio NetBIOS* (in sola lettura)
- Interfaccia **green** di tipo **bridge**
- *Indirizzo IP Domain Controller*: un indirizzo IP aggiuntivo libero a cui i servizi di Active Directory saranno associati. L'IP deve essere nella stessa subnet del bridge green

Se un'interfaccia bridge green non fosse presente, andrà creata dalla pagina *Rete* tramite il pulsante *Crea nuova interfaccia logica*.

Il *nome dominio NetBIOS* è un campo di sola lettura. Per modificarlo, consultare la pagina *Rete Windows*.

Avvertimento: Nel caso di sistemi virtualizzati, sarà necessario ricordarsi di abilitare **la modalità promiscua** nelle impostazioni dell'hypervisor, altrimenti non sarà permesso l'accesso ad AD ai client LAN

Per ulteriori informazioni, consultare anche la documentazione di NethServer 7, in particolare:

- la sezione «Installazione del provider locale Samba Active Directory», nel capitolo «Utenti e gruppi»
- il capitolo «Aggiornamento da NethServer 6»

4.32.6 Rischi legati all'upgrade e come ridurne l'impatto

Un aggiornamento della major version del sistema operativo è un'operazione rischiosa e deve essere pianificata attentamente.

- Assicurarsi che il sistema abbia abbastanza spazio **su disco**. La procedura controlla lo spazio libero, ma è sempre consigliabile verificarlo in anticipo, anche prima di installare il modulo *Upgrade tool*.
- Verificare di avere un backup completo o un'istantanea dell'intero sistema. Una **interruzione dell'alimentazione** o un **guasto hardware** durante la fase di aggiornamento, così come un **errore sconosciuto** in questa fase della procedura potrebbe compromettere il sistema
- Tenere contro del **downtime del sistema** e del conseguente impatto sugli utenti finali
- Creare un elenco dei moduli che dovranno essere configurati, sostituiti, **aggiornati manualmente** al termine della procedura automatizzata. Fare riferimento alla documentazione di aggiornamento di NethServer 7
- Durante l'aggiornamento, qualsiasi **template custom** esistente verrà archiviato in `/root/templates-custom.upgrade/`. Si consiglia di controllare i template personalizzati esistenti prima di iniziare la procedura di aggiornamento e decidere se e come ripristinarli
- Il sistema verrà **disconnesso dalla rete** durante la fase di aggiornamento e fino al completamento della fase post-aggiornamento. Se durante questi passaggi si dovesse verificare un errore, sarà necessario un **accesso alla console** diretto per intervenire.

CAPITOLO 5

Best practice

5.1 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
```

5.1.1 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`.

5.1.2 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*.

5.1.3 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 private
signal-event firewall-adjust
signal-event runlevel-adjust
```

5.1.4 Avvio e arresto

NethServer usa il runlevel standard 3.

Il software installato con yum dovrebbe già essere configurato per partire nel runlevel 3. Per controllare la configurazione, eseguire il comando **`chkconfig`**. Il comando mostra una lista dei servizi con la relativa configurazione.

Per abilitare un servizio al boot:

```
chkconfig mysoftware on
```

Per disabilitare un servizio al boot:

```
chkconfig mysoftware off
```

CAPITOLO 6

Appendice

6.1 Migrazione da NethService/SME Server

La migrazione è il processo che consente di convertire un'installazione SME Server/NethService (*origine*) in un nuovo server NethServer (*destinazione*).

1. Sulla macchina origine, effettuare un backup completo e spostarlo sul server destinazione.
2. Sul server destinazione, installare 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. Iniziare il processo di migrazione su NethServer segnalando l'evento `migration-import`:

   ```
   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
   ```

Nota: Nessun template custom sarà migrato durante il processo di migrazione. Controllare i nuovi template prima di copiare frammenti personalizzati dal vecchio backup.

6.1.1 Email

Prima di mettere NethServer in produzione, vanno fatte alcune considerazioni sulla configurazione esistente della rete e dei client di posta elettronica: quali porte sono in uso, se vengono utilizzati SMTPAUTH e TLS. Per maggiori informazioni, fare riferimento alle sezioni *Configurazione client* e *Politiche SMTP di invio speciali*.

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`, per ri-sincronizzare le caselle di posta di destinazione con il server di origine. `/usr/share/doc/nethserver-mail-server-<VERSION>/sync_maildirs.sh`. Lo script gira sul server di destinazione:

```
Usage:
  ./sync_maildirs.sh [-h] [-n] [-p] -s IPADDR
      -h          help message
      -n          dry run
      -p PORT     ssh port on source host (default 22)
      -s IPADDR   rsync from source host IPADDR
```

Il server di origine con indirizzo `IPADDR` deve essere accessibile dall'utente `root`, mediante `ssh` con autenticazione a chiave pubblica.

6.2 Licenza della documentazione

CAPITOLO 7

Indici

- Indice generale
- Ricerca

Indice

P

Q

R

S

T

U

V

W

X

Z