
NethServer Documentation

Release 7 Final

Nethesis

18 set 2020

1	Note di rilascio 7	3
1.1	Cambiamenti principali al 05/05/2020	3
1.2	Cambiamenti principali al 07/10/2019	4
1.3	Cambiamenti principali al 27/12/2018	4
1.4	Cambiamenti principali al 11/06/2018	5
1.5	Cambiamenti principali al 26/10/2017	6
1.6	Cambiamenti principali al 31/07/2017	6
1.7	Cambiamenti principali al 30/01/2017	6
1.8	Funzionalità e pacchetti obsoleti	7
1.9	Aggiornare NethServer 6 a NethServer 7	8
2	Installazione	11
2.1	Requisiti minimi	11
2.2	Tipi di installazione	11
2.3	Installazione da ISO	12
2.4	Installazione su CentOS	15
2.5	Passi successivi	15
3	Accesso al Server Manager	17
3.1	Login	17
3.2	Suggerimenti	18
3.3	Cambiare la password attuale	18
3.4	Logout	18
4	Subscription	19
4.1	Registrando il sistema	19
4.2	Rimozione di una subscription	20
5	Software center	21
5.1	Installazione applicazioni	21
5.2	Aggiornamenti software	21
6	Base system	25
6.1	Sistema	25
6.2	Applicazioni	28
6.3	Terminale	29
6.4	Delega	29

6.5	Autenticazione a due fattori (2FA)	30
7	Utenti e gruppi	33
7.1	Account provider	33
7.2	Utenti	37
7.3	Gruppi	39
7.4	Account admin	39
7.5	Gestione password	39
7.6	Importazione ed eliminazione account da file plain-text	41
8	DNS	43
8.1	Hosts	43
8.2	Alias	44
8.3	Reindirizzamento domini	44
9	Server DHCP e PXE	45
9.1	Configurazione DHCP	45
9.2	IP riservato a un host	46
9.3	Configurazione per l'avvio da rete	46
10	TLS policy	49
10.1	Policy 2020-05-10	49
10.2	Policy 2018-10-01	49
10.3	Policy 2018-06-21	50
10.4	Policy 2018-03-30	50
10.5	Politica upstream predefinita	51
11	Web server	53
11.1	Dashboard Web server	53
11.2	Impostazioni	54
11.3	Virtual host	54
11.4	Reverse proxy	56
11.5	Server FTP	56
12	Firewall	57
12.1	Generale	57
12.2	Dashboard	58
12.3	WAN	58
12.4	Gestione banda	58
12.5	SNAT	58
12.6	Oggetti	58
12.7	Port forward	59
12.8	Regole	59
12.9	Regole locali	59
12.10	Connessioni	60
12.11	Impostazioni	60
13	Email	61
13.1	Domini	62
13.2	Filtro	63
13.3	Caselle di posta	66
13.4	Indirizzi	69
13.5	Connettori	69
13.6	Sincronizzazione	69
13.7	Coda	70

13.8	Relay	70
13.9	Impostazioni	71
13.10	Log	72
13.11	Configurazione client	73
14	Backup	75
14.1	Impostazioni	75
14.2	Ripristino selettivo dei file	77
15	Disaster recovery	79
15.1	Nuovo Server Manager	79
15.2	Vecchio Server Manager	80
15.3	Disabilitare ripristino della rete	81
16	Personalizzazione backup	85
16.1	Backup dati	85
16.2	Backup configurazione	89
16.3	Ripristino da linea di comando	90
16.4	Formattazione di un disco locale	91
17	Legacy backup	93
17.1	Backup configurazione	93
17.2	Backup dati	93
18	Webmail	95
18.1	Plugins	95
18.2	Accesso	96
18.3	Rimozione	96
19	WebTop 5	97
19.1	Autenticazione	97
19.2	Autenticazione a due fattori (2FA)	98
19.3	Sincronizzazione con ActiveSync (EAS)	99
19.4	Sincronizzazione con CalDAV e CardDAV	100
19.5	Condividere le cartelle e-mail o l'intero account	102
19.6	Condivisione di calendari e rubriche	102
19.7	Etichette sulle Mail	103
19.8	Anteprima mail sulla riga del messaggio	103
19.9	Archiviazione mail	103
19.10	Sottoscrizione di cartelle IMAP	104
19.11	Esportazione eventi (CSV)	105
19.12	Integrazione con Nextcloud	105
19.13	Usa il Cloud personale per inviare e ricevere documenti	107
19.14	Integrazione chat	109
19.15	Chiamate WebRTC audio e video con chat (Beta)	109
19.16	Invio SMS dai contatti	110
19.17	Pulsanti di collegamento personalizzati	111
19.18	Notifiche del browser	111
19.19	Gestione firme utenti e di dominio	112
19.20	Configurare più firme per un singolo utente	114
19.21	Gestisci identità	115
19.22	Sottoscrizione di risorse remote	115
19.23	Gestione impostazioni utente	117
19.24	Modifica del logo	118
19.25	Modifica dell'URL pubblico	118

19.26	Modifica il limite predefinito «Dimensione massima del file»	118
19.27	Importazione di contatti e calendari	119
19.28	Nascondi il destinatario suggerito automaticamente nelle ricerche	121
19.29	Modificare l'oggetto di una mail e salvarlo	121
19.30	Importazione da PST Outlook	121
19.31	Troubleshooting	123
19.32	WebTop vs SOGo	124
19.33	Integrazione Google	125
20	Connettore POP3	127
21	Chat	129
21.1	Server to server (S2S)	129
21.2	Client	130
21.3	Amministratori	130
21.4	Gestione archivio messaggi	130
21.5	Altre opzioni	130
22	Team chat (Mattermost)	133
22.1	Configurazione	133
22.2	Autenticazione	134
23	UPS	137
23.1	Device personalizzato	137
23.2	Statistiche UPS	138
24	Report	139
24.1	Dashboard	139
24.2	Impostazioni	139
25	Server FAX	141
25.1	Modem	141
25.2	Client	142
25.3	Stampante virtuale Samba	142
25.4	Mail2Fax	142
25.5	Modem virtuali	143
26	Firewall e gateway	145
26.1	Policy	145
26.2	Regole	146
26.3	Multi WAN	148
26.4	Port forward	149
26.5	sNAT 1:1	150
26.6	Gestione banda	151
26.7	Oggetti firewall	152
26.8	Binding IP/MAC	153
27	Proxy web	155
27.1	Modalità autenticata	155
27.2	Configurazione client	156
27.3	Proxy SSL	156
27.4	Bypass	156
27.5	Regole di priorità e di instradamento	157
27.6	Report	157
27.7	Cache	157

27.8	Porte sicure	158
27.9	Log	158
28	Filtro contenuti web	159
28.1	Filtri	159
28.2	Antivirus	160
28.3	Risoluzione problemi	160
29	IPS (Suricata)	161
29.1	Categorie regole	161
29.2	Bypass	164
29.3	EveBox	164
30	Reverse proxy	165
30.1	Regole di virtual host e path	165
30.2	Configurazione manuale	166
31	Virtual hosts	167
31.1	Nomi dei virtual host (FQDN)	167
31.2	Configurare un'applicazione web	167
31.3	Permessi Apache	168
32	Cartelle condivise	169
32.1	Requisiti	169
32.2	Permessi di accesso	170
32.3	Accesso alla rete	170
32.4	Cestino di rete	171
32.5	Nascondere una cartella condivisa	171
32.6	Share home	171
32.7	Modifica autorizzazioni delle risorse dai client Windows	171
32.8	Accesso amministrativo	172
32.9	Auditing	172
33	Monitor banda	173
33.1	Dashboard	173
33.2	Impostazioni	174
33.3	Log	174
34	Statistiche (collectd)	175
34.1	Latenza di rete	175
35	VPN	177
35.1	OpenVPN	177
35.2	IPsec	180
36	Nextcloud	181
36.1	Installazione	181
36.2	Configurazione	182
37	FTP	185
37.1	Utenti di sistema	185
38	Phone Home	187
38.1	Disabilitazione	187
39	SNMP	189

40 Hotspot (Dedalo)	191
40.1 Come funziona?	191
40.2 Installazione	192
40.3 Configurazione	192
41 FreePBX	195
41.1 Installazione	195
41.2 Accesso Web	195
41.3 FwConsole	195
41.4 Documentazione avanzata	196
42 Macchine virtuali	197
42.1 Risorse esterne	197
43 Fail2ban	199
43.1 Installazione	199
43.2 Impostazioni	199
43.3 Unban IP	200
43.4 Statistiche	200
43.5 Strumenti	200
43.6 Whois	201
44 Rspamd	203
44.1 Interfaccia web di Rspamd	203
44.2 Moduli	205
44.3 Domande frequenti	206
45 Antivirus	207
46 Threat shield	209
46.1 Configurazione	209
46.2 Incident response	210
46.3 Statistiche	210
47 Aggiornamento Email a Rspamd	211
47.1 Funzionalità modificate	211
47.2 Procedure di aggiornamento manuale	212
48 Collabora Online	213
48.1 Installazione	213
48.2 Utente admin	214
49 Docker	215
49.1 Official documentation	215
49.2 Installation	215
49.3 Docker repository	216
49.4 Configuration	216
49.5 Web user Interface	216
49.6 Default network	217
49.7 Aqua network	217
49.8 Aeria network	217
49.9 Macvlan	218
49.10 Issues	219
49.11 Sources	219

50	SOGGo	221
50.1	Installation	221
50.2	Official documentation	222
50.3	Usage	222
50.4	Esmith database	222
50.5	Access SOGo on an exclusive hostname	223
50.6	Maximum IMAP command	223
50.7	ActiveSync	224
50.8	Backup	224
50.9	Fine tuning	224
50.10	Clients	226
50.11	Nightly build	228
50.12	Issues	228
50.13	Sources	228
51	PhpVirtualBox	229
51.1	Installation	229
51.2	User permissions	230
51.3	Authentication	231
51.4	Uploading ISOs	231
51.5	Oracle VM VirtualBox Extension Pack	232
51.6	The RDP console	232
51.7	VM networking	232
51.8	Esmith database	232
51.9	Documentation	233
52	HotSync	235
52.1	Terminologia	236
52.2	Installazione	236
52.3	Configurazione	236
52.4	Ripristino: promuovere lo SLAVE in produzione	237
52.5	Troubleshooting	238
52.6	Pacchetti supportati	239
53	Microsoft SQL Server	241
53.1	Installazione	241
53.2	Default configuration	241
53.3	Install mssql-server service	242
53.4	Helpful actions	242
53.5	Backup and restore	242
53.6	SQLCMD utility	242
54	Third-party software	243
54.1	Installazione	243
54.2	Backup	243
54.3	Firewall	244
54.4	Avvio e arresto	244
55	Migrazione da NethService/SME Server	245
55.1	Account provider	245
55.2	Email	246
55.3	Apache	246
55.4	Ibay	246
55.5	Migrazione da backup	247
55.6	Migrazione con rsync	247

56	Aggiornamento da NethServer 6	249
56.1	Account provider	249
56.2	Cartelle condivise	251
56.3	Server mail	251
56.4	TLS policy	252
56.5	Let's Encrypt	252
56.6	Owncloud e Nextcloud	252
56.7	Librerie Perl	252
56.8	Upgrade da backup	253
56.9	Upgrade tramite rsync	253
56.10	Upgrade tramite Upgrade tool (beta)	255
57	Licenza della documentazione	257
58	List of NethServer 7 ISO releases	259
58.1	7.8.2003	259
58.2	7.7.1908	259
58.3	7.6.1810	259
58.4	7.5.1804	259
58.5	7.4.1708	260
58.6	7.3.1611	260
58.7	7.2.1511	260
59	Public issue trackers	261
60	Index	263
61	Chat	265
62	Windows file server	267
63	Reverse proxy	269
63.1	Creare /Modificare	269
63.2	Eliminare	269
64	Groupware SOGo	271
65	TLS policy	273
	Indice	275



See also

- [Sito web](#)
- [Community](#)
- [Wiki](#)
- [Manuale sviluppatore](#)

NethServer versione 7

- La ISO release 7.8.2003 «final» sostituisce la precedente ISO 7.7.1908
- Questa versione è basata su [CentOS 7 \(2003\)](#)
- CentOS 7 riceverà aggiornamenti di sicurezza fino al 30/06/2024
- [List of NethServer 7 ISO releases](#)
- Lista delle [principali modifiche](#)
- [Lista di bug noti](#)
- [Analisi dei possibili bug](#)

1.1 Cambiamenti principali al 05/05/2020

- La ISO release 7.8.2003 «final» sostituisce la precedente ISO 7.7.1908
- il nuovo Server Manager basato su Cockpit è ora in versione stabile
- Su nuove installazioni, l'opzione *Sistema > Impostazioni > Policy shell > Ignora la shell degli utenti* è abilitata di default. Gli utenti normali potranno accedere al nuovo Server Manager solo se l'opzione *Sistema > Impostazioni > Pagina impostazioni utente > Abilita la pagina impostazioni utente* è stata abilitata o se l'utente è stato delegato per accedere ad almeno un modulo.

L'accesso a SSH è limitato a `root` e agli utenti all'interno del gruppo amministrativo designato (`Domain Admins` per impostazione predefinita). Permessi più granulari possono essere assegnati dalla pagina *SSH*.

- Tutte le azioni IMAP vengono tracciate di default all'interno di `/var/log/imap`
- Il flag `visti condivisi` è abilitato di default per le cartelle di posta condivise.
- Il limite di connessione al server di posta per ciascun utente è stato aumentato per evitare errori sui client di posta web

- Quando si crea un nuovo connettore POP3, i filtri sono disabilitati per impostazione predefinita
- Il server roadwarrior di OpenVPN utilizza la **topologia** di tipo `subnet` come impostazione predefinita
- Per aumentare la sicurezza, quando la modalità di autenticazione è impostata su `Nome utente`, `password` e `certificato`, il server OpenVPN roadwarrior impone una corrispondenza tra nome utente e CN del certificato
- La dimensione massima della memoria PHP predefinita è stata aumentata da 128MB a 512MB
- Nextcloud ora utilizza lo stack PHP 7.3 per migliorare le prestazioni e supportare un più ampio numero di plug-in
- Ejabberd è stato aggiornato alla versione 20.03
- Il proxy POP3 (P3Scan) è stato deprecato e non può più essere installato dal Software Center
- PHP 7.1 è ora obsoleto ed è stato rimosso dai repository upstream: le macchine ripristinate dovranno migrare le applicazioni personalizzate su PHP 7.2 o versioni successive

1.2 Cambiamenti principali al 07/10/2019

- La ISO release 7.7.1908 «final» sostituisce la precedente ISO 7.6.1810
- Il nuovo Server Manager basato su Cockpit ha raggiunto lo stato di Beta ed è disponibile di default su tutte le installazioni. I sistemi esistenti possono installare il nuovo Server Manager dalla pagina del Software Center. Vedi anche *Accesso al Server Manager*.
- L'opzione *Origine aggiornamenti software* (bloccata/sbloccata) è stata rimossa dalla pagina «Software Center». NethServer può essere aggiornato manualmente dalla pagina Software Center quando viene rilasciata la «point release» successiva. Vedi anche *Software center*.
- I delta RPM sono stati rimossi dalla distribuzione upstream e non sono più disponibili nei repository YUM
- La configurazione di OpenSSH è stata rimossa dalle impostazioni dei criteri TLS e ripristinata ai valori upstream predefiniti.
- Nel nuovo Server Manager basato su Cockpit, la funzione *Mailbox condivise* del modulo Mail è stata rinominata *Cartelle pubbliche*.
- La cartella pubblica “Junk” viene creata durante l'installazione del modulo Email ed è accessibile in IMAP dall'utente root; ulteriori permessi possono essere aggiunti dall'applicazione Email del nuovo Server Manager o con un client IMAP/ACL, per esempio Roundcube.
- Solo gli utenti con la shell abilitata possono accedere al nuovo Server Manager. Dal vecchio Server Manager, aprire la pagina *Utenti e gruppi* e abilitare l'opzione *Shell remota (SSH)*. Dal nuovo Server Manager, aprire la pagina *Utenti e gruppi* e abilitare l'opzione *Shell* per l'utente selezionato.
- Le firme antivirus ufficiali di ClamAV sono ora disabilitate di default.
- L'interfaccia web per il restore selettivo è stata eliminata dal vecchio Server Manager. Una nuova interfaccia è disponibile su Cockpit, vedi *Ripristino selettivo dei file*.
- Di default, l'analizzatore di utilizzo disco (duc) esamina i contenuti del file system root. Gli altri mount point vengono ignorati.

1.3 Cambiamenti principali al 27/12/2018

- La ISO release 7.6.1810 «final» sostituisce la precedente ISO 7.6.1804

- PHP 5.6 da SCL è giunto a fine vita (endo-of-life) ed è perciò deprecato. Vedi [PHP 5.6 SCL](#)
- La policy TLS adottata di default è la 2018-10-01
- La politica di conservazione dei log di sistema è stata aumentata a 52 settimane
- Il protocollo di rete Zeroconf è ora disabilitato di default
- Per impostazione predefinita, gli eventi Evebox vengono conservati per 30 giorni. Il nuovo valore predefinito viene applicato ai sistemi aggiornati come correzione di un bug
- Il modulo NDPI è stato aggiornato alla versione 2.4 ed alcuni vecchi protocolli non vengono più riconosciuti. Vedi [NDPI 2.4](#) per una lista completa dei protocolli rimossi
- Il server SMTP può essere utilizzato direttamente dalle reti fidate
- Le connessioni PPPoE utilizzano di default il plugin rp-pppoe per migliorare la velocità di rete
- Per i repository che supportano la firma dei metadati GPG, YUM esegue ora un controllo di integrità (`repo_gpgcheck = 1`) per maggiore sicurezza. Questa nuova impostazione predefinita viene applicata automaticamente a meno che un file `.repo` sia stato modificato localmente. In tal caso viene creato un file `.rpmnew` invece di sovrascrivere le modifiche locali. Rinominare il file `.rpmnew` in `.repo` per applicare i nuovi valori di default. Questa è la lista dei file da controllare:
 - `/etc/nethserver/yum-update.d/NsReleaseLock.repo`
 - `/etc/yum.repos.d/NethServer.repo`
 - `/etc/yum.repos.d/NsReleaseLock.repo`

1.4 Cambiamenti principali al 11/06/2018

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

1.5 Cambiamenti principali al 26/10/2017

- Rilascio della ISO 7.4.1708 «final» che sostituisce le precedenti ISO 7.4.1708 «beta1» e 7.3.1611 «update 1»
- Il provider di account AD locale applica automaticamente gli aggiornamenti all'istanza Samba DC (#5356) La versione più recente di Samba DC è la 4.6.8
- La pagina del Software center avvisa quando una nuova upstream release è disponibile (#5355)
- Aggiunto il modulo FreePBX 14
- Squid è stato patchato per una migliore esperienza di navigazione web in caso di utilizzo del proxy trasparente SSL
- Ntopng 3 sostituisce Bandwidthd, il Server Manager contiene una nuova pagina «top talkers» che traccia l'utilizzo della banda da parte degli host
- Suricata può essere configurato con molteplici categorie di regole
- EveBox può segnalare anomalie di traffico rilevate da Suricata
- Nextcloud 12.0.3
- Web antivirus basato su ICAP invece che su ECAP
- Filtri web: ufdbGuard aggiornato alla versione 1.33.4, apportati piccoli miglioramenti UI all'interfaccia web
- Strumenti di diagnostica: aggiunto speedtest
- ufdbGuard aggiornato alla versione 1.33.4
- WebTop4 è stato rimosso

1.6 Cambiamenti principali al 31/07/2017

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

1.7 Cambiamenti principali al 30/01/2017

- Rilascio della ISO 7.3.1611 «Final» che sostituisce la precedente ISO 7.3.1611 «RC4»
- Installatore: aggiunta modalità di installazione manuale

- Account provider: il gruppo “administrators” è stato sostituito dal gruppo “domain admins” (*Accesso al Server Manager*)
- Mail server: sistemata l’espansione di pseudonimi per i gruppi
- Mail server: le caselle di posta condivise sono ora abilitate per default (*Caselle di posta condivise*)
- Mail server: gli pseudonimi specifici per dominio hanno ora la precedenza su quelli generici
- OpenVPN: abilitato l’avvio automatico dei client VPN al boot
- Filtro web: corretti i profili basati su gruppi
- Firewall: corretta la selezione delle condizioni temporali
- IPS: configurazione aggiornata per l’ultima release di pulledpork

1.8 Funzionalità e pacchetti obsoleti

1.8.1 PHP 5.6 SCL

PHP 5.6 del repository SCL ha raggiunto il fine vita (EOL)¹².

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

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

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

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

1.8.2 NDPI 2.4

I seguenti protocolli sono stati rimossi:

- tds
- winmx
- imesh
- http_app_veohtv
- quake
- meebo
- skyfile_prepaid
- skyfile_rudics
- skyfile_postpaid
- socks4

¹ Red Hat Software Collections Product Life Cycle – <https://access.redhat.com/support/policy/updates/rhsc>

² PHP supported versions – <http://php.net/supported-versions.php>

- timmeu
- torcedor
- tim
- simet
- opensignal
- 99taxi
- easytaxi
- globotv
- timsomdechamada
- timmenu
- timportasabertas
- timrecarga
- timbeta

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

1.9 Aggiornare NethServer 6 a NethServer 7

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

1.9.1 Accesso al Server Manager

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

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

1.9.2 Caselle di posta condivise

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

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

1.9.3 Pacchetti rimossi

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

- nethserver-collectd-web: sostituito con nethserver-cgp
- nethserver-password: integrato in nethserver-sssd
- nethserver-faxweb2: vedere la discussione [faxweb2 vs avantfax](#).

- nethserver-fetchmail: sostituito con getmail
 - nethserver-ocsinventory, nethserver-adagios: a causa di problemi di compatibilità con Nagios, questi moduli verranno supportati solo su NethServer 6
 - nethserver-ipsec: i tunnel IPSec sono ora implementati in nethserver-ipsec-tunnels, la funzione L2TP è stata eliminata
 - nethserver-webvirtmgr
-

Riferimenti

2.1 Requisiti minimi

I requisiti minimi sono:

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

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

2.1.1 Compatibilità hardware

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

2.2 Tipi di installazione

Sono supportati due modi per installare NethServer. In breve:

Installazione da ISO

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

Installazione da YUM

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

2.3 Installazione da ISO

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

2.3.1 Creazione sorgente d'installazione

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

Chiavetta USB

Su una macchina Linux, aprire il terminale ed eseguire:

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

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

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

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

DVD

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

2.3.2 Modalità di installazione

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

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

NethServer *interactive installation*

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

Altre modalità di installazione di NethServer

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

Installazione standard di CentOS

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

Tools

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

Avvio da disco locale

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

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

Parametri di avvio opzionali

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

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

```
raid=none
```

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

```
disks=sdx, sdy
```

Per abilitare la *cifratura del filesystem*, usare:

```
fspassword=s3cr3t
```

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

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

Altre opzioni disponibili (solo modalità *unattended*):

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

Indirizzo IP di default

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

- IP 192.168.1.1
- netmask 255.255.255.0

Password amministratore di sistema

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

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

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

Lingua

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

2.3.3 Modalità interattiva e Manuale

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

Le scelte richieste sono:

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

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

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

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

Problemi noti

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

2.3.4 Modalità unattended

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

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

2.4 Installazione su CentOS

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

Abilitare i repository NethServer specifici con il comando:

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

Per installare il sistema di base eseguire:

```
nethserver-install
```

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

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

2.5 Passi successivi

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

Accesso al Server Manager

Nota: La documentazione relativa al vecchio Server Manager è disponibile qui.

NethServer può essere configurato usando l'interfaccia web denominata *Server Manager*. E' necessario un browser web come Mozilla Firefox o Google Chrome per accedere all'interfaccia utilizzando l'URL `https://a.b.c.d:9090` or `https://nome-server:9090` dove *a.b.c.d* e *nome-server* sono rispettivamente l'indirizzo IP e il nome host configurati durante l'installazione.

Siccome, di default, il Server Manager utilizza un certificato SSL auto-firmato, al primo accesso verrà richiesto di accettare il certificato. Nonostante l'avviso, la connessione è sicura e cifrata, ma è consigliato configurare un certificato valido, in seguito.

3.1 Login

La pagina di login consente l'accesso fidato all'interfaccia web. Accedere come **root** e digitare la password scelta durante l'installazione di NethServer.

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

Oltre a root, tutti gli utenti con almeno una *delega* possono accedere al Server Manager.

La lingua dell'interfaccia web è selezionata automaticamente in base alla configurazione del proprio browser. Se si desidera cambiare lingua, selezionarla dal menù *Display Language* sul proprio nome utente nell'angolo in alto a destra dello schermo.

3.1.1 Accesso a server remoti

La pagina di login permette di accedere alla macchina locale (default) o a macchine remote. Per accedere ad un server remoto, per prima cosa, assicurarsi che il server sia accessibile via SSH. Poi fare clic su *Other options* a inserire l'hostname (o l'indirizzo IP) del server remoto nel campo *Connect to*.

Il Server Manager prova ad accedere al sistema remoto in SSH sulla porta 22. Se il server remoto utilizza una porta diversa, è possibile specificarla con la sintassi `host:port` (es. `a.b.c.d:222`).

3.2 Suggerimenti

Dopo il login, il sistema è pronto all'uso, ma viene suggerito di controllare un elenco di suggerimenti per configurare correttamente la macchina. I suggerimenti vengono mostrati sotto forma di marcatori gialli con un numero sopra le voci del menù di sinistra.

Come miglior prassi si dovrebbe almeno:

- cambiare la password di default per l'utente root
- configurare correttamente data e ora

3.3 Cambiare la password attuale

Tutti gli utenti con accesso al Server Manager possono cambiare la propria password dal menù *Impostazioni*.

Gli utenti senza accesso alla shell devono usare il vecchio Server Manager. Vedere `access-section`.

3.4 Logout

Concludere la sessione corrente del Server Manager cliccando *Esci* sul proprio nome utente nell'angolo in alto a destra dello schermo.

Una installazione di NethServer può essere registrata su un'istanza pubblica o privata Dartagnan¹, ottenendo l'accesso al portale di monitoraggio ed ai repository di aggiornamento stabili.

Suggerimento: La NethServer Subscription di Nethesis² consente l'accesso a un'istanza Dartagnan pubblica pronta all'uso, insieme a servizi di supporto professionale immediati per le proprie implementazioni di NethServer. Per più informazioni <https://my.nethserver.com>

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

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

4.1 Registrando il sistema

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

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

¹ Documentazione Dartagnan: <https://nethesis.github.io/dartagnan/>

² Sito ufficiale Nethesis: <http://www.nethesis.it>

4.2 Rimozione di una subscription

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

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

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

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

Nota: Per il vecchio Server Manager vedi `software_center_legacy-section`.

NethServer è altamente modulare: al termine dell'installazione è disponibile solo un set minimo di funzionalità come la *configurazione di rete* e il *backup*. La pagina *Software Center* consente all'amministratore di selezionare e **installare applicazioni** aggiuntive, e anche di elencare e **aggiornare** i *pacchetti* già installati.

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

Un *pacchetto* software è un'unità indivisibile. Viene reso pubblico da un repository software. NethServer i pacchetti sono sotto forma di file RPM¹. Dunque in questo preciso contesto, i termini *pacchetto* e *RPM* possono essere usati come sinonimi.

5.1 Installazione applicazioni

La sezione *Applicazioni* elenca tutti i moduli che possono essere installati. Questo elenco può essere filtrato per categoria. Per **installare un'applicazione**, selezionare la casella corrispondente e fare clic su *Installa applicazioni*.

Una volta che un modulo è stato installato, è elencato nella sezione *Applicazioni*.

5.2 Aggiornamenti software

5.2.1 Subscription enterprise e community

NethServer riceve gli aggiornamenti controllati da una serie di repository software. Vedi *Procedura di aggiornamento automatico* per ricevere nuove funzionalità e correggere bug e problemi di sicurezza.

¹ RPM Package Manager – <http://rpm.org>

5.2.2 Community senza subscription

Un sistema NethServer 7 riceve aggiornamenti da diversi progetti software:

- il progetto NethServer stesso²
- il progetto CentOS³
- repository EPEL⁴

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

Fare riferimento al forum della community⁵ e *Note di rilascio 7* per ulteriori informazioni sugli aggiornamenti di NethServer.

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

Maggiori informazioni sugli aggiornamenti CentOS:

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

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

Maggiori informazioni sugli aggiornamenti EPEL:

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

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

Procedura di aggiornamento manuale

Quando sono disponibili aggiornamenti, l'elenco dei nuovi pacchetti è disponibile nella sezione *Aggiornamenti*.

Maggiori dettagli sono disponibili cliccando il pulsante *Changelog*.

Per espandere l'elenco degli aggiornamenti, cliccare sul pulsante *Dettagli*, è quindi possibile aggiornare un singolo pacchetto di NethServer facendo clic sul pulsante *Aggiorna*. Per avviare un aggiornamento completo del sistema, fare clic sul pulsante *Aggiorna tutto*.

² NethServer – <http://www.nethserver.org>

³ CentOS – Community ENTERprise Operating System <https://www.centos.org/>

⁴ EPEL – Extra Packages for Enterprise Linux <https://fedoraproject.org/wiki/EPEL>

⁵ NethServer community forum – <http://community.nethserver.org>

Suggerimento: Sulle macchine community senza alcun tipo di subscription, è indispensabile ricordare di aggiornare regolarmente il software installato per correggere bug, problemi di sicurezza e ricevere nuove funzionalità

Procedura di aggiornamento automatico

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

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

La disponibilità degli aggiornamenti viene verificata da un'attività che viene eseguita in un momento casuale durante la notte. Per modificare la politica di aggiornamento fare clic sul pulsante *Configura*.

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

Riferimenti

Nota: Documentation about the old Server Manager is available [here](#).

Questo capitolo descrive tutti i moduli disponibili al termine dell'installazione. Tutti i moduli al di fuori di questa sezione possono essere installati dalla pagina del *Software center*.

L'installazione predefinita include i seguenti moduli principali:

- *Sistema*
- *Applicazioni*
- *Software center*
- *Terminale*
- *Subscription*

L'utente *root* può visualizzare tutte le pagine di configurazione ma l'accesso a ciascuna sezione e applicazione può anche essere delegato ad altri utenti. Vedi la sezione *Delega*.

Diverse applicazioni nel Server Manager utilizzano netdata per visualizzare utili grafici. Netdata non è presente di default, è possibile installarlo attraverso il *Software center*.

6.1 Sistema

La pagina Sistema è la sezione che viene visualizzata a seguito di un login riuscito. La pagina visualizzerà lo status e la configurazione del sistema.

Dalla dashboard di sistema, l'amministratore può:

- modificare il nome FQDN del server ed i relativi *Alias*
- configurare i server *DNS* upstream
- configurare date-time-section

- personalizzare l'anagrafica della azienda

Il sistema basa include inoltre:

- *Rete*
- *Servizi*
- *Backup*
- `server_certificate-section`
- *Utenti e gruppi*
- *TLS policy*
- *Server DHCP e PXE*
- *DNS*
- *SSH*
- *Storage*
- `trusted_networks-section`
- `duc-section`
- *Impostazioni*
- *Log*

6.1.1 Rete

Oltre a tutte le funzionalità disponibili nel vecchio Server Manager (vedi `network-section`), questa pagina consente di:

- controllare lo stato della rete con strumenti diagnostici integrati come ping, trace route e risoluzione dei nomi
- creare un'interfaccia di rete logica senza un ruolo: tale interfaccia può essere utilizzata in seguito da altri moduli come l'hotspot Dedalo

6.1.2 Servizi

Un sistema remoto può connettersi ad un servizio di rete, che è un software in esecuzione sullo stesso NethServer.

Ogni servizio può avere un elenco di porte «aperte» che accettano connessioni locali o remote. Per controllare quali zone o host possano accedere a un servizio di rete, consultare la sezione *Firewall e gateway*.

I servizi esistenti possono essere avviati e arrestati direttamente dalla pagina *Servizi*.

6.1.3 Storage

La sezione storage consente di configurare e monitorare i dischi. L'amministratore può montare nuovi dischi locali o remoti, gestire array RAID e volumi LVM.

6.1.4 SSH

La pagina SSH mostra il numero di connessioni SSH attive. Da questa sezione l'amministratore può modificare la porta di ascolto OpenSSH, disabilitare l'accesso root e l'autenticazione della password.

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

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

6.1.5 Impostazioni

La pagina impostazioni consente la configurazione di alcune opzioni che potrebbero avere un impatto su più applicazioni di sistema.

Smart host

Molte applicazioni di sistema, come cron, possono generare notifiche via mail. Se il server non dovesse essere in grado di recapitare direttamente questi messaggi, l'amministratore può configurare un server di inoltro SMTP. Quando lo smarthost è abilitato, tutti i messaggi di posta verranno recapitati attraverso il server configurato.

Notifiche email

Per impostazione predefinita, le notifiche vengono inviate alla maildir locale di root. L'amministratore può cambiare l'indirizzo di inoltro a root aggiungendo uno o più indirizzi di posta elettronica nel campo *Destinazione*.

È buona pratica impostare un *Indirizzo mittente* personalizzato: i messaggi dell'utente root (come le notifiche cron) verranno inviati usando l'indirizzo specificato. Una buona scelta potrebbe essere: `no-reply@<domain>` (in cui `<domain>` è il dominio del server). Se non impostato, i messaggi verranno inviati usando `root@<fqdn>` come indirizzo mittente.

Server Manager

Per impostazione predefinita, l'accesso al Server Manager è autorizzato da tutte le zone del firewall. Da questa sezione l'amministratore può limitare l'accesso al Server Manager solo a un elenco di indirizzi IP affidabili.

File di log

Tutti i file di log sono gestiti da logrotate. Logrotate è progettato per facilitare l'amministrazione di un gran numero di file di log. Consente la rotazione, la compressione e la rimozione automatica dei log. Ogni file può essere gestito giornalmente, settimanalmente, mensilmente.

L'amministratore può impostare la configurazione predefinita di logrotate da questa pagina. La configurazione si applicherà a tutte le applicazioni. Tuttavia, alcune applicazioni possono ignorare tale configurazione per rispondere ad esigenze specifiche.

Suggerimenti di configurazione

La maggior parte delle pagine del Server Manager possono visualizzare alcuni suggerimenti per aiutare l'amministratore ad adottare una migliore configurazione del sistema. I suggerimenti sono solo dei consigli e possono essere disabilitati da questo menu.

Cambio password

La pagina delle impostazioni include anche un pannello per consentire agli utenti, incluso l'utente root, di cambiare la propria password.

Criteri shell

Questa impostazione può essere utilizzata per abilitare o disabilitare la shell, necessaria per utilizzare il nuovo Server Manager e il servizio SSH. Se questa opzione è attiva, la shell è considerata sempre abilitata e la relativa impostazione per l'utente nella pagina *Utenti e gruppi* viene ignorata.

Pagina impostazioni utente

Quando l'opzione *Abilita pagina impostazioni utente* è abilitata, gli utenti possono modificare la propria password e altre impostazioni del profilo attraverso una pagina Web esterna a Cockpit (sulla porta 443). La pagina predefinita è */user-settings*. Questa funzione può essere abilitata solo se è attiva l'opzione *Criteri Shell*.

L'accesso alla pagina può essere limitato alle sole reti fidate.

6.1.6 Log

Il sistema fornisce un registro indicizzato denominato journal. Il journal può essere sfogliato da questa pagina: i messaggi possono essere filtrati per servizio, gravità e data.

6.2 Applicazioni

La pagina *Applicazioni* elenca tutte le applicazioni installate. Una applicazione è un modulo del Server Manager generalmente composto da più pagine tra cui una dashboard, una o più sezioni di configurazione e l'accesso ai registri dell'applicazione. Un clic sul pulsante *Impostazioni* aprirà l'applicazione.

Esistono anche applicazioni più semplici che includono solo un collegamento a pagine Web esterne. Per accedere a tali applicazioni fare clic sul pulsante *Apri*.

6.2.1 Scorciatoie

L'amministratore può aggiungere dei collegamenti per le applicazioni utilizzate più di frequente. I collegamenti alle applicazioni saranno mostrati nel menu di sinistra.

Solo l'utente *root* ha accesso a questa funzionalità.

6.2.2 Aggiungi alla home page

Il Launcher è un'applicazione del nuovo Server Manager disponibile per tutti gli utenti su porte HTTPS e HTTP. Il launcher è accessibile tramite l'FQDN del server (ad es. `https://my.server.com`) e viene automaticamente abilitato se non esiste alcuna home page già configurata all'interno del server Web (nessuna index page nel percorso `/var/www/html`)

Le applicazioni installate possono essere aggiunte al launcher facendo clic sul pulsante *Aggiungi alla home page*. Tutti gli utenti saranno in grado di accedere al link pubblico dell'applicazione.

Solo l'utente *root* ha accesso a questa funzionalità.

6.2.3 Rimozione applicazioni

Per rimuovere un modulo installato, fare clic sul pulsante *Rimuovi* dell'applicazione corrispondente.

Avvertimento: Quando si disinstalla un modulo, è possibile che vengano rimossi anche altri moduli! Leggere attentamente l'elenco dei pacchetti interessati per evitare di rimuovere delle funzionalità necessarie.

Questa funzionalità non è supportata in NethServer Enterprise

6.3 Terminale

Eseguire una shell standard all'interno di un terminale direttamente accessibile dal browser. La shell e i processi verranno eseguiti con i privilegi dell'utente.

6.4 Delega

In ambienti strutturati, l'utente *root* può :index: *delegare* l'accesso ad alcune sezioni a gruppi specifici di utenti locali.

Un utente locale può essere delegato ad accedere a:

- una o più pagine della sezione *Sistema*
- una o più applicazioni installate
- una o più sezioni tra *Subscription*, *Software Center*

La delega si basa su gruppi locali, ogni utente appartenente ad un gruppo ne eredita le deleghe. Gli utenti appartenenti ai *domain admins* vengono automaticamente delegati a tutti i pannelli.

Per creare una nuova delega, accedere alla sezione gruppi nella pagina *Utenti & Gruppi*, quindi modificare un gruppo esistente - o crearne uno nuovo - selezionando uno o più elementi dai menu *Viste sistema* e *Applicazioni*.

Anche se un utente è stato delegato, gli deve essere concesso esplicitamente l'accesso alla shell prima di poter accedere a Server Manager.

Le sezioni seguenti sono sempre accessibili da tutti gli utenti:

- dashboard
- applicazioni
- terminale

6.5 Autenticazione a due fattori (2FA)

L'autenticazione a due fattori (2FA) può essere utilizzata per aggiungere un ulteriore livello di sicurezza per l'accesso al nuovo Server Manager. Innanzitutto, gli utenti inseriranno nome utente e password, quindi dovranno fornire un codice di verifica temporaneo generato da un'applicazione in esecuzione sul proprio smartphone.

Il 2FA è disabilitato per impostazione predefinita. Ogni utente può abilitarlo accedendo alla sezione *Autenticazione a due fattori* sotto la pagina *Impostazioni* del proprio profilo, quindi seguendo questi passaggi:

1. scaricare e installare nello smartphone l'applicazione 2FA preferita
2. scansionare il QR code con l'applicazione 2FA
3. generare un nuovo codice e copiarlo all'interno del campo *Codice di verifica*, quindi fare clic su *Verifica codice*
4. se il codice di verifica è corretto, fare clic sul pulsante *Salva*

L'autenticazione a due fattori è attivabile per:

- il nuovo Server Manager
- SSH quando si utilizzano nome utente e password (l'accesso con chiave pubblica non richiederà mai il 2FA)

6.5.1 Codici di recupero

È possibile utilizzare i codici di ripristino anziché dei codici temporanei se l'utente non può accedere all'applicazione 2FA sullo smartphone. Ogni codice di ripristino è una one-time password e può essere utilizzato una sola volta.

Per generare nuovi codici di ripristino, disabilitare il 2FA, quindi riattivarlo registrando nuovamente l'applicazione, seguendo i passaggi precedenti.

6.5.2 Applicazioni per smartphone

Esistono diverse applicazioni, commerciali e open source, per il 2FA:

Disponibili sia per Android che per iOS:

- **FreeOTP**: disponibile sia per Android che per iOS
- **Authenticator**: disponibile solo per iOS
- **andOTP**: disponibile sia per Android che per iOS

6.5.3 Ripristino d'emergenza

In caso di emergenza, il 2FA può essere disabilitato accedendo al server da una console fisica, come una tastiera e un monitor, un cavo seriale o una connessione VNC - o simili - per macchine virtuali:

1. accedere al sistema con nome utente e password
2. eseguire:

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

Successivamente, l'utente root potrà ottenere i codici di recupero per un utente utilizzando il seguente comando, sostituendo <user> con il nome utente effettivo:


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

Esempio per l'utente goofy:

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


7.1 Account provider

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

I tipi di account provider supportati sono:

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

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

Prestare attenzione alla seguente nota relativa agli account provider:

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

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

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

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

7.1.1 Scegliere l'account provider giusto

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

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

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

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

7.1.2 Installazione del provider locale OpenLDAP

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

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

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

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

7.1.3 Installazione del provider locale Samba Active Directory

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

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

Pertanto l'indirizzo IP aggiuntivo deve soddisfare tre condizioni:

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

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

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

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

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

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

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

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

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

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

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

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

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

DNS e dominio AD

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

Esempio:

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

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

Installazione su macchina virtuale

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

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

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

VirtualBox

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

VMWare

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

KVM

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

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

```
ifconfig br0 promisc
```

Hyper-V

Configurare il MAC Address Spoofing per gli adattatori di rete virtuali²

7.1.4 Rimozione account provider locale

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

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

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

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

7.1.5 Join ad un dominio Active Directory esistente

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

² <https://technet.microsoft.com/en-us/library/ff458341.aspx>

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

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

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

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

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

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

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

7.1.6 Collegamento ad un server LDAP remoto

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

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

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

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

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

7.2 Utenti

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

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

- Nome utente
- Nome completo (nome e cognome)

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

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

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

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

7.2.1 Modifica della password

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

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

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

7.2.2 Credenziali per i servizi

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

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

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

Forma lunga username *goofy@example.com*

Forma breve username *goofy*

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

7.2.3 Cartelle home dell'utente

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

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

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


7.3 Gruppi

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

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

- *domain admins*: gli utenti di questo gruppo hanno gli stessi permessi di root nel Server Manager.
- *managers*: gli utenti di questo gruppo hanno l'accesso alle pagine della sezione Gestione.

7.4 Account admin

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

Suggerimento: Per abilitare l'utente *admin* impostare una password. Ricordare inoltre di abilitare la shell se l'utente admin deve accedere al nuovo Server Manager.

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

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

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

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

7.5 Gestione password

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

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

7.5.1 Complessità

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

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

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

- lunghezza minima 7 caratteri
- contenere almeno 1 numero

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

La policy di default è *strong*.

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

7.5.2 Scadenza

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

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

Per esempio, supponendo che

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

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

7.5.3 Effetti della password scaduta

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

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

Quando una password è scaduta

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

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

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

- SOGo

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

7.6 Importazione ed eliminazione account da file plain-text

7.6.1 Importazione utenti

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

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

Esempio:

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

quindi eseguire:

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

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

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

Per utilizzare un carattere separatore alternativo:

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

7.6.2 Importazione email

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

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

Si potrà poi utilizzare lo script `import_emails`. Fare riferimento alla sezione *Importazione ed eliminazione account da file plain-text* per un esempio di invocazione del comando.

7.6.3 Importazione gruppi

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

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

Esempio:

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

quindi eseguire:

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

Per esempio, se il file è `/root/groups.tsv`, eseguire il seguente comando:

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

La gestione dei gruppi è disponibile anche da linea di comando per mezzo degli eventi `group-create` e `group-modify`

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

7.6.4 Eliminazione utenti

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

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

Esempio:

```
mario <NEWLINE>
```

quindi eseguire:

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

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

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

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

Per utilizzare un carattere separatore alternativo:

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

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

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

Quando si effettua una risoluzione nomi, il server potrà:

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

Nota: E' obbligatorio specificare almeno un DNS esterno all'interno della scheda *Network > Server DNS* nel vecchio Server Manager. Altrimenti fare click sull'indirizzo DNS nella guilabel:*Dashboard* del nuovo Server Manager.

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

8.1 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.

8.2 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.

8.3 Reindirizzamento domini

L'amministratore può configurare un override del DNS upstream per domini specifici. Uno scenario di utilizzo tipico è l'impostazione del server Active Directory come resolver per le query sul dominio interno.

Tali modifiche possono essere apportate utilizzando la proprietà `DomainRedirection` d riga di comando. La proprietà accetta un elenco di coppie separato da virgole nel formato `<domain>:<ip_address>`.

Esempio:

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

La configurazione `my.domain.org:192.168.1.1` invierà tutte le query per `my.local.domain.org` al server `192.168.1.1`.

Il carattere speciale `#` può essere utilizzato per inviare le query al server DNS predefinito. Esempio:

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

In questo esempio tutte le query per `domain.org` andranno inviate a `1.1.1.1` mentre le query per `sub.domain.org` andranno inviate al DNS upstream predefinito.

Server DHCP e PXE

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

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

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

9.1 Configurazione DHCP

Il server DHCP può essere abilitato su tutte le interfacce *green* e *blue* (vedi network-section). 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.

9.1.1 Opzioni avanzate

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

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

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

³ Preboot eXecution Environment https://en.wikipedia.org/wiki/Preboot_Execution_Environment

9.2 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.

9.3 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/tftpboot`.

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

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

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

```
yum install syslinux
cp /usr/share/syslinux/{pxelinux.0,menu.c32,memdisk,mboot.c32,chain.c32} /var/lib/
↪tftpboot/
config setprop dnsmasq dhcp-boot pxelinux.0
signal-event nethserver-dnsmasq-save
mkdir /var/lib/tftpboot/pxelinux.cfg
```

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

```
default menu.c32
prompt 0
timeout 300

MENU TITLE PXE Menu

LABEL CentOS
```

(continues on next page)

² Trivial File Transfer Protocol <https://en.wikipedia.org/wiki/Tftp>

(continua dalla pagina precedente)

```
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

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

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

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

Le seguenti sezioni descrivono ciascun identificatore di policy.

10.1 Policy 2020-05-10

Questo criterio disabilita le versioni 1.0 e 1.1 del protocollo TLS. Si applica ai seguenti servizi:

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

Riferimento: <https://access.redhat.com/articles/1462183>

10.2 Policy 2018-10-01

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

Ejabberd (XMPP)

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

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

10.3 Policy 2018-06-21

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

- Apache
- Dovecot
- Postfix

Slapd (openldap-servers)

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

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

10.4 Policy 2018-03-30

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

Apache

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

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

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

Dovecot

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

- Cipher suite

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

- Disabilita SSLv2 e SSLv3

Postfix

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

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

- Exclude ciphers

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

10.5 Politica upstream predefinita

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

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

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

Nota: Questo capitolo descrive le funzionalità dell'applicazione *Web server*, disponibile nel nuovo Server Manager.

L'applicazione *Web server* è immediatamente disponibile al termine dell'installazione di NethServer. Serve a configurare e avviare il web server HTTP Apache.

L'applicazione *Web server* mette a disposizione le seguenti funzionalità:

- Apache HTTP web server
- Integrazione con i certificati del sistema per HTTPS
- Hosting di siti web multipli
- reverse proxy HTTP
- Linguaggio di scripting PHP per eseguire applicazioni Web
- FTP server

Le seguenti sezioni descrivono le pagine dell'applicazione *Web server*. Alcune di esse richiedono componenti software aggiuntivi che vengono scaricati, installati e configurati automaticamente quando sono richiesti per la prima volta.

11.1 Dashboard Web server

La pagina *Dashboard del server Web* mostra lo stato e le statistiche correnti del server Web. Elenca anche i componenti aggiuntivi installati sul sistema.

La configurazione predefinita di Apache serve il contenuto di `/var/www/html` ed è in grado di eseguire script PHP sul *Default web stack*.

11.2 Impostazioni

La pagina *Impostazioni* consente di modificare i parametri di configurazione di PHP per l'allocazione delle risorse (ad es. Memoria massima dello script e tempo di esecuzione).

Le modifiche influiscono sulla configurazione globale di PHP: sono pertanto valide sia per le applicazioni Web che per gli script da riga di comando, a meno che non vengano sovrascritti in qualche modo.

Le impostazioni di PHP possono anche essere modificate per un sito web specifico dalla pagina *Virtual hosts* (vedi anche :ref:'webservers-phpversions-section'), o sovrascritte con un file di configurazione personalizzato. Per questo scopo:

1. per PHP 7.2, verificare le impostazioni correnti di PHP-FPM in `/etc/opt/rh/rh-php72/php-fpm.d/000-virtualhost.conf`;
2. creare un file nella stessa directory (es `/etc/opt/rh/rh-php72/php-fpm.d/001-custom.conf`) e fare riferimento alla [documentazione ufficiale di PHP-FPM](#) per adeguare le necessarie direttive;
3. aggiungere il file creato al *backup della configurazione*.

11.3 Virtual host

È possibile ospitare più siti web su NethServer. È possibile configurare lo spazio di hosting del sito web dalla pagina *Virtual Host*.

Quando viene creato un nuovo virtual host con uno o più *nomi server*, il nuovo Server Manager crea contestualmente, per ciascuno di essi, un nome alias nel servizio DNS locale.

Nota: Un nome alias del server è accessibile dai client web se questi utilizzano il NethServer stesso come il loro server DNS. Per i siti Web pubblici, consultare la documentazione del provider DNS e assicurarsi che il nome alias del server sia impostato correttamente nel DNS pubblico.

I nomi alias del server sono elencati nella *dashboard* del nuovo Server Manager e da lì possono essere direttamente modificati.

11.3.1 Restrizioni accesso sito web

È possibile limitare il modo in cui i client web accedono ad un sito web con le seguenti opzioni, disponibili nella sezione *Impostazioni avanzate*.

1. Abilitando l'opzione `:guilabel: Consenti accesso solo da reti fidate`. Fare riferimento alla sezione `trusted_networks-section` per maggiori informazioni.
2. Abilitare l'opzione *Richiedi autenticazione HTTP* per concedere l'accesso ai client solo tramite password. Le applicazioni Web di solito forniscono un metodo di autenticazione autonomo: questa opzione potrebbe essere utile per proteggere i contenuti di siti Web statici.
3. Se fosse necessario accedere al sito web sempre tramite un canale crittografato, è possibile abilitare l'opzione *Richiedi connessione crittografata SSL*. Qualsiasi richiesta di risorse ricevuta tramite il protocollo HTTP verrà reindirizzata su HTTPS.

11.3.2 Certificato SSL/TLS

A ciascun virtual host può essere assegnato un *certificato SSL/TLS* dedicato oppure si può utilizzare quello predefinito di sistema. In qualunque caso, i nomi usati per il virtual host devono essere presenti tra i nomi alternativi del certificato, altrimenti i client web potrebbero rifiutare di connettersi.

11.3.3 Configurare un'applicazione web

Quando viene definito un nuovo virtual host, viene creata anche la relativa directory radice web. Il percorso completo della radice web viene visualizzato sotto *Host virtuali > Elenco > Web root path*.

Se l'opzione *Abilita accesso FTP* è attiva, è possibile caricare i dati, i file di configurazione e gli script nella root web utilizzando un client FTP.

Suggerimento: La password di autenticazione HTTP dovrebbe essere diversa da quella FTP, poiché FTP viene utilizzato per caricare i contenuti del virtual host mentre HTTP viene utilizzato per visualizzarli dal web.

Il sito web visualizza una pagina di «Benvenuto» fino a quando un file chiamato `index.html` o `index.php` non viene caricato nella directory web principale. Se non si desidera questo comportamento, è possibile abilitare l'opzione *Elenco dei file della directory principale*, come alternativa alla pagina di benvenuto.

I file caricati via FTP sono di proprietà del gruppo *apache* con autorizzazioni di sola lettura. Se fossero necessarie autorizzazioni di scrittura o di esecuzione, sarà possibile concederle tramite un client FTP.

Avvertimento: Se un sito web contiene codice eseguibile, ad esempio script PHP, le implicazioni di sicurezza delle autorizzazioni dei file devono essere valutate attentamente. Si consiglia di concedere l'accesso in scrittura solo a una serie limitata di file e directory speciali, come richiesto dalla documentazione dell'applicazione web.

La configurazione di Apache può essere sovrascritta caricando un file chiamato `.htaccess`. Fare riferimento alla documentazione ufficiale di Apache per ulteriori informazioni su questa funzione¹.

11.3.4 Versioni e configurazione PHP

Se la versione di PHP fornita da *Default web stack* non si adatta ad un'applicazione web, è possibile selezionarne e installarne una alternativa e sovrascrivere le impostazioni predefinite globali di PHP, come spiegato nella sezione *Impostazioni*.

11.3.5 Disabilitazione di un virtual host

L'azione *Disabilita* nasconde il virtual host, rendendolo inaccessibile ai client web. Questa operazione è reversibile, selezionando l'azione *Abilita*.

11.3.6 Cancellazione di un virtual host

L'azione `:guilabel:` *Cancella* rimuove la configurazione del virtual host e ne cancella la directory web principale. Questa operazione non è reversibile.

¹ Documentazione Apache per i file `.htaccess` <https://httpd.apache.org/docs/2.4/howto/htaccess.html>

11.4 Reverse proxy

In alternativa a un virtual host, che ospita file statici o un'applicazione web PHP in una directory radice web locale, è possibile inoltrare richieste web a un altro server HTTP e fornire risposte per conto di esso. Questo comportamento può essere configurato dalla pagina *Reverse proxy*.

Ogni elemento del reverse proxy è in realtà una regola che può corrispondere a una richiesta web in entrata. A seconda del valore del campo *Nome*, la corrispondenza può verificarsi per:

- A) il **nome del sito web** richiesto, se *Nome* inizia con qualsiasi carattere, tranne la barra `' / '`, oppure
- B) il **resource path** richiesto, se *Nome* inizia con un carattere barra `' / '`.

Se la regola corrisponde, la richiesta viene inoltrata a un altro server web, definito dal campo *URL di destinazione*.

11.4.1 Impostazioni avanzate reverse proxy

Quando la regola del reverse proxy corrisponde a un **nome di sito web** è possibile assegnargli un certificato dedicato, scegliendolo dall'elenco *Certificato SSL/TLS*.

Non è possibile selezionare il certificato se la regola corrisponde a un **resource path**. In questo caso è possibile utilizzare solo il certificato predefinito.

Indipendentemente dal tipo di regola, sono disponibili anche le seguenti impostazioni:

- *Accesso dalle reti CIDR*: limita l'accesso ad un dato elenco di reti CIDR. Solo i client web che si connettono da tali reti sono autorizzati ad aprire il sito web.
- *Richiedi connessione crittografata SSL*: se abilitato, qualsiasi richiesta `'http://'` viene reindirizzata a `'https://'`.
- *Accetta certificato SSL non valido dalla destinazione*: se l'URL di destinazione inizia con `https://` e viene restituito un certificato non valido, abilitando questa opzione si ignora l'errore di convalida del certificato.
- *inoltra l'intestazione «Host» HTTP alla destinazione*: se abilitato, un'intestazione HTTP *Host* contenente il nome host della richiesta originale viene inoltrata all'URL di destinazione. Ciò potrebbe essere richiesto dall'applicazione del server di destinazione per funzionare correttamente.

11.5 Server FTP

Avvertimento: Il protocollo FTP non è sicuro. Le password e i dati dei file vengono inviati in chiaro sulla rete.

Il File Transfer Protocol è un protocollo di rete standard utilizzato per il trasferimento di file tra un client e un server². La pagina *FTP* abilita il servizio FTP e permette di configurare account utente aggiuntivi limitati al solo servizio FTP.

Gli utenti del servizio FTP possono essere limitati ad accedere alla propria directory home abilitando *Chroot utente nella home directory*. Quando questa opzione è abilitata, l'utente non può vedere le altre directory di sistema. Questa configurazione è anche nota come *jailing*.

Quando viene creato un virtual host, gli viene assegnato un nome utente FTP casuale. È possibile quindi caricare il contenuto del virtual host attraverso FTP. Fare riferimento a *Configurare un'applicazione web* per maggiori informazioni.

Riferimenti

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

Nota: Questo capitolo descrive le modifiche introdotte dall'applicazione *Firewall* del nuovo Server Manager. Il comportamento di base del firewall è invariato e rimane quello descritto nella sezione *Firewall e gateway*.

Si noti che alcune delle modifiche apportate nel nuovo Server Manager potrebbero non riflettersi nella interfaccia precedente.

12.1 Generale

Principali differenze rispetto al vecchio Server Manager:

- il pannello delle regole è stato separato in 3 diverse pagine:
 - *Regole*
 - *Regole locali*
 - *Gestione banda*
- tutte le pagine utilizzano la funzione di *Applica e ripristina*
- ricerca intelligente: nella maggior parte dei pannelli è possibile utilizzare la ricerca full-text per trovare rapidamente regole o oggetti esistenti
- proprietà avanzate: quando si creano nuove regole, vengono visualizzati solo i campi più comuni. Per mostrare altri parametri meno comuni è necessario fare clic sull'etichetta *Avanzate*
- supporto indirizzo «grezzo»: l'utente può utilizzare direttamente indirizzi IP (o reti CIDR) ogni volta che crea una regola. Tali indirizzi possono essere successivamente convertiti in oggetti firewall utilizzando le azioni *Crea Host* e *Crea rete CIDR* che appariranno accanto all'indirizzo IP
- grafici in tempo reale: molte pagine hanno grafici in tempo reale che mostrano i dati raccolti da *netdata*. *Netdata* non è installato di default, è possibile installarlo attraverso il *Software center*.
- lista delle *Connessioni* attive

12.1.1 Applica e ripristina

Ogni volta che la configurazione viene modificata, le modifiche non vengono applicate immediatamente ma salvate in un archivio temporaneo. Per rendere effettive le modifiche, fare clic sul pulsante *Applica* presente nell'angolo in alto a destra della pagina.

Finché non sono state applicate le nuove regole create, è possibile riportare il sistema allo stato precedente facendo clic sul pulsante `:guilabel: Ripristina` presente nell'angolo in alto a destra della pagina.

12.2 Dashboard

La dashboard visualizza la topologia della rete firewall locale insieme al numero di connessioni stabilite, al conteggio degli oggetti configurati e all'elenco dei servizi attivi.

12.3 WAN

Tutte le interfacce red sono elencate nella parte superiore della pagina, appena sotto i grafici di utilizzo banda. La banda in download e upload può essere calcolata automaticamente utilizzando il pulsante *Speedtest*. Ogni interfaccia di rete red può anche essere abilitata e disabilitata direttamente dall'elenco.

Per modificare la modalità WAN e le opzioni di monitoraggio dei provider, fare clic sul pulsante *Configura*.

Le regole possono essere create dalla sezione *Regole* nella stessa pagina. Dopo aver creato o modificato delle regole, assicurarsi di *apply* le modifiche per metterle in produzione.

12.4 Gestione banda

Le classi per la gestione banda vengono utilizzate per dedicare una data larghezza di banda ad uno specifico traffico di rete. La larghezza di banda di ogni classe può essere specificata usando valori percentuali per indicare la banda disponibile o valori assoluti espressi in kbps.

Come impostazione predefinita, una classe di gestione banda viene applicata a tutte le interfacce di rete red. Tale comportamento può essere modificato selezionando un'interfaccia red esistente nel menu `:guilabel: Collega a` all'interno della sezione *Avanzate*. Le classi vincolate e la banda espressa in kbps non sono utilizzabili nel vecchio Server Manager.

Le regole possono essere create dalla sezione *Regole* nella stessa pagina. Dopo aver creato o modificato delle regole, assicurarsi di *apply* le modifiche per metterle in produzione.

12.5 SNAT

SNAT è disponibile solo se esiste almeno un alias IP configurato sulle interfacce di rete red. Vedi anche *sNAT 1:1*.

12.6 Oggetti

La pagina degli oggetti del firewall offre le stesse funzionalità presenti nel *vecchio Server Manager*.

12.7 Port forward

I port forwarding sono raggruppati per host di destinazione e supportano l'utilizzo di oggetti firewall e indirizzi IP «diretti».

I seguenti protocolli sono supportati solo nel nuovo Server Manager:

- AH
- ESP
- GRE

Per maggiori informazioni sui port forward dare riferimento alla documentazione del *vecchio Server Manager*.

12.8 Regole

Questa pagina consente la gestione delle regole applicate solamente al traffico di rete che attraversa il firewall. Per creare regole per il traffico da/verso il firewall stesso, consultare la sezione *Regole locali*.

Una regola si compone di cinque parti principali:

- Sorgente
- Destinazione
- Servizio (opzionale)
- Azione
- Condizione temporale (opzionale)

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

Le regole supportano l'inserimento diretto di indirizzi IP e contemplano due zone extra:

- *ivpn*: tutto il traffico proveniente da VPN IPSec
- *ovpn*: tutto il traffico proveniente da VPN OpenVPN

Entrambe le zone sono disponibili solo se è installata l'applicazione VPN. Le regole che usano tali zone, non possono essere modificate dal *vecchio Server Manager*.

12.8.1 Policy

Per visualizzare le policy attive fare clic sul pulsante *Policy*. Le policy sono influenzate dalle modifiche introdotte nella pagina *Impostazioni*.

12.9 Regole locali

Questa pagina consente la gestione delle regole applicate solo al traffico di rete generato dal firewall o diretto al firewall stesso. La configurazione è la stessa disponibile nella pagina *Regole*.

12.10 Connessioni

Questa pagina tiene traccia di tutte le connessioni attive. Le connessioni possono essere filtrate per *Protocollo* e *Stato*. L'elenco delle connessioni non viene aggiornato in tempo reale. Per visualizzare le nuove connessioni fare clic sul pulsante *Aggiorna*.

L'amministratore può cancellare una singola connessione o svuotare l'intera tabella di tracciamento della connessione usando il pulsante *Elimina tutte le connessioni*.

12.11 Impostazioni

Qui si trovano le impostazioni globali che influenzano l'intero comportamento del firewall, come la validazione del MAC. Quando viene modificata l'opzione *Traffico verso Internet (interfacce red)*, le modifiche si riflettono nella sezione *Policy*.

Il modulo Email è composto da tre parti principali:

- server SMTP per l'invio e la ricezione¹
- server IMAP e POP3 per la lettura della posta², e linguaggio Sieve per organizzarla³
- Filtro antispam, antivirus e blocco degli allegati⁴

Vantaggi

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

Vedi anche gli argomenti correlati:

- Come funziona la posta elettronica⁵
- Record DNS di tipo MX⁶
- Simple Mail Transfer Protocol (SMTP)⁷
- firma DKIM⁸

¹ Postfix mail server <http://www.postfix.org/>

² (1, 2) Dovecot Secure IMAP server <http://www.dovecot.org/>

³ Sieve mail filtering language [https://en.wikipedia.org/wiki/Sieve_\(mail_filtering_language\)](https://en.wikipedia.org/wiki/Sieve_(mail_filtering_language))

⁴ Rspamd: sistema di filtraggio di spam veloce, gratuito e open source. <https://rspamd.com/>

⁵ Posta elettronica, https://it.wikipedia.org/wiki/Posta_elettronica

⁶ Il record DNS MX, https://it.wikipedia.org/wiki/MX_record

⁷ SMTP, https://it.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

⁸ Domain Keys Identified Mail (DKIM) è un metodo di autenticazione e-mail progettato per rilevare lo spoofing delle e-mail – *Wikipedia*
<https://en.wikipedia.org/wiki/DomainKeys_Identified_Mail> _

Nota: Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *pop3_proxy-section* sono basate sul motore di filtraggio Rspamd. Le precedenti installazioni di NethServer verranno automaticamente aggiornate a Rspamd come descritto nella sezione *Aggiornamento Email a Rspamd*

13.1 Domini

NethServer può gestire un numero illimitato di domini di posta, configurabili dalla pagina *Email > Domini*. Per ogni dominio ci sono due alternative:

- *Consegna* dei messaggi alle caselle di posta locali, secondo il formato Maildir⁹.
- *Relay* dei messaggi ad un altro mail server

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 consente di conservare una *copia nascosta* di tutti i messaggi diretti ad un certo dominio: saranno consegnati al destinatario finale *e in più* ad un indirizzo email personalizzabile. La copia nascosta è abilitata dall'interruttore *Copia messaggi in ingresso* (precedentemente *Spedisci sempre una copia (Bcc)*).

Avvertimento: In alcuni paesi abilitare l'opzione *Copia messaggi in ingresso* può essere contro le leggi sulla privacy.

Se il destinatario finale non può essere raggiunto (ad esempio se l'indirizzo del destinatario non esiste), il messaggio viene normalmente rifiutato. A volte (ad esempio quando viene migrato un dominio di posta elettronica) potrebbe essere utile accettare e consegnare il messaggio ad una casella di posta di tipo *catch-all*. Questo comportamento può essere ottenuto abilitando l'opzione `:guilabel:'Accetta messaggi a destinatari ignoti'`.

13.1.1 Aggiungere un avviso legale

Avvertimento: Dal NethServer 7.5.1804 questa funzionalità è distribuita in un pacchetto separato e opzionale: `nethserver-mail-disclaimer`. Questo pacchetto è *deprecato* perché il progetto alterMIME¹⁰ su cui si basa l'attuale implementazione, non è più sviluppato e potrebbe smettere di funzionare in qualsiasi momento.

Se l'RPM opzionale `nethserver-mail-disclaimer` è stato installato dal terminale, NethServer può automaticamente aggiungere una nota legale ai messaggi inviati. Questo testo è anche conosciuto come «disclaimer» e serve per ottemperare a determinati requisiti legali.

Per configurare ed abilitare la nota legale allegata, abilitare l'interruttore dell'opzione *Email > Domini [Elemento lista] > Modifica > Aggiungi una nota legale in calce ai messaggi inviati*.

Il disclaimer può contenere codice Markdown¹¹ che consente la formattazione del testo.

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

⁹ The Maildir format, <https://en.wikipedia.org/wiki/Maildir>

¹⁰ alterMIME è un piccolo programma che viene utilizzato per modificare il tuo mailpack con codifica mime – <https://pldaniels.com/altermime/>

¹¹ The Markdown plain text formatting syntax, <https://en.wikipedia.org/wiki/Markdown>

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

Esempio di disclaimer:

```
This email and any files transmitted with it are confidential and
intended solely for the use of the individual or entity to whom they
are addressed. If you have received this email in error please
notify the system manager. This message contains confidential
information and is intended only for the individual named.
```

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

Esempio di firma:

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

13.1.2 Firma DKIM

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

Per attivare la firma DKIM per un dominio di posta, abilitare l'interruttore *Firma* sotto *Email > Domini > [elemento lista] > Configura DKIM*.

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

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

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

13.2 Filtro

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

- Allegati
- Antivirus
- Antispam

13.2.1 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.

13.2.2 Antivirus

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

13.2.3 Antispam

Il filtro antispam⁴ analizza i messaggi rilevando e classificando lo *spam*¹⁵ tramite criteri euristici, regole predeterminate e valutazioni statistiche sul contenuto dei messaggi.

Il filtro può anche verificare se il server mittente è elencato in una o più black list (DNSBL¹⁴). Un punteggio è associato a ciascuna regola.

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

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

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

I filtri statistici possono quindi essere addestrati con qualsiasi client IMAP semplicemente spostando un messaggio dentro e fuori da *Junk folder*. Come prerequisito, la cartella Junk deve essere abilitata con l'opzione *Email > Caselle di posta [Impostazioni generali] > Configura [Opzioni Avanzate] > Sposta lo spam nella cartella «Junk»* (precedentemente *Email > Caselle di posta > Spostare nella cartella «Junk»*).

- *Spostando un messaggio dentro la cartella «Junk»*, 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 «Junk»*, i filtri apprendono che è *ham*: a messaggi simili sarà assegnato un punteggio più basso.

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

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

È importante capire come funzionino i test bayesiani:

¹⁵ SPAM <https://it.wikipedia.org/wiki/Spam>

¹⁴ DNSBL <https://it.wikipedia.org/wiki/DNSBL>

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

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

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

Mentre il sistema riceve dati, l'avanzamento dell'addestramento dei filtri bayesiani può essere osservato dalla barra di progresso *Email > Filtro [Statistiche] > Allenamento bayesiani*.

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

13.2.4 Regole per le liste bianche e nere

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 *Email > Filtro [Regole] > Dettagli* (precedentemente *Regole di accesso per indirizzi email*) consente la creazione di tre tipi di regole:

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

Le regole di tipo *Accetta* hanno una precedenza maggiore rispetto a quelle di tipo *Blocca*. Se una regola *Accetta* corrisponde, i controlli antispam e antivirus vengono ignorati, la regola *Blocca* non viene valutata e il messaggio viene accettato.

Avvertimento: I controlli antivirus e antispam vengono ignorati se una regola *Accetta* corrisponde.

È possibile creare una regola *Accetta* o *Blocca* anche per un intero dominio, non solo per un singolo indirizzo e-mail: è sufficiente specificare il nome del dominio (ad esempio `dev.nethserver.org`).

Quando viene specificato un nome di dominio di secondo livello, la regola corrisponde anche per i suoi sottodomini. Per esempio `nethserver.org` include `nethserver.org` stesso, ma anche `dev.nethserver.org`, `demo.nethserver.org` e così via.

13.2.5 Interfaccia web di Rspamd

Il modulo antispam è implementato da Rspamd⁴ che è corredato della sua interfaccia web di amministrazione, disponibile all'URL

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

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

13.2.6 Quarantena (beta)

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

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

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

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

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

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

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

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

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

13.3 Caselle di posta

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

La lista delle caselle di posta è visibile nella pagina *Email > Caselle di posta*. Ci sono tre tipi di caselle di posta: Utenti, Gruppi, Cartelle pubbliche.

13.3.1 Caselle di posta utenti

Il pulsante *Modifica* consente di disabilitare l'Accesso ai servizi email (IMAP, POP3, SMTP/AUTH) per un utente specifico. I messaggi inviati a questo utente possono essere inoltrati a indirizzi email esterni multipli.

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

13.3.2 Caselle di posta gruppi

Gli *alias automatici per le caselle di posta dei gruppi* sono inizialmente disabilitati. Se abilitati, gli indirizzi come `<groupname>@<domain>` diventano indirizzi email validi. Un certo indirizzo di gruppo può essere disabilitato ed abilitato nuovamente in un momento successivo, una volta che le caselle di posta dei gruppi sono abilitate. Per disabilitare gli alias automatici globalmente fare riferimento a *Impostazioni generali*.

Una casella di gruppo non occupa spazio disco. Quando un messaggio viene spedito a una casella di gruppo, la copia di esso è consegnata a ciascun membro del gruppo, secondo le individuali preferenze di consegna ed inoltro.

13.3.3 Cartelle di posta pubbliche

Nota: Nel vecchio Server Manager la dicitura *Mailbox condivise* era impiegata al posto di *Cartelle pubbliche*.

Le cartelle di posta pubbliche possono essere condivise tra gruppi di utenti. La pagina *Email > Caselle di posta > Cartelle pubbliche* consente la creazione di una nuova cartella pubblica e la definizione di uno o più gruppi proprietari. Le cartelle pubbliche possono anche essere create da un qualsiasi client IMAP che supporta l'estensione del protocollo IMAP ACL (RFC 4314).

13.3.4 Impostazioni generali

La pagina *Email > Caselle di posta [Impostazioni generali]* mostra l'elenco dei protocolli disponibili per l'accesso alle caselle di posta degli utenti:

- IMAP¹² (raccomandato)
- POP3¹³ (sconsigliato)

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

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

Dalla stessa pagina il *Limite quota* di una casella di posta può essere impostato ad un valore comune di base. Se alle caselle di posta è applicata una quota, la pagina *Email > Caselle di posta* riassume l'utilizzo dello spazio disco di ogni utente. Il valore mostrato è aggiornato quando un utente accede alla casella di posta o un nuovo messaggio viene

¹² IMAP https://it.wikipedia.org/wiki/Internet_Message_Access_Protocol

¹³ POP3 https://it.wikipedia.org/wiki/Post_Office_Protocol

consegnato. La quota può essere personalizzata per un utente particolare mediante *Email > Caselle di posta [utente] > Modifica > Quota email personalizzata*.

I messaggi marcati come **spam** (vedi *Filtro*) possono essere spostati automaticamente nella cartella *Junk* abilitando l'opzione *Sposta lo spam nella cartella «Junk»*. I messaggi di spam vengono automaticamente rimossi trascorso il periodo *Conserva spam per*. Tale periodo può essere personalizzato per un utente particolare dal controllo *Email > Caselle di posta [Utenti] > Modifica > Eliminazione automatica spam*.

L'utente `root` può impersonare un altro utente, acquisendo pieni diritti sui contenuti della casella di posta e sui permessi delle cartelle di quest'ultimo. L'opzione *Root può accedere impersonando un altro utente* controlla questa facoltà, conosciuta con il nome di *master user* in Dovecot².

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

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

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

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

Opzioni aggiuntive:

- Se le *caselle di posta gruppi* sono state abilitate in *Email > Caselle di posta > Gruppi* deselezionare l'opzione *Alias automatici per i gruppi* per disabilitarli di nuovo.
- È possibile registrare le azioni IMAP abilitando *Registra le azioni IMAP*. Vedere inoltre *Log*.
- A differenza della quasi totalità dei client IMAP, Outlook non sposta i messaggi eliminati nel cestino, ma si limita a marcarli «cancellati».

È possibile spostare automaticamente i messaggi nella cartella cestino abilitando *Sposta le mail cancellate nel cestino (Outlook)*.

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.

- *Massimo di connessioni per IP* cambia il limite di connessioni per utente provenienti dal medesimo indirizzo IP. Questo limite può essere aumentato se messaggi come *Maximum number of connections* compaiono nei file di log (vedere *Log*).

13.3.5 Configurazione *visti condivisi*

Gli utenti possono condividere la propria casella di posta (o parte di essa, cioè specifiche cartelle) con account selezionati del sistema. Chiunque abbia accesso a una casella di posta condivisa può leggerne o eliminarne i messaggi in base alle autorizzazioni concesse dal proprietario.

Il flag IMAP `/Seen` viene utilizzato per contrassegnare se un messaggio è stato letto o meno. In una casella di posta condivisa, ogni utente ha la propria copia dei messaggi letti, ma a volte un team che condivide una casella di posta potrebbe preferire sapere se un messaggio è già stato letto da qualcun altro. Per abilitare la condivisione del flag `Seen` per tutte le caselle di posta condivise, utilizzare i seguenti comandi:

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

È opportuno sottolineare che la modifica dello stato di `SharedSeen` ripristina il flag `/Seen` per tutti gli utenti su tutte le cassette postali.

Le cartelle pubbliche vengono create dall'amministratore e in genere sono visibili a tutti gli utenti (o ai grandi gruppi). Il flag `/Seen` viene gestito per ciascun utente e non può essere condiviso.

13.4 Indirizzi

In aggiunta alle caselle di posta Utenti, Gruppi e Pubbliche, descritte nella sezione precedente, il sistema consente la creazione di un numero illimitato di indirizzi di posta dalla pagina *Email > Indirizzi*. Ogni *indirizzo email* è associato con una o più destinazioni. Una *destinazione* può essere dei seguenti tipi:

- casella utente
- casella gruppo
- cartella pubblica
- indirizzo email esterno

Un indirizzo email può essere legato a qualsiasi dominio di posta o essere specifico per un certo dominio. Per esempio:

- Primo dominio: `miodominio.it`
- Secondo dominio: `esempio.com`
- L'indirizzo email *info* collegato a qualsiasi dominio: `info@mydomain.net`, `info@example.com`
- L'indirizzo email *goofy* specifico per un solo dominio: `goofy@example.com`

A volte le aziende proibiscono l'uso di indirizzi e-mail personali per le comunicazioni dell'organizzazione verso l'esterno. L'opzione *Interna* (precedentemente *Solo reti locali*) e i pulsanti *Rendi interno* e *Rendi pubblico* impediscono ad un indirizzo di ricevere e-mail dall'esterno. Tuttavia un indirizzo *interno* può ancora essere utilizzato per scambiare messaggi con gli altri account del sistema.

13.5 Connettori

La pagina *Email > Connettori* è descritta in *Connettore POP3*.

13.6 Sincronizzazione

La pagina *Email > Sincronizzazione* si basa su uno tool di migrazione IMAP chiamato *Imapsync*. Lo scopo è migrare i messaggi e-mail da un account IMAP remoto a uno locale.

La migrazione è ricorsiva e incrementale e può essere ripetuta tutte le volte che è necessario. Le e-mail verranno copiate solo se non esistono sul server locale.

L'amministratore di sistema del NethServer locale non necessita di conoscere la password dell'utente locale. Tuttavia, l'amministratore deve conoscere la password dell'account IMAP remoto, a meno che l'autenticazione dell'amministratore IMAP sia implementata anche per il server di posta remoto.

Se anche il server IMAP remoto è un NethServer, l'utente amministratore IMAP è `vmail` e la sua password può essere ricavata da `:file: /var/lib/nethserver/secrets/vmail`. Il nome utente con il suffisso `*vmail` (ad es. `nomeutente@dominio.com*vmail`) e la password di `vmail` dovranno essere impostati nel pannello di sincronizzazione IMAP.

Nota: Un elenco di [Server IMAP con autenticazione admin](#) è disponibile nella documentazione di *Imapsync*

13.7 Coda

La pagina *Email > Coda* elenca i messaggi in attesa di essere trasferiti nella coda di posta SMTP. In condizioni normali questa coda dovrebbe essere vuota o contenere al più alcuni messaggi.

Il link *Email > Coda [Grafici] > Mostra grafici* mostra in tempo reale lo stato della coda di posta degli ultimi minuti, aggiornato finché la pagina viene lasciata aperta. Il grafico mostra il numero dei messaggi nella coda e le dimensioni totali della coda in kilobyte.

Mentre i messaggi sono nella coda, l'amministratore può richiedere un tentativo immediato di spedizione, premendo il pulsante *Rispedisci tutti* (precedentemente *Tenta l'invio*), o svuotare completamente la coda mediante il pulsante *Elimina tutti*.

È anche possibile eseguire su un singolo messaggio in coda *Rispedisci* o *Elimina* dai pulsanti azione degli elementi di *Email > Coda [Lista]*.

13.8 Relay

La pagina *Email > Relay* configura come i messaggi sono accettati e instradati dal server SMTP di NethServer ad altri server SMTP.

13.8.1 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. Vedere anche *Configurazione client*.

Per semplificare la configurazione di ambienti preesistenti, la sezione *Email > Relay [Configurazione] > Details* (precedentemente *Email > SMTP access*) consente di specificare delle eccezioni ai criteri di accesso SMTP di default.

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

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

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

In più nella stessa sezione ci sono ulteriori opzioni:

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

Per evitare l'uso non autorizzato degli indirizzi e-mail e lo spoofing dell'indirizzo del mittente, abilitare l'opzione *Forza corrispondenza mittente/login*.

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

13.8.2 HELO personalizzato

Il primo passo di una sessione SMTP è lo scambio del comando *HELO* (o *EHLO*). Tale comando richiede come parametro il nome del server completo di dominio valido (RFC 1123).

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 nome host completo di dominio (FQDN) come valore per il comando HELO. Se questo non è registrato nel DNS pubblico, tale valore può essere cambiato nel campo di testo *HELO personalizzato*.

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.

13.8.3 Relay host

La pagina *Email > Relay* consente di descrivere la rotta di un messaggio e-mail spedendolo attraverso un relay host esterno specificando porta, autenticazione e impostazioni TLS.

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

Il relay host è identificato **dall'indirizzo del mittente SMTP**. È possibile abbinare l'indirizzo completo del mittente o solo il suo dominio.

13.8.4 Impostazioni del relay host di default

Se l'indirizzo del mittente non corrisponde ad alcuna delle regole di relay descritte nella sezione precedente è possibile (anche se non raccomandato) configurare un relay host di default invece di basarsi sulle regole di relay dello standard SMTP.

Nota: Spedire tramite uno *smarthost* è in genere sconsigliato, a meno che il server non sia temporaneamente in una blacklist¹⁴, o il traffico SMTP sia bloccato dall'ISP.

La sezione *Sistema > Impostazioni > Smart host* consente di affidare l'invio di tutti i messaggi in uscita ad uno speciale server SMTP, tecnicamente denominato *smarthost*. Uno smarthost consente l'inoltro dei messaggi se sono verificate determinate condizioni. È possibile che verifichi:

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

Fare riferimento anche a *Smart host* per maggiori informazioni.

13.9 Impostazioni

Dalla pagina *Email > Impostazioni*, il controllo *Dimensione massima messaggio* (precedentemente *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 *Ritenta l'invio per* (precedentemente *Tenta l'invio per*) cambia questo limite. Di default è impostato a *4 giorni*.

L'opzione *Inoltra una copia di tutti i messaggi* (precedentemente *Spedisci sempre una copia (Bcc)*) abilita la copia nascosta di qualsiasi messaggio attraverso 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: In alcuni paesi abilitare l'opzione *Inoltra una copia di tutti i messaggi* può essere contro le leggi sulla privacy.

13.10 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 e in più le azioni IMAP, se abilitate secondo *Impostazioni generali*.

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

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

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

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

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

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

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

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

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

Resa

```

/var/log/maillog:May 15 02:05:02 mail postfix/smtpd[25846]: A785B308622AB: client=my.
↪example.com[10.154.200.17]
/var/log/maillog:May 15 02:05:02 mail postfix/cleanup[25849]: A785B308622AB: message-
↪id=<5afa242e.hp5p/mry+fTNNjms%no-reply@example.com>
/var/log/maillog:May 15 02:05:02 mail rspamd[27538]: <8ae27d>; proxy; rspamd_message_
↪parse: loaded message; id: <5afa242e.hp5p/mry+fTNNjms%no-reply@example.com>; queue-
↪id: <A785B308622AB>; size: 2348; checksum: <b1035f4fb07162ba88053d9e38df9c93>
/var/log/maillog:May 15 02:05:03 mail rspamd[27538]: <8ae27d>; proxy; rspamd_task_
↪write_log: id: <5afa242e.hp5p/mry+fTNNjms%no-reply@example.com>, qid:
↪<A785B308622AB>, ip: 10.154.200.17, from: <no-reply@example.com>, (default: F (no_
↪action): [-0.64/20.00] [BAYES_HAM(-3.00){100.00%;},AUTH_NA(1.00){},MID_CONTAINS_
↪FROM(1.00){},MX_INVALID(0.50){},MIME_GOOD(-0.10){text/plain;},IP_SCORE(-0.04){ip:_
↪(0.22), ipnet: 10.154.192.0/20(0.18), asn: 14061(0.23), country: US(-0.81);},ASN(0.
↪00){asn:14061, ipnet:10.154.192.0/20, country:US;},DMARC_NA(0.00){example.com;},
↪FROM_EQ_ENVFROM(0.00){},FROM_NO_DN(0.00){},NEURAL_HAM(-0.00){-0.656;0;},RCPT_COUNT_
↪ONE(0.00){1;},RCVD_COUNT_TWO(0.00){2;},RCVD_NO_TLS_LAST(0.00){},R_DKIM_NA(0.00){},R_
↪SPF_NA(0.00){},TO_DN_NONE(0.00){},TO_DOM_EQ_FROM_DOM(0.00){},TO_MATCH_ENVRCPT_ALL(0.
↪00){}), len: 2348, time: 750.636ms real, 5.680ms virtual, dns req: 47, digest:
↪<b1035f4fb07162ba88053d9e38df9c93>, rcpts: <jsmith@example.com>, mime_rcpts:
↪<jsmith@example.com>
/var/log/maillog:May 15 02:05:03 mail postfix/qmgr[27757]: A785B308622AB: from=<no-
↪reply@example.com>, size=2597, nrcpt=1 (queue active)
/var/log/maillog:May 15 02:05:03 mail postfix/lmtp[25854]: A785B308622AB: to=
↪<vmail+jsmith@mail.mynethserver.org>, orig_to=<jsmith@example.com>, relay=mail.
↪mynethserver.org[/var/run/dovecot/lmtp], delay=0.82, delays=0.8/0.01/0.01/0.01,_
↪dsn=2.0.0, status=sent (250 2.0.0 <vmail+jsmith@mail.mynethserver.org> gK8pHS8k+lr/
↪ZAAAJc5BcA Saved)
/var/log/maillog:May 15 02:05:03 mail postfix/qmgr[27757]: A785B308622AB: removed

```

13.11 Configurazione client

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

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

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

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

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

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

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

Riferimenti

La documentazione del backup è divisa nei seguenti capitoli:

- *Impostazioni*: impostazioni generali backup dati
- *Legacy backup*: configurazione dal vecchio Server Manager
- *Disaster recovery*: come ripristinare un sistema guasto
- *Personalizzazione backup*: personalizzazione avanzata, best practice e strumenti da riga di comando

Il sistema gestisce due tipi di backup:

- backup della configurazione
- backup dei dati

Backup configurazione

Il backup della configurazione contiene solo i file di configurazione del sistema ed è completamente automatico. Lo scopo di questo tipo di backup è ripristinare rapidamente una macchina in caso di *disaster recovery*. La configurazione del sistema può essere salvata, scaricata, caricata e ripristinata di nuovo attraverso la pagina *Backup*. La politica di conservazione del backup della configurazione può essere modificata facendo clic sul pulsante *Configura*. Assicurarsi di scaricare regolarmente il backup della configurazione e di salvarlo in un luogo sicuro.

Backup dati

Il backup dei dati contiene tutti i dati memorizzati nel sistema (directory home dell'utente, cartelle condivise, e-mail, ecc.). L'amministratore può pianificare più backup dei dati.

14.1 Impostazioni

Il backup dei dati può essere eseguito utilizzando diversi engine:

- **restic**: molto veloce, deduplicazione e crittografia abilitate per impostazione predefinita, il più adatto per l'archiviazione su cloud
- **rsync**: deduplicazione parziale semplice e veloce, perfetta per l'archiviazione su USB e SFTP
- **duplcity**: consolidato e affidabile, utilizza la compressione e può eseguire backup completi o incrementali, nessuna crittografia, la scelta migliore per un filesystem in rete locale

Backend di archiviazione disponibili:

- filesystem di rete in LAN: Windows File Share (CIFS), Network File System (NFS)
- filesystem di rete remoti: WebDAV, SSH File Transfer Protocol (SFTP)
- disco locale collegato ad una porta USB/SATA
- provider cloud: Amazon S3 (o qualsiasi server compatibile S3)
- Backblaze [B2](#)

Quando si utilizza WebDAV come back-end di archiviazione, assicurarsi che il server disponga di un certificato SSL valido, altrimenti il sistema non riuscirà a montare il filesystem

14.1.1 Pianificazione

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

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

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

Per configurare un nuovo backup, accedere alla pagina *Backup* e fare clic sul pulsante *Pianifica*. L'interfaccia Web avvierà una procedura guidata che suggerirà automaticamente il motore migliore in base al tipo di destinazione.

14.1.2 Personalizzazione backup dati

Ogni volta che un nuovo modulo di NethServer viene installato, tutte le relative directory contenenti dati vengono aggiunte automaticamente al backup dei dati.

L'elenco dei percorsi inclusi nel backup è visibile facendo clic sul pulsante *Configura* dalla pagina *Backup*. Dalla stessa pagina, è anche possibile personalizzare ciò che è incluso o escluso.

Quando l'opzione *Includi i log* è abilitata, tutti i registri verranno automaticamente aggiunti al set di backup.

Per ulteriori personalizzazioni vedere *Personalizzazione backup*.

14.1.3 Notifiche

Al termine del backup è possibile inviare una notifica e-mail all'amministratore di sistema o a un elenco di indirizzi e-mail personalizzati.

Di norma le notifiche vengono inviate in caso di errore del backup. È possibile disabilitarle del tutto o abilitarle anche in caso di backup riuscito modificando il campo *Notifica in caso di* nel passaggio finale della procedura guidata di configurazione del backup.

Se fosse necessario ottimizzare le opzioni di notifica globali, come un realy SMTP, fare riferimento al capitolo *Impostazioni*.

14.2 Ripristino selettivo dei file

L'applicazione *Ripristino dati* deve essere installata esplicitamente dal Software Center. Si noti che il ripristino selettivo sarà disponibile solo per i backup eseguiti dopo l'installazione dell'applicazione.

Assicurarsi che la destinazione del backup sia raggiungibile (ad esempio, il disco USB deve essere collegato), quindi accedere alla applicazione *Ripristino dati*.

Dalla applicazione *Ripristino dati*, selezionare il nome del backup e la data di esecuzione. Quindi cercare un file o una directory inserendo il nome nel campo *File o directory*. Per risultati migliori, selezionare la modalità di ricerca più adatta alle proprie esigenze dal menu *Selezionare modalità*: la ricerca può essere limitata alle sole cartelle di posta, a file normali di applicazioni come Nextcloud. Se viene selezionata la modalità *Advanced*, è possibile usare *espressioni regolari* all'interno del campo *Pattern*.

Infine, selezionare i file da ripristinare e fare clic sul pulsante *Ripristina*.

Se l'opzione *Sovrascrivi* è selezionata, i file ripristinati sovrascriveranno quelli esistenti. Diversamente i file verranno ripristinati nello stesso percorso di quelli esistenti, rinominati con il prefisso `.restore` e con la data inclusa nel nome, ad esempio `.restore-20190729-153318-myfile`.

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

Altre configurazioni ripristinate:

- Utenti e gruppi
- Certificati SSL

Avvertimento: Non ripristinare un backup della configurazione proveniente da una minor version in una versione più recente. Il backup dovrebbe provenire da un NethServer avente la stessa versione del sistema operativo della nuova installazione. Ad esempio, evitare di ripristinare il backup della configurazione di una installazione 7.4.1708 su un nuovo sistema 7.6.1810, poiché potrebbero verificarsi comportamenti inaspettati.

15.1 Nuovo Server Manager

Si prega di seguire i seguenti passi:

1. Installare la nuova macchina (fare riferimento alla sezione *installazione*), accedere al nuovo Server Manager e assicurarsi che la macchina sia in grado di accedere a Internet e risolvere correttamente i nomi pubblici
2. Se la macchina ha una subscription Community, seguire le indicazioni della sezione *Subscription*, altrimenti ignorare questo passaggio
3. Installare tutti gli aggiornamenti core disponibili da *Aggiornamenti software*
4. Accedere alla pagina *Backup* e fare click sul pulsante *Ripristina* nella sezione **Backup configurazione**, quindi caricare il backup della configurazione o scaricarlo direttamente da un URL HTTP/S.

Nella versione Enterprise di NethServer , tutti i backup in cloud verranno automaticamente scaricati e resi disponibili per essere selezionati tramite il campo *Dal backup*.

5. Mappare i nomi delle interfacce di rete dal backup al sistema in esecuzione. Questo passaggio è necessario solo se l'opzione *Ripristina configurazione di rete* è abilitata.
6. Preme il pulsante *Ripristina* per iniziare il processo di ripristino.

Nota: Se si è connessi ad un'interfaccia di rete che cambierà indirizzo IP durante il ripristino, si verrà disconnessi dal Server Manager e sarà necessario ricollegarsi usando il nuovo indirizzo IP.

7. Verificare che il sistema sia funzionante, quindi accedere alla pagina *Backup*. Per ripristinare tutti i file, fare click sul pulsante *Ripristina* nella sezione **Backup dati**, selezionare il nome del backup e fare click sul pulsante *Ripristina*.

Si tenga presente che il processo di ripristino può durare da pochi minuti a diverse ore

Se *Ripristina configurazione di rete* non fosse stato abilitato, potrebbero essere necessari ulteriori passaggi per ripristinare tutte le applicazioni. Fare riferimento alla sezione *Disabilitare ripristino della rete* per maggiori dettagli.

15.2 Vecchio Server Manager

Si prega di seguire i seguenti passi:

1. Installare la nuova macchina (fare riferimento alla sezione *Installazione*), accedere al Server Manager e seguire la procedura di prima configurazione per completare la configurazione di base del sistema
2. Assicurarsi che NethServer sia in grado di accedere ad internet e risolvere correttamente i nomi con il DNS pubblico
3. Installare tutti gli aggiornamenti core disponibili dal *Software Center*
4. Ripristinare il backup della configurazione utilizzando il pannello *Backup (configurazione)*
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 il backup dei dati eseguendo dalla console

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

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

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

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

15.2.1 Assegnamento delle interfacce di rete

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

- dopo il ripristino del backup della configurazione su un nuovo hardware

- una o più schede di rete sono state sostituite
- i dischi del sistema sono stati spostati su una nuova macchina

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

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

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

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

Premendo il pulsante *Salva* le modifiche vengono applicate.

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

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

15.3 Disabilitare ripristino della rete

La configurazione di rete viene ripristinata per impostazione predefinita, ma in alcune situazioni è necessario ripristinare un'installazione su un hardware differente senza migrarne la configurazione di rete. Questo è uno scenario comune quando si sposta una macchina virtuale da un provider VPS a un altro.

Per disabilitare il ripristino della rete, assicurarsi di disabilitare l'opzione *Ripristina configurazione di rete* dal nuovo Server Manager.

Poiché alcune configurazioni dell'applicazione dipendono dai nomi delle interfacce di rete, non tutto può essere ripristinato automaticamente.

15.3.1 DHCP

I server DHCP su interfacce inesistenti verranno eliminati. Se necessario, riconfigurare il DHCP tramite il Server Manager. Fare riferimento alla sezione *:ref dhcp-section* per maggiori informazioni.

15.3.2 Samba Active Directory

Avvertimento: Il ripristino di un Samba Active Directory locale senza l'opzione *Ripristina configurazione di rete* abilitata è altamente sconsigliato. Leggere attentamente quanto riportato di seguito.

Samba Active Directory richiede un bridge di rete e un indirizzo IP aggiuntivo, inutilizzato, nella zona *green* per attivare il container locale.

Se il bridge esiste e l'indirizzo IP si adatta alla configurazione di rete corrente, il container continuerà a funzionare anche dopo il ripristino.

Viceversa Samba Active Directory verrà arrestato forzatamente. Per abilitarlo di nuovo:

- dalla pagina *Rete*, creare il bridge, ad esempio `br0`

- individuare un indirizzo IP inutilizzato sulla rete green, ad esempio 192.168.1.11
- riconfigurare il container da riga di comando:

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

- correggere le ACL di sysvol del DC:

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

Per maggiori informazioni fare riferimento alla sezione *Installazione del provider locale Samba Active Directory*.

15.3.3 Firewall

Al termine del ripristino il firewall provvederà a:

- eliminare tutti i provider WAN
- eliminare tutte le zone connesse alle interfacce di rete inesistenti
- disabilitare tutte le regole relative ad una zona inesistente o un ruolo inesistente

L'amministratore potrà accedere al Server Manager per creare zone e ruoli mancanti. Infine, tutte le regole precedentemente disabilitate potranno essere nuovamente abilitate manualmente.

Fare riferimento alla sezione *Firewall*.

15.3.4 Proxy Web

Le regole di priorità del proxy Web che utilizzano zone inesistenti verranno disabilitate. Prima di riattivare tali regole, assicurarsi che le zone siano state create.

Per maggiori informazioni fare riferimento alla sezione *Regole di priorità e di instradamento*.

15.3.5 Tunnel OpenVPN

I server tunnel OpenVPN contengono un campo chiamato *Indirizzo pubblico*. Se tale campo utilizza solo nomi DNS pubblici, non è richiesta alcuna azione. In caso contrario, si dovrà inserire il nuovo indirizzo IP pubblico all'interno del campo e aggiornare i client del tunnel di conseguenza.

Per maggiori informazioni fare riferimento alla sezione *Tunnel (net2net)* della pagina OpenVPN.

15.3.6 OpenVPN roadwarrior

Il server OpenVPN roadwarrior espone un campo chiamato *Contatta questo server su IP / host pubblico*. Se tale campo utilizza solo nomi DNS pubblici, non è richiesta alcuna azione. In caso contrario, si dovrà inserire il nuovo indirizzo IP pubblico nel campo e aggiornare i client roadwarrior di conseguenza.

Per maggiori informazioni fare riferimento alla sezione *Roadwarrior* della pagina OpenVPN

15.3.7 Tunnel IPSec

Solo i tunnel IPSec configurati su un'interfaccia red dinamica saranno disabilitati. Si dovrà accedere al Server Manager, modificare il tunnel disabilitato selezionando una nuova interfaccia red e abilitarlo nuovamente.

Per maggiori informazioni fare riferimento alla sezione *IPsec*.

15.3.8 Hotspot Dedalo

L'hotspot Dedalo sarà disabilitato se il sistema non ha un'interfaccia di rete configurata con il ruolo `hotspot`. Se Dedalo verrà disabilitato, sarà possibile riconfigurarli seguendo le indicazioni del capitolo *Hotspot (Dedalo)*.

15.3.9 ntopng

ntopng dovrà essere riconfigurato accedendo alla pagina *Monitor di banda* all'interno del vecchio Server Manager, abilitando il servizio e selezionando le interfacce di rete da monitorare.

Per maggiori informazioni fare riferimento alla sezione *Monitor banda*.

La personalizzazione di base può essere effettuata direttamente dal nuovo Server Manager. Vedi *Personalizzazione backup dati*.

16.1 Backup dati

Il backup dei dati può essere eseguito utilizzando diversi engine:

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

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

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

- incrementale: confronta i dati con l'ultimo backup completo e copia solo gli elementi modificati o aggiunti. Il backup completo e tutti gli incrementali intermedi sono necessari per il processo di ripristino. È richiesto che venga eseguito regolarmente un backup completo.
- snapshot: crea un backup completo solo la prima volta, successivamente crea solo backup differenziali. Le istantanee possono essere eliminate e consolidate ed è necessario un solo backup completo

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

16.1.1 Backend di archiviazione

Supportati da tutti gli engine:

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

Supportati da restic ed rsync

- SFTP: SSH File Transfer Protocol

Supportati solo da restic

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

16.1.2 Engine

Duplicity

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

Backend di archiviazione supportati:

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

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

Restic

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

Backend di archiviazione supportati:

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

Quando si configura un backup utilizzando l'engine restic e un back-end di archiviazione remoto, assicurarsi di disporre di una larghezza di banda sufficiente per completare il primo backup entro 24 ore. In caso contrario, restic creerà molteplici istantanee diverse. Se si dispone di una connessione lenta e si desidera ancora utilizzare un back-end di archiviazione remoto, attenersi alla seguente procedura:

- configurare il backup con restic
- eseguire manualmente il backup cliccando su *Esegui ora*
- disabilitare il backup configurato, in modo che non venga avviato alla successiva esecuzione pianificata
- terminato il backup manuale, riabilitare il backup per consentirne l'esecuzione pianificata

Rsync

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

Backend di archiviazione supportati:

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

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

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

È necessario accedere alla destinazione con l'utente `root`.

16.1.3 Esecuzione da riga di comando

Per lanciare un backup da riga di comando, utilizzare:

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

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

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

16.1.4 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.

Inclusione

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

Ad esempio, per includere nel backup un software installato nella directory `/opt`, aggiungere questa riga:

```
/opt/mysoftware
```

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

Esclusione

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

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

```
**Download**
```

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

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

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

Personalizzazione inclusioni ed esclusioni

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

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

In cui `name` è il nome del backup.

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

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

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

Esempio

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

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

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

3. Creare un file exclude custom vuoto:

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

4. Applicare la configurazione:

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

Avvertimento: Assicurarsi di non lasciare righe vuote all'interno file modificati.

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

16.2 Backup configurazione

Il backup della configurazione è un'attività automatizzata che viene eseguita ogni notte alle 00.15 e che crea un nuovo archivio, `/var/lib/nethserver/backup/backup-config.tar.xz`, se la configurazione è cambiata nelle 24 ore precedenti.

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

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

16.2.1 Inclusione

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

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

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

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

16.2.2 Esclusione

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

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

16.3 Ripristino da linea di comando

Nel caso in cui l'interfaccia web `select_restore-section` non fosse sufficiente, il ripristino può essere eseguito dalla riga di comando.

Tutti i file rilevanti sono conservati nella directory `/var/lib/nethserver/`:

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

Per ottenere un elenco dei dati contenuti in un backup, utilizzare:

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

Per ripristinare tutti i dati nella loro posizione originale, utilizzare:

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

Per ripristinare un file o una directory, utilizzare:

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

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

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

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

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

16.4 Formattazione di un disco locale

I dischi locali possono essere formattati direttamente dalla *interfaccia web*. Se qualcosa andasse storto o fosse necessario un partizionamento personalizzato, seguire i seguenti passaggi.

I migliori filesystem per dischi di backup SATA/USB sono EXT3 o EXT4. Il filesystem FAT è supportato ma *non raccomandato*, mentre NTFS **non è supportato**. EXT3 o EXT4 sono obbligatori in caso di utilizzo dell'engine rsync.

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

```
# dmesg | tail -20

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

Un altro buon comando da utilizzare è 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:

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

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

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

- Scollegare e ricollegare il disco USB:

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

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

- A questo punto l'etichetta *backup* sarà visualizzata nella pagina *Backup*.

Nota: Un nuovo modulo di backup è disponibile nel nuovo Server Manager. Vedere *Backup*.

NethServer gestisce due tipi di backup: il backup della configurazione e il backup dei dati. Vedere *Backup* per maggiori informazioni.

17.1 Backup configurazione

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

La pagina permette di creare un nuovo backup su richiesta, cliccando sul pulsante *Crea backup*. Di default, il sistema mantiene gli ultimi tre backup della configurazione. La politica di conservazione può essere modificata con il pulsante *Configura*.

17.2 Backup dati

Nota: Il vecchio Server Manager può gestire un singolo backup. La stessa configurazione può essere gestita anche dal nuovo Server Manager, modificando il backup denominato `backup-data`.

Il backup dei dati viene eseguito utilizzando l'engine Duplicity e può essere configurato dalla pagina *Backup (dati)*. Duplicity è l'engine di backup predefinito per NethServer. Ha un buon algoritmo di compressione che ridurrà l'utilizzo dello spazio sulla destinazione. Duplicity richiede un backup completo una volta alla settimana e, quando il set di dati è molto grande, il completamento del processo potrebbe richiedere più di 24 ore. NethServer non implementa la crittografia per il backup quando si utilizza Duplicity.

Backend di archiviazione supportati:

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

Il restore selettivo di file può essere eseguito solo dal nuovo Server Manager. Vedere *Ripristino selettivo dei file*.

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

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

La webmail è raggiungibile ai seguenti indirizzi:

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

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

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

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

18.1 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
```

18.2 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
```

18.3 Rimozione

Se si desidera rimuovere Roundcube, eseguire il seguente comando.

```
yum autoremove nethserver-roundcubemail
```

WebTop è un groupware completo che implementa il protocollo ActiveSync.

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

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

19.1 Autenticazione

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

Esempio

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

Nota: Il protocollo Active Sync è supportato solo su Android e IOS. Outlook non è supportato.

19.1.1 Utente admin

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

Le credenziali di default sono:

- Utente: admin
- Password: admin

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

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

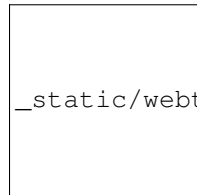
E' possibile controllare la posta dell'utente admin di sistema usando questo login: `admin@<dominio>` dove `<dominio>` è il dominio del server che fa parte del FQDN.

Esempio

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

Cambio della password di admin

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



Selezionare *Impostazioni* quindi cliccare sul tasto `gui-label:Cambia password`.

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

```
curl -sL https://git.io/fjhn8 -o webtop-set-admin-password
bash webtop-set-admin-password <newpassword>
```

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

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

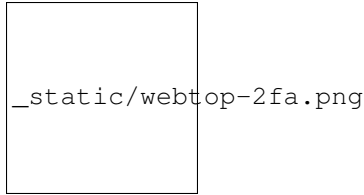
19.2 Autenticazione a due fattori (2FA)

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

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

Per abilitare 2FA:

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



19.3 Sincronizzazione con ActiveSync (EAS)

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

19.3.1 Apple iOS

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

Compilare i campi richiesti con:

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

Nota: I device iOS richiedono un certificato SSL valido sul server. Vedi [server_certificate-section](#)

19.3.2 Google Android

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

Compilare i campi richiesti con:

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

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

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

19.3.3 Calendari e Rubriche multiple

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

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

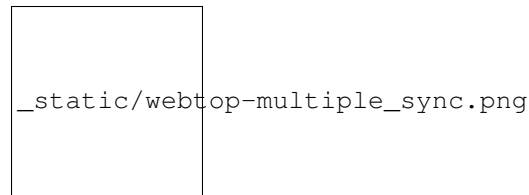
I device mobili basati su Apple iOS supportano integralmente le cartelle/categorie per calendario, contatti e attività (chiamati promemoria), inclusi i colori originali.

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

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

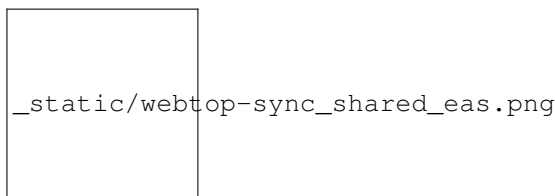
Sui dispositivi Android, i contatti delle rubriche condivise vengono uniti a quelli della rubrica personale e visualizzati in un'unica vista. I contatti possono essere modificati e le modifiche verranno recepite dalla sorgente originale.

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



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

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



L'impostazione predefinita è «Disattiva».

19.4 Sincronizzazione con CalDAV e CardDAV

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

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

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

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

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

- **Password:** inserire la password

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

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

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

19.4.1 Google Android

Un buon client di terze parti Android gratuito è [Opensync](#).

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

19.4.2 Apple iOS

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

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

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

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

19.4.3 Client per desktop

Thunderbird

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

- L'add-on *Cardbook* funziona bene, il setup è semplice e supporta l'autodiscovery.
- Il componente aggiuntivo *Lightning* non supporta l'autodiscovery: qualsiasi calendario deve essere aggiunto manualmente.

Outlook

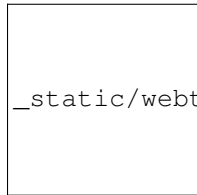
- Il client open source *Outlook CalDav Synchronizer* funziona bene, e supporta sia CardDAV che CalDAV.

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

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

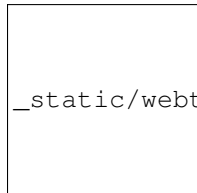
19.5 Condividere le cartelle e-mail o l'intero account

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



_static/webtop-sharing_mail_folder_1.png

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



_static/webtop-sharing_mail_folder_2.png

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

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

19.6 Condivisione di calendari e rubriche

19.6.1 Condivisione Calendario

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



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



19.6.2 Condivisione Rubrica

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

19.7 Etichette sulle Mail

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

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

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

19.8 Anteprima mail sulla riga del messaggio

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

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



19.9 Archiviazione mail

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

Nota: Archivio mail non è un backup

Il sistema crea automaticamente una nuova cartella speciale di archivi



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

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

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



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



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



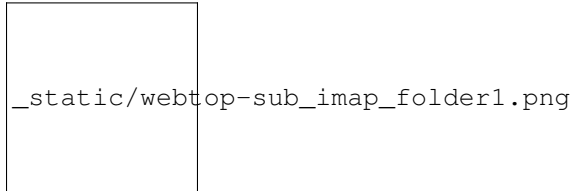
Il sistema elaborerà l'archiviazione in base alle ultime impostazioni scelte.

19.10 Sottoscrizione di cartelle IMAP

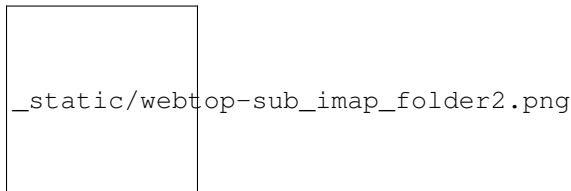
Su WebTop, per impostazione predefinita, tutte le cartelle IMAP sul server vengono automaticamente sottoscritte e sono quindi visibili dal primo accesso.

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

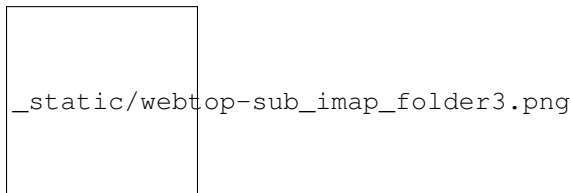
Ad esempio, se si desidera nascondere la sottocartella «cartella1» da questo elenco, è sufficiente fare clic con il pulsante destro del mouse su di essa e selezionare «Nascondi dall'elenco»:



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

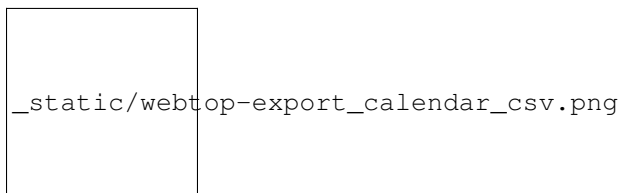


Ad esempio, se si desidera ripristinare la sottoscrizione della «cartella1» appena nascosta, basta selezionarla dall'elenco delle cartelle nascoste e fare clic sull'icona a sinistra:



19.11 Esportazione eventi (CSV)

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



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

19.12 Integrazione con Nextcloud

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

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

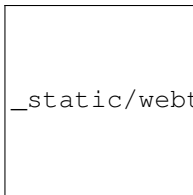
Ad esempio, se si desidera attivare il servizio per tutti gli utenti di WebTop, procedere come segue:

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



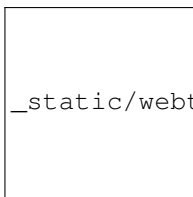
_static/webtop-admin_panel_groups.png

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

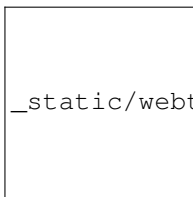


_static/webtop-admin_panel_permission.png

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

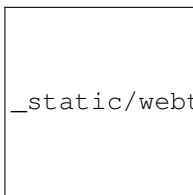


_static/webtop-admin_panel_nextcloud_auth_1.png



_static/webtop-admin_panel_nextcloud_auth_2.png

in modo da ottenere questo:



_static/webtop-admin_panel_nextcloud_auth_3.png

4. salvare e chiudere.

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

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



Si aprirà una procedura guidata precompilata:



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

Procedere con il tasto Next fino a completamento del Wizard.

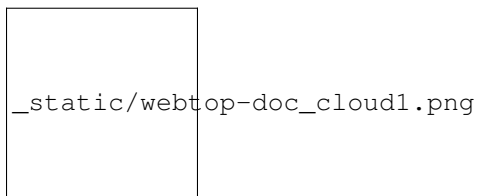
19.13 Usa il Cloud personale per inviare e ricevere documenti

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

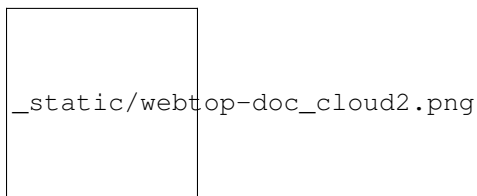
Nota: Il server deve essere raggiungibile sulla porta HTTP 80

19.13.1 Come creare un link per inviare un documento

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



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

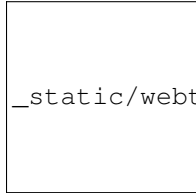


è possibile impostare una *password* per proteggerlo:

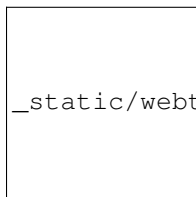


`_static/webtop-doc_cloud3.png`

Il link verrà generato e verrà inserito nella nuova mail:



`_static/webtop-doc_cloud4.png`



`_static/webtop-doc_cloud5.png`

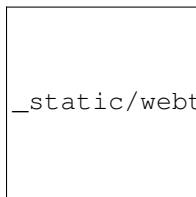
Il download del file genera una notifica al mittente:



`_static/webtop-doc_cloud6.png`

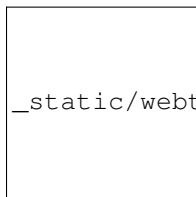
19.13.2 Richiesta di un documento

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



`_static/webtop-doc_cloud7.png`

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



`_static/webtop-doc_cloud8.png`

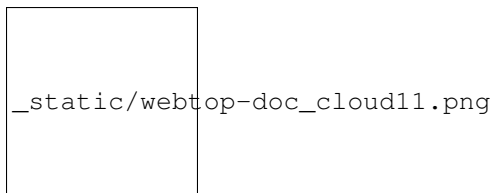
Una mail di richiesta verrà inviata per caricare il documento sul Cloud:



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



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



19.14 Integrazione chat

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

Per abilitare l'integrazione con il server chat:

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

19.15 Chiamate WebRTC audio e video con chat (Beta)

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

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

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

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

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

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

`url` : URL ice server

`username` : nome utente server (opzionale)

`credential` : password server (opzionale)

Ad esempio:

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

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

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

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

19.16 Invio SMS dai contatti

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

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

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

`sms.provider = smshosting o twilio`

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

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

`sms.sender = (default opzionale)`

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

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

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

19.17 Pulsanti di collegamento personalizzati

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



`_static/webtop_launchers.png`

Per ciascun pulsante, inserisci questi tre valori

Nome : testo descrittivo che appare con il mouseover

“ URL link“: URL aperto in un nuovo browser

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

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

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

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

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

19.18 Notifiche del browser

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

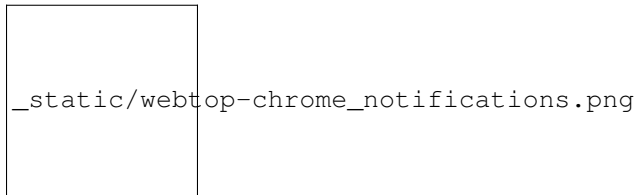
Per attivarla, accedere semplicemente alle impostazioni generali dell'utente:



È possibile abilitare la notifica sul desktop in due modalità:

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

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



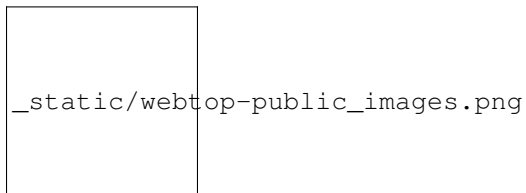
Se è necessario abilitare questo consenso più tardi su un altro browser, basta fare clic sul pulsante appropriato:



19.19 Gestione firme utenti e di dominio

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

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



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

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

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

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

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

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



```
_static/webtop-edit_mailcard.png
```

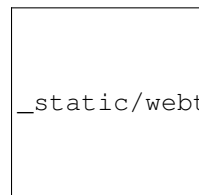
L'immagine pubblica appena caricata sarà possibile richiamarla all'interno dell'editor HTML della firma con questo pulsante:



```
_static/webtop-public_signature.png
```

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

Accedendo le impostazioni dell'utente dalla pagina di amministrazione di WebTop (*Domains* → *NethServer* → *Utenti* → *Click destro sull'utente*) è inoltre possibile impostare una mailcard generale per il dominio che verrà impostata automaticamente per tutti gli utenti che non hanno configurato la propria mailcard personale:



```
_static/webtop-domain_mailcard.png
```

Inoltre, sarà anche possibile modificare le informazioni personali:



```
_static/webtop-personal_information.png
```

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

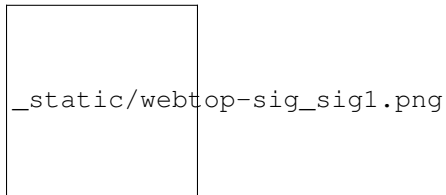


In questo modo è possibile creare un'unica firma che verrà automaticamente personalizzata per ogni utente che non utilizzi la propria firma.

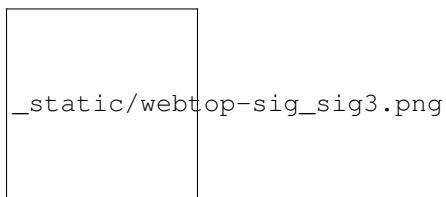
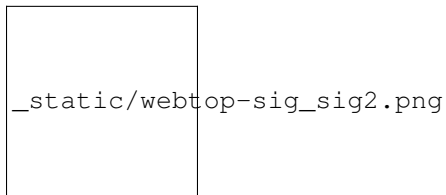
19.20 Configurare più firme per un singolo utente

È possibile configurare più firme HTML per ogni singolo utente.

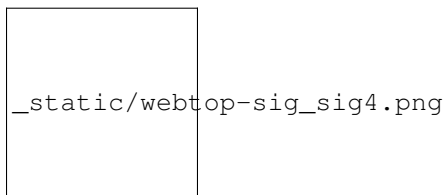
Accedere a *Impostazioni* -> *Posta* -> *Identità* e creare identità multiple:



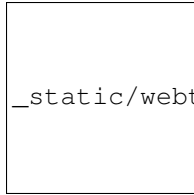
Per modificare ogni singola firma selezionare *Impostazioni* -> *Posta Elettronica* -> *Identità*, quindi selezionare ogni singola firma e cliccare sul pulsante *modifica firma*



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



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



_static/webtop-sig_sig5.png

19.21 Gestisci identità

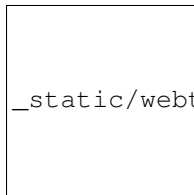
In *Impostazioni* → *Posta Elettronica* → *Identità* cliccare su *Aggiungi* quindi compilare i campi



_static/webtop_manageident1.png

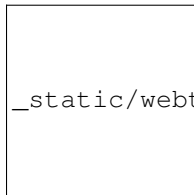
È possibile associare la nuova identità a una cartella del proprio account o di un account condiviso

Account Locale



_static/webtop_manageident2.png

Account condiviso



_static/webtop_manageident3.png

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

19.22 Sottoscrizione di risorse remote

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

19.22.1 Calendari remoti

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

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

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

- 1) Prelevare dal proprio calendario Google il link ICS (formato iCal) di accesso pubblico: *Opzioni del calendario -> Impostazioni e condivisione -> Indirizzo segreto in formato iCal*
- 2) Su WebTop, aggiungere un calendario Internet di tipo Webcal ed incollare l'URL copiato senza inserire le credenziali di autenticazione nel passo 1 del wizard.
- 3) Il wizard effettuerà la connessione al calendario, dando la possibilità di modificarne il nome e il colore, quindi effettuerà la prima sincronizzazione.

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

19.22.2 Rubrica remota

Esempio di rubrica remota CarDAV Google

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

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



_static/webtop-remote_phonebook.png

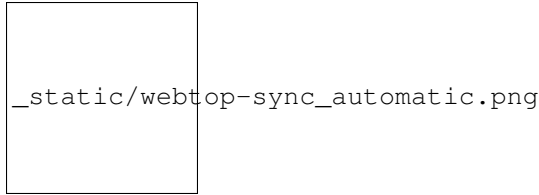
- 3) La procedura guidata nei passaggi seguenti si collegherà alla rubrica, dando la possibilità di cambiare il nome e il colore, quindi eseguirà la prima sincronizzazione.

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

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

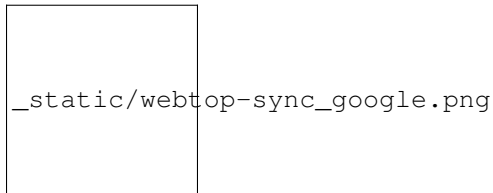
Sincronizzazione automatica

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

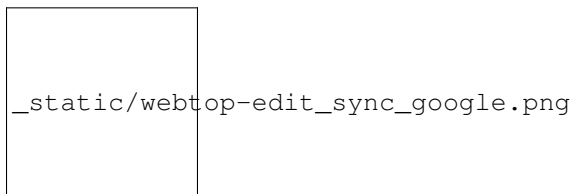


Sincronizzazione manuale

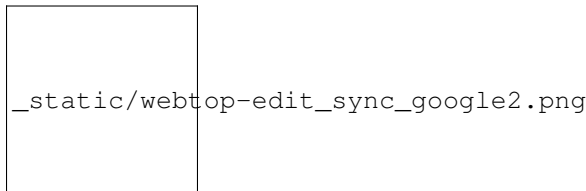
Per aggiornare ad esempio una rubrica remota, fare clic su di essa con il tasto destro del mouse e selezionare la voce «Sincronizza»:



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



Selezionare la modalità desiderata accanto al pulsante di sincronizzazione:



19.23 Gestione impostazioni utente

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

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

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

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

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

19.24 Modifica del logo

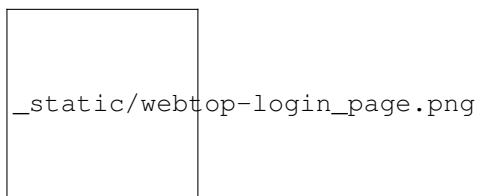
Per modificare e personalizzare il logo iniziale visualizzato nella pagina di accesso di WebTop, è necessario caricare il file immagine personalizzato sulle immagini pubbliche dell'utente amministratore e rinominarlo con «login.png».

Procedere come segue:

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



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



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

19.25 Modifica dell'URL pubblico

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

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

eseguire i seguenti comandi

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

19.26 Modifica il limite predefinito «Dimensione massima del file»

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

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

Per modificare questi valori predefiniti per tutti gli utenti, è possibile aggiungere le seguenti chiavi tramite l'interfaccia di amministrazione: :guilabel: *Proprietà (sistema)* -> *Aggiungi*

Dimensione massima del file per i caricamenti della chat

- Servizio: `com.sonicle.webtop.core`
- Chiave: `im.upload.maxfilesize`

Dimensione massima del file allegato per un singolo messaggio di posta

- Servizio: `com.sonicle.webtop.mail`
- Chiave: `attachment.maxfilesize`

Dimensione massima del file per i caricamenti interni al cloud

- Servizio: `com.sonicle.webtop.vfs`
- Chiave: `upload.private.maxfilesize`

Dimensione massima del file per i caricamenti pubblici su cloud

- Servizio: `com.sonicle.webtop.vfs`
- Chaive: `upload.public.maxfilesize`

Nota: Il valore deve essere espresso in Byte (Esempio 10MB = 10485760)

19.27 Importazione di contatti e calendari

WebTop supporta l'importazione di contatti e calendari da vari formati di file.

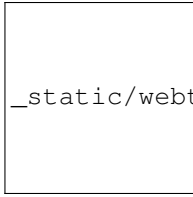
19.27.1 Contatti

Formato dei contatti supportati:

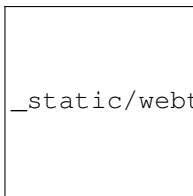
- CSV - Comma Separated values (*.txt, *.csv)
- Excel (*.xls, *.xlsx)
- VCard (*.vcf, *.vcard)
- LDIF (*.ldif)

Per importare i contatti:

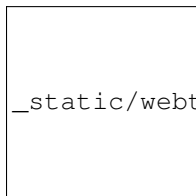
1. Fare clic con il tasto destro sulla rubrica di destinazione, quindi selezionare: *Importa contatti*



2. Selezionare il formato di importazione assicurandosi che i campi del file corrispondano a quelli disponibili su WebTop



Se stai importando una rubrica esportata da Outlook, assicurarsi di impostare: guilabel: *Qualificatore di testo* con questo valore ".

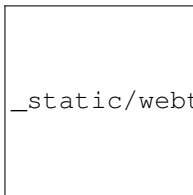


19.27.2 Calendari

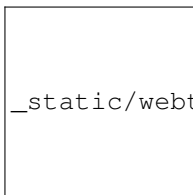
Formato del calendario supportato: iCalendar (*.ics, *.ical, *.icalendar)

Per importare eventi:

1. Fare clic con il tasto destro sul calendario di destinazione, quindi selezionare *Importa eventi*



2. Selezionare il formato di importazione



3. Quindi scegliere se si desidera eliminare tutti gli eventi esistenti e importarne di nuovi o semplicemente aggiungere i dati importati agli eventi del calendario esistenti



19.28 Nascondi il destinatario suggerito automaticamente nelle ricerche

Per disabilitare il suggerimento di indirizzi salvati automaticamente, accedere al pannello di amministrazione ->: guilabel: *Proprietà (sistema)* ->: guilabel: *Aggiungi* -> selezionare: guilabel: *com.sonicle.webtop.core (WebTop)* e inserire i dati nei campi: guilabel: *Chiave* e: guilabel: *Valore* in base alla chiave da configurare:

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

19.29 Modificare l'oggetto di una mail e salvarlo

Per abilitare la modifica dell'oggetto nelle e-mail ricevute e inviate, accedere al pannello di amministrazione ->: guilabel: *Proprietà (sistema)* ->: guilabel: *Aggiungi* -> selezionare: guilabel: *com.sonicle.webtop.mail (Posta Elettronica)* e inserire i dati nei campi: guilabel: *Chiave* e: guilabel: *Valore* in base alla chiave da configurare:

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

19.30 Importazione da PST Outlook

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

Prima di utilizzare lo script, è necessario installare il pacchetto *libpst*:

```
yum install libpst -y
```

Assicurarsi inoltre che la timezone di PHP corrisponda a quella del server:

```
config getprop php DateTimezone
```

La time zone di PHP può essere modificata utilizzando il comando seguente:

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

19.30.1 Mail

Script iniziale per l'importazione dei messaggi mail: `/usr/share/webtop/doc/pst2webtop.sh`

Per iniziare l'importazione, lanciare lo script specificando il file PST e l'utente di sistema:

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

Esempio:

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

Tutti i messaggi mail saranno importati. Contatti e calendari saranno salvati in un file temporaneo e lo script genererà a schermo gli ulteriori comandi da utilizzare per importare contatti e calendari.

Esempio:

```
Events Folder found: Outlook/Calendar/calendar
pst2webtop_cal.php goody '/tmp/tmp.Szorhi5nUJ/Outlook/Calendar/calendar' <foldername>
...
log created: /tmp/pst2webtop14271.log
```

Tutti i comandi saranno riportati anche nel file di log generato dallo script.

19.30.2 Contatti

Script importazione Contatti: `/usr/share/webtop/doc/pst2webtop_card.php`.

Lo script utilizzerà i file generati nella fase di importazione della posta:

```
/usr/share/webtop/doc/pst2webtop_card.php <user> <file_to_import> <phonebook_category>
```

Esempio

Ipotizziamo che lo script `pst2webtop.sh` abbia generato il seguente output a seguito dell'importazione delle mail:

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

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

```
/usr/share/webtop/doc/pst2webtop_card.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/
↪Contacts/contacts' WebTop
```

19.30.3 Calendari

Script importazione Calendari: `/usr/share/webtop/doc/pst2webtop_cal.php`

Lo script utilizzerà i file generati nella fase di importazione della posta:

```
/usr/share/webtop/doc/pst2webtop_cal.php <user> <file_to_import> <foldername>
```

Esempio

Ipotizziamo che lo script `pst2webtop.sh` abbia generato il seguente output a seguito dell'importazione delle mail:

```
Events Folder found: Personal folders/Calendar/calendar
Import to webtop:
./pst2webtop_cal.php foo '/tmp/tmp.0vPbWYf8Uo/Personal folders/Calendar/calendar'
↪<foldername>
```

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

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

Limitazioni note:

- verrà importata solamente la prima occorrenza di eventi ricorrenti
- I promemoria di Outlook verranno ignorati

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

19.31 Troubleshooting

19.31.1 Dopo l'accesso viene visualizzato un «mail account authentication error»

Se un intero account di posta è condiviso tra diversi utenti, è possibile raggiungere un limite di connessione Dovecot. Questo è l'errore visualizzato:



In `/var/log/imap` si rilevano messaggi come i seguenti:

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

Per elencare le connessioni IMAP attive per utente, eseguire:

```
doveadm who
```

Per risolvere il problema, basta aumentare il limite (es. 50 connessioni per ogni utente/IP):

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

Infine, eseguire il logout e di nuovo il login in WebTop.

19.31.2 Pagina vuota dopo il login

È possibile accedere a WebTop utilizzando l'utente amministratore di sistema (NethServer Administrator) utilizzando il nome di accesso completo, ad es. `admin@nethserver.org`.

Se l'accesso fallisce, soprattutto quando si aggiorna da WebTop 4, significa che l'utente admin non ha un indirizzo mail

Per risolvere il problema, eseguire il seguente comando:

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

19.31.3 Gli eventi sincronizzati mostrano una differenza di orario

Può capitare che gli eventi di calendario creati sui device mobili e sincronizzati tramite EAS vengano riportati sull'interfaccia con una differenza di orario di 1 o 2 ore.

Il problema è dovuto al Time Zone di PHP che può risultare disallineato rispetto a quello di sistema.

Con questo comando è possibile vedere l'attuale Time Zone impostato per il PHP:

```
config getprop php DateTimezone
```

Esempio di output:

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

Se il Time Zone non fosse quello desiderato (ad esempio Europe/Rome) è possibile correggere in questo modo:

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

Per mettere in produzione la modifica eseguire:

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

Elenco dei time zone supportati da PHP: <http://php.net/manual/it/timezones.php>

19.31.4 Eliminare gli indirizzi email suggeriti automaticamente

Quando si compila il destinatario di una mail, vengono suggeriti alcuni indirizzi email salvati automaticamente. Se è necessario eliminarne qualcuno perché è sbagliato, spostarsi con i tasti freccia finché non si seleziona quello che si vuole eliminare (senza fare clic su di esso), quindi eliminarlo con *Shift + Canc*

19.32 WebTop vs SOGo

WebTop e SOGo possono essere installati sulla stessa macchina, anche se è sconsigliato mantenere tale configurazione a lungo termine.

ActiveSync è abilitato per impostazione predefinita sia su SOGo che su WebTop, ma se entrambi i pacchetti sono installati, SOGo avrà la precedenza.

Per disabilitare ActiveSync su SOGo:

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

Per disabilitare ActiveSync su WebTop modificare il file di configurazione `/etc/httpd/conf.d/webtop5-zpush.conf`.

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

19.33 Integrazione Google

Gli utenti possono aggiungere i propri account Google Drive all'interno di WebTop. Prima di procedere, l'amministratore deve creare una coppia di credenziali di accesso API.

19.33.1 Google API

- Accedere a <https://console.developers.google.com/project> e creare un nuovo progetto
- Creare una nuova coppia di credenziali di tipo "OAuth 2.0 clientID" avendo cura di compilare la sezione "OAuth consent screen"
- Inserire la coppia di credenziali appena create (Client ID e Client Secret) nella configurazione di WebTop

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

```
googledrive.clientid = (Google API client_ID)
```

```
googledrive.clientsecret = (Google API client_secret)
```

Connettore POP3

Nota: Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *pop3_proxy-section* sono basate sul motore di filtraggio Rspamd. Le precedenti installazioni di NethServer verranno automaticamente aggiornate a Rspamd come descritto nella sezione *Aggiornamento Email a Rspamd*

Il Connettore POP3 fa parte dell'applicazione *Email* nel nuovo Server Manager ed è accessibile dall'elenco delle caselle di posta. La stessa configurazione è accessibile dal vecchio Server Manager, dalla pagina *Connettore POP3*.

Gli account esterni configurati verranno controllati regolarmente e i messaggi scaricati saranno consegnati agli utenti locali.

Non è consigliabile utilizzare il connettore POP3 come metodo principale per la gestione della posta elettronica. Il recapito della posta può essere influenzato dallo spazio su disco e dai problemi di connettività del server del provider. Inoltre, il filtro antispam sarà meno efficace a causa della perdita delle informazioni contenute nell'envelope della mail originale.

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

- l'indirizzo email (come identificativo univoco per l'account)
- il protocollo (IMAP/POP3/IMAP con SSL/POP3 con SSL)
- l'indirizzo del server remoto
- le credenziali dell'account
- l'utente locale a cui consegnare i messaggi
- se un messaggio vada eliminato dal server remoto dopo la consegna
- controlli antispam e antivirus

Nota: È consentito associare più account esterni ad uno locale. L'eliminazione di un account *non* cancellerà i messaggi già consegnati.

Completata la configurazione di un account, questo viene automaticamente controllato per rilevare la presenza di nuovi messaggi di posta.

L'implementazione è basata su *Getmail*¹. Dopo aver scaricato i messaggi dal provider POP3/IMAP remoto, Getmail applica tutti i filtri attivati (spam e virus), quindi consegna il messaggio localmente. I messaggi vengono filtrati in base alle *regole configurate*.

Tutte le operazioni di download sono riportate nel file `/var/log/maillog`.

Avvertimento: Se un account scelto per la consegna venisse successivamente eliminato, la configurazione diventerebbe inconsistente. Se questo dovesse accadere la relativa configurazione esistente nella pagina *Connettore POP3* dovrà essere disabilitata o eliminata.

Riferimenti

¹ Getmail è un programma per il download di email da remoto <http://pyropus.ca/software/getmail/>

Il servizio di chat utilizza il protocollo standard Jabber/XMPP, supporta TLS sulla porte XMPP standard (5222 o 5223).

La principali funzionalità sono:

- messaggi fra gli utenti del sistema
- amministratori chat
- messaggi broadcast
- chat di gruppo
- messaggi offline
- trasferimenti file in LAN
- S2S
- Archiviazione dei messaggi

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

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

21.1 Server to server (S2S)

Il sistema XMPP è federato nativamente. Se S2S è abilitato, gli utenti con account su un server possono comunicare con gli utenti su server remoti. S2S consente ai server di comunicare tra loro, formando una rete IM globale «federata».

A tale scopo, il record DNS SRV deve essere configurato per il proprio dominio (https://wiki.xmpp.org/web/SRV_Records#XMPP_SRV_records) e il server deve disporre di un certificato SSL/TLS valido.

21.2 Client

I client Jabber sono disponibili per tutte le piattaforme desktop e mobile.

Fra i client più diffusi:

- Pidgin disponibile per Windows e Linux
- Adium per Mac OS X
- BeejibellIM per Android e iOS, o Xabber solo Android

Quando si configura il client, assicurarsi che sia abilitato TLS (o SSL). Inserire il nome utente e il dominio della macchina.

Se NethServer è anche il server DNS della rete, i client dovrebbero trovare automaticamente l'indirizzo del server attraverso speciali record DNS preconfigurati. In caso contrario, specificare l'indirizzo del server nelle opzioni avanzate.

Con le funzionalità TLS, server o client rigorosamente configurati potrebbero rifiutare la connessione con il server Ejabberd se nel certificato SSL/TLS non corrispondesse il nome di dominio. Inoltre, il certificato dovrebbe contenere due sottodomini `pubub.*` e `conference.*`. Un certificato con tali caratteristiche può essere generato gratuitamente con Let's Encrypt (vedi `server_certificate-section`).

21.3 Amministratori

Tutti gli utenti all'interno del gruppo `jabberadmins` sono considerati amministratori del server di chat.

Il gruppo `jabberadmins` deve essere creato e configurato dalla pagina *Gruppi*.

Gli amministratori possono:

- inviare messaggi broadcast
- controllare lo stato degli utenti collegati

21.4 Gestione archivio messaggi

Message Archive Management (`mod_mam`) implementa la gestione dell'archivio messaggi come descritto in *XEP-0313* <<http://xmpp.org/extensions/xep-0313.html>> . Se abilitato, tutti i messaggi verranno archiviati all'interno del server e i client XMPP compatibili potranno utilizzarlo per archiviare la propria cronologia chat sul server.

Il database può memorizzare fino a 2 GB di messaggi, i messaggi archiviati possono essere eliminati automaticamente. Per configurare i criteri di conservazione dei messaggi, impostare l'opzione *Elimina messaggi più vecchi di X giorni*.

Nota: Se abilitato, questo modulo memorizzerà ogni messaggio inviato tra gli utenti. Questa funzionalità impatterà sulla privacy degli utenti.

21.5 Altre opzioni

L'amministratore può configurare tutte le opzioni sopra descritte anche tramite il nuovo Server Manager.

Altre opzioni disponibili:

- velocità di trasferimento in upload e download
- abilita/disabilita l'interfaccia di amministrazione via web

Team chat (Mattermost)

Il modulo team chat installa la piattaforma Mattermost Team Edition all'interno di NethServer.

Mattermost è un cloud privato Open Source Slack-alternative. L'eccellente documentazione ufficiale del progetto è disponibile qui: <https://docs.mattermost.com/>.

22.1 Configurazione

L'installazione di Mattermost richiede un virtual host dedicato, un FQDN come `chat.nethserver.org`.

Prima di procedere con la configurazione, assicurarsi di aver creato il record DNS corrispondente. Se NethServer svolge il ruolo di server DNS della LAN, fare riferimento alla sezione *DNS*.

Se il server utilizza il certificato Let's Encrypt come predefinito, assicurarsi anche di avere un record DNS pubblico corrispondente. Vedi `server_certificate-section` per maggiori informazioni.

<p>Avvertimento: Si tenga presente che l'applicazione per smartphone non può connettersi a server che utilizzano certificati auto-firmati!</p>
--

Come configurare:

1. Accedere alla pagina `guiabel:Team chat` del Server Manager
2. Spuntare l'opzione *Abilita Mattermost Team Edition*, quindi inserire un FQDN valido nel campo *Nome virtual host* (ad esempio `chat.nethserver.org`)
3. Accedere al nome DNS indicato attraverso il browser, ad esempio `https://chat.nethserver.org`. Al primo accesso una procedura guidata creerà l'utente amministratore

Le seguenti funzionalità sono abilitate di default:

- notifiche mail
- notifiche push per le app mobile

- redirect da HTTP ad HTTPS

22.2 Autenticazione

L'autenticazione per Mattermost *non* è integrata con alcun Account Provider. L'amministratore di Mattermost dovrà occuparsi della creazione di utenti e team.

Nota: L'amministratore deve sempre utilizzare la procedura guidata di Mattermost per creare l'utente amministratore, quindi inviare il link di invito del team a ciascun utente.

22.2.1 Importazione di utenti

Se l'amministratore di sistema ha ancora bisogno della creazione di massa degli utenti, può usare il comando `mattermost-bulk-user-create`.

Il comando provvederà a:

- creare il team di default utilizzando il nome dell'azienda definito nella sezione `organization_contacts-section`
- leggere tutti gli utenti dall'Account Provider locale o remoto e ri-crearli all'interno di Mattermost

Si noti che:

- gli utenti disabilitati nel Server Manager o già esistenti in Mattermost saranno omessi
- per ogni utente verrà generata una password casuale
- il primo utente importato verrà impostato come amministratore se nessun amministratore è già stato creato

Esempio di Invocazione:

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

Nota: Gli utenti non vengono automaticamente sincronizzati all'interno di Mattermost. Ogni volta che un utente viene creato o rimosso, è necessario ricordarsi di eseguire il comando `mattermost-bulk-user-create` o di creare manualmente l'utente usando l'interfaccia web di amministrazione di Mattermost.

22.2.2 Forzare una password predefinita comune

È possibile impostare una password predefinita per ogni nuovo utente Mattermost, basta aggiungere la password predefinita in fase di esecuzione del comando.

Esempio:


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


NethServer supporta la gestione di UPS (Uninterruptible Power Supply) collegati al sistema.

Il server può essere configurato in due modalità:

- *master*: l'UPS è direttamente collegato al server, il server accetta connessioni dagli slave
- *slave*: l'UPS è collegato ad un altro server raggiungibile via rete

Nota: Si consiglia di consultare la lista dei modelli supportati prima dell'acquisto. Installare il pacchetto UPS da *Amministrazione > Software center*. In *Configurazione* appare la nuova voce di menù *UPS* dove si può trovare il dispositivo supportato inserendo il modello all'interno del campo di ricerca *Cerca driver per modello*.

Nella modalità master, l'UPS può essere collegato al server:

- su una porta seriale
- su una porta USB
- con un adattatore da USB a seriale

Nella modalità slave sarà necessario fornire l'indirizzo IP del server master.

La configurazione di default prevede uno spegnimento controllato in caso di assenza di alimentazione.

23.1 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
```

23.2 Statistiche UPS

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

Nota: La pagina di configurazione di questo modulo è disponibile solo nel nuovo Server Manager.

Questo modulo gestisce la configurazione di [Dante](#).

Dante raccoglie dati da registri, database e servizi, li aggrega e li visualizza in un report strutturato come una dashboard personalizzabile. Il report può essere inviato via e-mail, con pianificazione e destinatari configurabili.

24.1 Dashboard

La pagina *Dashboard* è composta da una serie di widget, ognuno dei quali mostra un'informazione sul sistema. L'utente può personalizzare il layout della dashboard aggiungendo, rimuovendo, ridimensionando e trascinando i widget.

I tipi di widget attualmente supportati sono:

- **Grafico:** grafici a torta, a barre, a linee o ad area
- **Contatore:** una card che mostra un valore numerico aggregato e una tendenza in un intervallo di tempo
- **Tabella:** una tabella con intestazioni di riga e colonna opzionali
- **Rancking:** un elenco dei primi N elementi, ordinati in base al loro valore
- **Etichetta:** un testo che mostra un'informazione
- **Titolo:** un semplice testo digitato dall'utente per organizzare il layout della dashboard

24.2 Impostazioni

La pagina *Impostazioni* gestisce la configurazione del modulo.

24.2.1 Configurazione host

- **Host pubblico:** questo è il nome dell'host che ospita il report. Deve essere un nome che può essere risolto da Internet
- **URL finale:** questo campo visualizza l'URL pubblico in cui è ospitato il report

24.2.2 Configurazione report

- **Tema:** i temi disponibili per la dashboard sono *chiaro* e *scuro*
- **Tavolozza:** ci sono 9 tavolozze di colori tra cui scegliere
- **Intervallo:** intervallo di tempo su cui vengono aggregati i dati. Può essere *Settimana*, *Mese* o *Sei mesi*
- **Lingua:** lingua utilizzata per visualizzare il report
- **Anonimizzazione:** opzione che controlla l'anonimizzazione dei dati sensibili nel report
- **Numero massimo di voci:** numero massimo di elementi da visualizzare nei widget di tipo ranking
- **Indirizzi:** configurazione dei destinatari e-mail e programmazione della spedizione via e-mail del report

24.2.3 Test mail

- **Indirizzo:** e-mail del destinatario dell'e-mail di prova contenente il report
- **Includi indirizzi configurati:** opzione per controllare se l'e-mail di prova deve essere inviata anche agli altri indirizzi configurati in *Configurazione rapporto* oltre che all'*Indirizzo* specificato

Nota: La pagina di configurazione di questo modulo è disponibile solo nel vecchio Server Manager e non verrà portata nel nuovo.

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

25.1 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.

25.2 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

25.2.1 Autenticazione

Il sistema supporta due metodi di autenticazione per l’invio di fax:

- Host Based: utilizza l’indirizzo IP del computer che invia la richiesta
- PAM: utilizza nome utente e password, gli utenti devono appartenere al gruppo *faxmaster*. Il gruppo *faxmaster* deve essere creato espressamente.

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

25.3 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 requisiti:

- Deve contenere esattamente la stringa “Numero Fax: ”, contenente il numero fax, per esempio:

`Numero Fax: 12345678`

- La stringa può essere presente in qualsiasi posizione del documento, ma su una riga singola.
- La stringa deve essere scritta con carattere non bitmap (ad esempio Truetype)

I fax spediti avranno come mittente l’id dell’utente specificato. Questa informazione sarà ben visibile nella coda dei fax.

25.4 Mail2Fax

Avvertimento: Per abilitare questa funzione, assicurarsi che sia installato il modulo “Email”.

Tutte le email inviate da rete locale all'indirizzo `sendfax@<nomedominio>` saranno trasformate in fax ed inviate al destinatario.

Il `<nomedominio>` deve corrispondere ad un dominio di posta configurato per la consegna locale.

Le mail devono rispettare questo formato:

- Il numero del destinatario deve essere specificato nel campo oggetto (o subject)
- L'email deve essere in formato solo testo
- Può contenere allegati di tipo PDF o PS che saranno convertiti e inviati insieme al fax

Nota: Questo servizio è abilitato solo per i client che inviano mail dalla rete green.

25.5 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

Firewall e gateway

Nota: È disponibile il nuovo server manager basato su Cockpit. Vedi [Firewall](#).

NethServer è in grado di svolgere il ruolo di firewall e gateway all'interno della rete in cui viene installato. Tutto il traffico fra i computer della rete locale e Internet passa attraverso il server che decide come instradare i pacchetti di rete (routing) e quali regole applicare.

Funzioni principali:

- Configurazione di rete avanzata (bridge, bond, alias, ecc...)
- Supporto WAN multiple (fino a 15)
- Gestione regole firewall
- Gestione banda (QoS)
- Port forwarding
- Regole per routing traffico su una specifica WAN
- Intrusion Prevention System (IPS)
- Deep packet inspection (DPI)

La modalità firewall e gateway viene attivata solo se:

- il pacchetto *nethserver-firewall-base* è installato
- è configurata almeno una scheda di rete con ruolo red

26.1 Policy

Ogni interfaccia di rete è identificata da un colore che ne indica il ruolo all'interno del sistema. Vedi [network-section](#).

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*.

26.2 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 cinque parti principali:

- *Azione*: azione da intraprendere quando si applica la regola
- *Origine traffico*: indirizzo di origine del traffico, può essere una zona, una rete o un singolo host
- *Destinazione traffico*: indirizzo di destinazione del traffico, può essere una zona, una rete o un singolo host
- *Servizio*: porta e protocollo che individua un determinato tipo di traffico
- *Condizione temporale*: la regola si applica solo nell'intervallo temporale specificato

Le azioni disponibili sono:

- *ACCEPT*: accetta il traffico
- *REJECT*: blocca il traffico ed informa il mittente che la richiesta effettuata non è permessa
- *DROP*: blocca il traffico, i pacchetti vengono scartati e il mittente non viene notificato
- *ROUTE*: instrada il traffico al provider WAN specificato. Vedi anche *Multi WAN*.
- *Priority*: marca il traffico come alta/bassa priorità. Vedi *Gestione banda*.

Nota: Se non ci sono interfacce red configurate, il firewall non genera regole per le zone blue e orange.

26.2.1 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.

26.2.2 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`.

26.2.3 Deep Packet Inspection (DPI)

La Deep Packet Inspection (DPI)¹ è una tecnica avanzata di filtraggio dei pacchetti di rete.

Attivando il modulo DPI, vengono rese disponibili delle voci aggiuntive per il campo *Servizi* disponibile nelle schermate di creazione/modifica delle regole firewall. Queste voci sono etichettate come *protocollo DPI* tra le usuali voci *servizio* e *servizio di rete*.

Il modulo DPI utilizza la libreria *nDPI* <<https://www.ntop.org/products/deep-packet-inspection/ndpi/>> _ in grado di identificare oltre 250 tipi di traffico di rete suddiviso in protocolli di rete (ad esempio OpenVPN, DNS) e applicazioni Web (ad esempio, Netflix, Spotify).

Le regole del firewall che utilizzano i servizi DPI vengono generate all'interno della tabella *mangle*, per questo motivo tali regole hanno alcune limitazioni:

- L'azione *reject* non è supportata, va utilizzata l'azione *drop* per bloccare il traffico
- non è possibile utilizzare gli oggetti *tutti (any)* e *firewall* come sorgente o destinazione
- l'azione *devia su X* non è supportata: l'identificazione del protocollo inizia spesso dopo che la connessione è già stata stabilita, quindi la policy di routing non può essere modificata

Anche se DPI può identificare il traffico da/per specifici siti web come Facebook, è più adatto per bloccare o prioritizzare protocolli come VPN, FTP, ecc. L'accesso ai siti Web deve essere disciplinato utilizzando il *Proxy web*.

E' opportuno sottolineare che alcuni protocolli DPI (come Amazon) possono corrispondere a grandi *CDN*, quindi è opportuno non bloccare tali protocolli usando le regole DPI a meno che non si desideri impedire l'accesso a migliaia di siti.

La marcatura DPI viene applicata automaticamente anche al traffico proveniente dal firewall stesso, come il traffico HTTP dal proxy web

L'elenco completo dei protocolli DPI, insieme ai contatori per il traffico corrispondente, è disponibile nella pagina *DPI* sotto la categoria *Stato* del menu di sinistra.

26.2.4 Regole sulle connessioni esistenti

Per default, quando una nuova regola viene creata, si applica solo alle nuove connessioni. Ma in alcuni scenari, l'amministratore può aver la necessità di applicare la regola anche sulle connessioni esistenti.

Se l'opzione *Applica alle connessioni esistenti* è abilitata, la regola sarà applicata a tutte le connessioni incluse quelle già stabilite.

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

Nota: Questa opzione è disponibile solo all'interno del nuovo Server Manager. Vedi [Firewall](#).

26.2.5 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: -

26.3 Multi WAN

Con il termine *WAN* (Wide Area Network) si indica una rete pubblica esterna al server, solitamente collegata a Internet. I fornitori di collegamenti WAN sono detti *provider*.

Il sistema supporta fino ad un massimo di 15 connessioni WAN. Se sul server sono configurate due o più schede red, è obbligatorio procedere alla configurazione dei campi *Peso link*, *Banda entrante* e *Banda uscente* della pagina *Rete*.

Ogni provider configurato rappresenta una connessione WAN ed è associato ad una scheda di rete. Ciascun provider definisce un *peso*: maggiore è il peso maggiore è la priorità della scheda di rete associata al provider stesso.

Il sistema può utilizzare le connessioni WAN in due modalità (pulsante *Configura* nella pagina *Multi WAN*):

- *Balance*: tutti i provider sono utilizzati contemporaneamente in base al loro peso
- *Active backup*: i provider sono utilizzati uno alla volta 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](#).

26.3.1 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.

26.4 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

26.4.1 Esempio

Dato il seguente scenario:

- Server interno con IP 192.168.1.10, detto Server1
- Server web in ascolto sulla porta 80 su Server1
- Server SSH in ascolto sulla porta 22 su Server1
- Altri servizi nell'intervallo di porte tra 5000 e 6000 sul Server1

In caso si voglia rendere accessibile dall'esterno il server web direttamente sulla porta 80, si dovrà creare un port forward fatto così:

- porta origine: 80
- porta destinazione: 80
- indirizzo host: 192.168.1.10

Tutto il traffico che arriva sulle reti red del firewall sulla porta 80, verrà redirezionato alla porta 80 di Server1.

In caso si voglia rendere accessibile dall'esterno il server SSH sulla porta 2222, si dovrà creare un port forward fatto così:

- porta origine: 2222
- porta destinazione: 22
- indirizzo host: 192.168.1.10

Tutto il traffico che arriva sulle reti red del firewall sulla porta 2222, verrà redirezionato alla porta 22 di Server1.

Nel caso in cui si desideri rendere il server accessibile dall'esterno usare un intervallo di porte tra 5000 e 6000, sarà necessario creare un port forward come questo:

- porta origine: 5000:6000
- porta destinazione:
- indirizzo host: 192.168.1.10

Tutto il traffico che arriva sulle reti red del firewall per l'intervallo di porte compreso tra 5000 e 6000 verrà redirezionato alle stesse porte sul Server1.

26.4.2 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 o 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

26.5 sNAT 1:1

Il NAT uno-a-uno consiste nell'associare un indirizzo IP privato ad un indirizzo IP pubblico per configurare, ad esempio, sistemi che si trovano dietro ad un firewall.

Se si hanno a disposizione diversi IP pubblici e si vuole associare uno di questi ad un determinato host della rete, è possibile farlo, appunto, mediante il NAT 1:1.

Questa funzionalità si applica solo per il traffico generato verso internet dall'host di rete specifico oggetto della regola.

La regola non interessa in alcun modo il traffico genareato da internet verso l'Alias IP, se dovesse essere necessario instradare traffico specifico verso l'host interno andranno definite delle normali regole di port forward.

Se dovesse essere necessario instradare tutto il traffico verso l'host interno (configurazione non raccomandata) andrà definita una regola di port forward per i protocolli TCP & UDP che abbia come porte sorgenti il range 1:65535.

26.5.1 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.

26.6 Gestione banda

La gestione banda (traffic shaping) permette di applicare regole di priorità sul traffico che attraversa il firewall. In tal modo è possibile ottimizzare la trasmissione, controllare la latenza e sfruttare al meglio la banda disponibile.

Per abilitare il traffic shaping è necessario conoscere l'esatta quantità di banda disponibile in download e upload. Accedi alla pagina guilabel *Network* e imposta attentamente i valori di larghezza di banda.

Se la larghezza di banda di download e upload non è impostata per un'interfaccia red, le regole di shaping non saranno abilitate per quell'interfaccia.

Nota: Assicurati di specificare una stima accurata della larghezza di banda sulle interfacce di rete. Per scegliere un'impostazione appropriata, si prega di non fidarsi del valore nominale, ma utilizzare strumenti online per verificare la reale velocità del provider.

In caso di congestione da parte del provider, non c'è nulla da fare per migliorare le prestazioni.

La configurazione del traffic shaping è composta da 2 passaggi:

- Creazione di classi per gestione della banda
- assegnazione del traffico di rete a una classe specifica

26.6.1 Classi

Il traffic shaping viene ottenuto controllando il modo in cui la larghezza di banda viene allocata alle classi.

Ogni classe può avere una percentuale riservata. Una percentuale riservata è la larghezza di banda che una classe avrà a disposizione in caso di necessità. La larghezza di banda disponibile è data dalla somma della larghezza di banda non impegnata e della larghezza di banda impegnata di una classe, ma non attualmente utilizzata dalla classe stessa.

Ogni classe può avere anche una banda massima. Se impostato, la classe può superare la banda stabilita, fino alla banda massima. Una classe supererà la sua banda riservata solo se è disponibile abbastanza banda.

Le classi di traffic shaping possono essere definite nella pagina *Traffic shaping*. Quando crei una nuova classe, compila i seguenti campi:

- *Class name*: un nome rappresentativo
- *Min download (%)*: Download minimo consentito, se vuoto non verrà creato alcun limite
- *Max download (%)*: Download massimo consentito, se vuoto non verrà creato alcun limite
- *Min upload (%)*: Upload minimo consentito, se vuoto non verrà creato alcun limite
- *Max upload (%)*: Upload massimo consentito, se vuoto non verrà creato alcun limite
- *:* guilabel:*Description*: descrizione facoltativa per la classe

Il sistema fornisce due classi preconfigurate:

- *high*: traffico ad alta priorità generico, può essere assegnato tipo ad SSH

- *low*: traffico a bassa priorità, può essere assegnato a un servizio come scambio di file peer to peer

Il sistema cerca sempre di prevenire la saturazione della banda quando ci sta un carico di rete elevato.

Le classi ricevono la banda non allocata in proporzione alla loro banda minima . Per esempio, se una la classe A ha 1Mbit di banda minima e la classe B ha 2Mbit, allora la classe B riceverà il doppio della banda non allocata rispetto alla classe A. In ogni caso, tutta la banda non allocata verrà utilizzata dalle classi.

Per più info,vedere² .

26.7 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: `web_server`, `goofy_pc`
- **Gruppi di host**: rappresentano gruppi omogenei di computer. Gli host all'interno di un gruppo devono essere raggiungibili attraverso la stessa interfaccia. Esempio: `servers`, "router"
- **Range IP**: una lista di indirizzi IP espressa come un intervallo. Esempio: `myrange`, composto da IP dal `192.168.1.100` al `192.168.1.120`
- **Reti CIDR**: utilizzare una rete CIDR per semplificare e rendere più leggibili le regole.

Esempio 1: gli ultimi 14 indirizzi IP della rete sono assegnati 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.

- **Condizione temporali**: possono essere associati alle regole del firewall per limitarne l'effetto ad un determinato periodo di tempo.

Nota: Le regole che hanno condizioni temporali sono applicate solo per le nuove connessioni. Esempio: se si stanno bloccando le connessioni HTTP dalle 09:00 alle 18:00, tutte le connessioni stabilite prima delle ore 09:00 saranno permesse fino a quando non termineranno. Qualsiasi nuova connessione effettuata dopo le 09:00 sarà bloccata.

- **Servizi**: rappresentano un servizio in ascolto su un host. Esempio: `ssh`, `https`
- **MAC address**: un host identificato da un indirizzo MAC. Il MAC address deve essere collegato ad una zona inesistente.

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.

² FireQOS tutorial: <https://github.com/firehol/firehol/wiki/FireQOS-Tutorial>

26.8 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.

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

27.1 Modalità autenticata

Prima di abilitare il proxy web in modalità autenticata, assicurarsi di aver configurato un account provider locale o remoto.

Quando viene installato Samba Active Directory o il server è attestato ad un dominio remoto Active Directory, le postazioni Windows possono utilizzare l'autenticazione integrata Kerberos. Su tutti i client Windows è **necessario** configurare il proxy utilizzando l'FQDN del server.

Tutti gli altri client possono utilizzare il meccanismo di basic authentication.

Nota: L'autenticazione NTLM è deprecata e non è più supportata.

27.2 Configurazione client

Il proxy è sempre in ascolto sulla porta **3128**. Quando si utilizzano le modalità Manuale o Autenticato, tutti i client devono essere esplicitamente configurati per utilizzare il proxy. La configurazione è accessibile dal pannello impostazioni del browser. La maggior parte dei client verranno comunque configurati automaticamente attraverso il protocollo WPAD. In questo caso è utile attivare l'opzione *Blocca porta HTTP e HTTPS* per evitare il bypass del proxy.

Se il proxy è installato in modalità trasparente, tutto il traffico web proveniente dai client viene intercettato dal firewall e indirizzato attraverso il proxy. Nessuna configurazione è necessaria sui singoli client.

Nota: Per rendere accessibile il file WPAD dalla rete ospiti, aggiungere l'indirizzo della rete blue nel campo *Consenti host* per il servizio httpd nella pagina *Servizi di rete*.

27.3 Proxy SSL

In modalità trasparente SSL, il proxy implementa la cosiddetta tecnica «peek and splice»: stabilisce la connessione SSL con i siti remoti e verifica la validità dei certificati senza decifrare il traffico. Quindi il server può filtrare gli URL richiesti utilizzando il filtro web e ritornare la risposta al client.

Nota: Non è necessario installare alcun certificato sui client, è sufficiente abilitare il proxy SSL.

27.4 Bypass

In alcuni casi può essere necessario fare in modo che il traffico originato da specifici ip della rete o verso alcune destinazioni non passi per il proxy HTTP/HTTPS, ma sia instradato direttamente; il traffico in questione non sarà più sottoposto a proxy.

Il proxy consente di creare:

- bypass per domini
- bypass per sorgente
- bypass per destinazione

27.4.1 Bypass per domini

I bypass per i domini possono essere configurati dalla sezione *Domini senza proxy*. Tutti i domini elencati all'interno di questa pagina possono essere acceduti direttamente dai client LAN. Nessun filtro antivirus o dei contenuti viene applicato a questi domini.

Ogni dominio elencato sarà espanso anche per i relativi sotto-domini. Ad esempio, aggiungendo *nethserver.org* verranno bypassati anche *www.nethserver.org*, *mirror.nethserver.org*, e così via.

Nota: Tutti i client della LAN **devono** utilizzare il server stesso come DNS, direttamente o come *forwarder*.

27.4.2 Bypass per origine e destinazione

Un bypass per origine consente l'accesso diretto a tutti i siti HTTP/HTTPS da host selezionati, gruppi host, intervalli IP e CIDR di rete. I bypass per origine sono configurabili dalla sezione *Host senza proxy*.

Un bypass per destinazione consente l'accesso diretto da qualsiasi client della LAN a siti HTTP/HTTPS ospitati su host specifici, gruppi host o CIDR di rete. I bypass per destinazione sono configurabili dalla sezione *Siti senza proxy*.

Queste regole di bypass vengono configurate anche all'interno del file WPAD.

27.5 Regole di priorità e di instradamento

Le regole del firewall per il routing del traffico su un provider specifico o per la modifica della priorità del traffico vengono applicate solo al traffico di rete che attraversa il gateway. Queste regole non si applicano se il traffico passa attraverso il proxy perché il traffico viene generato dal gateway stesso.

In uno scenario in cui il proxy web è abilitato in modalità trasparente e il firewall contiene una regola per abbassare la priorità di un host specifico, la regola si applica solo ai servizi non HTTP, come SSH.

La scheda *Regole* consente la creazione di regole di priorità e di instradamento anche per il traffico intercettato dal proxy.

L'interfaccia web consente di creare regole per il traffico HTTP/S per:

- aumentare la priorità di un host o una rete
- abbassare la priorità di un host o di una rete
- Instradare la sorgente su un provider specifico con failover automatico se il provider dovesse andare fuori servizio
- forzare la sorgente su uno specifico provider senza failover automatico

27.6 Report

Installando il modulo `nethserver-lightsquid` il sistema genererà automaticamente i report di navigazione web.

LightSquid è un analizzatore di log per Squid leggero e veloce che ogni giorno genera un nuovo report HTML, riassumendo le abitudini di navigazione degli utenti del proxy. L'interfaccia di Lightsquid è accessibile dal tab *Applicazioni* della *Dashboard*.

27.7 Cache

Nel pannello *Cache* è presente un form per configurare i parametri di cache:

- La cache può essere abilitata o disabilitata (*disabilitata* di default)
- **Dimensione cache disco:** valore massimo della cache di squid sul disco (in MB)
- **Dimensione minima oggetto:** può essere lasciato a 0 per mettere in cache tutto, ma può essere alzato se gli oggetti piccoli non sono desiderati in cache (in kB)
- **Dimensione massima oggetto:** gli oggetti più grandi di questa dimensione non vengono salvati in cache. Se si preferisce la velocità al salvataggio della banda, può essere impostato ad un valore basso (in kB)

Il pulsante *Svuota cache* funziona anche se il proxy è disabilitato, potrebbe essere utile per liberare spazio su disco.

27.7.1 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
```

27.8 Porte sicure

Le porte sicure sono una lista di porte accessibili attraverso il proxy. Se una porta non è all'interno della lista delle porte sicure, il proxy si rifiuterà di collegarsi al server. Per esempio, dato un servizio HTTP che gira sulla porta 1234, tale servizio non sarebbe accessibile usando il proxy.

L'opzione `SafePorts` è una lista di porte separata da virgole. Le porte elencate saranno aggiunte alla lista preconfigurata di porte sicure.

Per esempio, per aprire l'accesso alle porte 446 e 1234:

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

27.9 Log

I log di Squid vengono conservati in formato compresso per 5 settimane, per gestire l'utilizzo dello spazio su disco. I log del proxy Web sono molto dettagliati e sono una insostituibile risorsa per approfondire gli eventuali problemi. Le attività di navigazione Web sono registrate in formato aggregato e leggibile attraverso Lightsquid.

Negli ambienti in cui sia necessario conservare i log per più di 5 settimane, è possibile modificare manualmente la configurazione di `logrotate /etc/logrotate.d/squid`. E' inoltre necessario rammentare di aggiungere `/etc/logrotate.d/squid` al backup della configurazione usando l'inclusione personalizzata.

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

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.

Il filtro dei contenuti Web è incluso nell'applicazione «Proxy Web e filtro» del nuovo Server Manager.

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.

28.1 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*.

28.1.1 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`.

28.2 Antivirus

È possibile verificare la presenza di contenuti dannosi durante la navigazione Web, ma solo per il protocollo in chiaro HTTP. Se il proxy è configurato in modalità trasparente SSL (*Proxy SSL*), il contenuto scaricato tramite HTTPS **non verrà** scansionato. Vedi *Antivirus* per maggiori informazioni.

28.3 Risoluzione problemi

Nel caso una pagina indesiderata non venga bloccata, verificare che:

- il client stia navigando attraverso il proxy
- il client non abbia un bypass configurato nella sezione *Host senza proxy*
- il sito visitato non abbia un bypass configurato nella sezione *Siti senza proxy*
- il client sia associato ad un profilo in cui la pagina non è permessa
- il client non stia navigando in un periodo di tempo in cui il filtro ha una configurazione permissiva

IPS (Suricata)

Suricata è un *IPS* (Intrusion Prevention System), un sistema per la prevenzione delle intrusioni in rete. Il software analizza tutto il traffico che attraversa il firewall alla ricerca di attacchi noti e anomalie.

Quando un attacco o un'anomalia sono stati rilevati, il sistema può decidere se bloccare il traffico o limitarsi a salvare l'evento sul log (`/var/log/suricata/fast.log`).

Suricata può essere configurato utilizzando set di regole organizzati per categorie specifiche. Ogni categoria può essere configurata come:

- Abilitata: il traffico che intercetta le regole della categoria verrà segnalato
- Bloccata: il traffico che intercetta le regole della categoria verrà rifiutato
- Disabilitata: le regole della categoria verranno ignorate

Nota: L'utilizzo di un IPS impatta su tutto il traffico che attraversa il firewall. Assicurarsi di aver compreso a fondo tutte le possibili implicazioni prima di attivare la funzionalità. In particolare, prestare attenzione alle regole di blocco che potrebbero interferire con gli aggiornamenti del sistema stesso.

29.1 Categorie regole

Suricata utilizza regole free scaricate da <https://rules.emergingthreats.net/>.¹

Le regole sono divise nelle categorie elencate di seguito.

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

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

¹ Documentazione sulle categorie: [proofpoint - ETPro Category Descriptions](#)

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

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

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

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

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

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

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

Deleted Rules removed from the rule set.

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

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

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

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

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

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

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

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

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

Info General rules to track suspicious host network traffic.

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

Malware Malware and Spyware related, no clear criminal intent. The threshold for inclusion in this set is typically some form of tracking that stops short of obvious criminal activity. This set was originally intended to be just spyware. That's enough to several rule categories really. The line between spyware and outright malicious bad

stuff has blurred to much since we originally started this set. There is more than just spyware in here, but rest assured nothing in here is something you want running on your net or PC. There are URL hooks for known update schemed, User-Agent strings of known malware, and a load of others.

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

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

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

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

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

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

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

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

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

SMTP-events Rules that will log SMTP operations.

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

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

Stream-events Rules for matching TCP stream engine events.

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

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

TLS-Events Regole per individuare eventi e anomalie TLS

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

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

User Agents User agent identification and detection.

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

Web Client Web client side attacks and vulnerabilities.

Web Server Rules for attacks and vulnerabilities against web servers.

Web Specific Apps Rules for very specific web applications.

WORM Traffic indicative of network based worm activity.

29.2 Bypass

Il bypass disabilita la protezione IPS per gli host selezionati: il traffico dal/al host selezionato non sarà analizzato.

Per creare un bypass accedere al nuovo Server Manager e aprire l'applicazione *IPS*. quindi accedere alla pagina *Bypass* e fare click sul pulsante *Aggiungi bypass*

Compilare il campo *Bypass* quindi fare click sul pulsante *Salva*. Il campo *Bypass* supporta:

- oggetti host
- oggetti gruppi di host
- Oggetti IP range
- indirizzo IP

29.3 EveBox

EveBox è uno strumento web per la gestione di allarmi ed eventi generati da Suricata.

Il modulo è accessibile dal Server Manager, attraverso il link nella pagina *Applicazioni*

Nota: La configurazione del reverse proxy è parte dell'applicazione *Server Web* all'interno del nuovo Server Manager.

La funzionalità reverse proxy è utile quando si desidera accedere a siti interni dalla rete esterna.

30.1 Regole di virtual host e path

Una richiesta di un client Web può essere inoltrata a un altro server Web in modo trasparente, in base a due tipi di regole di corrispondenza:

- Richieste che corrispondono a un percorso URL, come «`http://mydomain.com/mysite`»
- Richieste che corrispondono a un nome virtual host, come `http://my.secondary-domain.com`

Lo scenario tipico per una **URL path rule** è la seguente:

- NethServer è il firewall della LAN
- Si possiede il dominio `http://mydomain.com`
- Si desidera che `http://mydomain.com/mysite` inoltri le richieste al server interno (IP privato: 192.168.2.100)

In questo scenario creare un nuovo record nella pagina *Reverse proxy*. Impostare il *Name* dell'elemento a `mysite` e *Target URL* a `http://192.168.2.100`.

Se sono consentite solo connessioni cifrate, abilitare l'opzione *Richiedi connessione SSL cifrata*.

Si può restringere l'accesso solo ai client appartenenti ad alcune reti, specificando un elenco separato da virgola di reti in notazione CIDR nel campo *Accedi da reti CIDR*.

Una **virtual host name rule** può inoltrare richieste HTTP a un altro server Web ed è definita nella pagina *Reverse proxy > Virtual hosts*. Per esempio:

- NethServer è il firewall della LAN
- Hai un dominio `http://my.secondary-domain.com`

- Si desidera che `http://my.secondary-domain.com` inoltri le richieste al server web interno `192.168.2.101`, porta `9000`.

In questo scenario creare un nuovo record nella pagina *Reverse proxy*. Impostare il *Name* dell'elemento a `my.secondary-domain.com` e *Target URL* a `http://192.168.2.101:9000`.

Fare riferimento anche a *the UI description of Reverse Proxy* per ulteriori informazioni sulle funzionalità avanzate, come *Forward HTTP «Host» header to target* e `:guilabel'Accept invalid SSL certificate from target'`.

30.2 Configurazione manuale

Se la pagina *Reverse proxy* non è abbastanza, è sempre possibile configurare Apache manualmente, creando un nuovo file nella directory `/etc/httpd/conf.d/`.

Esempio

Creare il file `/etc/httpd/conf.d/myproxypass.conf` con il seguente contenuto:

```
<VirtualHost *:443>
    SSLEngine On
    SSLProxyEngine On
    ProxyPass /owa https://myserver.exchange.org/
    ProxyPassReverse /owa https://myserver.exchange.org/
</VirtualHost>

<VirtualHost *:80>
    ServerName www.mydomain.org
    ProxyPreserveHost On
    ProxyPass / http://10.10.1.10/
    ProxyPassReverse / http://10.10.1.10/
</VirtualHost>
```

Per ulteriori informazioni, consultare la documentazione ufficiale di Apache: https://httpd.apache.org/docs/2.4/mod/mod_proxy.html

Nota: La configurazione dei virtual host è parte dell'applicazione *Server Web* all'interno del nuovo Server Manager.

Il virtual hosting consente di ospitare nomi di dominio multipli su un singolo server. Su NethServer, dalla pagina *Virtual hosts*, è possibile configurare i siti web come virtual host Apache.

31.1 Nomi dei virtual host (FQDN)

È la lista dei nomi di dominio FQDN che sono associati al virtual host. I valori devono essere separati con «,» (virgola). Per raggiungere il virtual host sarà anche necessario un record DNS. Se abilitata l'opzione nella sezione «Azioni aggiuntive», un alias per ogni FQDN verrà automaticamente creato su «DNS > Alias Server», ma è utile solo per i client che usano il server come DNS.

31.2 Configurare un'applicazione web

Quando si crea un virtual host, viene creata automaticamente una cartella `/var/lib/nethserver/vhost/NOME`. Se è stato abilitato l'accesso FTP, sarà possibile caricare file sul virtual host usando un client FTP e il nome del virtual host come username.

<p>Avvertimento: L'FTP è disabilitato di default, bisogna anche abilitarlo dalla pagina di configurazione FTP</p>
--

La password di autenticazione HTTP dovrebbe essere diversa da quella dell'FTP, in quanto l'FTP è usato per caricare contenuti, la password HTTP per limitare l'accesso alla lettura dei contenuti.

31.3 Permessi Apache

I file caricati via FTP sono di proprietà del gruppo «apache». Se è necessario consentire il permesso di scrittura o esecuzione ad apache, è possibile cambiare i permessi del gruppo usando il client FTP.

<p>Avvertimento: Se un virtual host contiene del codice eseguibile, come script PHP, i permessi utente e le implicazioni di sicurezza vanno valutati attentamente</p>
--

Cartelle condivise

Una *cartella condivisa* è un posto dove i file sono accessibili da un gruppo di persone tramite Samba (SMB/CIFS).

Le cartelle condivise fanno parte dell'applicazione File server nel nuovo Server Manager. La dashboard dell'applicazione integra il modulo Samba status che visualizza lo stato delle cartelle condivise in tempo reale.

Per creare, modificare e rimuovere una cartella condivisa andare alla pagina *Cartelle condivise*.

32.1 Requisiti

Le cartelle condivise utilizzano ACL (Access Control List) per fornire permessi flessibili su file e directory.

Per abilitare le ACL, il filesystem deve essere montato con l'opzione `acl`. L'opzione `acl` è già abilitata su XFS, il filesystem CentOS predefinito, e di solito anche su filesystem `Ext3` e `Ext4`.

32.1.1 Abilitazione ACL

Sui filesystem `Ext2/3/4`, è possibile usare il comando `tune2fs` per verificare se l'opzione `acl` è già abilitata:

```
tune2fs -l /dev/sdXY | grep "Default mount options:"
```

In cui `sdXY` è il nome della partizione, l'output dovrebbe essere simile a questo:

```
Default mount options:   user_xattr acl
```

Se l'opzione `acl` non è abilitata, aggiungere l'opzione all'interno di `/etc/fstab`:

```
/dev/mapper/VolGroup-lv_root /                               ext4          defaults,acl   0
```

Oppure utilizzare `tune2fs` per abilitare la feature come opzione di mount predefinita:

```
tune2fs -o acl /dev/sdXY
```

32.2 Permessi di accesso

Se si è selezionato **Active Directory** come account provider, una cartella condivisa appartiene a un gruppo di utenti (*Owning group*). Ogni membro del gruppo è autorizzato a leggere il contenuto della cartella. Facoltativamente, il gruppo può avere il diritto di modificare il contenuto della cartella e l'autorizzazione di lettura può essere estesa a chiunque acceda al sistema. Questo semplice modello di autorizzazione si basa sulle tradizionali autorizzazioni del file system UNIX.

I permessi di accesso possono essere ulteriormente raffinati utilizzando le *ACL*, consentendo a singoli utenti o ad altri gruppi i permessi di lettura o scrittura.

Le *ACL* possono anche essere impostate su singoli file e directory da un client Windows, se l'utente dispone delle sufficienti autorizzazioni – fare riferimento alla sezione *Modifica autorizzazioni delle risorse dai client Windows* per i dettagli.

Avvertimento: Alcune impostazioni *ACL* supportate dai client Windows non possono essere convertite in *ACL* *POSIX* supportate da NethServer, quindi andranno perse in fase di propagazione

In qualsiasi momento, il pulsante *Reimposta permessi* propaga le autorizzazioni UNIX e le *ACL* *POSIX* alla cartella condivisa ai suoi contenuti.

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

Se non è stato scelto alcun account provider o si è scelto *LDAP*, qualsiasi accesso alle cartelle condivise viene considerato come *Accesso ospite* in modo che a tutti sia consentito leggerne e scriverne il contenuto.

32.3 Accesso alla rete

SMB/CIFS è un protocollo molto diffuso che consente di condividere file in una rete di computer. Il nome della cartella condivisa diventa il nome della condivisione *SMB*.

Per esempio, l'indirizzo di rete *SMB* per la condivisione `docs` potrebbe essere

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

Avvertimento: L'accesso autenticato alle cartelle condivise è disponibile con un account provider *Active Directory*. Il provider *LDAP* consente solo l'accesso come *guest*.

Quando si accede ad una condivisione *SMB*, alcune interfacce utente forniscono un unico campo per indicare lo username. In questi casi fornire lo **user short name** anteposto dal **nome di dominio NetBIOS**. Ad esempio, se il nome di dominio NetBIOS fosse «DOMAIN» ed il nome utente fosse «john.smith», la stringa da utilizzare per accedere alla condivisione *SMB* sarebbe:

```
DOMAIN\john.smith
```

Al contrario, altre applicazioni mostrano dei campi di input separati per il nome di dominio NetBIOS e per il nome utente; in tal caso riempire i campi separatamente.

32.4 Cestino di rete

Se l'opzione *Cestino di rete* è abilitata, i file rimossi da una cartella condivisa vengono in realtà spostati in una directory «cestino» speciale. L'opzione *Mantieni più copie dei file con lo stesso nome* assicura che i file nel cestino abbiano sempre nomi distinti, impedendone la sovrascrittura.

32.5 Nascondere una cartella condivisa

Se è attiva l'opzione *Visibile*, la cartella condivisa sarà elencata fra le cartelle disponibili. Questa opzione non influisce sui permessi di accesso della cartella.

32.6 Share home

Ciascun utente di NethServer ha una condivisione personale mappata sulla sua home directory Unix. Il nome SMB della share corrisponde allo **user short name**. Ad esempio:

- user short name `john.smith`
- nome server `MYSERVER`
- indirizzo server `192.168.1.2`

L'indirizzo di rete SMB è:

```
\\MYSERVER\john.smith
\\192.168.1.2\john.smith
```

Fornire le credenziali dell'utente John come spiegato nella sezione *Accesso alla rete*.

Suggerimento: La directory home Unix viene creata al primo accesso dell'utente tramite SMB o via SFTP/SSH.

32.7 Modifica autorizzazioni delle risorse dai client Windows

Quando un utente si connette a una cartella condivisa con un client Windows, può modificare le autorizzazioni su singoli file e directory. Le autorizzazioni sono espresse dagli elenchi di controllo di accesso (ACL).

Avvertimento: Alcune impostazioni ACL supportate dai client Windows non possono essere convertite in ACL POSIX implementate da NethServer, quindi andranno perse in fase di propagazione

Solo il proprietario di una risorsa (che sia file o directory) ha il pieno controllo su di essa (lettura, scrittura, modifica delle autorizzazioni). L'autorizzazione per eliminare una risorsa è concessa agli utenti con permessi di scrittura sulla directory principale. L'unica eccezione a questa regola è descritta nella sezione *Accesso amministrativo*.

Quando viene creata una nuova risorsa, il proprietario può essere definito da una delle seguenti regole:

- il proprietario è l'utente che crea la risorsa
- il proprietario viene ereditato dalla directory padre

Per applicare una di queste regole, spostarsi nel menu *Windows file server* e selezionare l'opzione corrispondente nella sezione *Quando viene creato un nuovo file o directory in una cartella condivisa*.

Avvertimento: L'impostazione *Owning group* di una cartella condivisa non influisce sul proprietario di una risorsa. Vedi anche la sezione *Permessi di accesso* qui sopra

32.8 Accesso amministrativo

La pagina *Windows file server* consente di concedere privilegi speciali ai membri del gruppo `Domain Admins`:

- estendere l'autorizzazione del proprietario abilitando il *Assegna il controllo completo sulle cartelle condivise al gruppo Domain Admins*
- accedere alle home directory degli altri utenti abilitando *Concedi il pieno controllo sulle home directory al gruppo Domain Admins (home \$ share)*. Per accedere alle home directory, è sufficiente connettersi alla condivisione nascosta `home $`. Ad esempio, l'indirizzo di rete SMB è:

```
\\MYSERVER\home$  
\\192.168.1.2\home$
```

32.9 Auditing

Nota: Il modulo di audit è stato integrato all'interno dell'applicazione File server nel nuovo Server Manager.

Samba audit è un modulo che consente di tenere traccia di tutte le attività effettuate dagli utenti sulle cartelle condivise. Il controllo è disabilitato per impostazione predefinita e deve essere abilitato esplicitamente per ogni cartella.

Le azioni vengono registrate su un file durante il giorno e vengono spostate durante la notte in un database consultabile.

L'interfaccia web del report è disponibile nel vecchio Server Manager dalla pagina *Applicazioni*, mentre il nuovo Server Manager (Cockpit) integra una nuova interfaccia all'interno dell'applicazione *File server*.

Il modulo **Monitor di Banda** consente di analizzare il traffico di rete in tempo reale utilizzando il motore di [ntopng](#). **ntopng** è un potente strumento che valuta la larghezza di banda utilizzata dai singoli host e identifica i protocolli di rete più comunemente utilizzati.

33.1 Dashboard

La *Dashboard* fornisce una panoramica sull'uso della rete e mostra le informazioni sul traffico attraverso alcuni widget grafici.

33.1.1 Stato

La sezione *Status* indica lo stato di attivazione del monitor di banda e mostra il pulsante *Apri app monitor di banda* che consente accedere agevolmente all'interfaccia web **ntopng**.

33.1.2 Top host locali

Questa tabella mostra in tempo reale l'elenco di host appartenenti alle reti locali che stanno generando maggior traffico, sia in download che in upload. Questo widget può aiutare a identificare gli host che utilizzano molta di banda.

33.1.3 Top host remoti

Questa tabella mostra in tempo reale l'elenco degli host remoti che stanno generando maggior traffico, sia in download che in upload.

33.1.4 Traffico per interfaccia

Questo grafico traccia il throughput generato negli ultimi 5 minuti dalle interfacce monitorate.

33.1.5 Traffico per protocollo

Questo grafico traccia il traffico degli ultimi 5 minuti diviso per protocollo. **ntopng** tenta di riconoscere vari protocolli di livello 7 come HTTP, TLS, DNS, SIP, Facebook, Spotify, Zoom, ecc.

33.2 Impostazioni

Nella pagina *Impostazioni* è possibile gestire la configurazione del ****monitor di banda**** attraverso i seguenti controlli:

- *Abilita monitoraggio di banda*: se abilitato, verrà analizzato tutto il traffico che passa attraverso le interfacce di rete selezionate. A seconda delle capacità del server, potrebbe causare un rallentamento della rete e un aumento del carico del sistema.
- *Interfacce*: le interfacce di rete sulle quali **ntopng** resterà in ascolto.
- *Porta dell'interfaccia Web*: la porta TCP su cui sarà disponibile l'interfaccia web **ntopng**. Per impostazione predefinita, la porta TCP è la **3000** ed è possibile accedervi dalla zona green.
- *Abilita autenticazione*: se abilitato, l'interfaccia web di **ntopng** richiederà le credenziali di accesso. Il nome utente è `admin` e la password predefinita è `admin`.

Quando il **Monitor di banda** è abilitato**, l'interfaccia web di ****ntopng** è disponibile all'url: `http://<SERVER_NAME>:<WEB_INTERFACE_PORT>`. Un link diretto all'interfaccia web di **ntopng** è presente nella *Dashboard* e nella pagina *Impostazioni*.

33.3 Log

Nella pagina *Log* è possibile esaminare il log di **ntopng**.

Statistiche (collectd)

Collectd è un software che raccoglie periodicamente statistiche sulle performance del sistema e le salva in speciali file RRD. Le statistiche sono quindi consultabili attraverso un'interfaccia web.

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

L'interfaccia web è accessibile dalla pagina *Grafici*.

Al termine dell'installazione, il sistema collezionerà le seguenti informazioni:

- utilizzo CPU
- carico di sistema
- numero di processi
- utilizzo memoria RAM
- utilizzo memoria virtuale (swap)
- tempo di accensione
- utilizzo spazio su disco
- operazioni di lettura e scrittura su disco
- interfacce di rete
- latenza di rete

Per ciascun controllo, l'interfaccia mostra un grafico che contiene sia l'ultimo valore raccolto, sia i valori minimi, massimi e medi.

34.1 Latenza di rete

Il plugin ping misura la latenza di rete. Ad intervalli regolari, collectd invia un ping al DNS configurato. Se la multi WAN è attiva, anche tutti i provider abilitati verranno controllati.

Host aggiuntivi possono essere monitorati (es. server web) usando una lista separata da virgole all'interno della proprietà `PingHosts`.

Esempio:

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

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

OpenVPN Roadwarrior, tunnel IPsec e tunnel OpenVPN ora fanno parte dell'applicazione VPN nel nuovo Server Manager.

35.1 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

35.1.1 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
- System user name, password and certificate

- System user name, One Time Password (OTP) and certificate

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.

On the other hand, it's mandatory to choose a system account if you want to use authentication with user name and password or with one time password (2FA).

2. Scaricare il file contiene la configurazione e i certificati. In alternativa, il file può essere inviato all'utente via mail (disponibile solo nel nuovo Server Manager).
3. Importare il file all'interno del client ed avviare la VPN.

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

Accounting

Ogni volta che un client si connette al server OpenVPN, l'accesso viene registrato in un database di accounting. Le statistiche di accesso sono disponibili nel nuovo Server Manager. Per ogni utente, le statistiche includono:

- nome client
- indirizzo IP virtuale
- indirizzo IP reale
- orario della connessione
- orario della disconnessione
- byte trasmessi

35.1.2 Tunnel (net2net)

Quando si crea una connessione OpenVPN net2net, un server ricopre il ruolo di master. Tutti gli altri server sono considerati slave (client).

Un client può essere collegato ad un altro NethServer od ad un qualsiasi altro firewall che utilizzi OpenVPN.

Tutti i tunnel utilizzano OpenVPN in modalità routed, ma esistono due tipi di topologie: *subnet* e *p2p* (Point to Point)

Topologia: subnet

Questa è la topologia consigliata. Nella topologia subnet, il server accetterà le connessioni e agirà come server DHCP per ogni client connesso.

In questo scenario

- il server gestisce l'autenticazione dei client utilizzando certificati TLS
- il server può eseguire il push delle rotte locali verso i client remoti
- il client si possono autenticare con certificati TLS o tramite nome utente e password

Topologia: P2P

Nella topologia p2p, l'amministratore deve configurare un server per ciascun client.

In questo scenario:

- l'unico metodo di autenticazione supportato è la PSK (Pre-Shared Key). Si consiglia di utilizzare un canale sicuro (come SSH o HTTPS) per scambiare la PSK
- l'amministratore deve selezionare un IP per entrambi gli end point
- le rotte per le reti remote devono essere configurate su ogni end point

Per configurare un tunnel procedere come segue:

1. Accedere al server del tunnel e aprire la pagina *OpenVPN tunnels*, spostarsi nella scheda *Tunnel servers* e cliccare sul bottone *Create new*
2. Valorizzare i campi richiesti ponendo attenzione al fatto che:
 - *guiabel:Public IPs and/or public FQDN* è una lista di IP pubblici o di nomi host che verranno usati dai client per collegarsi al server attraverso Internet
 - *Local networks* è una lista di reti locali che saranno accessibili dai server remoti. Se la topologia è di tipo p2p, la stessa lista sarà utilizzata per valorizzare il campo *Remote networks* del client
 - *Remote networks* è una lista di reti remote che si trovano dietro al server remoto e che saranno accessibili dagli host della rete locale
3. Dopo aver salvato la configurazione, cliccare sull'azione *Download* e selezionare *Configurazione client*
4. Accedere al client del tunnel, aprire la pagina *OpenVPN tunnels*, spostarsi sulla scheda *Tunnel clients* e cliccare sul bottone *Upload*

Funzionalità avanzate

L'interfaccia web consente di configurare funzionalità avanzate quali:

- lato client, nel campo *Remote hosts* possono essere specificati indirizzi multipli per ridondanza; il client OpenVPN tenterà di connettersi a ciascun host rispettando l'ordine di inserimento
- WAN priority: se il client ha più WAN (interfacce red), l'opzione consente di selezionare l'ordine in cui le WAN saranno utilizzate per connettersi al server remoto.
- Protocollo: è importante rammentare che OpenVPN è progettata per funzionare in modo ottimale in UDP, ma è possibile utilizzare TCP nelle situazioni in cui non è possibile fare ricorso ad UDP
- cifratura: l'algoritmo crittografico utilizzato per crittografare tutto il traffico. Se non viene selezionato in modo esplicito, il server e il client cercheranno di negoziare la migliore cifratura disponibile su entrambi i lati
- compressione LZO: abilitata di default, può essere disabilitata quando si utilizzano server or client legacy

Modalità legacy

I tunnel possono ancora essere creati utilizzando gli account roadwarrior.

I passi da eseguire sul server master sono:

- Abilitare il server roadwarrior
- Creare un account solo VPN per ciascun slave che dovrà collegarsi
- Durante la creazione dell'account ricordarsi di specificare la rete remota configurata dietro allo slave

I passi da eseguire sullo slave sono:

- Creare un client dalla pagina *Client* specificando i dati di collegamento al server master
- Copiare e incollare il contenuto dei certificati scaricati dalla pagina di configurazione del master

35.2 IPsec

Il protocollo IPsec (IP Security) è lo standard “de facto” nei tunnel VPN, viene utilizzato tipicamente per creare tunnel di tipo net to net ed è supportato da tutti i produttori. È possibile utilizzare questo protocollo per creare tunnel VPN tra un NethServer ed un dispositivo di un altro produttore nonché tunnel VPN tra 2 NethServer.

Nota: IPsec non è progettato per collegare singoli host ma per la configurazione net2net, questo implica due gateway su entrambe le estremità (almeno un’interfaccia RED e una GREEN).

35.2.1 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.

Nextcloud è una soluzione flessibile per la sincronizzazione dei file e la loro condivisione. È possibile avere i propri file sempre a portata di mano su ogni dispositivo, utilizzando un dispositivo mobile, un personal computer, una workstation o un accesso web. La condivisione viene realizzata in maniera semplice, sicura e privata che significa avere il pieno controllo dei propri dati.

Funzionalità:

- configurazione di Nextcloud con database MariaDB e delle credenziali d'accesso di default
- integrazione automatica con gli utenti e gruppi di sistema di NethServer
- backup dei dati automatico tramite nethserver-backup-data
- personalizzazione dell'URL di accesso HTTPS (virtual host personalizzato)

36.1 Installazione

È possibile installare NethServer tramite l'interfaccia web di NethServer. Dopo l'installazione:

- collegarsi all'URL https://your_nethserver_ip/nextcloud
- usare le credenziali di default **admin/Nethesis,1234**
- cambiare la password di default

Ciascun utente presente nel sistema può accedere automaticamente a Nextcloud tramite le sue credenziali, indipendentemente dall'account provider utilizzato (vedi *Utenti e gruppi*). Dopo l'installazione sarà presente anche un nuovo widget per l'applicazione nella dashboard di NethServer.

Nota: La procedura di aggiornamento/cambio di versione di Nextcloud disabilita le app per evitare problemi di compatibilità. I registri del server tengono traccia di quali app sono state disabilite. Dopo una corretta procedura di aggiornamento / cambio di versione è possibile utilizzare la pagina Applicazioni per aggiornare e riattivare le app.

36.1.1 Lista utenti

Tutti gli utenti vengono elencati nel pannello dell'amministratore di Nextcloud utilizzando un identificativo alfanumerico univoco. In questo modo il sistema garantisce l'assenza di duplicati nei nomi utente interni, come spiegato nella sezione *Internal Username* della [Documentazione ufficiale di NextCloud](#).

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

36.2 Configurazione

Dopo l'installazione, l'applicazione può essere configurata dal nuovo Server Manager.

36.2.1 Host virtuale personalizzato

In alcuni casi è opportuno riservare un virtual host completo per accedere a Nextcloud come `nextcloud.nethserver.org`.

È opportuno sottolineare che, dopo la configurazione di un virtual host personalizzato, Nextcloud non sarà più accessibile dall'URL predefinito `https://ip_del_nethserver/nextcloud`.

Se la macchina utilizza Let's Encrypt, è necessario ricordarsi di aggiungere il nome di dominio del virtual host dedicato all'elenco dei domini validi nel certificato.

36.2.2 Trusted domains

I Trusted domains sono una lista di domini su cui l'utente può effettuare il login. Quelli presenti di default sono:

- nome dominio
- indirizzo IP

L'elenco dei domini fidati può essere personalizzato usando il campo *Domini fidati*: aggiungere un dominio per riga.

36.2.3 CalDAV e CardDAV

Alcuni client CalDAV e CardDAV possono avere delle difficoltà nel trovare l'URL di sincronizzazione appropriato e richiedono il rilevamento automatico dei servizi. Il servizio di discovery viene abilitato di default se si utilizza un virtual host personalizzato per Nextcloud.

Per abilitare il servizio di discovery anche se Nextcloud è in esecuzione sull'URL predefinito, selezionare il campo *Abilita rilevamento automatico CalDAV e CardDAV*.

Nota: Quando si abilita l'auto-discovery DAV, assicurarsi che WebTop o SOGo *non* siano già installati.

36.2.4 Collabora Online

Fare riferimento a *Collabora Online module da NethForge*.

36.2.5 ONLYOFFICE

Dalla versione 18 di Nextcloud, ONLYOFFICE Community Document Server può essere installato direttamente sul sistema senza ulteriori configurazioni. Per abilitare l'integrazione con ONLYOFFICE, accedere a Nextcloud con l'utente `admin`, quindi:

- Accedere alla pagina *Apps* e spostarsi nella sezione *Office & text*
- Scaricare e abilitare l'applicazione ONLYOFFICE
- Scaricare e abilitare l'applicazione *Community Document Server*. Sarà necessario pazientare, il download e l'installazione richiederà del tempo.
- Accedere alla pagina *Settings* e spostarsi nella pagina dell'applicazione ONLYOFFICE nella sezione *Administration*
- Verificare che il campo *Document Editing Service address* contenga già l'indirizzo pubblico del server Nextcloud

Nota: L'installazione del server ONLYOFFICE completo non è supportata su NethServer.

Nota: Il server FTP è parte dell'applicazione *Server Web* all'interno del nuovo Server Manager.

Avvertimento: 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.

37.1 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
```

Phone Home

Il phone home viene utilizzato per tenere traccia di tutte le installazioni di NethServer nel mondo. Ogni volta che un nuovo `product!` viene installato, questo strumento invia alcuni dettagli sull'installazione a un server centrale. Le informazioni sono conservate in un database e vengono utilizzate per mostrare il numero totale di installazioni raggruppato per paese e versione: <https://www.nethserver.org/phone-home/index.html>

Il phone home è abilitato di default ed invia le seguenti informazioni:

- **UUID:** salvato in `/var/lib/yum/uuid`
- **RELEASE:** ottenuto da `/sbin/e-smith/config getprop sysconfig Version`
- **TYPE:** tipo di installazione (`subscription`, `enterprise` o `community`)

38.1 Disabilitazione

Il phone home può essere disabilitato da linea di comando. Eseguire questi comandi in una shell di root:

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

Nota: La pagina di configurazione di questo modulo è disponibile solo nel vecchio Server Manager e non verrà riportata in quello nuovo.

Il protocollo SNMP (Simple Network Management Protocol) consente la gestione e il monitoraggio di apparati collegati in rete. Il server **SNMP** è in grado di rispondere a richieste specifiche riportando lo stato attuale del sistema.

Il server è disabilitato di default.

Per abilitarlo è necessario configurare tre parametri principali:

- il nome della comunità SNMP
- il nome del luogo in cui risiede il server
- il nome e l'indirizzo mail dell'amministratore di sistema

L'implementazione si basa sul progetto Net-SNMP. Per ulteriori informazioni, consultare la pagina ufficiale del progetto: <http://www.net-snmp.org/>

Hotspot (Dedalo)

L'obiettivo principale di un hotspot è fornire connettività internet via wi-fi agli utenti occasionali. Gli utenti vengono inviati a un captive portal attraverso il quale possono accedere alla rete autenticandosi tramite social, sms o email. Il servizio di hotspot consente la regolamentazione, la responsabilità e il prezzo dell'accesso a internet in luoghi pubblici, come punti internet, hotel e fiere.

Funzioni principali:

- Separazione rete aziendale e rete ospiti
- gli ospiti possono autenticarsi utilizzando l'accesso social (Facebook, Instagram, LinkedIn) così come gli sms od una e-mail
- servizio a pagamento basato su voucher
- hotspot manager con livelli di accesso diversi (amministratore, cliente, desk)
- limitazione di banda per ciascun utente
- Esportazione elenco account e report delle connessioni (non ancora implementato)

40.1 Come funziona?

L'implementazione è basata su 2 componenti:

- un hotspot manager remoto con una Web GUI in esecuzione su un server cloud che consente di:
 - creare un'istanza hotspot: in genere ogni istanza viene indirizzata a una posizione specifica (ad esempio Art Cafè, Ritz Hotel e così via)
 - modificare la pagina del captive portal
 - scegliere il tipo di login da utilizzare
 - vedere le sessioni e gli utenti collegati
- una parte client (dedalo) installata su un NethServer fisicamente connesso alla rete di access point: consente di assegnare gli indirizzi IP ai client della rete Wi-Fi e li reindirizza al captive portal per l'autenticazione.

Per informazioni più dettagliate, consultare <https://nethesis.github.io/icaro/docs/components/>.

40.2 Installazione

- installare il componente server: <https://nethesis.github.io/icaro/docs/provisioning/> Questa procedura utilizza Vagrant per fornire un droplet Digital Ocean (DO). Se si preferisse utilizzare un altro provider cloud, il file Vagrant andrà modificato di conseguenza.
- configurare il server in modo da rendere possibile l'accesso: <https://nethesis.github.io/icaro/docs/configuration/>
- installare il componente client nel proprio NethServer: https://nethesis.github.io/icaro/docs/client_installation/
- è importante ricordare che per l'installazione sono necessarie almeno 3 interfacce Ethernet:
 - 1 per i client LAN, contrassegnata con il ruolo green (necessaria anche se non utilizzata, può essere una VLAN)
 - 1 (o più) per la connessione Internet, contrassegnato con il ruolo red
 - 1 per Dedalo, con il ruolo hotspot

40.3 Configurazione

40.3.1 Interfaccia hotspot manager

- accedere all'hotspot manager
- spostarsi nella sezione *Manager* e creare un nuovo *Manager* di tipo *Rivenditore* o *Cliente*. Maggiori informazioni su possibili *Ruoli* sono disponibili qui: <https://nethesis.github.io/icaro/docs/manager/>.
- eseguire il logout e accedere con il nuovo manager appena creato
- spostarsi nella sezione *Hotspot* e creare una nuova istanza hotspot
- fare clic sul nome dell'hotspot e configurare il captive portal

40.3.2 Unità Hotspot su NethServer

- spostarsi nella sezione *Unità Hotspot* su NethServer
- modificare i parametri nella pagina *Registrazione unità hotspot*:
 - Nome host: nome pubblico dell'Hotspot Manager
 - Nome utente: account utente funzionante (rivenditore o cliente)
 - Password: password

Successivamente, scegliere l'interfaccia ethernet su cui l'hotspot sarà attivato.

Se il proxy web è attivo, un flag specifico nella pagina dell'unità hotspot consentirà di inoltrare tutto il traffico hotspot (protocolli http e https) al proxy web per scopi di registrazione (attenzione alle implicazioni sulla privacy!).

- connettere un AP all'interfaccia hotspot.

40.3.3 Configurazione Access Point

L'Access Point (AP) deve svolgere la sola funzione di abilitare la connessione con il firewall, dove comportarsi come un normale switch di rete. È necessario ricordare di:

- configurare l'access point senza autenticazione e senza DHCP
- disabilitare qualsiasi servizio (servizi di sicurezza, ecc.) per evitare interferenze con il comportamento dell'hotspot
- se si usano più AP configurali con SSID diversi (es: 1-SCUOLA / SCUOLA-2 / ...) per identificare facilmente eventuali AP malfunzionanti
- configurare l'AP con un indirizzo IP statico su un segmento di rete (rfc-1918) diverso da quello utilizzato dall'hotspot
- se possibile, abilitare la «client isolation», per evitare il traffico tra i client connessi all'access point
- configurare l'AP per lavorare su diversi canali per ridurre al minimo le interferenze, un buon AP consente di gestire i canali automaticamente o di selezionarli manualmente
- non utilizzare prodotti troppo scadenti, AP di bassa qualità possono provocare frequenti disconnessioni che poi impattano sulla qualità del servizio generale, la raccomandazione è ancora più importante nel caso si utilizzino dei repeater

A scopo di test, è possibile collegare un laptop o un PC tramite cavo ethernet all'interfaccia hotspot invece di una rete Wi-Fi. Questo può essere molto utile se si verificano problemi e si desidera verificare se siano causati dal servizio hotspot o dalla rete AP.

40.3.4 Modalità Free e Modalità Voucher

La modalità Free (predefinita) consente di effettuare il login in autonomia senza la necessità di alcun codice, cliccando sul social desiderato (o tramite sms od e-mail).

La modalità Voucher obbliga a creare un voucher (in pratica «un codice») che andrà utilizzato da tutti gli utenti, solo gli utenti con il voucher potranno effettuare il login.

Nota: La pagina di configurazione di questo modulo è disponibile solo nel vecchio Server Manager.

FreePBX è una applicazione web open source che controlla e gestisce Asterisk (PBX), un software di comunicazione open source (<https://www.freepbx.org/>).

41.1 Installazione

E' possibile installare FreePBX dal gestore pacchetti di NethServer, il modulo si chiama «FreePBX».

Tutte le configurazioni e i dati di FreePBX sono salvati nei backup configurazione e dati.

41.2 Accesso Web

Dopo l'installazione, FreePBX è accessibile all'indirizzo https://ip_address/freepbx dalle interfacce green. E' anche possibile configurare l'accesso da interfaccia red della pagina «Accesso PBX» nel Server Manager di NethServer.

41.3 FwConsole

La fwconsole è uno strumento che consente all'utente di compiere alcune azioni amministrative su FreePBX (vedi il wiki di FreePBX <<https://wiki.freepbx.org/pages/viewpage.action?pageId=37912685>>'). Per poterla usare con NethServer è necessario utilizzare scl:

```
/usr/bin/scl enable rh-php56 "/usr/sbin/fwconsole"
```

41.4 Documentazione avanzata

Per ulteriori informazioni è possibile consultare la documentazione di FreePBX all'indirizzo: <https://wiki.freepbx.org>

Macchine virtuali

NethServer è in grado di eseguire macchine virtuali attraverso un modulo basato su KVM e libvirt, ma non una interfaccia web per la loro gestione.

Il software per la virtualizzazione può essere installato e avviato utilizzando la linea di comando, eseguendo:

```
yum install --setopt=base.enablegroups=1 @virtualization-hypervisor @virtualization-  
->tools @virtualization-platform  
systemctl enable libvirtd  
systemctl start libvirtd
```

Se NethServer svolge il ruolo di server DHCP, l'istanza di Dnsmasq avviata da libvirtd provocherà un conflitto con principale. Per evitare il problema è necessario rimuovere la rete NAT default di libvirt:

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

Successivamente il sistema sarà pronto per essere gestito attraverso [Virtual Machine Manager \(virt-manager\)](#), un'interfaccia utente per desktop Linux per la gestione di macchine virtuali tramite libvirt.

Lanciato virt.-manager sul proprio desktop Linux, sarà sufficiente creare una nuova connessione verso NethServer utilizzando il protocollo SSH.

42.1 Risorse esterne

Per maggiori informazioni fare riferimento a:

- [Sito ufficiale Virtual Machine Manager](#)
- [Virtual Machine Manager on RHEL](#)
- [Introduction to virtualization](#)

- [FAQ KVM/Libvirt](#)

Fail2ban esegue la scansione dei file di log (ad esempio `/var/log/apache/error_log`) e blocca gli IP che manifestano comportamenti potenzialmente dannosi: troppi errori di password, ricerca di exploit, ecc. In generale Fail2Ban viene quindi utilizzato per aggiornare le regole del firewall per rifiutare le richieste da questi indirizzi IP per un determinato periodo di tempo, sebbene sia possibile configurare qualsiasi altra azione arbitraria (ad esempio l'invio di un'e-mail). Fail2Ban viene fornito con a bordo una serie di filtri per vari servizi (Apache, Dovecot, Ssh, Postfix, ecc.).

Fail2Ban è in grado di ridurre il numero di tentativi di autenticazione errati, tuttavia non può eliminare il rischio che presenta un'autenticazione debole. Per migliorare la sicurezza, aprire l'accesso ai servizi alle sole reti conosciute e protette utilizzando il firewall.

43.1 Installazione

Installare il modulo dal Software Center o usando la riga di comando:

```
yum install nethserver-fail2ban
```

43.2 Impostazioni

Fail2ban è configurabile tramite una apposita voce presente nella categoria sicurezza del server-manager. La maggior parte delle impostazioni possono essere modificate nella scheda *Configurazione*, solo le impostazioni più avanzate devono essere configurate dal terminale.

43.2.1 Jail

Le jail vengono abilitate e iniziano a proteggere i vari servizi non appena si installa un nuovo modulo, la jail relativa ad un servizio (se esistente) viene automaticamente attivata dopo l'installazione del pacchetto.

Ogni jail può essere individualmente disabilitata dalle impostazioni Jail

Numero di tentativi Numero di corrispondenze (vale a dire il valore del contatore) che attiva l'azione di divieto sull'IP.

Arco di tempo Il contatore viene impostato a zero se non viene trovata nei log alcuna corrispondenza entro i secondi di «ricerca» configurati.

Tempo di ban Periodo di permanenza in ban di un IP.

Ban recidivo Estende il blocco degli attaccanti recidivi. Il ban recidivo può avere 2 comportamenti diversi:

- ****Tempo di ban statico:** blocca gli host recidivi per 2 settimane, come i bot eseguono attacchi di forza bruta. La regola si applica quando un IP è già stato bloccato più volte.
- *Temp di ban incrementale:* aumenta il tempo di blocco ad ogni tentativo fallito nel log. Quando abilitato, se si configura un tempo di blocco breve, un utente valido sarà bloccato per poco tempo mentre un attaccante verrà bloccato per un periodo molto lungo.

43.2.2 Consenti ban sulla LAN

Consente i ban sulla LAN Per impostazione predefinita, i tentativi falliti dalla rete locale vengono ignorati, tranne quando è stata attivata l'opzione.

IP/reti in whitelist Gli IP elencati nell'area di testo non verranno mai bannati da fail2ban (va indicato un IP per riga). E' possibile consentire intere reti inserendole nel pannello Reti fidate.

43.2.3 Email

Invia notifiche email Abilitando l'opzione verranno inviate email agli amministratori.

Email amministratori Elenco di indirizzi email degli amministratori (un indirizzo per riga).

Notifica eventi di abilitazione/disabilitazione di una jail Invia notifiche via email all'avvio o all'arresto di una jail.

43.3 Unban IP

Gli IP sono oggetto di ban quando vengono trovati più volte nei log, in uno specifico arco di tempo. Vengono archiviati in un database per essere nuovamente bannati ogni volta che si riavvia il server o il servizio. Per sbloccare un IP è possibile utilizzare la scheda *unban IP* disponibile nella categoria stato del server-manager.

43.4 Statistiche

La scheda *Ban statistics*, disponibile nella categoria stato del server-manager, fornisce il numero di ban per jail e totale.

43.5 Strumenti

43.5.1 Fail2ban-client

Fail2ban-client fa parte dell'rpm di fail2ban, fornisce lo stato di fail2ban e tutte le jail disponibili:

```
fail2ban-client status
```

Per ispezionare una jail specifica:

```
fail2ban-client status sshd
```

Per verificare quali file di log siano monitorati da una jail:

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

43.5.2 Fail2ban-listban

Fail2ban-listban permette di contare gli IP attualmente bannati nelle varie jail attivate e mostra anche gli IP che risultano bannati da shorewall.

```
fail2ban-listban
```

43.5.3 Fail2ban-regex

Fail2ban-regex è uno strumento che viene utilizzato per testare le regex sui log, è una parte del software fail2ban. È consentito un solo filtro per jail, ma è possibile specificare diverse azioni, su righe separate.

La documentazione è **consultabile sul sito del progetto fail2ban**<http://fail2ban.readthedocs.io/en/latest/filters.html>.

```
fail2ban-regex /var/log/YOUR_LOG /etc/fail2ban/filter.d/YOUR_JAIL.conf --print-all-
↳matched
```

È possibile anche testare direttamente una regex personalizzata:

```
fail2ban-regex /var/log/secure '^%(__prefix_line)s(?:error: PAM: )?[aA]uthentication_
↳(?:failure|error) for .* from <HOST>( via \S+)?\s*$'
```

43.5.4 Fail2ban-unban

Fail2ban-unban è utilizzabile per sbloccare un IP nel caso in cui il ban debba essere rimosso manualmente.

```
fail2ban-unban <IP>
```

È possibile utilizzare anche il comando integrato con fail2ban-client:

```
fail2ban-client set <JAIL> unbanip <IP>
```

43.6 Whois

Se si desidera ottenere informazioni sull'origine dell'IP bannato via e-mail, è possibile utilizzare il database whois installando l'rpm whois.

Rspamd è il nuovo motore antispam di NethServer, sostituisce SpamAssassin e Amavisd-new.

La documentazione ufficiale di Rspamd è disponibile all'indirizzo <https://rspamd.com>

Rspamd viene installato dal modulo *Email*, disponibile nel *Software center*. Il menu attraverso cui attivarlo e modificarne le impostazioni si trova nella pagina *Email > Filtro*. Per maggiori informazioni fare riferimento alla sezione *Email filter*.

44.1 Interfaccia web di Rspamd

Il componente antispam è implementato tramite Rspamd che fornisce una sua interfaccia web amministrativa all'url:

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

L'URL è disponibile anche nella pagina *Applicazioni* del *server-manager*. Di default, l'accesso all'interfaccia è concesso ai membri del gruppo `domain admins` ed all'utente `admin` (vedi anche *Account admin*). Esiste anche un account speciale aggiuntivo `rspamd` che può essere usato per accedervi. Le sue credenziali sono disponibili da *Email > Filtro > Interfaccia utente Rspamd (URL Web)*: è sufficiente seguire il link indicato.

Interfaccia utente Web di Rspamd

- visualizza messaggi e contatori delle azioni,
- mostra la configurazione del server,
- tiene traccia della cronologia dei messaggi recenti,
- consente di addestrare i filtri Bayesiani inviando un messaggio attraverso una interfaccia web.

44.1.1 Status

È il menu principale, le statistiche globali sono relative al servizio Rspamd.

44.1.2 Troughput

I grafici visualizzati in questo menu illustrano l'attività del software antispam. È possibile regolare la scala temporale (oraria, giornaliera, settimanale, mensile) e modificare alcune altre impostazioni per adattare i grafici alle proprie necessità

44.1.3 Configuration

Il menu *Configuration > Lists* consente di modificare la lista di IP/domini/mime autorizzati per i vari moduli. Quelli disponibili sono:

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

Volendo creare una lista di eccezioni per un modulo, sarà sufficiente utilizzare il percorso `/var/lib/rspamd/`, la lista sarà modificabile direttamente dall'interfaccia web di Rspamd.

44.1.4 Symbols

Rspamd usa il concetto di simbolo per aumentare o diminuire il punteggio di spam quando le relative regole vengono intercettate. Il peso del simbolo è modificabile, il punteggio negativo è relativo a messaggi di posta elettronica validi, quello positivo a messaggio di spam.

Individuare le corrispondenze dei simboli

Il metodo più comodo è quello offerto dall'interfaccia web, menu *History > History*.

Modificare il peso di un simbolo

Il modo più semplice per cambiare il peso del simbolo è utilizzare l'interfaccia utente di Rspamd: *Symbols > Symbols*. Per rintracciare un simbolo e modificarne il peso è disponibile una campo di ricerca.

- Il punteggio di spam associato ad un simbolo è indicato in rosso (punteggio positivo)
- Il punteggio di ham associato ad un simbolo è indicato in verde (punteggio negativo)

Se si desidera rimuovere le impostazioni personalizzate, è possibile modificare il file `/var/lib/rspamd/rspamd_dynamic` o rimuoverli tramite l'interfaccia Web di Rspamd: *Configuration > Lists > rspamd_dynamic*

È possibile modificare manualmente i punteggi dei simboli attraverso i file `/etc/rspamd/scores.d/*_group.conf` in cui i simboli sono raccolti per gruppi. Come per i moduli, è possibile sovrascrivere le impostazioni riportate nei file `/etc/rspamd/local.d/*_group.conf` e `:file:/etc/rspamd/override.d/*_group.conf`.

Ordine di priorità

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

44.1.5 Learning

Lo scopo del menu *Learning* è di addestrare il filtro Bayes, attraverso cui è possibile far apprendere a rspamd se una e-mail è uno spam o un ham utilizzando direttamente la sorgente della email attraverso l'area di testo dedicata.

44.1.6 Scan

Il menu *Scan* può essere usato per scansionare direttamente un'e-mail e controllarne il punteggio e i simboli corrispondenti.

44.1.7 History

L'interfaccia web di Rspamd può essere utilizzata per visualizzare il punteggio di spam totalizzato da un'email e la eventuale azione intrapresa dal sistema, vedi *History* > *History*

Si può visualizzare l'elenco di simboli facendo clic sul campo dell'email, aiuterà a capire l'azione eseguita (reject, add_header, no_action, rewrite_subject, greylist) e raccogliere informazioni utili come:

- il mittente
- il destinatario
- l'oggetto
- il punteggio totale

44.2 Moduli

Rspamd ha un approccio modulare, non tutti i moduli sono abilitati di default e sono personalizzabili dall'amministratore di sistema. Le impostazioni di default di ogni modulo sono contenute nel file `/etc/rspamd/modules.d/MODULE_NAME.conf`, il cui il nome è relativo al modulo.

Per esigenze particolari fare riferimento alla documentazione con la [lista completa dei moduli](#).

44.2.1 Disabilitare un modulo

La disabilitare un modulo andrebbe fatta solo se strettamente necessario. Ad esempio, se un mittente avesse il suo IP in una blacklist, il modulo `ip_score` potrebbe fornire un punteggio alto di spam.

In questo caso si potrebbe disabilitare il modulo ma molti moduli (come `ip_score`) implementano una whitelist per evitare di controllare un IP o un dominio contro il filtro spam.

Creare un file (con il nome inerente al relativo modulo) `/etc/rspamd/override.d/MODULE_NAME.conf` che contenga

```
enabled = false;
```

Riavviare Rspamd

```
systemctl restart rspamd
```

44.2.2 Modificare la configurazione di un modulo

Tutte le configurazioni predefinite di un modulo sono contenute nel file `/etc/rspamd/modules.d/MODULE_NAME.conf`, NethServer utilizza il file `/etc/rspamd/local.d/MODULE_NAME.conf` per modificare i parametri predefiniti. Quindi il metodo più indicato per effettuare delle modifiche ai valori di default di Rspamd e di NethServer. Il file override usa i nuovi parametro con una priorità più alta, tutte le precedenti impostazioni vengono mantenute.

Ordine di priorità

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

In questo esempio si vuole implementare un elenco di IP da mettere in whitelist per il modulo `ip_score`.

Creare un file `/etc/rspamd/override.d/ip_score.conf` con il seguente contenuto

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

Riavviare rspamd

```
systemctl restart rspamd
```

La whitelist è modificabile dall'interfaccia web di Rspamd, dal menu *Configuration > Lists > ip_score_whitelist*

Nota: Il percorso `/var/lib/rspamd` è di proprietà di Rspamd, tutti i file contenuti sono modificabili dal software

44.3 Domande frequenti

Le FAQ ufficiali per Rspamd sono disponibili al link <https://rspamd.com/doc/faq.html>

Antivirus

Nota: La pagina di configurazione di questo modulo è disponibile solo nel nuovo Server Manager.

ClamAV is the open source antivirus engine of NethServer. The server runs two different ClamAV instances: one for scanning received mail (see [Email](#)) and the other one for analyzing HTTP web traffic (see [Filtro contenuti web](#)).

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

Available options:

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

Nota: La pagina di configurazione di questo modulo è disponibile solo nel nuovo Server Manager.

La Threat Shield blocca le connessioni da e verso host dannosi, prevenendo attacchi, abusi del servizio, malware e altre attività di criminalità informatica mediante blacklist di IP. Inoltre, blocca le richieste DNS per domini dannosi mediante blacklist DNS. Il pacchetto può essere installato sia su firewall che su macchine senza interfaccia red, come server di posta o PBX.

46.1 Configurazione

IP blacklist e *DNS blacklist* possono essere abilitati e configurati nelle corrispondenti pagine del menu dedicato. La loro configurazione è pressoché identica.

Innanzitutto, è necessario impostare il *Download URL* per le blacklist. Dopo aver impostato l'URL, l'amministratore può scegliere quali categorie di blacklist abilitare. Ogni categoria può avere un punteggio *Fiducia* tra 0 e 10. Le categorie con una maggiore fiducia sono meno soggette a falsi positivi.

Le categorie abilitate verranno aggiornate automaticamente a intervalli regolari.

Il Download URL deve contenere un repository GIT valido. Gli amministratori possono scegliere un repository pubblico o abbonarsi a un servizio commerciale. Se la macchina dispone di una subscription Community o Enterprise, l'accesso all'URL verrà autenticato utilizzando l'LK di sistema e il token.

Una nota blacklist di IP gratuita è [Firehol](#). Gli amministratori esperti possono anche [configurare il proprio server di blacklist](#).

Un esempio di blacklist DNS è disponibile [qui](#).

Avvertimento: Se il *Proxy web* è abilitato, in qualsiasi modalità, la *blacklist DNS* non funzionerà per gli host proxati.

46.1.1 Whitelist

In caso di falso positivo, è possibile aggiungere un indirizzo IP o una rete CIDR alla *Whitelist* locale. Se è installato il modulo firewall, la *Whitelist* accetterà anche oggetti firewall di tipo host e CIDR.

Gli host dovrebbero essere aggiunti alla whitelist solo per un periodo di tempo limitato. Come best practice, quando viene trovato un falso positivo, si invita a segnalarlo al manutentore della blacklist.

46.2 Incident response

La pagina *Analisi* mostra gli attacchi e le richieste DNS più recenti, che possono essere filtrati per sorgente, destinazione e altri attributi. Usando la sezione *Controlla indirizzo IP o dominio*, gli amministratori possono anche verificare se un determinato IP o dominio sia stato inserito nella blacklist da una delle categorie abilitate.

Per un'analisi avanzata dei log con supporto delle espressioni regolari, usare la pagina *Log*.

46.3 Statistiche

La pagina *Dashboard* offre una panoramica dello stato corrente delle blacklist IP e DNS e visualizza informazioni grafiche sugli attacchi bloccati.

La dashboard della blacklist IP fornisce:

- Numero totale di minacce bloccate nella giornata
- Gli host di origine maggiormente bloccati nella giornata
- Gli host di destinazione maggiormente bloccati nella giornata

La dashboard della blacklist DNS fornisce:

- Numero totale di minacce bloccate nella giornata
- Numero totale di richieste DNS della giornata
- Percentuale delle minacce della giornata
- Lista dei client che eseguono il maggior numero di richieste DNS
- Principali domini bloccati
- Domini più richiesti

Aggiornamento Email a Rspamd

Con il rilascio di NethServer 7.5.1804 le nuove installazioni di *Email*, *Connettore POP3* e *pop3_proxy-section* sono basate sul motore di filtraggio Rspamd¹.

- Installazioni precedenti di NethServer verranno automaticamente aggiornate con Rspamd come descritto in questa sezione.
- Le nuove funzionalità di configurazione, specifiche dell'implementazione basata su Rspamd, sono documentate nella sezione *Email*. Ecco una breve lista:
 - Firma DKIM
 - Interfaccia web di Rspamd
 - Soglia Greylist³

47.1 Funzionalità modificate

47.1.1 Aggiungere un avviso legale

La funzionalità *Email*> *Domini*> *Aggiungi una nota legale ai messaggi inviati* (nota anche come «Disclaimer») è stata divisa in un pacchetto opzionale separato: *nethserver-mail2-disclaimer*. Le nuove installazioni dovrebbero evitarne l'uso, poiché si basa su un vecchio pacchetto⁴ che potrebbe venire rimosso nelle versioni future.

47.1.2 Blocco porta 25

Il blocco della porta 25 può prevenire l'abuso da parte dei PC in LAN. Se il sistema è il gateway della rete, l'amministratore può creare una regola di firewall in *Regole*.

¹ Rspamd – Fast, free and open-source spam filtering system. <https://rspamd.com/>

³ Greylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using greylisting will «temporarily reject» any email from a sender it does not recognize – [Wikipedia](#)

⁴ alterMIME is a small program which is used to alter your mime-encoded mailpack – <https://pldaniels.com/altermime/>

47.1.3 Host alias addizionali

I seguenti nomi di host erano automaticamente registrati nel servizio DNS, se `postfix/MxRecordStatus` era enabled:

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

In caso di aggiornamento dal vecchio modulo Email basato su Amavisd, il record `postfix/MxRecordStatus` viene rimosso e gli alias spostati come record di tipo `self` nel DB `hosts`. Possono essere modificati dalla pagina *DNS > Alias server*.

47.1.4 Record MX per i client della LAN

Il nuovo modulo Email basato su Rspamd non implementa più l'override del record MX per gli host della LAN. Assicurarsi che i client email della LAN siano configurati per usare l'SMTP/AUTH o siano elencati in *Email > Accesso SMTP > Consenti relay dai seguenti indirizzi IP* prima di aggiornare.

47.2 Procedure di aggiornamento manuale

Le procedure di aggiornamento manuale non sono più necessarie: l'aggiornamento avviene automaticamente.

Dopo l'aggiornamento, i servizi del vecchio motore antispam forniti da amavisd e spamassassin vengono disabilitati e i loro pacchetti possono essere rimossi.

Per rimuovere gli rpm del vecchio antispam eseguire

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

Riferimenti

Nota: Questo pacchetto non è supportato in NethServer Enterprise

Collabora Online Collabora Online è una potente suite office online basata su LibreOffice che supporta tutti i principali formati di documenti, fogli elettronici e file di presentazione, e può essere integrata nella propria infrastruttura. Per ulteriori informazioni fare riferimento al [sito web ufficiale](#).

48.1 Installazione

Installare il modulo dal Software Center o usando la riga di comando:

```
yum install nethserver-collabora
```

48.1.1 Configurazione virtual host

Collabora Online richiede un virtual host dedicato ed è accessibile solo da HTTPS con un certificato valido.

Nota: Collabora Online **non sarà abilitato** senza un virtual host dedicato

Per configurare Collabora Online, eseguire:

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

Dopo la configurazione del virtual host, andrà richiesto un certificato HTTPS valido tramite Let's Encrypt dalla sezione **Certificato server** dell'interfaccia **Server Manager**.

48.1.2 Utilizzo

Collabora Online verrà automaticamente abilitato per Nextcloud se il pacchetto `nethserver-nextcloud` è presente nel momento in cui viene configurato il virtual host virtuale, altrimenti è possibile abilitarlo successivamente con:

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

Se l'istanza di Nextcloud non è installata nello stesso server di Collabora Online, è necessario impostare il nome host di Nextcloud nella prop `AllowWopiHost`:

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

E configurare manualmente l'applicazione di Nextcloud [richdocuments](#).

48.2 Utente admin

Al termine dell'installazione, la dashboard di amministrazione può essere abilitata con `loolconfig set-admin-password` e accessibile al url:

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

Nota: This package is not supported in NethServer Enterprise

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

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

49.1 Official documentation

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

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

49.2 Installation

Install from the Software Center or use the command line:

```
yum install nethserver-docker
```

49.3 Docker repository

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

To upgrade to the latest stable version of docker:

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

to enable it permanently:

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

49.4 Configuration

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

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

Review the current settings with

```
config show docker
```

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

After each change, you have to restart docker

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

49.5 Web user Interface

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

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

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

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

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

49.6 Default network

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

Example of nginx container on port 9001:

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

49.7 Aqua network

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

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

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

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

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

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

49.8 Aeria network

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

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

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

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

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

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

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

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

Aeria uses a docker plugin. To update the plugin

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

49.9 Macvlan

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

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

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

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

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

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

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

Create the network

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

Then trigger the event

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

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

Docker creation example on macvlan

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

The container can be contacted at the relevant IP

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

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

49.10 Issues

Please raise issues on community.nethserver.org.

49.11 Sources

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

Nota: This package is not supported in NethServer Enterprise

SOGGo is a fully supported and trusted groupware server with a focus on scalability and open standards. SOGGo is released under the GNU GPL/LGPL v2 and above. SOGGo provides a rich AJAX-based Web interface and supports multiple native clients through the use of standard protocols such as CalDAV, CardDAV and GroupDAV, as well as Microsoft ActiveSync. SOGGo is the missing component of your infrastructure; it sits in the middle of your servers to offer your users a uniform and complete interface to access their information. It has been deployed in production environments where thousands of users are involved.

Nota: SOGGo provides EAS (Exchange ActiveSync) support, but not EWS (Exchange Web Service). Outlook 2013, 2016 for Windows works well with EAS. Mainstream mobile devices (iOS, Android, BlackBerry 10) work well with EAS, they can sync mails, calendars, contacts, tasks. Apple Mail.app, and Outlook for Mac support EWS. But not EAS. **Clients work very well with POP3/IMAP account, caldav/carddav account**

Avvertimento: `nethserver-sogo` doesn't integrate OpenChange and Samba4 for native MAPI support, so SOGGo groupware doesn't provide full support for Microsoft Outlook clients, Mac OS X Mail.app and all iOS devices, don't try to add your mail account as an Exchange account in these mail clients. You have to add account as POP3/IMAP account, caldav/carddav account instead.

50.1 Installation

Nota: You need first to set an account provider which can be local (`nethserver-directory` for `openldap` or `nethserver-dc` for Samba AD) or remote (whatever `openldap` or `samba AD` choice). You cannot mix your choice by `openldap` and Samba AD, preferably if you plan to host samba shares with user authentication, you need `samba AD` (`nethserver-dc`)

Then install from the Software Center or use the command line:

```
yum install nethserver-sogo
```

50.2 Official documentation

Please read [official documentation](#): your solution is in this book.

50.3 Usage

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

50.4 Esmith database

You can modify the available properties of SOGo:

```
sogod=service
  ActiveSync=enabled
  AdminUsers=admin
  BackupTime=30 0
  Certificate=
  Dav=enabled
  DraftsFolder=Drafts
  IMAPLoginFieldName=userPrincipalName
  MailAuxiliaryUserAccountsEnabled=YES
  Notifications=Appointment,EMail           #'Folder'/'ACLs'/'Appointment'
  SOGoInternalSyncInterval=10
  SOGoMaximumPingInterval=10
  SOGoMaximumSyncInterval=30
  SOGoMaximumSyncResponseSize=2048
  SOGoMaximumSyncWindowSize=100
  SentFolder=Sent
  SxVMemLimit=512
  TrashFolder=Trash
  VirtualHost=
  WOWatchDogRequestTimeout=10
  WOWorkersCount=10
  status=enabled
```

Properties:

- **AdminUsers:** Parameter used to set which usernames require administrative privileges over all the users tables.
- **BackupTime:** Time to launch the backup, by default (“30 0”)each day at 00h30, you can change it if you set a cron compatible value * *
- **DraftsFolder:** name of draft folder, default is ‘Drafts’
- **IMAPLoginFieldName:** adjust the imap login field to your good trusted value in your ldap (see <https://community.nethserver.org/t/sogo-and-ad-brainstorming/8024/31>)
- **SentFolder:** name of the sent folder, default is ‘Sent’

- `TrashFolder`: name of the trash folder, default is ‘Trash’
- `WOWorkersCount`: The amount of instances of SOGo that will be spawned to handle multiple requests simultaneously
- `MailAuxiliaryUserAccountsEnabled`: Parameter used to activate the auxiliary IMAP accounts in SOGo. When set to YES, users can add other IMAP accounts that will be visible from the SOGo Webmail interface.
- `Notifications`: enabled notifications. The value is a comma separated list. Default value is “Appointment, EMail”

Notes

Terms highlighted in **bold** are documented in SOGo [installation and configuration guide](#).

- `AdminUsers` comma separated list of accounts allowed to bypass SOGo ACLs. See **SOGoSuperUsernames** key
- `Notifications` comma separated list of values (no spaces between commas). Known item names are `ACLs`, `Folders`, `Appointments`. See **SOGoSendEMailNotifications**
- `{Drafts, Sent, Trash}Folder` See respective **SOGoFolderName** parameters
- `VirtualHosts` SOGo is reachable from the default host name plus the host (FQDN) listed here. The host key is generated/removed in `hosts` DB, with `type=self` automatically.

50.5 Access SOGo on an exclusive hostname

To make SOGo accessible with an exclusive DNS hostname:

- In “DNS and DHCP” UI module (Hosts), create the DNS host name as a server alias (i.e. `webmail.example.com`)
- Add the host name to `sogod/VirtualHost` prop list:

```
config setprop sogod VirtualHost webmail.example.com
signal-event nethserver-sogo-update
```

Same rule applies if SOGo must be accessible using server IP address. For example:

```
config setprop sogod VirtualHost 192.168.1.1
signal-event nethserver-sogo-update
```

If the `VirtualHost` prop is set, requests to the root (i.e. `webmail.example.com`) are redirected to the (mandatory) `/SOGo` subfolder (`webmail.example.com/SOGo`).

It is also possible to use a custom certificate for this virtualhost:

```
config setprop sogod Certificate example.crt
signal-event nethserver-sogo-update
```

50.6 Maximum IMAP command

Maximum IMAP command line length in kilo bytes. Some clients generate very long command lines with huge mailboxes, so you may need to raise this if you get «Too long argument» or «IMAP command line too large» errors often.

Set by default to 2048KB:

```
config setprop dovecot ImapMaxLineLenght 2048
signal-event nethserver-sogo-update
```

50.7 ActiveSync

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

ActiveSync is enabled by default on SOGo and WebTop. At installation of SOGo, Webtop-ActiveSync is disabled and SOGo will take precedence.

SOGo-ActiveSync can be disabled in the server-manager at the SOGo-panel or with:

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

To enable ActiveSync on SOGo again:

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

50.8 Backup

Each night (by default) a cron run to backup user data (filter rules, specific settings, events, contacts) and save it to `/var/lib/sogo/backups` you can restore the data with a tool `sogo-restore-user`, for example:

```
sogo-restore-user /var/lib/sogo/backups/sogo-2017-12-10_0030/ stephane
```

or for all users

```
sogo-restore-user /var/lib/sogo/backups/sogo-2017-12-10_0030/ -A
```

if you want to change the time of your backup for example (in this example, run at 4h01 AM):

```
config setprop sogod BackupTime '1 4'
signal-event nethserver-sogo-update
```

50.9 Fine tuning

50.9.1 Adjust Setting

SOGo **must be tuned** following the number of users, some settings can be tested.

Nota: Keep in mind to set one worker per active user for the activesync connection. The `SxVMemLimit` could be be adjusted also, between 25MB to 45 MB per active user with the activesync service.

100 users, 10 EAS devices:

```
config setprop sogod WWorkersCount 15
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 30
signal-event nethserver-sogo-update
```

100 users, 20 EAS devices:

```
config setprop sogod WWorkersCount 25
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 40
signal-event nethserver-sogo-update
```

1000 users, 100 EAS devices:

```
config setprop sogod WWorkersCount 120
config setprop sogod SOGoMaximumPingInterval 3540
config setprop sogod SOGoMaximumSyncInterval 3540
config setprop sogod SOGoInternalSyncInterval 60
signal-event nethserver-sogo-update
```

SxVMemLimit (default 512MB):

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

50.9.2 Increase sogod log verbosity

Read the [SOGGo FAQ](#) for other debugging features.

50.9.3 SOGo floods /var/log/messages

You can see this log noise in /var/log/message:

```
Dec 4 12:36:01 ns7ad1 systemd: Created slice User Slice of sogo.
Dec 4 12:36:01 ns7ad1 systemd: Starting User Slice of sogo.
Dec 4 12:36:01 ns7ad1 systemd: Started Session 163 of user sogo.
Dec 4 12:36:01 ns7ad1 systemd: Starting Session 163 of user sogo.
Dec 4 12:36:01 ns7ad1 systemd: Removed slice User Slice of sogo.
Dec 4 12:36:01 ns7ad1 systemd: Stopping User Slice of sogo.
```

These messages are normal and expected – they will be seen any time a user logs in. To suppress these log entries in /var/log/messages, create a discard filter with rsyslog, e.g., run the following command:

```
echo 'if $programname == "systemd" and ($msg contains "Starting Session" or $msg_
↳contains "Started Session" or $msg contains "Created slice" or $msg contains
↳"Starting User" or $msg contains "Removed slice User" or $msg contains "Stopping_
↳User") then stop' > /etc/rsyslog.d/ignore-systemd-session-slice-sogo.conf
```

and restart rsyslog

```
systemctl restart rsyslog
```

this solution comes from [RedHat solution](#)

50.10 Clients

50.10.1 Android

Currently you have 2 ways to integrate your Android device with Sogo.

Integration via Caldav /Cardav/imap

Nota: The drawback is that you need to set all settings (Url/Username/Password) in each application.

- Email

Imaps(over ssl) is a good choice, you can use the K9-mail software to retrieve your email or the default email application

- Contacts and calendars

There are various working clients, including [DAVdroid](#) (open-source) and [CalDAV-Sync/CardDav-Sync](#). Advantages Full integration into Android, so that almost all calendar and contacts apps can access synchronized data.

Integration via ExchangeActiveSync

Nota: The advantage is that you set the Url/Username/Password only in one location

Step-by-step configuration

- Open the account menu, choose add an exchange account
- Fill your full email address and password in Account Setup page:
- If it asks you to choose Account Type, please choose Exchange:
- In detailed account setup page, fill up the form with your server address and email account credential
 - DomainUsername: your full email address
 - Password: password of your email account
 - Server: your server name or IP address
 - Port: 443

Nota: Please also check Use secure connection (SSL) and Accept all SSL certificates

- In Account Settings page, you can choose Push. it's all up to you.
- Choose a name for your Exchange account.
- Click Next to finish account setup. That's all.

50.10.2 Mozilla Thunderbird and Lightning

Alternatively, you can access SOGo with a GroupDAV and a CalDAV client. A typical well-integrated setup is to use Mozilla Thunderbird and Mozilla Lightning along with Inverse's SOGo Connector plug in to synchronize your address books and the Inverse's SOGo Integrator plug in to provide a complete integration of the features of SOGo into Thunderbird and Lightning. Refer to the documentation of Thunderbird to configure an initial IMAP account pointing to your SOGo server and using the user name and password mentioned above.

With the [SOGo Integrator plug in](#), your calendars and address books will be automatically discovered when you login in Thunderbird. This plug in can also propagate specific extensions and default user settings among your site. However, be aware that in order to use the SOGo Integrator plug in, you will need to repackage it with specific modifications. Please refer to the [documentation published online](#).

If you only use the SOGo Connector plug in, you can still easily access your data.

- To access your personal address book:
- Choose Go > Address Book.
- Choose File > New > Remote Address Book.
- Enter a significant name for your calendar in the Name field.
- Type the following URL in the URL field: <http://localhost/SOGo/dav/jdoe/Contacts/personal/>
- Click on OK.

To access your personal calendar:

- Choose Go > Calendar.
- Choose Calendar > New Calendar.
- Select On the Network and click on Continue.
- Select CalDAV.
- Type the following URL in the URL field: <http://localhost/SOGo/dav/jdoe/Calendar/personal/>
- Click on Continue.

50.10.3 Windows Mobile

The following steps are required to configure Microsoft Exchange ActiveSync on a Windows Phone:

Locate the Settings options from within your application menu.

- Select Email + Accounts.
- Select Add an Account.
- Select the option for Advanced Setup.
- Enter your full email address and password for your account. Then press the sign in button.
- Select Exchange ActiveSync.
- Ensure your email address remains correct.
- Leave the Domain field blank.
- Enter the address for Server (domain name or IP)
- Select the sign in button.
- You might need to accept all certificates, if you are not able to sync

Once connected, you will see a new icon within your settings menu with the name of your new email account.

50.10.4 Outlook

You can use it with

- IMAP + commercial plugin as `cfos` or `outlookdav` for calendars/contacts
- ActiveSync since Outlook 2013

There is no support for Openchange/OutlookMAPI.

50.11 Nightly build

SOGo is built by the community, if you look to the last version, then you must use the nightly built. This version is not considered as stable, but bugs are fixed quicker than in stable version. You are the QA testers :)

50.11.1 NethServer 7 - SOGo 3

Execute:

```
sudo rpm --import 'http://pgp.mit.edu/pks/lookup?op=get&search=0xCB2D3A2AA0030E2C'  
sudo rpm -ivh http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm  
sudo cat >/etc/yum.repos.d/SOGo.repo <<EOF  
[sogo3]  
name=SOGo Repository  
baseurl=https://packages.inverse.ca/SOGo/nightly/3/rhel/7/\$basearch  
gpgcheck=1  
EOF
```

Then to install:

```
yum install nethserver-sogo --enablerepo=sogo3
```

50.12 Issues

Please raise issues on community.nethserver.org.

50.13 Sources

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

Developer manual on [github](#).

Nota: This package is not supported in NethServer Enterprise

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

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

51.1 Installation

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

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

Install from the Software Center or use the command line:

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

51.1.1 Usage

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

- username: admin
- password: admin

More information are available at the Authentication section

51.1.2 Network access

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

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

51.1.3 Access on an exclusive hostname

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

- In “DNS and DHCP” UI module (Hosts), create the DNS host name as a server alias (i.e. `webmail.example.com`)
- Add the host name to DomainName prop list (default is “”):

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

51.1.4 Advanced settings

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

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

51.1.5 VM ownership and quota

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

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

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

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

51.2 User permissions

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

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

51.3 Authentication

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

Example:

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

51.3.1 internal

The default credentials are :

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

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

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

51.3.2 LDAP (openldap)

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

51.3.3 AD (active directory)

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

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

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

51.4 Uploading ISOs

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

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

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

51.5 Oracle VM VirtualBox Extension Pack

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

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

51.6 The RDP console

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

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

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

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

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

51.7 VM networking

The networking side is probably the most difficult part of the virtualization, you should consult the [VirtualBox Documentation](#)

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

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

Example script

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

51.8 Esmith database

You can modify the available properties of phpvirtualhost:

```

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

```

Example:

```

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

```

51.9 Documentation

VirtualBox The official [VirtualBox documentation](#) is available on the [VirtualBox website](#).

phpVirtualbox The official [phpVirtualbox documentation](#) is available on the [github website](#).

HotSync

Nota: Questo pacchetto non è supportato in NethServer Enterprise

Avvertimento: Il modufflo HotSync è da considerarsi una [release beta](#). Pertanto è opportuno provarla in ambienti di test prima di procedere in produzione.

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

HotSync mira a ridurre i tempi di inattività in caso di problemi, sincronizzando il NethServer con un altro sistema gemello, che verrà attivato manualmente in caso di guasto del server master.

Normalmente, quando si verifica un problema hardware, il tempo necessario per ripristinare il servizio è:

1. riparazione/approvvigionamento nuovo server: da 4h a 2 giorni
2. installazione sistema operativo: 30 minuti
3. ripristino backup: da 10 minuti a 8 ore

In summary, users are able to start working again with data from the night before failure after a few hours/days. Using HotSync, time 1 and 3 are 0, 2 is 5 minutes (time to activate spare server). Users are able to start working again in few minutes, using data from a few minutes before the crash.

Per impostazione predefinita, tutti i dati inclusi nel backup vengono sincronizzati ogni 15 minuti. Anche i database MariaDB sono sincronizzati, a meno che la sincronizzazione dei database non sia disabilitata. Le applicazioni che utilizzano PostgreSQL sono sincronizzate (Mattermost, Webtop5) a meno che la sincronizzazione dei database non sia disabilitata.

52.1 Terminologia

- MASTER è il sistema di produzione SLAVE è il server di riserva
- SLAVE è acceso, con un indirizzo IP diverso da MASTER
- Ogni 15 minuti, MASTER esegue un backup su SLAVE
- If an error occurs, an email is sent to root (admin if mail server is installed)
- SLAVE check updates and makes some system operations every 60 minutes

52.2 Installazione

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

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

52.3 Configurazione

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

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

52.3.1 Master

```
[root@master]# config setprop rsyncd password <PASSWORD>
[root@master]# config setprop hotsync role master
[root@master]# config setprop hotsync SlaveHost <SLAVE_IP>
[root@master]# signal-event nethserver-hotsync-save
```

52.3.2 Slave

```
[root@slave]# config setprop rsyncd password <PASSWORD>
[root@slave]# config setprop hotsync role slave
[root@slave]# config setprop hotsync MasterHost <MASTER_IP>
[root@slave]# signal-event nethserver-hotsync-save
```

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

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

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

52.3.3 Abilitazione/Disabilitazione

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

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

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

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

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

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

52.4 Ripristino: promuovere lo SLAVE in produzione

La seguente procedura mette in produzione lo SLAVE in caso di arrewsto anomalo del master.

1. Switch off MASTER.
2. If the SLAVE machine must run as network gateway, connect it to the router/modem with a network cable.
3. On SLAVE, if you are connected through an SSH console, launch the `screen` command, to make your session survive to network outages:

```
[root@slave]# screen
```

As best practice, execute following procedure using a local console and not via SSH connection.

4. lanciare sullo SLAVE il seguente comando e leggere attentamente l'output generato

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

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

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

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

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

5. If necessary go to Server Manager or Cockpit GUI, in page [Network](#) and reassign roles to network interfaces as master one. Remember also to recreate bridge if you have configured DC. In case of DC errors consult troubleshooting section before proceed with network restore.

6. After everything has been restored, launch the command

```
[root@slave]# /sbin/e-smith/signal-event post-restore-data
```

7. Update the system to the latest packages version

```
[root@slave]# yum clean all && yum -y update
```

8. If an USB backup is configured on MASTER, connect the backup HD to SLAVE

52.5 Troubleshooting

52.5.1 After restore on different hardware DC is not working

Console could report some errors like these

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

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

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

52.5.2 After restore permissions on ibays are not correct

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

52.5.3 After network restore server is unreachable

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

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

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

52.5.4 Suggested check after restore

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

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

52.6 Pacchetti supportati

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

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

- nethserver-mattermost
- nethserver-mysql
- nethserver-ndpi
- nethserver-netdata
- nethserver-nextcloud
- nethserver-ntopng
- nethserver-nut
- nethserver-openssh
- nethserver-openvpn
- nethserver-pulledpork
- nethserver-restore-data
- nethserver-roundcubemail
- nethserver-samba
- nethserver-samba-audit
- nethserver-squid
- nethserver-squidclamav
- nethserver-squidguard
- nethserver-sssd
- nethserver-subscription
- nethserver-suricata
- nethserver-vpn-ui
- nethserver-vsftpd
- nethserver-webtop5 (lo stato di z-push non è sincronizzato)

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

<p>Avvertimento: To avoid errors on the slave host, do not make any changes to the modules from the Cockpit GUI except the HotSync module.</p>

Microsoft SQL Server

Nota: This package is not supported in NethServer Enterprise

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

53.1 Installazione

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

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

53.2 Default configuration

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

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

Database example:

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

53.3 Install mssql-server service

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

You can do this also from command line:

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

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

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

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

Now your SQL Server is ready to use!

53.4 Helpful actions

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

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

53.5 Backup and restore

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

53.6 SQLCMD utility

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

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

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
```

54.1 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`.

54.2 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*.

54.3 Firewall

Se il software necessita di porte aperte sul firewall, creare un servizio chiamato `fw_<softwarename>`.

Ad esempio, dato il software *mysoftware* che necessita la porta 3344 e 5566 aperta sulla LAN, usare questi comandi:

```
config set fw_mysoftware service status enabled TCPPorts 3344,5566 access green
signal-event firewall-adjust
signal-event runlevel-adjust
```

54.4 Avvio e arresto

NethServer usa il target standard multi utente di `systemd`.

Il software installato con yum dovrebbe già essere configurato per partire al boot del sistema. Per controllare la configurazione, eseguire il comando **systemctl**. Il comando mostra una lista di servizi con il relativo stato.

Per abilitare un servizio al boot:

```
systemctl enable mysoftware
```

Per disabilitare un servizio al boot:

```
systemctl disable mysoftware
```

Migrazione da NethService/SME Server

La migrazione è il processo che consente di convertire una macchina per SME Server/NethService (*sorgente*) in un NethServer (*destinazione*). Il processo può essere tramite *backup* o *utilizzando rsync*.

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

Avvertimento: Prima di eseguire la procedura di migrazione, leggere attentamente tutte le sezioni di questo capitolo.

55.1 Account provider

E' necessario configurare un *provider account* prima di avviare la procedura di migrazione.

- Se il sistema originale era collegato ad un dominio Active Directory (il ruolo Samba era ADS), configurare un *Active Directory remoto* come account provider.
- Se il sistema originale era un Controller di dominio NT (Samba con ruole PDC), installare un *Active Directory locale* come provider account.
- Se l'accesso alle Cartelle Condivise nella destinazione richiede l'autenticazione utente, utilizzare un *Active Directory locale* come provider account.
- In ogni altro caso, installare un *LDAP locale* come provider account.

Se si sceglie un account provider di tipo *Active Directory* locale, ricordarsi di configurare completamente ed avviare il DC prima di eseguire l'evento `migration-import`. Vedi `account-provider`.

Inoltre i seguenti account vengono ignorati dalla procedura di migrazione perché sono già forniti da Active Directory:

- `administrator`
- `guest`

- `krbtgt`

55.2 Email

Prima di mettere in produzione NethServer, è necessario fare qualche valutazione relativa alla rete ed alla configurazione dei client mail esistenti: quali porte siano utilizzate, se SMTPAUTH e TLS siano abilitati. Fare riferimento alle sezioni configurazioni client e *Politiche SMTP di invio speciali* per ulteriori informazioni.

Nella migrazione di un server di posta, il server di origine può rimanere in produzione anche dopo che il backup è stato eseguito e nuovi messaggi di posta continuano ad essere consegnati finché non viene spento definitivamente.

Uno script `rsync` di aiuto è fornito dal pacchetto `nethserver-mail-server`. Va eseguito sulla destinazione e serve a sincronizzare le caselle di posta di destinazione con il server di origine:

```
Usage:
  /usr/share/doc/nethserver-mail-server-<VERSION>/sync_maildirs.sh [-h] [-n] [-p] -
  ↪s IPADDR
      -h          help message
      -n          dry run
      -p PORT      ssh port on source host (default 22)
      -s IPADDR    rsync from source host IPADDR
      -t TYPE      source type: sme8 (default), ns6
```

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

55.3 Apache

La configurazione di cifratura SSL non verrà migrata automaticamente perché il sistema sorgete adotta di default un sistema di cifrature debole. Per effettuare manualmente la migrazione di tale configurazione andranno eseguiti i seguenti comandi:

```
MIGRATION_PATH=/var/lib/migration
config setprop httpd SSLCipherSuite $(db $MIGRATION_PATH/home/e-smith/db/
  ↪configuration getprop modSSL CipherSuite)
signal-event nethserver-httpd-update
```

55.4 Ibay

Le *ibay* sono state sostituite dalle *Cartelle condivise*. I protocolli supportati per accedere alle Cartelle condivise sono:

- SFTP, messo a disposizione dal demone `sshd`
- il protocollo di condivisione file SMB, tipico delle infrastrutture Windows, implementato attraverso Samba

Avvertimento: Leggere attentamente la sezione *Cartelle condivise* del capitolo *Aggiornamento da NethServer 6*, le credenziali per la connessione potrebbero variare a seguito dell'upgrade a NethServer 7.

A partire da NethServer 7, le Cartelle condivise non possono più essere esposte via HTTP. Successivamente all'evento `migration-import` le vecchie *ibay* potranno essere migrate rispettando le seguenti regole generali:

1. Se l'ibay aveva un **virtual host** associato, si dovrà installare il modulo «Web server» dalla pagina *Software center*. Sarà poi necessario copiare il contenuto della ibay nella directory root del virtual host. Fare riferimento a *Virtual hosts*.
2. Se l'accesso alla ibay era limitato da una **password** (ad esempio per condividere i contenuti con un gruppo di persone attraverso internet), sarà possibile replicare questa configurazione dalla pagina *Virtual hosts*. E' anche possibile pensare di sostituire la ibay utilizzata in questa configurazione con il modulo *Nextcloud*.
3. Se il contenuto della ibay era accessibile attraverso un URL come `http://<IP>/ibayname` il modo più semplice per mantenere la funzionalità sarà quello di spostare il percorso nella radice di Apache:

```
mv -iv /var/lib/nethserver/ibay/ibayname /var/www/html/ibayname
chmod -c -R o+rX /var/www/html/ibayname
db accounts delete ibayname
signal-event nethserver-samba-update
```

Dopo la migrazione, le ibay manterranno un profilo retro-compatibile. Per sfruttare le nuove funzionalità, incluso Samba Audit, la configurazione delle ibay deve essere passata al nuovo profilo. Da riga di comando eseguire:

```
db accounts setprop ibay_name SmbProfileType default
signal-event ibay-modx ibay_name
```

In cui `ibay_name` è il nome della ibay da configurare.

55.5 Migrazione da backup

1. Sulla macchina origine, effettuare un backup completo e spostarlo sul server destinazione.
2. Sul server destinazione, installare NethServer 7 **utilizzando la ISO più recente**, e, una volta registrato, **installare tutti gli aggiornamenti per il core disponibili**
3. Sul server destinazione, installare tutti i moduli che implementano i servizi presenti sulla macchina origine.
4. Estrarre il backup in una directory; per esempio, creare la directory `/var/lib/migration`.
5. Scatenare l'evento `migration-import` nell'host di destinazione:

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

Questa operazione potrebbe richiedere molti minuti.

6. Consultare il log di sistema file:`/var/log/messages` ed assicurarsi che non si siano verificati errori:

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

55.6 Migrazione con rsync

Questa procedura è più rapida rispetto a quella effettuata a partire da un backup.

Prima di iniziare assicurarsi di avere:

- una installazione NethService/SME attiva, che chiameremo server origine o server sorgente
- una installazione di NethServer 7 attiva con **tutti gli update più recenti installati** e con a disposizione lo stesso spazio su disco del server sorgente, che chiameremo server destinazione
- una connessione di rete attiva tra i due server

Assicurarsi che il server sorgente consenta il login all'utente root con password ed attraverso una chiave SSH.

55.6.1 Sincronizzazione dei file

Lo script di sincronizzazione copia tutti i dati utilizzando rsync su SSH. I file vengono salvati nel percorso `/var/lib/migration`. Se il server di destinazione non dispone di chiavi SSH, lo script creerà anche una coppia di chiavi RSA e ne copierà la chiave pubblica nel server di origine. Tutte le directory escluse dai dati di backup non verranno sincronizzate.

Nella macchina di destinazione, eseguire il seguente comando:

```
screen rsync-migrate <source_server_name> [ssh_port]
```

In cui

- `source_server_name` è il nome host o IP del server origine
- `ssh_port` è la porta SSH del server origine (la porta di default è la 22)

Esempio:

```
screen rsync-migrate mail.nethserver.org 2222
```

Quando richiesto, inserire la password di root del server origine quindi prepararsi un caffè e aspettare con pazienza.

Lo script non eseguirà alcuna azione sulla macchina di origine e può essere rilanciato più volte.

55.6.2 Sincronizzazione e migrazione

Se impartito con l'opzione `-m`, `rsync-migrate` eseguirà una sincronizzazione finale e l'aggiornamento della macchina destinazione.

Prima di eseguire lo step finale di migrazione, installare tutti i pacchetti che coprono le stesse funzionalità del server d'origine.

Esempio:

```
screen rsync-migrate -m mail.nethserver.org 2222
```

Lo script si incaricherà di:

- fermare ogni servizio sulla macchina origine (ad eccetto di SSH)
- eseguire l'evento di `pre-backup` sulla macchina origine
- sincronizzare tutti i dati rimanenti
- eseguire l'evento `migration-import` sulla macchina destinazione

Al termine della procedura verificare la presenza di eventuali errori in `/var/log/messages`:

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

Aggiornamento da NethServer 6

L'aggiornamento da NethServer 6 a NethServer 7 può essere eseguito utilizzando uno dei tre seguenti metodi:

- *backup* (vedere anche *Disaster recovery*)
- *rsync*
- *upgrade-tool* (beta)

<p>Avvertimento: Prima di procedere con l'aggiornamento, leggere attentamente tutte le sezioni di questo documento. Si prega di fare riferimento anche alla sezione <i>Pacchetti rimossi</i>.</p>
--

Nota: Per l'intera durata del processo di upgrade tutti i servizi di rete saranno inaccessibili.

56.1 Account provider

Esistono differenti scenari di aggiornamento, a seconda di come è configurata la macchina di origine.

- In caso di sistema di origine Primary Domain Controller NT (ruolo del server Samba *Primary Domain Controller* – PDC) o di file server standalone (ruolo *Workstation* – WS), fare riferimento alla sezione *Aggiornamento Primary Domain Controller e Workstation*.
- In caso di sistema origine attestato ad un dominio Active Directory (ruolo server Samba *Active Directory member* – ADS), fare riferimento alla sezione *Aggiornamento membro Active Directory*.
- In tutti gli altri casi il server LDAP viene automaticamente aggiornato a «Account provider LDAP locale», preservando utenti, password e gruppi preesistenti.

56.1.1 Aggiornamento Primary Domain Controller e Workstation

Successivamente alla procedura di ripristino, spostarsi nella pagina *Accounts provider* e selezionare la procedura *Upgrade to Active Directory*. Il bottone sarà disponibile unicamente se la configurazione di rete sarà stata adattata al nuovo hardware.

I seguenti account vengono ignorati dalla procedura di aggiornamento perché sono già forniti da Samba Active Directory:

- administrator
- guest
- krbtgt

E' necessario fornire un indirizzo IP, aggiuntivo e libero, della rete *green* al container Linux per attivare l'account provider Active Directory locale.

Ad esempio:

- IP server (green): 192.168.98.252
- IP aggiuntivo e libero della rete green: 192.168.98.7'

Assicurarsi che sia attiva una connessione internet:

```
# curl -I http://packages.nethserver.org/nethserver/  
HTTP/1.1 200 OK
```

Per maggiori informazioni relative all'account provider Active Directory locale, fare riferimento alla sezione *Installazione del provider locale Samba Active Directory*.

Le connessioni alle cartelle condivise potrebbero richiedere delle modifiche.

Avvertimento: Leggere attentamente la sezione *Cartelle condivise*, le credenziali per la connessione potrebbero variare a seguito dell'upgrade a NethServer 7.

La procedura di upgrade preserva utenti, gruppi e account dei computer.

Avvertimento: Gli utenti non abilitati per Samba in NethServer 6 saranno migrati come utenti bloccati. Per abilitare questi utenti bloccati, l'amministratore dovrà semplicemente impostargli una nuova password.

56.1.2 Aggiornamento membro Active Directory

Successivamente al **ripristino della configurazione**, attestare il server ad un dominio Active Directory esistente tramite l'interfaccia web. Per ulteriori informazioni consultare la sezione *Join ad un dominio Active Directory esistente*.

Al termine, procedere con il **ripristino dei dati**.

Avvertimento: Gli alias e-mail non vengono importati automaticamente da AD!

56.2 Cartelle condivise

Le cartelle condivise sono state separate in due pacchetti:

- La pagina «Cartelle condivise» permette di configurare solamente delle condivisioni SMB; fornisce l'accesso ai dati utilizzando il protocollo CIFS/SMB e può essere utilizzata per condividere file tra workstation Windows e Linux
- Il pannello «Virtual host» fornisce l'accesso via HTTP ed FTP ed è stato concepito per ospitare siti ed applicazioni web

56.2.1 Accesso SMB

Il modello di protezione SMB adottato da NethServer 7 si basa su Active Directory. Di conseguenza, quando si esegue l'aggiornamento (o la migrazione) di un file server nel ruolo del controller di dominio primario (PDC) o di standalone workstation (WS), si applica la seguente regola:

Quando ci si connette a una cartella condivisa, il nome di dominio NetBIOS deve essere anteposto al nome utente (ad esempio MYDOMAIN\username) o inserito nel campo specifico del modulo di autenticazione.

La procedura di upgrade abilita l'obsoleto metodo di autenticazione NTLM¹ al fine di preservare la compatibilità con i client della rete più vecchi, come stampanti e scanner.

Avvertimento: Si consiglia caldamente di correggere la configurazione dei client SMB più vecchi quindi di disattivare l'autenticazione NTLM.

- Modificare `/var/lib/machines/nsdc/etc/samba/smb.conf`
- Rimuovere la riga `ntlm auth = yes`
- Riavviare il DC samba con il comando `systemctl -M nsdc restart samba`

56.2.2 Accesso HTTP

Ogni cartella condivisa con accesso web configurata in NethServer 6 può essere migrata a virtual host direttamente dall'interfaccia web selezionando l'azione *Migra a virtual host*. Dopo la migrazione, i dati contenuti nel nuovo virtual host saranno accessibili solamente tramite i protocolli FTP ed HTTP.

Fare riferimento alla sezione *Virtual hosts* per ulteriori informazioni relative alla pagina *Virtual hosts*

56.3 Server mail

Tutte le opzioni delle cassette postali come la SPAM retention e la quota, così come le ACL, le cassette postali condivise dall'utente e le sottoscrizioni vengono conservate.

Le mailbox associate a gruppi con l'opzione *Consegna il messaggio in una cartella condivisa* abilitata, verranno convertite in cassette postali pubbliche condivise. La cartella pubblica condivisa verrà automaticamente sottoscritta da tutti i membri del gruppo, ma tutti i messaggi verranno contrassegnati come non letti.

¹ Vulnerabilità Badlock <http://badlock.org/>

56.4 TLS policy

La configurazione dei servizi di NethServer 7 può aderire a diverse *TLS policy*. Prima dell'aggiornamento, è necessario verificare la compatibilità dei client di rete con le caratteristiche delle policy disponibili.

Avvertimento: Un client di rete datato potrebbe fallire la connessione se i cifrari TLS da esso supportati sono considerati non validi

La versione della policy selezionata dalla procedura di aggiornamento dipende dal versione di NethServer come documentato in *Note di rilascio 7*.

56.5 Let's Encrypt

I certificati Let's Encrypt vengono ripristinati durante il processo, ma non verranno automaticamente rinnovati.

Dopo aver completato il processo di aggiornamento, accedere all'interfaccia web e riconfigurare Let's Encrypt dalla pagina *Certificato del server*.

56.6 Owncloud e Nextcloud

In NethServer 7, Owncloud è stato ufficialmente sostituito da Nextcloud.

Tuttavia Owncloud 7 è ancora disponibile per evitare interruzioni del servizio dopo l'aggiornamento.

Nota: In caso di *upgrade da LDAP locale ad Samba AD*, i dati utente all'interno di Owncloud non saranno accessibili né dall'interfaccia web né dai client desktop/mobile. In tal caso, installare e migrare a Nextcloud dopo che è stato completato l'aggiornamento a Samba Active Directory.

Da Nextcloud 13, la migrazione da Owncloud a Nextcloud non è più supportata.

Gli utenti dovranno sostituire i client per Owncloud con quelli per Nextcloud², assicurandosi di impostare il nuovo URL dell'applicazione: `https://<your_server_address>/nextcloud`.

56.7 Librerie Perl

In NethServer 7, la libreria perl `NethServer::Directory` è stata sostituita da `NethServer::Password`. Gli script personalizzati andranno adattati di conseguenza.

Esempio del vecchio codice:

```
use NethServer::Directory;
NethServer::Directory::getUserPassword('myservice', 0);
```

Nuovo codice:

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

² download client Nextcloud <https://nextcloud.com/install/#install-clients>

La documentazione è disponibile attraverso il comando perldoc:

```
perldoc NethServer::Password
```

56.8 Upgrade da backup

1. Assicurarsi di avere un backup recente del sistema di origine.
2. Installare NethServer 7 **utilizzando la ISO più recente disponibile** e completare gli step iniziali utilizzando il wizard di prima configurazione. La nuova macchina deve avere lo stesso hostname della vecchia per poter accedere correttamente al set di backup. Installare e configurare il modulo del backup.
3. Ripristinare il backup della configurazione utilizzando l'interfaccia web. Anche la configurazione della rete verrà ripristinata! Se dovesse verificarsi qualche problema, controllare il file di log `/var/log/messages` per informazioni più approfondite:

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

4. Se necessario, spostarsi nel menu *Network* e correggere la configurazione di rete conformemente al nuovo hardware. Se la macchina era attestata ad un dominio Active Directory esistente, leggere [Aggiornamento membro Active Directory](#).
5. Completare la procedura di ripristino con i seguenti comandi:

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

in cui *name* è il nome del backup configurato.

Nota: Di default il nome del *backup-data* configurato su NethServer 6 è `backup-data`

6. Verificare i log del ripristino:

```
/var/log/restore-data.log
/var/log/messages
```

7. La compatibilità con la versione 7 di ciascun file contenuto nel percorso `/etc/e-smith/templates-custom/` dovrà essere verificata manualmente.

Avvertimento: La macchina non va riavviata prima di aver eseguito la procedura di `restore-data`.

56.9 Upgrade tramite rsync

Il processo tramite rsync è più rapido rispetto ad un tradizionale backup e ripristino e consente di minimizzare il fermo servizi per gli utenti.

Prima di iniziare assicurarsi di avere:

- una installazione di NethServer 6 in produzione, che chiameremo server origine o server sorgente
- una installazione di NethServer 7 con almeno lo stesso spazio su disco del server di origine e **gli ultimi aggiornamenti installati**, che chiameremo server di destinazione

- una connessione di rete attiva tra i due server

Assicurarsi che il server sorgente consenta il login all'utente root tramite password ed attraverso una chiave SSH.

56.9.1 Sincronizzazione dei file

Lo script di sincronizzazione copia tutti i dati utilizzando rsync su SSH. Se il server di destinazione non dispone di chiavi SSH, lo script genererà una coppia di chiavi RSA per il server destinazione e copierà la chiave pubblica nel server di origine. Tutte le directory escluse dai dati di backup non verranno sincronizzate.

Nella macchina di destinazione, eseguire il seguente comando:

```
screen rsync-upgrade <source_server_name> [ssh_port]
```

In cui

- `source_server_name` è il nome host o l'IP del server origine
- `ssh_port` è la porta SSH del server origine (la porta di default è la 22)

Esempio:

```
screen rsync-upgrade mail.nethserver.org 2222
```

Quando richiesto, inserire la password di root del server origine quindi prepararsi un caffè e aspettare con pazienza.

Lo script non eseguirà alcuna azione sulla macchina di origine e può essere rilanciato più volte.

56.9.2 Sincronizzazione e migrazione

Se impartito con l'opzione `-u`, `rsync-upgrade` eseguirà una sincronizzazione finale e l'upgrade della macchina destinazione.

Esempio:

```
screen rsync-upgrade -u mail.nethserver.org 2222
```

Lo script si incaricherà di:

- chiudere l'accesso ad ogni servizio di rete della macchina sorgente (ad eccezione di SSH ed httpd-admin)
- eseguire gli eventi `pre-backup-config` e `pre-backup-data` nella macchina sorgente
- sincronizzare tutti i dati rimanenti
- eseguire il comando `restore-config` sulla macchina destinazione

Se l'`rsync-upgrade` termina senza perdita della connessione di rete,

1. Disconnettere il ns6 origine dalla rete, per evitare conflitti IP con il server di destinazione
2. Accedere all'interfaccia Server Manager e correggere la configurazione di rete dalla pagina *Rete*

Altrimenti, se durante l'`rsync-upgrade` **la connessione di rete viene persa**, è probabile che i server di origine e di destinazione abbiano un **conflitto IP**:

1. Disconnettere il ns6 origine dalla rete,
2. Da una console di root del ns7 lanciare il comando:

```
systemctl restart network
```


3. Quindi accedere nuovamente alla screen:

```
screen -r -D
```

Al termine dell'rsync-upgrade seguire i seguenti passi:

1. In caso di sistema di origine Primary Domain Controller NT (ruolo del server Samba *Primary Domain Controller* – PDC) o di file server standalone (ruolo *Workstation* – WS), fare riferimento alla sezione *Aggiornamento Primary Domain Controller e Workstation*.
2. In caso di sistema origine attestato ad un dominio Active Directory (ruolo server Samba *Active Directory member* – ADS), fare riferimento alla sezione *Aggiornamento membro Active Directory*.
3. Tornare alla CLI e scatenare l'evento `post-restore-data` sulla macchina di destinazione:

```
signal-event post-restore-data
```

4. Controllare nei log di ripristino eventuali occorrenze di messaggi di ERROR o di FAIL:

```
/var/log/restore-data.log  
/var/log/messages
```

5. La compatibilità con la versione 7 di ciascun file contenuto nel percorso `/etc/e-smith/templates-custom/` dovrà essere verificata manualmente.

Avvertimento: La macchina non va riavviata prima di aver scatenato la evento `post-restore-data`.

56.10 Upgrade tramite Upgrade tool (beta)

Il modulo Upgrade tool consente di eseguire un **aggiornamento in-place** di NethServer dalla versione 6 alla versione 7 tramite una procedura automatica.

Fare riferimento alla pagina [Upgrade tool](#) del Manuale Amministratore di NethServer 6.

Licenza della documentazione

La documentazione è distribuita sotto i termini di licenza **Creative Commons - Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)**



Sei libero di:

- **Condividere** — riprodurre, distribuire questo materiale con qualsiasi mezzo e formato
- **Modificare** — remixare, trasformare il materiale e basarti su di esso per le tue opere

Il licenziante non può revocare questi diritti fintanto che tu rispetti i termini della licenza.

Alle seguenti condizioni:

- **Attribuzione** — Devi riconoscere una menzione di paternità adeguata, fornire un link alla licenza e indicare se sono state effettuate delle modifiche. Puoi fare ciò in qualsiasi maniera ragionevole possibile, ma non con modalità tali da suggerire che il licenziante avalli te o il tuo utilizzo del materiale.
- **NonCommerciale** — Non puoi utilizzare il materiale per scopi commerciali.
- **StessaLicenza** — Se remixi, trasformi il materiale o ti basi su di esso, devi distribuire i tuoi contributi con la stessa licenza del materiale originario.

Divieto di restrizioni aggiuntive — Non puoi applicare termini legali o misure tecnologiche che impongano ad altri soggetti dei vincoli giuridici su quanto la licenza consente loro di fare.

Questo è un riassunto in linguaggio accessibile a tutti (e non un sostituto) della licenza. La licenza completa è accessibile a: <http://creativecommons.org/licenses/by-nc-sa/4.0/>

La documentazione sull'architettura deriva dal progetto SME Server e concessa con licenza GNU Free Documentation 1.3 (<http://www.gnu.org/copyleft/fdl.html>). Si veda <http://wiki.contribs.org/> per la documentazione originale.

List of NethServer 7 ISO releases

Each subsection corresponds to an upstream ISO release. See also the [ISO releases](#) on Developer's manual.

58.1 7.8.2003

- 2020-05-05 [final](#)

58.2 7.7.1908

- 2019-10-07 [final](#)

58.3 7.6.1810

- 2018-12-17 [final](#)
- 2018-12-10 [beta2](#)

58.4 7.5.1804

- 2018-06-11 [final](#)
- 2018-05-31 [rc](#)
- 2018-05-21 [beta](#)

58.5 7.4.1708

- 2017-10-26 `final` - GA 2017-10-30
- 2017-09-21 `beta1`

58.6 7.3.1611

- 2017-07-31 `update 1`
- 2017-01-30 `final` - GA 2017-02-08
- 2017-01-18 `rc4`
- 2016-12-16 `rc3`

58.7 7.2.1511

- 2016-11-09 `rc2`
- 2016-10-18 `rc1`
- 2016-09-02 `beta2`
- 2016-07-12 `beta1`
- 2016-05-23 `alpha3`
- 2016-02-12 `alpha2`

Public issue trackers

List of public issue trackers related to NethServer.

- NethServer 7: <https://github.com/NethServer/dev/issues>
- NethServer 6: <http://dev.nethserver.org/projects/nethserver/issues>
- NethServer Enterprise: <https://github.com/nethesis/dev/issues>
- CentOS: <https://bugs.centos.org/>
- Red Hat: <https://bugzilla.redhat.com>

CAPITOLO 60

Index

Il servizio chat utilizza il protocollo standard Jabber/XMPP. Vedi anche [Chat](#).

Interfaccia web di amministrazione Il server Jabber è dotato di un'interfaccia web amministrativa il cui accesso è consentito ai membri del gruppo jabberadmins.

Federation (S2S) XMPP consente ai server di intercomunicare tra loro, formando una rete IM globale «federata».

Massima velocità trasferimento file Limita la massima velocità per il trasferimento file al valore in Byte/secondo

Velocità standard di trasferimento file Limita la velocità standard per il trasferimento file al valore in Byte/secondo

Windows file server

Vedere anche *Cartelle condivise*

Workgroup/Nome dominio NetBIOS Il valore può essere modificato solo con se il provider account è LDAP e definisce il nome del gruppo di lavoro di Windows visibile dal pannello Risorse di rete nei sistemi Windows. Con l'account provider Active Directory il valore è determinato dal dominio a cui il server è attestato

Quando un nuovo file o directory viene creato in una cartella condivisa Stabilisce chi possiede un file o una directory appena creati: il creatore della risorsa o il proprietario della directory che contiene la nuova risorsa (nota anche come directory principale)

Concedere il controllo completo sulle home directory al gruppo Domain Admins (home\$ share) Permetti ai membri del gruppo `Domain Admins` di collegare la condivisione nascosta `home$` e concede loro l'accesso amministrativo a qualsiasi cartella home

Concede il pieno controllo sulle cartelle condivise al gruppo Domain Admins Consente ai membri del gruppo `Domain Admins` di connettere qualsiasi cartella condivisa e concedere loro l'accesso amministrativo sul suo contenuto

Questa pagina configura determinati paths e nomi di Virtual Host in Apache per essere offerti inoltrando la richiesta Web originale a un altro URL. Vedi anche *Reverse proxy*.

63.1 Creare /Modificare

Nome L'URL **path name** o il **virtual host name** (FQDN di un host). Un nome di percorso corrisponderà a URL come `http://somehost /<path name>/ ... ```, mentre un nome di un virtual host corrisponderà a un URL come ```http: //<virtual host name>/` Gli URL corrispondenti vengono inoltrati a *Target URL*.

Accesso dalle reti CIDR Limita l'accesso dall'elenco fornito di reti CIDR. Gli elementi devono essere separati con una «,» (virgola).

Certificato SSL / TLS Seleziona un certificato compatibile con il nome dell virtual host

Richiede una connessione crittografata SSL Se abilitato, è possibile accedere al percorso dell'URL o al nome dell' virtual host solo con una connessione SSL/TLS.

URL di destinazione L'URL in cui è inoltrata la richiesta originale. L'URL è formato come `<scheme>://<hostname>:<port>/<path>`.

Accetta il certificato SSL non valido dalla destinazione Se il *Target URL* ha lo schema `https`, accetta il suo certificato anche se non è valido.

Forward HTTP «Host» intestazione a destinazione Se abilitata, questa opzione passerà l'header «Host» HTTP dalla richiesta in entrata all'host proxy, invece del «hostname» specificato nel campo *Target URL* field.

63.2 Eliminare

Rimuove la voce selezionata.

Groupware SOGo

Vedere anche *SOG*.

Abilitazione CalDAV e CardDAV CalDAV consente agli utenti di accedere e condividere i dati del calendario presenti su un server. CardDAV consente agli utenti di accedere e condividere i contatti presenti su un server.

Abilitazione Microsoft ActiveSync ActiveSync è un'app per la sincronizzazione di dati mobili (e-mail, calendario, attività, contatti) sviluppata da Microsoft.

Consente agli utenti di aggiungere altri account IMAP Consente agli utenti di aggiungere altri account IMAP che saranno visibili dall'interfaccia di SOGo Webmail.

Amministratori Elenco degli utenti con privilegi amministrativi su tutti i dati utente.

Notifiche Sono disponibili diversi tipi di notifiche (basate su email). E' possibile attivarle in base alle proprie esigenze.

Rende raggiungibile SOGO solo da questo dominio (FQDN) SOGo è accessibile per impostazione predefinita da tutti i virtualhost del server, se si specifica qui un nome di dominio, SOGo sarà utilizzabile solo da questo nome di dominio.

Numero dei processi Questo parametro specifica il numero di istanze di SOGo che verranno generate per gestire più richieste contemporaneamente. E' consigliato almeno un worker per dispositivo activesync connesso.

Tempo massimo in secondi Parametro utilizzato per impostare la quantità massima di tempo, in secondi, che SOGo attenderà prima di eseguire un controllo interno per le modifiche dei dati (aggiunta, eliminazione e aggiornamento).

CAPITOLO 65

TLS policy

Livello di sicurezza applicato Configura i servizi di sistema come descritto nella sezione *TLS policy*



A

- account
 - service, 37
- active directory
 - change IP, 35
 - default accounts, 35
- ActiveSync, 99
- alias DNS, 44
- alias: DHCP, 44
- alias: HELO
 - EHLO, 70
- alias: PXE, 44
- alias: Trivial File Transfer Protocol
 - TFTP, 46
- allarmi, 164
- always send a copy
 - email, 62, 72
- anti-spam, *vedi antispam*
- anti-virus, *vedi antivirus*
- antispam
 - email, 64
- antivirus
 - email, 64
- applicazione, 28
- archivi di file, 63
- Asterisk, 195
- attachment
 - email, 63

B

- backup dei dati, 75
- backup della configurazione, 75
- bcc
 - email, 62, 72
- binding IP/MAC, 153
- blacklist, 209
 - email, 65
- bridged, 178

C

- CentOS
 - installation, 15
- change IP
 - active directory, 35
- chat, 129, 265
- Collectd, 175
- compatibility
 - hardware, 11
- complessità password, 39
- Connettore POP3, 127
- custom
 - quota, email, 67
 - spam retention, email, 68

D

- default accounts
 - active directory, 35
- delivery
 - email, 62
- device Android, 99
- DHCP, 44, 45
- disclaimer
 - email, 62
- DNS, 43
- DNSBL, 64
- domain
 - email, 62
- DPI, 147
- DROP, 147
- Duplicity, 86, 93
- Dynamic Host Configuration Protocol, 44

E

- email
 - always send a copy, 62, 72
 - antispam, 64
 - antivirus, 64
 - attachment, 63

- bcc, 62, 72
- blacklist, 65
- custom quota, 67
- custom spam retention, 68
- delivery, 62
- disclaimer, 62
- domain, 62
- filter, 63
- HELO, 70
- hidden copy, 62, 72
- internal visibility, 69
- legal note, 62
- local network only, 69
- master user, 68
- message queue, 71
- migration, 246
- private internal, 69
- queue, 69
- relay, 62, 70
- retries, 71
- signature, 62
- size, 71
- smarthost, 70
- spam retention, 68
- spam training, 64
- whitelist, 65

email address, 69

encryption

- file system, 13

EveBox, 164

F

- fax, 141
- file system
 - encryption, 13
- filter
 - email, 63
- filtro contenuti, 159
- firewall, 145
- FreePBX, 195
- FTP, 185
 - jail, 56
- FTP server, 53

G

- gateway, 145
- gestione banda, 151
- Getmail
 - software, 128
- Google Translate, 160

H

- hardware
 - compatibility, 11

- requirements, 11
- HELO
 - email, 70
- hidden copy
 - email, 62, 72
- HTTP, 51, 166
- HTTPS, 51

I

- imap
 - port, 211
- imaps
 - port, 211
- impersonare, 117
- impostazioni, 27
- installare, 11
- installation, 9
 - CentOS, 15
 - ISO, 12
 - USB, 15
 - VPS, 15
- internal
 - email private, 69
- internal visibility
 - email, 69
- Intrusion Prevention System, 161
- iOS device, 99
- IPsec, 180
- ISO
 - installation, 12

J

- Jabber, 129, 265
- jail
 - FTP, 56

L

- l'autenticazione a due fattori, 98
- latenza di rete, 175
- Launcher, 29
- legal note
 - email, 62
- local network only
 - email, 69
- log del firewall, 147
- logrotate, 27

M

- mac address, 152
- mailbox
 - public, 67
 - shared, 67
 - user, 66
- master, 137

master user
 email, 68
 message queue
 email, 71
 migration, 244
 email, 246
 modem virtuale, 141

N

NAT 1:1, 150
 net2net, 177
 Nextcloud, 181

O

oggetti firewall, 152
 Outlook, 121

P

password, 38
 peso, 148
 PHP, 53
 ping, 175
 policy, 146
 pop3
 port, 211
 pop3s
 port, 211
 port
 imap, 211
 imaps, 211
 pop3, 211
 pop3s, 211
 smtp, 211
 smtps, 211
 port forward, 149
 Preboot eXecution Environment, 44
 private
 internal, email, 69
 protocolli CalDAV e CardDAV, 100
 proxy web, 155
 pseudonym, 69
 PST, 121
 public
 mailbox, 67
 PXE, 44

Q

queue
 email, 69
 quota
 email custom, 67

R

regole, 146

REJECT, 147
 relay
 email, 62, 70
 report di navigazione web, 157
 requirements
 hardware, 11
 Restic, 87
 retries
 email, 71
 reverse proxy, 53, 165
 roadwarrior, 177
 Roundcube, 95
 routed, 178
 rsync, 87

S

S2S, 129
 scadenza password, 40
 score
 spam, 64
 service
 account, 37
 servizio di rete, 26
 SFTP, 27
 shared
 mailbox, 67
 shared folder, 168
 signature
 email, 62
 Sistema, 25
 size
 email, 71
 Slack, 133
 slave, 137
 smarthost
 email, 70
 smtp
 port, 211
 smtps
 port, 211
 SNMP, 189
 software
 Getmail, 128
 software di terze parti, 243
 spam, 64
 score, 64
 spam retention
 email, 68
 email custom, 68
 spam training
 email, 64
 SSH, 27
 statistiche, 175
 status, 25

storage, 26
strong, 39
Suricata, 161

T

team chat, 133
TFTP, 46
time conditions, 152
Time machine, 87
topologia p2p, 179
topologia subnet, 178
traffic shaping, 151
tunnel, 177

U

upgrade, 248
UPS, 137
USB
 installation, 15
user
 mailbox, 66

V

virtual hosts, 51, 166
virtual machines, 196
VPN, 177
VPS
 installation, 15

W

WAN, 148
WAN priority, 179
webmail, 95
whitelist
 email, 65

X

XMPP, 129, 265

Z

zone, 152