Manuale del cliente

Esapanel

Esalogica

15/11/2026

Indice

Primi passi....5
Entrare nel pannello....5
Com'è fatto il pannello....5
L'aiuto nel pannello....6
Una subscription sospesa o disattivata....6
Il vostro account....7
Profilo....7
Secondo fattore....7
Sessioni....8
Utenti e ruoli....9
Gli utenti....9
I ruoli....10
I dati aziendali....10
Le subscription....12
L'elenco delle subscription....12
La pagina di una subscription....12
I consumi....13
Lo stato della subscription....13
I backup della configurazione....14
La pagina Backup....14
Fare una copia adesso....14
La cifratura....14
La pianificazione....14
Ripristinare....15
Scaricare ed eliminare....16
Le notifiche....17
Chi decide chi riceve....17
Le email che potete ricevere....17
Se un avviso non arriva....18
Inviare i log al pannello....19
1. Introduzione....19
2. Dove trovare i valori....19
3. Le porte di ricezione....20
4. Aggiungere un apparato....21
5. Server Windows....23
6. Server Linux....24
7. Router, firewall e altri apparati....26
8. Controllare che i log arrivino....27

9. Problemi frequenti....29
Inviare i log da MikroTik....31
1. Che cosa riceve il pannello....31
2. Aggiungere il MikroTik nel pannello....31
3. L'invio dei log....31
4. Le regole del firewall....32
5. Controllare che i log arrivino....32
6. Problemi frequenti....32
Inviare i log da pfSense e OPNsense....33
1. Che cosa riceve il pannello....33
2. Aggiungere il firewall nel pannello....33
3. pfSense....33
4. OPNsense....34
5. Controllare che i log arrivino....35
6. Problemi frequenti....35
Gli apparati e la quarantena....36
La lista degli apparati....36
La pagina di un apparato....36
La quarantena....37
I codici degli agenti e dei link....38
Le porte 514 e 6514....38
Cercare e leggere i log....39
Cercare....39
I campi dell'evento....39
Le interruzioni della ricezione....39
I nomi degli indirizzi....39
Scaricare....40
Dove sono i log più vecchi....40
Avvisami se si ripete....40
Gli avvisi sugli eventi....41
Gli episodi....41
Le regole....41
Le vostre regole....42
Le eccezioni....43
Report e analisi....44
L'analisi....44
I report....44
Importare log da file....46
Come funziona....46
1. Inviare i file....46

2. Che cosa contengono i file....47
3. Le vostre scelte....47
Da sapere....47
Togliere un'importazione....47
Archivi e backup dei log....48
L'archivio dei log....48
I backup della subscription....48
La copia fuori sede....50
1. Introduzione....50
2. Le pagine della subscription....50
3. Lo spazio e dove collegarsi....51
4. Aggiungere un account....51
5. Collegare i programmi....52
6. Cifrare le copie....53
7. Gestire un account....53
8. Cartelle condivise....53
9. Controllare che le copie arrivino....54
10. I report....54
11. Quando lo spazio finisce....55
12. Subscription sospesa o eliminata....55
13. Problemi frequenti....55
14. Per amministratori e reseller....56
Host e check....57
Dove si trova....57
Aggiungere un host....57
Aggiungere i check....57
Gli stati....58
La pagina di un host....58
I problemi....59
Gli avvisi....59
Downtime e disponibilità....60
Che cosa succede durante un downtime....60
Pianificare un downtime....60
Tutti i downtime....60
La disponibilità....60
I report DMARC....62
I domini....62
Come arrivano i report....62
Leggere i report....63

Come usare il pannello Esapanel e i servizi della vostra subscription.

Primi passi

Il pannello Esapanel è il posto dove trovate i servizi che avete acquistato, le vostre **subscription**, e dove gestite gli utenti della vostra azienda. Questa pagina spiega come entrare, come è fatto il pannello e dove trovare aiuto.

Entrare nel pannello

L'indirizzo del pannello ve lo comunica il fornitore del servizio. Può essere un nome con il suo marchio, ad esempio `pannello.example.com`.

Nella pagina **Accedi** scrivete il **Nome utente** e la **Password** e premete **Accedi**. **Ricordami** fa ricordare l'accesso al browser: usatelo solo su un computer vostro.

Il primo accesso

Quando un amministratore della vostra azienda vi crea un utente, può:

- inviarvi un'email con un link per scegliere la password: aprite il link, scegliete la password e confermatela con **Salva la password**. Fino ad allora il vostro utente risulta **Invitato**;
- oppure impostare lui la password e comunicarvela.

Il nome utente è quello che vi ha comunicato chi ha creato l'utente.

Password dimenticata

Nella pagina **Accedi**, **Password dimenticata?** apre **Reimposta la password**: scrivete l'**Indirizzo email** del vostro account e premete **Invia il link**. L'email contiene un link per scegliere una nuova password.

Il secondo fattore

Se avete attivato il secondo fattore (vedi Il vostro account), dopo la password il pannello chiede il **Codice** che mostra in quel momento l'app di autenticazione del telefono. Senza il telefono, **Non hai il telefono? Usa un codice di recupero** permette di entrare con uno dei codici di recupero.

Troppi tentativi

Dopo troppi tentativi sbagliati il pannello chiede di aspettare prima di riprovare, e dice quanti secondi. Se l'accesso resta inattivo troppo a lungo, il pannello chiede di accedere di nuovo.

Uscire

Esci, in alto a destra, chiude la sessione. Su un computer condiviso uscite sempre alla fine del lavoro.

Com'è fatto il pannello

Il menu

Il menu sta a sinistra. Su un telefono si apre con il pulsante **Menu**, in alto. Le voci che un cliente può vedere sono:

Gruppo	Voce	Che cosa contiene
	Home	La pagina iniziale
Servizi	**Subscription**	Le vostre subscription, con i servizi di ciascuna (vedi Le subscription)
Organizzazione	**Utenti**	Le persone della vostra azienda che usano il pannello (vedi Utenti e ruoli)

Gruppo	Voce	Che cosa contiene
	Ruoli	Che cosa può fare ciascun utente
	Dati aziendali	Ragione sociale, dati fiscali, indirizzo
	Backup	Le copie della vostra organizzazione (vedi I backup della configurazione)
Moduli	**Host**, **Problemi**, **Downtime**	Con UCP (Uptime Check): gli host controllati di tutte le vostre subscription, i problemi aperti, i downtime (vedi Host e check)

Ognuno vede solo le voci che il suo **ruolo** permette: un utente con il ruolo **Revisore**, per esempio, vede le pagine ma non può modificarle. Se vi manca una voce che vi serve, chiedete a un amministratore della vostra azienda.

La pagina iniziale

Home apre il **Cruscotto**, con il benvenuto. Da qui si passa alle subscription con **Servizi › Subscription**.

Il vostro account

In alto a destra c'è il vostro nome utente: apre le pagine del vostro account, cioè profilo, secondo fattore e sessioni (vedi Il vostro account).

L'aiuto nel pannello

Il pannello spiega le sue pagine da solo, in due modi.

- **Aiuto**, in alto, con il punto interrogativo: apre **Informazioni su questa pagina**, una spiegazione breve di che cosa fa la pagina che state guardando e dei suoi pulsanti. In fondo, sotto **Serve assistenza?**, ci sono i contatti di assistenza del vostro fornitore.
- Il **punto interrogativo piccolo** accanto a un campo (**Che cos'è?**) spiega quel campo.

Questo manuale descrive le stesse pagine in modo più ampio, con il percorso per arrivarci e i casi tipici. Per i dettagli di una pagina, l'aiuto del pannello è sempre aggiornato alla versione installata.

Una subscription sospesa o disattivata

Se una subscription è **Sospesa** o **Disattivata**, le pagine dei suoi servizi non si aprono e il pannello mostra il motivo. Una subscription sospesa per aver superato un limite del piano torna attiva da sola quando il consumo rientra. Negli altri casi chiedete a chi vi fornisce il servizio. Gli stati sono spiegati in Le subscription.

Il vostro account

Ogni persona che usa il pannello ha il suo account. Le pagine dell'account si aprono dal vostro nome utente, in alto a destra, e sono tre: **Profilo**, **Secondo fattore** e **Sessioni**.

Quello che cambiate qui vale solo per voi. I dati dell'azienda, comuni a tutti gli utenti, sono in **Organizzazione › Dati aziendali** (vedi Utenti e ruoli).

Profilo

Campo	A che cosa serve
Nome utente	Il nome con cui accedete. Lo cambia solo un amministratore della vostra azienda
Nome	Il vostro nome, come lo vedono gli altri utenti
Cellulare	Facoltativo. Lo vede chi gestisce gli utenti della vostra azienda e il vostro fornitore. Per ora il pannello non vi manda messaggi
Fuso orario	Gli orari che il pannello vi mostra, e l'ora delle pianificazioni dei backup che salvate
Lingua	La lingua del pannello e delle email che ricevete
Palette dei colori	I colori del pannello, solo per voi

Premete **Salva il profilo** per salvare.

Scegliete il fuso orario della sede in cui lavorate: con un fuso sbagliato gli orari dei log e dei backup sembrano spostati.

Indirizzo email

L'indirizzo che riceve il link per reimpostare la password. Per cambiarlo scrivete il nuovo indirizzo e la **Password attuale**, poi **Cambia l'email**.

Password

Scrivete la **Password attuale**, la **Nuova password** e **Conferma la nuova password**, poi **Cambia la password**. Cambiare la password chiude tutte le altre sessioni: i dispositivi su cui avevate fatto l'accesso chiedono di accedere di nuovo.

Un amministratore della vostra azienda può dare a un ruolo il permesso di cambiare i dati del profilo ma non password ed email: in quel caso chiedete a lui.

Secondo fattore

Con il secondo fattore l'accesso chiede, oltre alla password, un codice di sei cifre generato da un'app sul telefono. Chi scopre la vostra password non può entrare senza il vostro telefono. È la protezione più utile che potete dare al vostro account.

Vi serve un'app di autenticazione, come Google Authenticator, Microsoft Authenticator o FreeOTP.

Attivarlo

1. In **Secondo fattore** scrivete la **Password attuale** e premete **Attiva**.

2. Inquadrate il codice QR con l'app. Se non potete inquadrarlo, inserite nell'app la **Chiave** mostrata sotto.
3. Scrivete il **Codice** che l'app mostra in quel momento e premete **Conferma**.

Finché non confermate il codice, l'accesso non cambia. Se il codice non viene accettato, controllate che l'ora del telefono sia giusta.

I codici di recupero

Quando il secondo fattore è attivo, il pannello mostra i **Codici di recupero**, una sola volta. Ognuno vi fa entrare una volta senza il telefono. Conservateli in un posto sicuro, lontano dal telefono, per esempio stampati o in un gestore di password.

La pagina dice quanti codici vi restano. **Genera codici nuovi** ne crea una serie nuova: quelli di prima smettono di funzionare.

Disattivarlo

Disattiva il secondo fattore: l'accesso torna a chiedere solo la password. Per riattivarlo dovrete inquadrare un nuovo codice QR.

Telefono perso

Se avete perso il telefono, entrate con un codice di recupero, disattivate il secondo fattore e attivatelo di nuovo con il telefono nuovo.

Se avete perso anche i codici di recupero, chiedete a un amministratore della vostra azienda: può disattivare il vostro secondo fattore dalla pagina del vostro utente. Per l'account principale dell'azienda (**Owner**) chiedete al vostro fornitore.

Sessioni

Sessioni aperte elenca i dispositivi e i browser su cui avete fatto l'accesso, con l'**Indirizzo IP** e l'**Ultima attività**. La sessione che state usando è segnata come **Questa sessione**.

- **Chiudi** chiude una sessione che non riconoscete.
- **Chiudi tutte le altre sessioni** chiude tutte le sessioni tranne quella che state usando, per esempio dopo aver usato un computer condiviso.

Se pensate che qualcun altro conosca la vostra password, chiudete le sessioni e cambiate la password dal **Profilo**.

Utenti e ruoli

Più persone della stessa azienda possono usare il pannello, ognuna con il proprio account. Ogni utente ha un **ruolo**, che decide che cosa può vedere e fare. Utenti, ruoli e dati dell'azienda sono nel gruppo **Organizzazione** del menu.

Per gestire utenti e ruoli serve un ruolo che lo permetta, come **Owner** o **Amministratore**.

Gli utenti

Organizzazione › **Utenti** elenca le persone della vostra azienda che usano il pannello, con **Ruolo**, **Stato** e **Ultimo accesso**.

L'**Owner** è l'account principale dell'azienda. Non si modifica da questa pagina: l'Owner cambia i propri dati dal suo profilo, e il vostro fornitore può cambiare l'Owner.

Aggiungere un utente

Nuovo utente chiede:

Campo	Che cosa scrivere
Nome utente	Il nome con cui la persona accede
Nome	Il nome della persona
Email	Il suo indirizzo: riceve l'invito e i link per reimpostare la password
Cellulare	Facoltativo
Ruolo	Che cosa può fare (vedi sotto)
Password	Come la persona avrà la password

Per la password ci sono due modi:

- **Invia un link per scegliere la password**: la persona riceve un'email e sceglie la password al primo accesso. Fino ad allora risulta **Invitato**. È il modo da preferire: la password la conosce solo lei.
- **Imposta ora la password**: la scrivete voi e la comunicate alla persona.

Gli stati di un utente

Stato	Che cosa vuol dire
Attivo	Accede normalmente
Invitato	Non ha ancora scelto la password
Sospeso	Non può accedere, per esempio durante un'assenza
Disattivato	Non può accedere

Un utente sospeso o disattivato viene fermato alla pagina successiva, anche se aveva una sessione aperta.

Modificare un utente

Modifica, sulla riga di un utente, apre i suoi dati, il ruolo e lo stato.

- **Invia di nuovo l'invito**, per un utente **Invitato** che non ha ricevuto l'email o l'ha persa.
- **Disattiva il secondo fattore**, per un utente che ha perso il telefono e i codici di recupero: entra con la sola password e può riattivarlo dal suo account.

- **Elimina l'utente**: l'utente non può più accedere. Non si annulla.

Non potete cambiare il ruolo o lo stato del vostro account: deve farlo un altro amministratore.

Quando una persona lascia l'azienda, eliminate il suo utente o disattivatelo: non lasciate account attivi di chi non lavora più con voi.

I ruoli

Un ruolo è un insieme di funzioni, ognuna **Concesso** o **Negato** per intero: per esempio **CSP · Vedere i log**, **CSP · Gestire gli apparati e la quarantena** o **Gestire utenti e ruoli**. **Organizzazione › Ruoli** mostra i ruoli e quanti utenti hanno ciascuno.

I ruoli di sistema

Sono uguali per tutti i clienti e non si modificano:

Ruolo	Che cosa può fare
Owner	L'account principale, con tutte le funzioni
Amministratore	Tutte le funzioni
Operatore	Lavora sui servizi, ma senza eliminazioni, esportazioni e ripristini
Revisore	Solo consultazione, oltre alla gestione del proprio account

Le funzioni di questi ruoli si aggiornano con le nuove versioni del pannello.

I ruoli personalizzati

Se un ruolo di sistema non va bene, createne uno vostro:

- **Duplica**, su un ruolo di sistema, crea una copia da modificare;
- oppure **Nuovo ruolo**, con un **Nome**, una **Descrizione** e l'**Accesso alle funzioni**.

Potete concedere solo le funzioni che avete voi. Le funzioni segnate come *comprende operazioni non reversibili*, come eliminazioni e ripristini, vanno date solo a chi ne ha davvero bisogno. Ogni ruolo può sempre vedere e modificare il proprio account.

Una modifica a un ruolo vale subito per tutti gli utenti che lo hanno. Un ruolo assegnato a qualche utente non si può eliminare: date prima un altro ruolo a quegli utenti.

Esempio: chi guarda solo i log

Per un consulente che deve consultare i log ma non cambiare nulla, il ruolo **Revisore** basta. Se deve anche scaricarli, duplicate **Revisore**, concedete nella copia la funzione **CSP · Esportare i log** e date al consulente il nuovo ruolo.

I dati aziendali

Organizzazione › Dati aziendali contiene i dati della vostra azienda, comuni a tutti i suoi utenti: **Ragione sociale**, **Partita IVA**, **Codice fiscale**, **Referente**, **Email di contatto**, **Telefono**, **Fax**, **Sito web** e l'indirizzo.

Tutti gli utenti li vedono. Solo gli amministratori dell'account possono modificarli, con **Salva i dati aziendali**.

- La **Partita IVA** si scrive nella forma internazionale, con il codice del paese davanti, per esempio `IT01234567890`. Se la scrivete senza, il pannello aggiunge il codice del paese scelto.
- **Telefono** e **Fax** prendono il prefisso internazionale scelto accanto al numero.

- Un **Sito web** scritto senza `https://` lo riceve.

Le subscription

Una **subscription** è un servizio che avete acquistato: per esempio la raccolta dei log dei vostri apparati, o lo spazio per le copie fuori sede. Una stessa azienda può avere più subscription, anche dello stesso servizio, per esempio una per sede.

Ogni subscription nasce da un **piano**, che il vostro fornitore sceglie con voi: il piano stabilisce quali servizi comprende e i suoi **limiti**, come il numero di apparati o lo spazio. Piano e limiti li cambia il fornitore. Voi usate i servizi e tenete d'occhio i consumi.

L'elenco delle subscription

Servizi › **Subscription** elenca le vostre subscription, con:

Colonna	Che cosa mostra
Nome	Il nome della subscription, utile quando ne avete più di una
Piano	Il piano da cui nasce, e se **Segue il piano** o è **Personalizzata**
Moduli	I servizi che comprende
Dal	Da quando è attiva
Stato	**Attiva**, **Sospesa** o **Disattivata**

Una subscription **Personalizzata** ha alcuni valori diversi dal suo piano, concordati con il fornitore.

Il nome della subscription apre la sua pagina.

La pagina di una subscription

In cima c'è il nome della subscription. Sotto, una **tessera** per ogni cosa che potete vedere o fare: ogni tessera apre una pagina.

Le tessere dipendono dai servizi della subscription e dal vostro ruolo. Un utente con un ruolo limitato vede meno tessere.

Le tessere dei servizi

Servizio	Tessere
CSP (Central Syslog), la raccolta dei log	**Log**, **Analisi**, **Report**, **Avvisi sugli eventi**, **Apparati**, **Backup**, **Archivio log**, **Quarantena**
UCP (Uptime Check), il controllo dei vostri server e servizi	**Host**
WFP (Web File), la copia fuori sede	**Copia fuori sede**, **Account**, **Cartelle condivise**, **Attività**, **Report**
DRP (DMARC Report), i report DMARC dei vostri domini	**DMARC**
LSP (License Server), la licenza di un prodotto	**Licenza**

Alcune tessere mostrano un numero quando c'è qualcosa che vi aspetta. Per esempio, **Quarantena** mostra quanti mittenti attendono una decisione, e **Host** quanti problemi sono aperti.

Ogni servizio ha le sue pagine in questo manuale. Per la raccolta dei log, per esempio, si comincia da Inviare i log al pannello.

Per una subscription di CSP la pagina mostra in alto anche il riquadro **Ricezione dei log**, con il server e le porte su cui gli apparati inviano.

I consumi

La tessera **Consumi** mostra quanto la subscription usa delle risorse che il pannello misura, come il volume mensile dei log o lo spazio dei backup.

- Per ogni risorsa c'è un grafico, con **Ultimi 30 giorni** (un punto al giorno) oppure **Ultimi 12 mesi** (il valore di fine mese).
- La **linea rossa** è il limite del piano, la **linea punteggiata** la soglia di preavviso.
- Il consumo si misura ogni notte per la giornata appena chiusa. Una subscription appena creata non ha ancora storico: il primo punto arriva con la misura della notte.
- **Ricalcola i consumi** misura subito, per esempio dopo aver cancellato vecchi backup per liberare spazio. Dopo un ricalcolo bisogna aspettare un poco prima di farne un altro.

Vicino al limite e oltre il limite

Quando una risorsa raggiunge la soglia di preavviso, il pannello manda un avviso una volta. Quando supera il limite, manda un avviso ogni giorno finché resta oltre. Chi riceve questi avvisi lo decide il vostro fornitore (vedi Le notifiche).

Che cosa succede oltre il limite dipende dal piano. Con alcuni piani la subscription viene **sospesa** finché il consumo non rientra: il servizio continua dietro le quinte (per esempio i log continuano ad arrivare), ma le sue pagine restano chiuse. Torna attiva da sola appena il consumo rientra, anche dopo un ricalcolo.

Per rientrare potete liberare spazio, per esempio eliminando backup vecchi, oppure chiedere al fornitore un piano più ampio o un'aggiunta al piano.

Lo stato della subscription

Stato	Che cosa vuol dire per voi
Attiva	Funziona normalmente
Sospesa	Vedete la subscription e il suo stato, ma non le pagine dei suoi servizi. Il servizio continua dietro le quinte: i log arrivano e vengono conservati, i controlli continuano. Gli avvisi dei servizi vanno al vostro fornitore invece che a voi
Disattivata	Il servizio è fermo: i log che arrivano vengono scartati, i controlli non girano. Quello che era stato ricevuto prima resta fino alla fine della sua conservazione, e le porte restano alla subscription: quando torna attiva, gli apparati riprendono a inviare senza essere riconfigurati

La sospensione, la disattivazione e la riattivazione le decide il vostro fornitore, salvo la sospensione automatica per un limite superato. Per una subscription sospesa o disattivata, chiedete a chi ve la fornisce.

I backup della configurazione

Un backup della vostra organizzazione è una copia di quello che avete impostato nel pannello: i dati aziendali, gli utenti e i ruoli e, per ogni subscription, il nome, gli apparati, il piano e i limiti. Può contenere anche i **log consultabili** delle subscription. Serve a rimettere le cose com'erano dopo un errore, per esempio un apparato o un utente eliminato per sbaglio.

I backup si trovano in **Organizzazione** › **Backup**. Per farli e ripristinarli serve un ruolo che lo permetta.

Questa pagina riguarda la copia dell'organizzazione. Le copie dei log di una singola subscription di CSP (Central Syslog) sono nella tessera **Backup** della subscription. Per una copia fuori sede di WFP (Web File) il backup contiene i suoi account e le cartelle condivise, non i file.

La pagina Backup

In cima la pagina riassume la situazione:

- **Ultima copia**, con il suo esito;
- **Prossima copia**, con la pianificazione detta in una frase (per esempio: ogni giorno alle 02:00, sempre completa, conserva le ultime 7 copie, sul server), oppure "Nessuna pianificazione: le copie si fanno solo a mano";
- **Spazio**, quello occupato dalle copie.

I pulsanti **Fai una copia adesso** e **Pianificazione** aprono le pagine descritte sotto. La lista **Copie** mostra ogni copia con **Data**, **Tipo**, **Contenuto**, **Chiave** e **Stato**, e i pulsanti **Scarica**, **Ripristina** ed **Elimina**.

Fare una copia adesso

Fai una copia adesso prepara una copia con tutto già scelto: basta confermare. La copia si fa in background: la lista mostra quando è pronta (**In coda**, **In corso**, **Completato**) e un'email ne dice l'esito.

Nelle **Opzioni avanzate** potete cambiare la **Cifratura** (vedi sotto) e l'indirizzo che riceve l'email con l'esito (**Invia l'esito a**).

La cifratura

Scelta	Che cosa vuol dire
Con la chiave del server	Il pannello cifra e decifra da solo. Il download arriva decifrato e il ripristino è automatico. È la scelta normale
Con la mia chiave personale age	Solo la vostra chiave privata apre il backup, nemmeno il server può leggerlo. Scrivete la **Chiave pubblica age** (inizia con `age1`). Se perdete la chiave privata, il backup è perso
In chiaro	Nessuna cifratura: chi ottiene il file lo legge, log compresi

La chiave personale serve a chi vuole conservare copie che nessun altro, nemmeno chi gestisce il server, può aprire. La chiave si crea con il programma `age`, sul vostro computer. Conservate la chiave privata in un posto sicuro e separato dalle copie.

La pianificazione

Pianificazione fa le copie da sola.

Campo	Che cosa scegliere
Esegui i backup secondo la pianificazione	Accende la pianificazione
Ogni e **Alle**	**Giorno**, **Settimana** o **Mese**, e l'ora. L'ora è nel fuso orario di chi salva la pianificazione
Un backup completo, poi incrementali con solo i log nuovi	Dopo una copia completa, le successive contengono solo i log nuovi: più piccole e più veloci. **Un nuovo backup completo ogni** settimana o mese
Copie da conservare	Quante copie tenere. Le più vecchie vengono eliminate; le copie fatte a mano non vengono mai toccate
Dove	**Sul server**, **Su una destinazione remota**, o **Sul server e su una destinazione remota**

Con gli incrementali una "copia" è un backup completo con gli incrementali che lo seguono. Il ripristino ricostruisce da solo la catena a partire dal completo.

Premete **Salva la pianificazione**.

Le destinazioni remote

Una **destinazione remota** è un vostro server dove la pianificazione copia i backup: un server **SFTP o FTP**, o uno storage compatibile **S3**. Così le copie restano anche fuori dal server del pannello. I file arrivano come sono sul server, cifrati se lo sono, e lo spazio remoto non conta nei vostri limiti.

In **Destinazioni remote**, **Aggiungi una destinazione** chiede il **Nome**, il **Tipo** e i dati di accesso:

- **SFTP o FTP**: **Server**, **Porta**, **Utente**, **Password** oppure **Chiave privata SSH**, la **Cartella**. Con FTP attivate **FTP con TLS (FTPS)** se il server lo supporta: senza TLS la password viaggia in chiaro.
- **S3**: **Bucket**, **Regione**, **Endpoint** (vuoto per Amazon S3), **Chiave di accesso**, **Chiave segreta**; **Indirizzi path-style** per MinIO e alcuni NAS.

Per SFTP il pannello legge l'**impronta** della chiave del server e vi chiede di confermarla: controllatela sul server con `ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub`. Da allora il pannello si collega solo a un server con quell'impronta.

Il pannello prova la destinazione quando la salvate. **Prova** la riprova quando volete; la lista dice se funziona e quando è stata provata. Se una copia non arriva sulla destinazione, il pannello lo segnala e il file resta sul server.

Eliminare una destinazione non elimina le copie già presenti lì, ma il pannello non le raggiunge più.

Ripristinare

Ripristina, sulla riga di una copia, apre una pagina a passi.

1. **Cosa ripristinare**: tutta la copia o una sua parte, per esempio una sola subscription; i log, la configurazione o entrambi. Per i log potete scegliere il periodo (**Log dal** … **al**).
2. **La chiave della copia**, solo per una copia cifrata con la vostra chiave personale: scrivete la chiave privata age (inizia con `AGE-SECRET-KEY-`). Si usa solo per questo ripristino e non viene conservata.
3. **Riepilogo e conferma**: che cosa succede, e la conferma.

Che cosa torna:

- **Log**: tornano quelli mancanti del periodo; quelli ancora nel pannello e quelli arrivati dopo restano.
- **Configurazione**: dati aziendali, utenti, ruoli e apparati tornano com'erano nella copia, e quello che è stato aggiunto dopo viene tolto. Per questo il pannello chiede di confermare con "Ho capito che la configurazione torna quella del ...".

Il ripristino si esegue in background; l'email e la lista ne dicono l'esito.

Prima di ripristinare la configurazione, pensate a quello che è cambiato dopo la copia: un utente creato dopo, per esempio, sparisce. Se vi serve solo recuperare dei log, ripristinate solo i log.

Scaricare ed eliminare

Scarica salva la copia sul vostro computer. Una copia con la chiave del server arriva decifrata.

Elimina la cancella per sempre. Per una copia completa con incrementali, elimina anche gli incrementali che la seguono.

Le notifiche

Il pannello manda un'email quando succede qualcosa che vi riguarda: una risorsa vicina al limite, un backup fallito, un apparato che smette di inviare log, un server che non risponde. Questa pagina dice quali email potete ricevere e chi le riceve.

Chi decide chi riceve

Chi riceve ciascun avviso lo decide il vostro **fornitore**, per tutti i suoi clienti: può mandarlo a voi, a sé stesso, o ad altri indirizzi, per esempio quello della sua assistenza. Anche i testi delle email sono i suoi. Voi non cambiate queste impostazioni dal pannello: se volete ricevere un avviso che non vi arriva, o smettere di riceverne uno, chiedete al fornitore.

Quando un avviso è per "il cliente", arriva all'account principale della vostra azienda (**Owner**).

Alcune email vanno a un indirizzo preciso e non dipendono da queste impostazioni:

- il link per reimpostare la password va all'utente che lo ha chiesto;
- l'esito di un backup o di un ripristino va all'indirizzo scritto quando lo avete chiesto o pianificato.

Voi decidete invece **quando** scattano alcuni avvisi dei servizi: per esempio **Avvisa se tace da** su un apparato di CSP (Central Syslog), o le regole degli **Avvisi sugli eventi**.

Le email arrivano nella lingua scelta nel profilo di chi le riceve, con il marchio e la firma del vostro fornitore.

Le email che potete ricevere

Il pannello

Evento	Quando arriva
Una risorsa di una subscription è vicina al limite	Una volta, quando il consumo raggiunge la soglia di preavviso
Una risorsa di una subscription è oltre il limite	Ogni giorno, finché il consumo resta oltre
Una subscription è sospesa per aver superato un limite	Una volta, quando viene sospesa
Una subscription sospesa per un limite superato è di nuovo attiva	Una volta, quando il consumo rientra
Un backup è fallito	A ogni backup non riuscito
Esito di un backup o di un ripristino	All'indirizzo indicato nella richiesta
Reset della password	All'utente che l'ha chiesto

CSP (Central Syslog)

Evento	Quando arriva
Un avviso sugli eventi dei log; ancora in corso; finito	Secondo le regole della tessera **Avvisi sugli eventi**
Un report dei log è pronto	Quando è pronto un report giornaliero, settimanale o mensile
Una sorgente ha smesso di inviare log; invia di nuovo	Secondo **Avvisa se tace da** di ogni apparato

UCP (Uptime Check)

Evento	Quando arriva
Un host è down; è di nuovo up	Quando un host smette di rispondere e quando torna
Un check ha un problema; è di nuovo OK	Quando un controllo cambia stato
Un problema è ancora aperto	Come promemoria, finché il problema resta aperto

WFP (Web File)

Evento	Quando arriva
Un account non carica da troppo tempo; carica di nuovo	Quando un apparato smette di mandare le sue copie, e quando riprende
Una copia è molto più piccola del solito	Quando una copia sembra incompleta
Un caricamento ha sostituito o cancellato gran parte dei file di un account	Può essere il segno di un ransomware o di un errore
Un report della copia fuori sede è pronto	Ogni settimana e ogni mese
Lo spazio ha superato il limite; è rientrato	Oltre il limite gli account vanno in sola lettura

Ogni servizio spiega i suoi avvisi nelle sue pagine di questo manuale.

Se un avviso non arriva

1. Controllate la cartella della posta indesiderata.
2. Controllate l'indirizzo email del destinatario: per l'Owner è nel suo **Profilo**.
3. Chiedete al fornitore: decide lui chi riceve ogni avviso, e può controllare l'elenco delle notifiche inviate.

Inviare i log al pannello

1. Introduzione

Che cosa fa il servizio

CSP (Central Syslog) di Esapanel raccoglie i **log** dei vostri server e dei vostri apparati di rete: accessi riusciti e falliti, errori, avvisi, eventi dei firewall e delle VPN. Li conserva nella vostra **subscription**, ve li fa cercare, analizzare e riassumere nei report, anche come supporto alla documentazione delle misure di sicurezza richieste dalla direttiva NIS2.

I log arrivano con il protocollo **syslog**, lo standard che quasi tutti gli apparati di rete conoscono. Per i server Windows e Linux c'è l'**agente Esapanel**, un piccolo programma che legge gli eventi del server e li invia al pannello.

A chi si rivolge questa guida

Al personale IT dell'azienda, o al fornitore che ne gestisce i sistemi. Serve sapere come si configura un server o un firewall; non serve conoscere Esapanel.

La guida tratta solo l'**invio dei log**: come configurare i server e gli apparati e come controllare che i log arrivino.

Che cosa serve

- Una **subscription** CSP attiva.
- Un utente del pannello che possa aprire la pagina **Apparati** della subscription (nel pannello: la subscription, poi la tessera **Apparati**).
- L'accesso amministrativo ai server e agli apparati da configurare.
- Che i server e gli apparati possano **uscire verso Internet** verso il server del pannello, sulle porte indicate più avanti. Non serve aprire nessuna porta in ingresso.

In questa guida i nomi e gli indirizzi sono esempi (`example.it`, `192.0.2.10`, `203.0.113.10`, `2001:db8::10`). I valori veri della vostra subscription sono nella pagina **Apparati**.

---

2. Dove trovare i valori

Il server e le porte della subscription sono in evidenza nella pagina della subscription, nel riquadro **Ricezione dei log** in alto: **Server**, **Porta in chiaro**, **Porta TLS** e **Porta degli agenti**.

Tutti i valori da inserire negli apparati sono anche nella pagina **Apparati** della subscription, nel riquadro **Invio dei log** in alto:

Campo della pagina	Che cosa contiene	Nella guida
Server	Il nome del server a cui inviare. Se la subscription riceve su un indirizzo dedicato, qui c'è quell'indirizzo	`<server>`
Porta	La porta della subscription, in chiaro	`<porta in chiaro>`
Protocolli	"UDP o TCP, syslog RFC 3164 o RFC 5424"	
Su TLS (cifrato)	Il nome del server e la porta TLS, nella forma `nome:porta`	`<nome del server>` e `<porta TLS>`
Porta degli agenti	Il nome del server e la	`<porta degli agenti>`

Campo della pagina	Che cosa contiene	Nella guida
	porta degli agenti, nella forma `nome:porta`	

Accanto a server e porta il pulsante **Copia** copia il valore.

Le istruzioni di ogni apparato (vedi il capitolo 4) ripetono questi valori, già compilati, e aggiungono il campo **Indirizzo**: l'indirizzo IP del server, per gli apparati che non accettano un nome.

Le porte sono assegnate a ogni subscription e sono diverse da una subscription all'altra: **usate sempre quelle della vostra pagina Apparati**, mai porte prese da altri esempi.

Se la pagina dice "La subscription non ha ancora una porta", la ricezione non è ancora pronta: contattate il fornitore del servizio.

---

3. Le porte di ricezione

Ogni subscription riceve i log su **tre porte**, tutte sullo stesso server.

Porta	Come arrivano i log	Per chi
Porta in chiaro (`<porta in chiaro>`)	UDP o TCP, senza cifratura	Gli apparati che non supportano TLS; rsyslog e NXLog
Porta TLS (`<porta TLS>`, riga **Su TLS (cifrato)**)	TCP con TLS: i log viaggiano cifrati. Il server dimostra il suo nome con il suo certificato; l'apparato non deve presentare un certificato	Router e firewall che supportano syslog su TLS
Porta degli agenti (`<porta degli agenti>`)	TCP con TLS, e l'agente si presenta con un **certificato client** suo	Solo l'agente Esapanel, che la usa da solo

La porta degli agenti non va configurata: l'agente la riceve dal pannello quando si installa. Va solo **consentita in uscita** nel firewall dei server con l'agente, prima dell'installazione: la trovate nel riquadro **Ricezione dei log** e nella pagina **Apparati**.

Quale porta usare

Chi invia	Come	Porta
Server Windows	Agente Esapanel (consigliato)	Sceglie da solo: porta degli agenti
Server Windows	NXLog Community Edition, in alternativa	Porta in chiaro, TCP
Server Linux (Debian, Ubuntu, Red Hat, Rocky, AlmaLinux)	Agente Esapanel (consigliato)	Sceglie da solo: porta degli agenti
Server Linux	rsyslog, in alternativa	Porta in chiaro, TCP
Router o firewall che supporta syslog su TLS	Impostazioni syslog dell'apparato	Porta TLS, con il nome del server
Router o firewall senza	Impostazioni syslog	Porta in chiaro, UDP o

Chi invia	Come	Porta
TLS	dell'apparato	TCP
Switch, access point, NAS, altri apparati	Impostazioni syslog dell'apparato	Porta TLS se la supportano, altrimenti porta in chiaro

Sicurezza, in breve

- **In chiaro:** i log attraversano Internet leggibili da chi si trova sul percorso. Va bene per log poco sensibili o quando l'apparato non offre altro.
- **TLS:** i log viaggiano cifrati e l'apparato verifica di parlare con il server giusto. È la scelta da preferire per la NIS2, che chiede di proteggere i dati in transito.
- **Certificato client (agente):** oltre alla cifratura, il pannello sa con certezza quale agente sta inviando: sulla porta degli agenti entrano solo gli agenti della vostra subscription, ciascuno con il suo certificato.

Condizioni del TLS

- **Usate il nome del server, non l'indirizzo IP.** Il certificato del server porta il suo nome: se l'apparato si collega con l'indirizzo IP, la verifica del certificato fallisce.
- Solo **TCP**: su UDP il TLS non c'è.
- L'apparato deve **fidarsi dell'autorità** che ha emesso il certificato del server e avere l'**orologio giusto**, altrimenti rifiuta il certificato.
- L'**agente Esapanel** usa il TLS da solo quando il certificato del pannello è valido (non autofirmato); non c'è niente da configurare.

Porte 514 e 6514 su un indirizzo dedicato

Alcuni apparati non permettono di scegliere la porta e inviano solo sulla porta standard **514** (syslog) o **6514** (syslog su TLS). Per questi casi la subscription può ricevere su un **indirizzo IP dedicato**, assegnato dal fornitore del servizio.

Con un indirizzo dedicato la pagina **Apparati** mostra:

- "Gli apparati possono inviare anche a `<indirizzo dedicato>` sulla porta standard 514": il pulsante **Ricevi anche sulla porta 514** la attiva, **Spegni la porta 514** la spegne;
- la stessa cosa per la **6514**, con **Ricevi anche sulla porta 6514** e **Spegni la porta 6514**.

Sono porte in più: la 514 porta i log alla porta in chiaro della subscription, la 6514 alla porta TLS. Le porte della subscription restano aperte. Senza indirizzo dedicato le porte 514 e 6514 non sono disponibili.

Con la 6514 l'apparato si collega all'indirizzo dedicato, ma il certificato porta il **nome del server**: l'apparato deve poter verificare quel nome. Se non ci riesce, usate il nome del server con la porta TLS della subscription.

---

4. Aggiungere un apparato

Il pannello accetta solo i log degli **apparati** della subscription. I log di un mittente che non è fra gli apparati non vanno persi subito: aspettano nella **Quarantena** (vedi il capitolo 8).

L'aggiunta guidata

Nella pagina **Apparati**, il pulsante **Aggiungi apparato** apre tre passi:

1. **Categoria**: "Che cosa vuoi aggiungere?" Server; Router e firewall; Switch e access point; Storage (NAS); Altro apparato.
2. **Modello**: i modelli della categoria (l'elenco è nel capitolo 7). Se il vostro non c'è, scegliete **Altro**.

3. **Nome e istruzioni**: il **Nome dell'apparato**, quello con cui lo riconoscete voi (per esempio "Firewall dell'ufficio"), e come il pannello lo riconosce.

Per i server Windows e per i server Linux con l'agente il terzo passo è diverso: vedete i capitoli 5 e 6.

Per gli altri apparati il terzo passo chiede:

Campo	Che cosa scrivere
Nome dell'apparato	Un nome per voi
Riconosciuto da	Come il pannello riconosce i log dell'apparato (vedi sotto); il pannello propone la scelta adatta al modello
Indirizzo o nome	Il valore corrispondente
Fuso orario	Il fuso orario dell'orologio dell'apparato, per esempio `Europe/Rome`
Avvisa se tace da	Un'email se l'apparato smette di inviare (vedi il capitolo 8)

Poi **Aggiungi e mostra le istruzioni**: l'apparato è registrato e la sua pagina mostra le istruzioni del modello, già compilate con i valori della subscription.

Come un apparato viene riconosciuto

Riconosciuto da	Esempio	Quando usarlo
Indirizzo IP	`203.0.113.10` o `2001:db8::10`	L'indirizzo pubblico **fisso** da cui l'apparato invia. È la scelta normale per router e firewall
Rete	`203.0.113.0/28`	Più indirizzi fissi della stessa rete
Nome DNS	`sede.example.it`	Un indirizzo che cambia, con un nome DNS (anche dinamico) che lo segue: il pannello lo risolve di nuovo periodicamente
Nome apparato	`FW-SEDE`	Il nome che l'apparato scrive in ogni log (il campo HOSTNAME del syslog). È accettato da qualsiasi indirizzo, ma solo sulle porte della vostra subscription: utile per una linea che cambia indirizzo, come una linea di backup
Agente Esapanel		Si iscrive da solo: niente da inserire

Da sapere:

- L'indirizzo è quello **che vede il pannello**, cioè l'indirizzo pubblico della connessione Internet da cui l'apparato esce. Più apparati dietro la stessa connessione (per esempio uno switch e un NAS in ufficio) escono con lo stesso indirizzo: un apparato riconosciuto da quell'indirizzo accetta i log di tutti. Se volete distinguerli, riconoscete ciascuno dal suo **Nome apparato**.

- Il **Nome apparato** è il modo meno rigido: chi conosce il nome e la porta potrebbe inviare log a suo nome. Preferite l'indirizzo IP quando è fisso, o l'agente sui server.
- Per un server Linux con rsyslog il nome nei log è quello che dà il comando `hostname` sul server.

Se la pagina **Apparati** dice "Questa subscription accetta log da qualsiasi sorgente", il vostro piano non controlla i mittenti: tutti i log arrivano, anche senza apparati nella lista.

Il limite degli apparati

Il piano stabilisce quanti apparati può avere la subscription: la pagina **Apparati** mostra il conteggio, per esempio "3 di 10 sorgenti". Ogni apparato conta uno, anche un agente.

Quando il limite è raggiunto, **Aggiungi apparato** scompare e la pagina dice "Il piano consente N sorgenti: rimuovine una, o chiedi un piano più ampio". Per liberare un posto, **Rimuovi** un apparato non più usato: i suoi log successivi andranno nella Quarantena.

Cambiare un apparato

Nella lista, il link **Istruzioni** (o il nome dell'apparato) apre la sua pagina: qui potete cambiare il **Nome dell'apparato** e il **Modello** e rivedere le istruzioni. Nella lista potete cambiare **Fuso orario** e **Avvisa se tace da**, con **Salva**.

---

5. Server Windows

Con l'agente Esapanel (consigliato)

L'agente è un servizio di Windows che legge il registro eventi e invia gli eventi al pannello. Si iscrive da solo nella subscription: non ci sono indirizzi da autorizzare, anche se il server cambia indirizzo o sta dietro un NAT.

Che cosa invia:

- tutto il registro **Sicurezza** (accessi, accessi falliti, account bloccati, utenti e gruppi cambiati);
- gli avvisi e gli errori di **Sistema** e **Applicazione**.

Parte dagli eventi nuovi: lo storico già presente nel registro non viene inviato. Se il pannello non risponde, gli eventi aspettano in una coda sul disco del server e partono quando torna; dopo un riavvio del server l'agente riprende da dove si era fermato.

Installazione:

1. Nella pagina **Apparati**: **Aggiungi apparato**, categoria **Server**, modello **Windows Server**.
2. Scrivete il **Nome dell'apparato** (per esempio "Server di posta") e premete **Mostra i comandi**.
3. Il pannello mostra i comandi PowerShell, con il codice di iscrizione e il nome già inseriti. **Copia i comandi**.
4. Sul server, aprite **PowerShell come amministratore** ed eseguite i comandi. Scaricano l'agente dal pannello in `C:\Program Files\Esapanel`, lo installano come servizio di Windows e lo iscrivono alla subscription.
5. La pagina del pannello resta "In attesa dell'iscrizione dell'agente" e si aggiorna da sola. Quando l'agente si è iscritto mostra "L'agente si è iscritto." con il link **Apri l'apparato**.

L'apparato compare nella lista **Apparati** con il nome scelto, riconosciuto da **Agente Esapanel**.

Il server deve poter raggiungere in uscita:

- l'indirizzo del pannello scritto nel comando (dopo `--panel`), in HTTPS: lo usa per iscriversi e, all'avvio e ogni 6 ore, per chiedere la sua configurazione;
- il server della subscription sulla porta degli agenti (o, se manca il certificato, sulla porta TLS o in chiaro), in TCP.

Il certificato dell'agente. All'installazione l'agente crea una sua chiave, che non lascia mai il server, e ottiene dal pannello un certificato client valido **un anno**. Lo rinnova da solo un mese prima della scadenza. La pagina dell'apparato mostra "L'agente invia su TLS con il suo certificato client, valido fino al …".

Comandi utili

In PowerShell come amministratore:

Comando	Che cosa fa
`& "C:\Program Files\Esapanel\esapanel-agent.exe" status`	Mostra il nome dell'agente, dove invia (server, porta, TLS, scadenza del certificato), che cosa legge e quanti dati aspettano nella coda
`& "C:\Program Files\Esapanel\esapanel-agent.exe" uninstall`	Ferma e toglie il servizio; i dati dell'agente restano
`& "C:\Program Files\Esapanel\esapanel-agent.exe" uninstall --purge`	Toglie il servizio e cancella anche i dati dell'agente (configurazione, iscrizione, chiave, coda)

I dati dell'agente (configurazione, certificato, coda, il suo log `agent.log`) sono in `C:\ProgramData\Esapanel\Agent`, leggibili solo dagli amministratori.

Disinstallare l'agente non toglie l'apparato dal pannello: toglietelo con **Rimuovi** nella pagina **Apparati**, così libera il suo posto nel limite del piano.

Aggiornare l'agente

Aprite la pagina dell'apparato nel pannello (link **Istruzioni** nella lista): per un agente già iscritto mostra i comandi che **aggiornano** l'agente mantenendo la sua iscrizione, quindi senza creare un nuovo apparato. Eseguiteli in PowerShell come amministratore.

Un server **reinstallato da zero** ha perso l'iscrizione: aggiungetelo di nuovo come nuovo apparato e togliete quello vecchio.

Con NXLog (alternativa)

Se non volete installare l'agente, nella stessa pagina dei comandi la sezione **Al posto dell'agente: NXLog Community Edition** mostra un'alternativa con un prodotto di terzi, gratuito:

1. Installate **NXLog Community Edition** dal sito nxlog.co (il sito chiede una registrazione gratuita prima del download).
2. Eseguite in PowerShell come amministratore i comandi che la pagina mostra: tengono una copia della configurazione di prima, scaricano quella del pannello e riavviano NXLog.

NXLog invia gli stessi eventi dell'agente (tutto Sicurezza, avvisi ed errori di Sistema e Applicazione) sulla **porta in chiaro**, in TCP, con syslog RFC 5424.

Con NXLog l'apparato **non si registra da solo**: i primi log arrivano nella **Quarantena**. Da lì autorizzate l'indirizzo del server (**Autorizza l'indirizzo**) o il suo nome (**Autorizza il nome apparato**); vedi il capitolo 8. Poi, nella pagina dell'apparato, indicate il modello **Windows Server**.

---

6. Server Linux

Per i server della famiglia **Debian** (Debian, Ubuntu) e **Red Hat** (Red Hat, Rocky, AlmaLinux) il pannello offre due modi: l'agente Esapanel, consigliato, e rsyslog.

Con l'agente Esapanel (consigliato)

L'agente è un servizio systemd che legge il **journal** del server.

Che cosa invia:

- tutti i messaggi del journal con gravità **avviso o peggiore** (warning, error, critical, ...);
- **tutti** i messaggi di accesso (facility auth e authpriv: sshd, sudo, su, login), a ogni gravità. Degli accessi SSH riporta l'utente e l'indirizzo, riusciti e falliti.

Come su Windows: si iscrive da solo, nessun indirizzo da autorizzare, coda su disco se il pannello non risponde, nessuna perdita dopo un riavvio; parte dai messaggi nuovi.

Installazione:

1. Nella pagina **Apparati**: **Aggiungi apparato**, categoria **Server**, modello **Linux Debian / Ubuntu** oppure **Linux Red Hat / Rocky / AlmaLinux**.
2. La pagina propone **Con l'agente di Esapanel (consigliato)**. Scrivete il **Nome dell'apparato** e premete **Mostra i comandi**.
3. **Copia i comandi** ed eseguiteli sul server **come root** (o con sudo). Scaricano l'agente adatto all'architettura del server (amd64 o arm64) in `/usr/local/bin/esapanel-agent`, lo installano come servizio systemd `esapanel-agent` e lo iscrivono alla subscription. Serve `curl`.
4. La pagina passa da "In attesa dell'iscrizione dell'agente" a "L'agente si è iscritto." con il link **Apri l'apparato**.

Il pannello riconosce da solo se il server è della famiglia Debian o Red Hat. Le connessioni in uscita e il certificato funzionano come per Windows (vedi il capitolo 5).

Comandi utili (come root):

Comando	Che cosa fa
`esapanel-agent status`	Nome, dove invia (server, porta, TLS, scadenza del certificato), coda
`esapanel-agent uninstall`	Ferma e toglie il servizio; i dati restano
`esapanel-agent uninstall --purge`	Toglie il servizio e cancella anche i dati dell'agente
`systemctl status esapanel-agent`	Lo stato del servizio

I dati dell'agente sono in `/var/lib/esapanel-agent`, con il suo log `agent.log`.

Aggiornare: la pagina dell'apparato di un agente già iscritto mostra i comandi che lo aggiornano mantenendo l'iscrizione. Un server reinstallato da zero va aggiunto di nuovo come nuovo apparato, togliendo il vecchio.

Con rsyslog (alternativa)

rsyslog è il servizio syslog già presente in molte distribuzioni. Non richiede di installare l'agente.

1. Nell'aggiunta del server scegliete **Usa rsyslog al suo posto**.
2. Compilate i campi (vedi il capitolo 4): di solito **Riconosciuto da** = **Nome apparato**, con il nome che dà il comando `hostname` sul server; oppure **Indirizzo IP**, se il server esce con un indirizzo fisso.
3. **Aggiungi e mostra le istruzioni**. La pagina dell'apparato mostra i comandi da eseguire come root:
    - installano rsyslog, se manca (Debian 12 e successive non lo installano più);
    - scaricano dal pannello il file `/etc/rsyslog.d/90-esapanel.conf` (con **Mostra il file** potete leggerlo prima);

- su Red Hat, Rocky e AlmaLinux aggiungono la porta della subscription alle porte che SELinux permette a rsyslog (dove SELinux è spento il comando dà un errore che si può ignorare);
- riavviano rsyslog e inviano un log di prova ("Esapanel test").

Il file di configurazione invia **tutti i log** del server sulla **porta in chiaro**, in **TCP**, con syslog RFC 5424, e tiene una coda su disco: se il pannello non risponde, i log aspettano sul server.

I comandi scaricano il file da un link della subscription. Il link contiene solo nome, indirizzo e porta, nessun segreto. **Codice nuovo per i link** (in fondo alla pagina Apparati) ferma i comandi copiati prima; la configurazione già sui server continua a funzionare.

Altri server

Per un server che non è Windows né della famiglia Debian o Red Hat, scegliete il modello **Altro** della categoria **Server** e usate le impostazioni generali del capitolo 7.

---

7. Router, firewall e altri apparati

Router, firewall, switch, access point e NAS inviano i log con le loro impostazioni syslog, dall'interfaccia web o dalla riga di comando. Aggiungete prima l'apparato nel pannello (vedi il capitolo 4), di solito riconosciuto dall'**indirizzo IP** pubblico da cui invia; poi configuratelo.

Impostazioni generali

Impostazione dell'apparato	Valore
Server syslog	`<server>`, oppure l'**Indirizzo** se l'apparato vuole un indirizzo IP
Porta	`<porta in chiaro>` (oppure 514 sull'indirizzo dedicato, se attiva)
Protocollo	UDP o TCP
Formato	syslog RFC 5424 o RFC 3164 (il "classico"): vanno bene entrambi
Livello dei messaggi	Almeno informazioni, avvisi ed errori; per firewall e VPN anche gli eventi di traffico e di accesso, se vi servono

Con TLS, se l'apparato lo supporta:

Impostazione dell'apparato	Valore
Server syslog	`<nome del server>` della riga **Su TLS (cifrato)**: il nome, mai l'indirizzo IP
Porta	`<porta TLS>` (oppure 6514 sull'indirizzo dedicato, se attiva)
Protocollo	TCP con TLS
Certificato client	Nessuno: l'apparato non deve presentarne uno

UDP o TCP? Per gli apparati basta UDP. TCP mantiene l'ordine dei log e non li perde su una linea carica; con UDP i log inviati mentre la ricezione è ferma (per esempio durante un riavvio del server) sono persi.

L'ora dei log. Ogni log ha l'ora in cui il pannello lo riceve, sempre giusta, con cui i log si cercano e si ordinano. Ha anche l'ora scritta dall'apparato:

- con **RFC 5424** l'apparato indica il suo fuso orario, e l'ora resta com'è;
- con **RFC 3164** l'apparato scrive l'ora del suo orologio **senza fuso orario**. Indicate nel pannello il **Fuso orario** dell'apparato (per esempio `Europe/Rome`, che comprende l'ora legale): il pannello trasforma quell'ora nell'istante giusto. "Ora così come arriva" la lascia com'è.

Il fuso orario si imposta quando si aggiunge l'apparato (il pannello propone il vostro) e si cambia nella lista **Apparati**; un cambio vale per i log successivi. Tenete comunque l'orologio dell'apparato sincronizzato (NTP).

Modelli con istruzioni proprie

Per questi modelli la pagina dell'apparato mostra dove si trovano le impostazioni nei menu, o i comandi da copiare, già compilati con i valori della subscription:

Categoria	Modelli
Router e firewall	DrayTek Vigor; Zyxel ZyWALL / USG FLEX; Fortinet FortiGate; Cisco ASA; Check Point; MikroTik; pfSense / OPNsense; Sophos Firewall; SonicWall; WatchGuard Firebox
Switch e access point	Cisco IOS (Catalyst); HPE Aruba; Ubiquiti UniFi; MikroTik
Storage (NAS)	Synology DSM; QNAP QTS

Alcune indicazioni delle istruzioni:

- **pfSense e OPNsense:** guida passo per passo in Inviare i log da pfSense e OPNsense.
- **MikroTik:** guida passo per passo in Inviare i log da MikroTik. Nelle regole del firewall serve un prefisso del log con l'azione (per esempio `DROP-WAN`): la riga di RouterOS non dice se il pacchetto è passato.
- **DrayTek Vigor:** System Maintenance › SysLog / Mail Alert Setup: attivate SysLog, indicate server e porta, scegliete i tipi di messaggio da inviare.
- **Zyxel:** se il modello non permette di cambiare la porta, serve l'indirizzo dedicato con la porta 514.
- **Cisco ASA:** usate **UDP**: con TCP, se il server non risponde, l'ASA può smettere di far passare il traffico.
- **Synology** e **QNAP:** scegliete il formato RFC 5424 (su Synology "IETF").

I menu cambiano con la versione del firmware: se il percorso indicato non corrisponde, cercate le impostazioni "syslog" o "remote log" dell'apparato e usate i valori delle impostazioni generali.

Per un modello che non è nell'elenco scegliete **Altro**: la pagina mostra i valori generali. Lo stesso vale per gli apparati della categoria **Altro apparato** (per esempio una stampante o un UPS che invia syslog).

---

8. Controllare che i log arrivino

La pagina dell'apparato

Dopo l'aggiunta, la pagina dell'apparato mostra:

- **Riconosciuto da**: come il pannello lo riconosce;
- **Ultimo log**: "Ultimo log da `<indirizzo>`, `<quando>`", oppure "Ancora nessun log";
- finché non arriva niente, "In attesa del primo log dell'apparato: la pagina si aggiorna da sola".

Per provare, generate un evento sull'apparato: per esempio un accesso alla sua interfaccia di amministrazione. I comandi rsyslog inviano da soli un log di prova.

Per un agente la lista **Apparati** mostra anche "Agente `<versione>`, ultimo battito `<quando>`": l'agente invia un battito ogni 5 minuti, anche quando il server non ha eventi. Appena iscritto mostra "Iscritto: in attesa del primo battito dell'agente".

I log arrivati si vedono nella tessera **Log** della subscription.

La Quarantena

I log che arrivano sulle porte della vostra subscription da un mittente che **non è fra gli apparati** vanno nella **Quarantena** (tessera **Quarantena**). Restano qualche giorno (la pagina indica quanti), poi vengono eliminati. Sono raggruppati per **Indirizzo** e **Nome apparato**, con il numero di log e il periodo.

Per ogni mittente:

Pulsante	Che cosa fa
Autorizza l'indirizzo	Il mittente diventa un apparato riconosciuto dall'indirizzo; i suoi log in quarantena passano nella subscription
Autorizza il nome apparato	Lo stesso, riconosciuto dal nome che scrive nei log, da qualsiasi indirizzo
Scarta	Elimina i suoi log in quarantena; i successivi tornano in quarantena
Ignora l'indirizzo / **Ignora il nome**	I suoi log in quarantena vengono eliminati e i successivi scartati all'arrivo, solo contati. Non conta fra gli apparati. **Non ignorare più**, nell'elenco **Mittenti ignorati**, lo annulla

Un mittente autorizzato conta fra gli apparati del piano: se il limite è raggiunto, la pagina chiede di toglierne uno dalla pagina Apparati. Dopo l'autorizzazione, nella pagina dell'apparato scegliete il suo **Modello**.

Ignorate solo mittenti che conoscete e non volete, come un apparato di prova: i loro log non vengono conservati da nessuna parte.

La Quarantena è il primo posto da guardare quando un apparato configurato non risulta: spesso i suoi log arrivano, ma da un indirizzo diverso da quello inserito.

Avviso se un apparato tace

La colonna **Avvisa se tace da** della lista **Apparati** (Mai, 15 minuti, 1 ora, 6 ore, 24 ore) fa partire un'**email** quando un apparato non invia log da più di quel tempo, ad esempio un firewall spento o una sede senza collegamento, e un'altra quando riprende. Nella lista l'apparato mostra "Silenziosa dal ...".

- Sceglietelo per gli apparati che inviano di continuo: molti inviano solo quando succede qualcosa.
- Per gli **agenti** è sempre utile: il battito ogni 5 minuti conta come attività, quindi un server tranquillo non sembra spento.
- Se nel frattempo sono arrivati log nella Quarantena, l'email ne indica i mittenti: spesso l'apparato ha un nuovo indirizzo.

---

9. Problemi frequenti

Non arriva niente

1. **La Quarantena.** Se i log sono lì, l'apparato invia ma non è riconosciuto: autorizzatelo, oppure correggete l'indirizzo o il nome nella lista **Apparati**. Ricordate che conta l'indirizzo **pubblico** con cui l'apparato esce su Internet, non quello della rete interna.
2. **Porta e protocollo.** Controllate che porta e protocollo siano quelli della pagina **Apparati**: la porta in chiaro accetta UDP e TCP; la porta TLS solo TCP con TLS. Un apparato configurato in chiaro sulla porta TLS, o con TLS sulla porta in chiaro, non consegna niente.
3. **Il firewall in uscita.** Il vostro firewall deve lasciar uscire il traffico verso il server del pannello sulla porta usata (UDP e/o TCP). Per l'agente: l'indirizzo del pannello del comando, in HTTPS, e la **Porta degli agenti** della pagina Apparati.
4. **Le porte 514 e 6514** funzionano solo sull'indirizzo dedicato e solo se attivate nella pagina **Apparati**.
5. **Un mittente ignorato.** Controllate l'elenco **Mittenti ignorati** nella Quarantena.
6. **Un agente.** Eseguite il comando `status` e guardate il log dell'agente (`agent.log` nella cartella dei dati): se i dati aspettano nella coda, l'agente non raggiunge il server.

L'ora dei log è sbagliata

- Se l'apparato invia RFC 3164, impostate il suo **Fuso orario** nella lista **Apparati** e salvate: vale per i log successivi.
- Controllate che l'orologio dell'apparato sia giusto (NTP).
- L'ora di ricezione del pannello è sempre giusta: la ricerca e l'ordine dei log usano quella.

L'iscrizione dell'agente è rifiutata

L'agente scrive "the panel refused the enrollment", seguito dal motivo.

Motivo	Che cosa fare
Il codice di iscrizione non è valido, o la subscription non è attiva	Qualcuno ha dato un **Codice nuovo** (sezione **Codici degli agenti e dei link**, in fondo alla pagina Apparati): i comandi copiati prima non iscrivono più agenti. Copiate di nuovo i comandi dalla pagina. Se la subscription è sospesa, contattate il fornitore del servizio
La subscription ha già il numero massimo di apparati	Togliete un apparato non più usato, o chiedete un piano più ampio
Troppe richieste	Aspettate un minuto e riprovate

Il codice di iscrizione permette di aggiungere apparati alla subscription: datelo solo a chi installa l'agente. Se è finito dove non doveva, date un **Codice nuovo**: gli agenti già iscritti continuano a funzionare.

L'agente invia senza certificato client

Se la pagina dell'apparato dice "L'agente invia senza certificato client", l'agente è stato installato prima dei certificati, oppure il pannello non poteva ancora firmarlo. L'agente richiede il certificato da solo all'avvio; se la scritta resta, reinstallatelo come nuovo apparato:

1. disinstallate l'agente con `uninstall --purge`;
2. togliete il vecchio apparato con **Rimuovi** (così non conta nel limite);
3. aggiungete il server come nuovo apparato ed eseguite i comandi della pagina.

Errori TLS

- **Il nome:** l'apparato deve collegarsi al **nome del server** della riga **Su TLS (cifrato)**, non all'indirizzo IP, altrimenti la verifica del certificato fallisce.

- **L'autorità:** se l'apparato rifiuta il certificato del server, probabilmente non conosce l'autorità che lo ha emesso. Su alcuni apparati l'elenco delle autorità si aggiorna con il firmware o si importa a mano: chiedete al fornitore del servizio quale autorità usa il certificato.
- **L'orologio:** un orologio sbagliato fa sembrare il certificato scaduto o non ancora valido.
- **Il protocollo:** TLS solo su TCP.
- Se l'apparato non riesce a usare il TLS, inviate sulla porta in chiaro.

Inviare i log da MikroTik

Questa guida completa Inviare i log al pannello per router e switch **MikroTik** con **RouterOS 7**. I valori da inserire (indirizzo e porta) sono nella pagina dell'apparato nel pannello, già compilati: qui sotto sono indicati come `<Indirizzo>` e `<porta in chiaro>`.

1. Che cosa riceve il pannello

Con il modello **MikroTik**, il pannello legge i log e li mostra nella sezione **Eventi** della pagina **Analisi** e nei report:

Nella sezione Eventi	Da dove viene
Accessi riusciti e falliti	Gli accessi di ogni servizio (Winbox, SSH, interfaccia web, API), con utente e indirizzo
Amministrazione	Le modifiche alla configurazione, con chi le ha fatte, da dove e il comando
Firewall bloccati e **Traffico** consentito	Le regole del firewall con il log attivo, con indirizzi, porte e interfaccia (vedi il capitolo 4)

Tutti gli altri log si cercano comunque nella tessera **Log**.

Il MikroTik invia in **UDP** sulla **porta in chiaro**.

---

2. Aggiungere il MikroTik nel pannello

1. Nella pagina **Apparati**, **Aggiungi apparato**.
2. Categoria **Router e firewall** (o **Switch e access point** per uno switch MikroTik), modello **MikroTik**.
3. **Nome dell'apparato**: un nome per voi, per esempio "Router sede".
4. **Riconosciuto da**: **Indirizzo IP**, con l'indirizzo pubblico fisso da cui il MikroTik esce su Internet. Se l'indirizzo cambia, vedete il capitolo 6.
5. **Aggiungi e mostra le istruzioni**.

La pagina dell'apparato mostra i comandi qui sotto già compilati con il vostro **Indirizzo** e la vostra porta, con il pulsante per copiarli.

---

3. L'invio dei log

Aprite il terminale del MikroTik: in Winbox **New Terminal**, oppure in SSH. Incollate i comandi della pagina dell'apparato; hanno questa forma:

```
/system logging action add name=esapanel target=remote remote=<Indirizzo> remote-port=<porta in
chiaro> remote-log-format=syslog
/system logging add topics=info action=esapanel
/system logging add topics=warning action=esapanel
/system logging add topics=error action=esapanel
/system logging add topics=critical action=esapanel
```

- Il primo comando crea la destinazione: il server con il suo **Indirizzo** (RouterOS accetta solo un indirizzo IP, non un nome) e la porta della subscription, nel formato syslog con data e fuso orario.
- Gli altri inviano a quella destinazione i messaggi informativi, gli avvisi, gli errori e quelli critici: comprendono gli accessi, le modifiche e i log del firewall.

Se RouterOS risponde che `remote-log-format` non esiste, la vostra versione non ha questa opzione: ripetete il primo comando senza `remote-log-format=syslog`. Il pannello legge anche il formato predefinito.

Le stesse impostazioni sono in Winbox in **System › Logging**: scheda **Actions** per la destinazione, scheda **Rules** per gli argomenti.

---

4. Le regole del firewall

RouterOS registra una regola del firewall solo se ha il log attivo, e la riga del log **non dice se il pacchetto è stato accettato o scartato**. Per questo:

1. In **IP › Firewall › Filter Rules** aprite la regola che volete vedere.
2. Scheda **Action**: spuntate **Log** e scrivete un **Log Prefix** che contiene l'azione, per esempio `DROP-WAN` per una regola che scarta, `ACCEPT-VPN` per una che accetta. Il pannello capisce l'esito da queste parole: **drop**, **reject**, **block**, **deny** (bloccato) e **accept**, **allow**, **pass** (consentito), maiuscole o minuscole.
3. Scheda **General**: per una regola che accetta, mettete **Connection State** a **new**, così si registra solo l'inizio di ogni connessione. Senza, ogni pacchetto diventa una riga e i log crescono molto in fretta.
4. **OK**.

Una regola con il log ma senza una di quelle parole nel prefisso compare fra i log del **Firewall**, senza esito.

Attivate il log solo sulle regole che contano: di solito quelle che scartano il traffico da Internet e quelle che lasciano entrare servizi o VPN.

---

5. Controllare che i log arrivino

1. Generate un evento: per esempio un accesso a Winbox o in SSH con una password sbagliata, poi quello giusto.
2. Nella pagina dell'apparato, **Ultimo log** mostra l'ora del log appena arrivato.
3. Nella tessera **Log** cercate i log dell'apparato: l'accesso fallito c'è.
4. Dopo qualche minuto la pagina **Analisi** mostra l'accesso fallito nella sezione **Eventi**, fra gli **Accessi** falliti.

---

6. Problemi frequenti

Non arriva niente

- Controllate la **Quarantena**: se i log arrivano da un indirizzo diverso da quello inserito (per esempio un router con due connessioni a Internet), sono lì. **Autorizza l'indirizzo** li fa entrare.
- Verificate in **System › Logging › Actions** che la destinazione `esapanel` abbia l'**Indirizzo** e la **porta in chiaro** della vostra subscription.
- Le regole del firewall nella catena **output** del MikroTik, o un firewall a monte, devono lasciar passare UDP verso `<Indirizzo>` sulla `<porta in chiaro>`.

Il MikroTik ha un indirizzo che cambia

Riconoscete il MikroTik dal **Nome apparato** invece che dall'indirizzo. Con il formato syslog il nome nei log è l'**identità** del MikroTik (**System › Identity**), che di fabbrica è `MikroTik`: date a ogni apparato un'identità sua prima di usarla nel pannello. Con il formato predefinito il nome non c'è: in questo caso serve l'indirizzo IP o un **Nome DNS**.

Arrivano troppi log

- Controllate che le regole che accettano abbiano **Connection State new**.
- Togliete il log dalle regole che vedono molto traffico e non vi servono.

Inviare i log da pfSense e OPNsense

Questa guida completa Inviare i log al pannello per i firewall **pfSense** e **OPNsense**. I valori da inserire (indirizzo e porta) sono nella pagina dell'apparato nel pannello, già compilati: qui sotto sono indicati come `<Indirizzo>` e `<porta in chiaro>`.

1. Che cosa riceve il pannello

Il firewall invia tutti i suoi log. Con il modello **pfSense / OPNsense**, il pannello li legge e li mostra nella sezione **Eventi** della pagina **Analisi** e nei report:

Nella sezione Eventi	Da dove viene
Firewall bloccati	Le connessioni bloccate dalle regole, con indirizzo di origine, destinazione, porta e interfaccia
Traffico consentito	Le connessioni passate dalle regole per cui avete attivato il log
Accessi riusciti e falliti	Gli accessi all'interfaccia web e in SSH, con utente e indirizzo
Amministrazione	Le modifiche alla configurazione, con chi le ha fatte e da dove
Attacchi rilevati	Gli indirizzi segnalati e bloccati dalla protezione contro i tentativi di accesso ripetuti
VPN	I tunnel IPsec stabiliti e quelli falliti

Tutti gli altri log (servizi, DHCP, sistema) si cercano comunque nella tessera **Log**.

Il firewall invia in **UDP** sulla **porta in chiaro**: pfSense non offre altro per l'invio remoto.

---

2. Aggiungere il firewall nel pannello

1. Nella pagina **Apparati**, **Aggiungi apparato**.
2. Categoria **Router e firewall**, modello **pfSense / OPNsense**.
3. **Nome dell'apparato**: un nome per voi, per esempio "Firewall sede".
4. **Riconosciuto da**: **Indirizzo IP**, con l'indirizzo pubblico fisso da cui il firewall esce su Internet. Se l'indirizzo cambia, vedete il capitolo 6.
5. **Aggiungi e mostra le istruzioni**.

La pagina dell'apparato mostra i passi qui sotto già compilati con il vostro **Indirizzo** e la vostra porta.

---

3. pfSense

Le impostazioni sono in **Status › System Logs › Settings**.

Usate l'indirizzo, non il nome

Nel campo del server remoto scrivete l'**Indirizzo** (l'indirizzo IP del server, nella pagina dell'apparato), non il nome del server: così l'invio non dipende dal DNS del firewall.

I passi

1. **General Logging Options › Log Message Format:** scegliete **syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps)**. Con questo formato ogni log porta il suo fuso orario.
2. Lasciate spuntato **Log packets matched from the default block rules in the ruleset**: sono le connessioni bloccate.
3. **Remote Logging Options:**
   - spuntate **Enable Remote Logging**;
   - **Source Address:** Default (any);
   - **IP Protocol:** IPv4;
   - **Remote log servers:** `<Indirizzo>:<porta in chiaro>`, per esempio `203.0.113.5:18670`.
4. **Remote Syslog Contents:** spuntate **Everything**.
5. **Save**.

Le connessioni consentite (facoltativo)

Per vedere nel pannello anche il traffico consentito, attivate il log nelle regole che vi interessano: **Firewall › Rules**, modificate la regola, **Extra Options**, spuntate **Log packets that are handled by this rule**, **Save** e **Apply Changes**.

Fatelo solo sulle regole che contano (per esempio l'accesso dall'esterno a un server, o le VPN): una regola che fa passare tutta la navigazione dell'ufficio produce moltissimi log.

I tunnel IPsec

Se avete tunnel IPsec, pfSense scrive molti messaggi di servizio (rinnovi delle chiavi, controlli che il tunnel sia vivo): possono essere la maggior parte dei log. Se riempiono i log, abbassatene i livelli in **VPN › IPsec › Advanced Settings › IPsec Logging Controls**. I tunnel stabiliti e quelli falliti restano visibili.

---

4. OPNsense

Le impostazioni sono in **System › Settings › Logging**, scheda **Remote**.

1. Il pulsante **+** aggiunge una destinazione.
2. Compilate:

Campo	Valore
Enabled	Spuntato
Transport	UDP(4)
Applications	Vuoto: tutte
Levels	Tutti tranne **debug**
Facilities	Vuoto: tutte
Hostname	`<Indirizzo>`
Port	`<porta in chiaro>`
RFC5424	Spuntato
Description	Esapanel

3. **Save**, poi **Apply**.

Scegliete i livelli: se il campo **Levels** resta vuoto, OPNsense invia anche i messaggi di debug, numerosi e senza utilità per il monitoraggio.

Per le connessioni bloccate e consentite, spuntate **Log** nelle regole che vi interessano (**Firewall › Rules**), con lo stesso criterio di pfSense: solo le regole che contano.

---

5. Controllare che i log arrivino

1. Generate un evento: per esempio un accesso all'interfaccia web del firewall con una password sbagliata, poi quello giusto.
2. Nella pagina dell'apparato, **Ultimo log** mostra l'ora del log appena arrivato.
3. Nella tessera **Log** cercate i log dell'apparato: l'accesso fallito c'è.
4. Dopo qualche minuto la pagina **Analisi** mostra l'accesso fallito nella sezione **Eventi**, fra gli **Accessi** falliti.

---

6. Problemi frequenti

Non arriva niente

- Controllate la **Quarantena**: se i log arrivano da un indirizzo diverso da quello inserito (per esempio un firewall con due connessioni a Internet), sono lì. **Autorizza l'indirizzo** li fa entrare.
- Verificate di aver scritto l'**Indirizzo** e la **porta in chiaro** della vostra subscription, non la porta 514.
- Un firewall a monte, o le regole in uscita del firewall stesso, devono lasciar passare UDP verso `<Indirizzo>` sulla `<porta in chiaro>`.

Il firewall ha un indirizzo che cambia

Riconoscete il firewall dal **Nome apparato** invece che dall'indirizzo. Il nome è quello che il firewall scrive nei log: su pfSense e OPNsense è il nome e il dominio indicati in **System › General Setup** (pfSense) o **System › Settings › General** (OPNsense), per esempio `pfSense.home.arpa`. Date a ogni firewall un nome suo, diverso da quello di fabbrica, prima di usarlo nel pannello.

Arrivano troppi log

- Togliete il log dalle regole che fanno passare molto traffico.
- Su pfSense abbassate i livelli di IPsec (vedi I tunnel IPsec); su OPNsense escludete il livello debug.
- Gli apparati della rete locale che si annunciano (per esempio sulla porta 5353, mDNS) possono fare la maggior parte delle connessioni bloccate: se non vi servono, non registrate le regole che li bloccano.

Gli apparati e la quarantena

In CSP (Central Syslog) un **apparato** è un server o un dispositivo di rete che invia i suoi log alla subscription. Solo i log degli apparati entrano nella subscription; quelli di un mittente sconosciuto aspettano nella **Quarantena**.

Come aggiungere un apparato e configurarlo è spiegato in Inviare i log al pannello. Questa pagina spiega come tenere in ordine gli apparati nel tempo: la lista, la pagina di ciascuno, la quarantena e i codici.

La lista degli apparati

La tessera **Apparati** della subscription mostra in alto il riquadro **Invio dei log**, con il server e le porte, e sotto la lista degli apparati. Il conteggio in alto, per esempio "3 di 10 apparati", dice quanti apparati consente il piano.

Per ogni apparato la lista mostra:

- il nome che gli avete dato e il **Modello**;
- **Riconosciuto da**: l'indirizzo IP, la rete, il nome DNS, il nome apparato o l'**Agente Esapanel**. Per un nome DNS la lista dice anche in che cosa risolve adesso;
- **Ultimo log**: "Ultimo log da `<indirizzo>`, `<quando>`", oppure "Ancora nessun log". Per un agente, "Agente `<versione>`, ultimo battito `<quando>`";
- **Fuso orario** e **Avvisa se tace da**, che si cambiano direttamente nella riga con **Salva**.

Rimuovi toglie un apparato: i suoi log successivi andranno nella quarantena, e il suo posto nel limite del piano si libera. I log che ha già inviato restano.

Avvisa se tace da

Avvisa se tace da (Mai, 15 minuti, 1 ora, 6 ore, 24 ore) fa partire un'email quando l'apparato non invia log da più di quel tempo, e un'altra quando riprende. Un apparato silenzioso mostra "Silenziosa dal ...".

Sceglietelo per gli apparati che inviano di continuo, come un firewall o un server con l'agente: molti apparati inviano solo quando succede qualcosa, e darebbero falsi allarmi. Il tempo in cui il server del pannello stesso non riceveva non conta.

Il fuso orario

Molti apparati scrivono nei log l'ora del loro orologio senza dire il fuso (syslog RFC 3164). Il **Fuso orario** dell'apparato, per esempio `Europe/Rome`, permette al pannello di trasformare quell'ora nell'istante giusto, ora legale compresa. **Ora così come arriva** la lascia com'è. Un cambio vale per i log successivi.

La pagina di un apparato

Il nome di un apparato nella lista apre la sua pagina, con le istruzioni per configurarlo già compilate. Qui potete:

- cambiare il **Nome dell'apparato** e il **Modello**: le istruzioni seguono il modello;
- scegliere il **Profilo dei log** (vedi sotto);
- vedere quando è arrivato l'ultimo log. Finché non arriva il primo, la pagina lo dice e si aggiorna da sola.

Un apparato autorizzato dalla quarantena non ha ancora un modello: sceglietelo qui per vedere le istruzioni.

Il profilo dei log

Il **Profilo dei log** è il modo in cui il pannello legge i log dell'apparato per riconoscere gli eventi: accessi, cambi di configurazione, traffico bloccato, VPN. Da questi eventi nascono la sezione **Eventi** dell'**Analisi**, una parte dei report e gli avvisi sugli eventi.

- **Automatico**, la scelta normale, usa il profilo del modello, oppure lo riconosce dai log.
- **Generic text (by words)** è per un apparato che nessun profilo legge: cerca parole come "login failed" o "denied". I suoi eventi non fanno partire avvisi.
- **Nessuno** non legge niente.

Ci sono profili per Linux, Windows, DrayTek Vigor, pfSense / OPNsense, MikroTik, Fortinet, Sophos, SonicWall, Zyxel, WatchGuard, Check Point, Cisco ASA e IOS, switch Aruba, gateway UniFi, Synology e QNAP, e profili generici per gli apparati che inviano CEF / LEEF, chiave=valore o iptables.

Riconoscilo come ...

Alcuni apparati, come i DrayTek Vigor, non scrivono il loro nome dove il pannello se lo aspetta, e risultano con il nome inverso del loro indirizzo. In questo caso la pagina propone **Riconoscilo come** seguito dal nome che l'apparato scrive davvero: da allora l'apparato viene accettato con quel nome da qualsiasi indirizzo, anche quando una linea di backup cambia l'indirizzo.

Un agente

Per un agente la pagina dice fino a quando è valido il suo certificato client: l'agente lo rinnova da solo un mese prima della scadenza. Per un agente già iscritto la pagina mostra i comandi che lo aggiornano senza creare un nuovo apparato.

La quarantena

La tessera **Quarantena** raccoglie i log arrivati sulle porte della subscription da mittenti che non sono fra gli apparati. Il numero sulla tessera dice quanti mittenti aspettano. I log restano qualche giorno, poi vengono eliminati; oltre un limite giornaliero la quarantena li conta soltanto, senza conservarli.

I mittenti sono raggruppati per **Indirizzo** e **Nome apparato**, con il numero di log e il periodo. Per ognuno:

Pulsante	Che cosa fa
Autorizza l'indirizzo	Il mittente diventa un apparato riconosciuto dal suo indirizzo, e i suoi log in quarantena passano nella subscription
Autorizza il nome apparato	Lo stesso, riconosciuto dal nome che scrive nei log, da qualsiasi indirizzo
Scarta	Elimina i suoi log in quarantena; i successivi tornano qui
Ignora l'indirizzo / **Ignora il nome**	I suoi log vengono scartati all'arrivo e solo contati, e quelli in quarantena eliminati

Prima di autorizzare potete scegliere il **Profilo** del mittente: **Riconosci da solo** di solito basta. Il profilo dice anche dove il mittente scrive il suo nome. Se non ne scrive uno proprio, il pannello permette di autorizzare solo l'indirizzo.

Un mittente autorizzato conta fra gli apparati del piano. Se il mittente era già un apparato, per esempio aggiunto nel frattempo dalla pagina **Apparati**, l'autorizzazione sposta soltanto i log rimasti in quarantena.

Mittenti ignorati

L'elenco **Mittenti ignorati** mostra i mittenti ignorati e quanti log hanno inviato da allora. **Non ignorare più** riporta i loro prossimi log in quarantena.

Ignorate solo mittenti che conoscete e non volete, come un apparato di prova: i loro log sono persi. Non serve ignorare gli scanner di Internet, che il firewall del server blocca comunque.

Quando guardare la quarantena

- Un apparato appena configurato non risulta: i suoi log sono quasi sempre in quarantena, con un indirizzo diverso da quello inserito. Autorizzatelo da qui, oppure correggete l'indirizzo nella lista **Apparati** e rimuovete quello sbagliato.
- Arriva l'email di un apparato silenzioso che segnala log in quarantena: l'apparato ha probabilmente cambiato indirizzo.

I codici degli agenti e dei link

In fondo alla pagina **Apparati**, **Codici degli agenti e dei link** contiene i due codici che usano le istruzioni dei server:

- il **codice degli agenti** iscrive agenti nella subscription: chi lo ha può aggiungere un apparato, entro il limite del piano. Datelo solo a chi installa l'agente;
- il **codice dei link** sta nei link che scaricano la configurazione di rsyslog. Questi link non contengono segreti, solo il nome, l'indirizzo e la porta.

Date un **Codice nuovo** (per i link, **Codice nuovo per i link**) quando un codice è finito dove non doveva. Gli agenti già iscritti e i server già configurati continuano a funzionare; smettono di funzionare solo i comandi copiati prima.

Le porte 514 e 6514

Quando la subscription riceve su un indirizzo IP dedicato, nella pagina **Apparati** potete attivare anche la porta standard **514** (syslog) e la **6514** (syslog su TLS), per gli apparati che non permettono di scegliere la porta. I dettagli sono in Inviare i log al pannello.

Cercare e leggere i log

La tessera **Log** della subscription di CSP (Central Syslog) mostra i log ricevuti, dal più recente, e permette di cercarli e scaricarli. Senza filtri la pagina mostra le ultime 24 ore.

Cercare

I filtri sono in cima alla pagina:

Filtro	Che cosa fa
Dal e **Al**	Il periodo
Apparato	Il nome o l'indirizzo dell'apparato
Categoria	**Errori**, **Avvisi**, **Informazioni**, oppure **Tutte**
Facility	La facility syslog, per esempio auth per gli accessi
Testo	Una parola o una frase del messaggio

Cerca applica i filtri, **Ultime 24 ore** li toglie. **Più recenti** e **Meno recenti** scorrono i risultati.

Per ogni log la pagina mostra **Ricevuto** (l'ora in cui il pannello lo ha ricevuto, nel vostro fuso orario), l'**Apparato**, la **Severity** e il **Messaggio**. La colonna **Apparato** mostra in evidenza il nome che l'apparato scrive nei suoi log, poi il nome che gli avete dato e il suo indirizzo.

L'ora di ricezione è quella con cui i log si cercano e si ordinano: è sempre giusta, anche se l'orologio di un apparato è sbagliato.

I campi dell'evento

Gli agenti Esapanel, e gli apparati che inviano syslog RFC 5424 con dati strutturati, danno a ogni log dei campi propri: per esempio **Utente**, **Indirizzo di origine**, **Evento** (su Windows, 4625 è un accesso fallito) ed **Esito**.

- **Dettagli**, sotto un log, mostra i suoi campi.
- Un clic su un utente o su un indirizzo (**Mostra solo i log con questo valore**) mostra solo i log con quel valore.
- In **Campi dell'evento** potete cercare per valore esatto: tutti gli accessi falliti di un utente, o tutto quello che ha fatto un indirizzo di origine. L'utente si confronta senza distinguere maiuscole e minuscole.

Esempio: chi ha provato a entrare in un server Windows

1. Filtrate l'**Apparato** con il nome del server.
2. In **Campi dell'evento** scrivete `4625` in **Evento**.
3. Il risultato sono gli accessi falliti. Aprite **Dettagli** su uno di essi e fate clic sull'**Indirizzo di origine** per vedere tutto quello che ha fatto quell'indirizzo.

Le interruzioni della ricezione

Una riga gialla segna un'interruzione della ricezione del server del pannello, per esempio durante un riavvio: i log che i vostri apparati hanno inviato in UDP in quell'intervallo non sono arrivati. I log inviati in TCP, o dall'agente, di solito vengono rimandati dall'apparato.

I nomi degli indirizzi

Se il vostro piano lo comprende, il pannello cerca nel DNS i nomi degli indirizzi pubblici che compaiono nei log, per esempio quelli di un attaccante nei log di un firewall, e li mostra fra parentesi

dopo l'indirizzo. I log più recenti possono non avere ancora i nomi. L'opzione è spenta se non viene chiesta, perché chi gestisce il DNS di un indirizzo può vedere che è stato cercato.

Scaricare

Scarica salva i log trovati con i filtri attuali, in **CSV** per un foglio di calcolo o come **testo** syslog. Un download contiene al massimo un numero fisso di log: per un periodo lungo, scaricate a parti, per esempio un mese alla volta. I download contengono i log come sono arrivati, senza i nomi degli indirizzi.

Per scaricare serve un ruolo che lo permetta (**CSP · Esportare i log**).

Dove sono i log più vecchi

Il piano stabilisce per quanto tempo i log restano consultabili in questa pagina. I log più vecchi non sono persi: ogni notte passano nella tessera **Archivio log**, da dove si scaricano (vedi Archivi e backup dei log).

Avvisami se si ripete

Su un log, **Avvisami se si ripete** apre il modulo di una nuova regola degli avvisi già compilato con il testo di quel log: è il modo più veloce per essere avvisati quando un messaggio si ripresenta (vedi Gli avvisi sugli eventi).

Gli avvisi sugli eventi

Conservare i log non basta: bisogna accorgersi quando succede qualcosa. Gli **avvisi sugli eventi** di CSP (Central Syslog) leggono i log nuovi della subscription ogni 3 minuti e vi scrivono quando c'è qualcosa che vale la pena guardare: tentativi di indovinare una password, un accesso all'amministrazione di un firewall di notte, una configurazione cambiata, un attacco sopra la norma. Non dovete scrivere regole: quelle predefinite sono già accese.

È anche un aiuto per la direttiva NIS2, che chiede di **rilevare** gli incidenti, non solo di conservare i log.

La tessera **Avvisi sugli eventi** c'è se il piano della subscription comprende il servizio. Per vedere la pagina basta poter vedere i log; per cambiare regole ed eccezioni serve un ruolo che permetta di gestire gli apparati.

Gli episodi

Gli eventi di una stessa regola che riguardano la stessa cosa (un indirizzo, un utente, un apparato, un'ora) e che si susseguono formano un **episodio**. Per esempio, 34 accessi falliti in 10 minuti dallo stesso indirizzo sono un episodio, non 34 avvisi.

- Ricevete un'email quando l'episodio inizia, e al massimo una all'ora finché continua.
- L'episodio finisce quando i suoi eventi smettono.
- **Episodi degli ultimi 30 giorni** li elenca, con quelli **In corso** e un collegamento ai loro log.
- Gli episodi del periodo compaiono anche nei report (vedi Report e analisi).

Chi riceve le email lo decide il vostro fornitore nelle notifiche (vedi Le notifiche).

Le regole

In **Regole** ogni regola si accende o si spegne (**Accesa**). Quelle con una soglia hanno una **Sensibilità**: **Bassa** scrive solo per molti eventi, **Alta** già per pochi, **Media** è il valore predefinito. I numeri di ogni regola sono nella sua descrizione.

Regola	Quando scrive
Accessi falliti ripetuti	Molti accessi falliti in 10 minuti dallo stesso indirizzo o per lo stesso utente: qualcuno prova a indovinare una password
Accesso riuscito dopo molti falliti	Un accesso riuscito subito dopo un episodio di falliti: il tentativo potrebbe aver funzionato
Accesso all'amministrazione di un apparato	Un accesso a un firewall o a un router fuori dall'orario di lavoro (dal lunedì al venerdì, dalle 8 alle 19) o da un indirizzo mai visto negli ultimi 30 giorni. Con **Ogni accesso**, ogni accesso
Configurazione cambiata	Una configurazione di un apparato cambiata, con chi e da dove
Firmware aggiornato	Un aggiornamento del firmware di un apparato di rete
Account creati o cambiati	Un utente creato, eliminato, bloccato o aggiunto a un gruppo, una password cambiata

Regola	Quando scrive
Registro di controllo cancellato o criteri cambiati	Su Windows, il registro di sicurezza cancellato o i criteri di controllo cambiati
Comandi con sudo	Un comando eseguito con sudo su un server Linux. Di solito è normale: è spenta per default
Attacchi bloccati sopra la norma	Gli eventi bloccati dal firewall in un'ora, molte volte più della stessa ora nei 14 giorni prima
Attacco dalla rete interna	Molti eventi bloccati da un indirizzo privato della vostra rete: un computer infetto o un dispositivo compromesso
VPN instabile	Una VPN che fallisce molte volte in un'ora. Un'email anche quando torna stabile

Premete **Salva** dopo le modifiche.

Che cosa serve perché funzionino

Le regole si basano sugli eventi che i **profili** riconoscono nei log dei vostri apparati (vedi Gli apparati e la quarantena).

- Un apparato senza profilo, o letto dal profilo generico a parole, non dà avvisi.
- I log importati, o arrivati con più di 15 minuti di ritardo, non danno avvisi.

Le vostre regole

In **Le tue regole** potete aggiungere regole vostre, quante ne permette il piano. Ogni regola ha:

Campo	Che cosa scegliere
Nome	Un nome per voi
Apparato	Un apparato, o **Tutti gli apparati**
Condizione	**Il testo del log contiene**, **Il tipo di evento è**, **L'utente è**, **L'indirizzo di origine è** o **La porta di destinazione è**
Parole o valore	Il testo o il valore da cercare
Più di (volte in 10 minuti)	Vuoto: al primo evento. Con un numero, l'avviso parte quando gli eventi superano quel numero in 10 minuti

Poi **Aggiungi la regola**.

Il testo si cerca senza maiuscole, anche come parte di una parola: "admin" trova "Administrator". Una soglia conta gli eventi di ogni apparato per conto suo. A differenza delle regole predefinite, le vostre guardano anche i log che nessun profilo legge.

Il modo più rapido per creare una regola è partire da un log: nella pagina **Log**, **Avvisami se si ripete** apre il modulo già compilato con il testo di quel log.

Esempi

- Un avviso a ogni accesso dell'utente `admin` su un apparato: condizione **L'utente è**, valore `admin`, soglia vuota.
- Un avviso quando un NAS segnala un disco in errore: apparato il NAS, condizione **Il testo del log contiene**, parole come appaiono nel log del vostro NAS.

Le eccezioni

Un'**eccezione** è un indirizzo, una rete o un utente che le regole non considerano, per una regola o per tutte. Serve per i falsi allarmi conosciuti: lo scanner di vulnerabilità dell'ufficio, l'utente che fa i backup e accede di notte.

Da un episodio, **Non considerare questo indirizzo** aggiunge l'eccezione per quella regola in un clic.

Un'eccezione nasconde alla regola gli eventi di quell'indirizzo, rete o utente per sempre. I log restano conservati e si possono cercare. Usatele con giudizio: un'eccezione troppo larga nasconde anche gli attacchi veri.

Report e analisi

CSP (Central Syslog) riassume i log della subscription in due modi:

- l'**Analisi** è una pagina sempre aggiornata, per vedere a colpo d'occhio come si comportano gli apparati;
- i **Report** sono documenti di un giorno, una settimana o un mese, composti quando il periodo si chiude e poi non più cambiati, da leggere, stampare o conservare.

L'analisi

La tessera **Analisi** conta i log della subscription per ora. In **Periodo** scegliete **Ultime 24 ore**, **Ultimi 7 giorni**, **Ultimi 30 giorni** o **Ultimi 12 mesi**.

Sezione	Che cosa mostra
Log per gravità	Quanti log sono arrivati in ogni ora, giorno o settimana, divisi in errori (errore e peggio), avvisi e informazioni. Un'interruzione della ricezione nel periodo è scritta sotto il grafico
Apparati	Gli apparati che hanno inviato di più, con i loro **Errori** e la **Variazione** rispetto allo stesso periodo prima. Un clic apre i log di quell'apparato nel periodo
Giorni e ore	Quando arrivano i log, nel vostro fuso orario
Eventi	Gli eventi riconosciuti dai profili degli apparati (vedi sotto)

I conteggi si aggiornano ogni cinque minuti e restano 25 mesi, anche dopo che i log sono stati cancellati.

Che cosa guardare

- Un apparato che all'improvviso invia **molto di più o molto di meno** del solito merita un'occhiata: un attacco, un guasto, una configurazione cambiata.
- In **Giorni e ore** l'attività di notte o nel fine settimana salta all'occhio.
- Un apparato segnato **nuovo** non aveva inviato nel periodo precedente.

Gli eventi

I **profili** degli apparati leggono i log e contano gli eventi per categoria: **Accessi**, **Amministrazione**, **Account**, **Firewall**, **VPN**, **Traffico** e altre, con il loro esito (riusciti e falliti, consentiti e bloccati). Accanto, i valori visti più spesso: **Indirizzi degli accessi falliti**, **Utenti degli accessi falliti**, **Indirizzi bloccati dal firewall**, **Porte di destinazione del traffico**.

Gli eventi si contano con i riassunti orari, quindi gli ultimi minuti arrivano un po' dopo. Un apparato senza profilo non dà eventi: il profilo si sceglie nella sua pagina (vedi Gli apparati e la quarantena).

I report

La tessera **Report** c'è se il piano della subscription comprende il servizio. Elenca i report composti, con **Periodo**, **Tipo** (**Giornaliero**, **Settimanale**, **Mensile**), **Copertura** e numero di **Log**.

Scegliere quali report

In **Le tue scelte**:

- **Un report ogni giorno**, **Un report ogni settimana, il lunedì**, **Un report ogni mese, il primo**: quali periodi volete;
- **Conserva i report per (mesi)**: da 25 mesi in su, fino al massimo del piano. I report più vecchi vengono cancellati.

Poi **Salva**. Un report si compone quando il suo periodo si chiude nel vostro fuso orario, e quando è pronto arriva un'email (chi la riceve lo decide il vostro fornitore nelle notifiche).

Che cosa contiene un report

Sezione	Contenuto
Copertura del monitoraggio	Per quanto del periodo la ricezione è stata attiva, le sue interruzioni, e gli apparati che non hanno inviato niente
Log per gravità	I log del periodo per gravità, confrontati con il periodo precedente
Apparati	Gli apparati e i loro log, confrontati con il periodo precedente
Errori e peggio	I messaggi più frequenti di gravità errore o peggiore
Eventi letti dai profili	Accessi, amministrazione, firewall, VPN e traffico con il loro esito, e gli indirizzi, gli utenti e le porte più frequenti
Avvisi sugli eventi	Gli episodi del periodo (vedi Gli avvisi sugli eventi)
Mittenti non autorizzati	Che cosa è arrivato in quarantena

Leggere, stampare, conservare

Aprite un report per leggerlo. **Stampa o salva in PDF** lo stampa o lo salva come PDF dal browser.

Un report, una volta composto, non cambia più. In fondo c'è l'**impronta SHA-256** dei suoi dati: una copia salvata in PDF si può confrontare con quella del pannello, per dimostrare che non è stata modificata.

I report e la NIS2

I report mensili sono una buona base per documentare il monitoraggio: dicono che i log sono stati raccolti, per quanto tempo la ricezione è stata attiva, quali apparati hanno taciuto e quali eventi sono stati rilevati. Salvateli in PDF insieme al resto della documentazione di sicurezza.

Importare log da file

Quando iniziate a usare CSP (Central Syslog), i log degli anni passati sono spesso in un altro server: il vecchio server syslog, un NAS, una cartella di file. **Importa log** li porta nella subscription: una volta importati si cercano, si analizzano e si archiviano come quelli ricevuti dal pannello.

Il pulsante **Importa log** è nella pagina **Log** della subscription. Serve un ruolo che permetta di importare, e il piano della subscription deve consentirlo.

Come funziona

Un'importazione passa per quattro passi:

1. inviate i file;
2. il pannello li legge e mostra i mittenti che ha trovato;
3. scegliete l'apparato di ogni mittente e l'orologio delle sue ore;
4. il pannello scrive le righe, in coda.

L'elenco delle importazioni mostra per ognuna **Quando**, i **File**, le **Righe**, il **Periodo** e lo **Stato**: **In attesa dei file**, **Lettura dei file**, **In attesa delle tue scelte**, **In coda**, **Importazione in corso**, **Importata**, **Non riuscita** o **Tolta**.

1. Inviare i file

Nuova importazione offre tre modi:

Modo	Quando usarlo
Da questo computer	I file sono sul vostro computer. **Invia i file** li carica, mostrando l'avanzamento
Da un server (SFTP)	I file sono su un server raggiungibile dal pannello in SFTP: il pannello li scarica da lì, senza passare dal vostro computer. Serve anche il permesso **CSP · Importare log vecchi da un server (SFTP)**
Da indirizzi web (HTTPS)	I file sono pubblicati su un server web: scrivete gli indirizzi, uno per riga

Da un server (SFTP)

Scrivete **Server**, **Porta**, **Utente** e **Cartella dei log**, e scegliete l'**Accesso**:

- **Con la chiave del pannello (consigliato)**: la pagina mostra la chiave pubblica del pannello, da aggiungere all'utente sul server (con **Copia**). Nessuna password esce dalle vostre mani, la chiave è solo della vostra organizzazione e potete toglierla dal server quando volete;
- **Con la password dell'utente**: si usa solo per questa importazione e poi non si conserva.

Con **Collegati**, il pannello mostra l'impronta del server: controllate che sia quella del vostro server e confermate con **Sì, è il mio server**. Poi scegliete i file e **Scarica e leggi i file scelti**.

Da indirizzi web (HTTPS)

Solo indirizzi HTTPS: il pannello verifica il certificato del server e non scarica da un server con un certificato non valido. Se il server pubblica l'impronta SHA-256 di un file, scrivetela dopo il suo indirizzo: un file che non corrisponde non viene importato.

Per l'**Accesso** potete scegliere **Nessuno**, **Utente e password** o **Token**: si usano solo per questa importazione e non si conservano. **Controlla gli indirizzi** verifica che rispondano; poi **Scarica e leggi i file**.

2. Che cosa contengono i file

Il pannello legge i file e mostra **Cosa contengono i file**: quante righe, in quanti file, dal giorno al giorno, e **Le prime righe, come le legge il pannello**. Le righe in un formato che il pannello non legge sono contate e restano fuori.

3. Le vostre scelte

Per ogni **Mittente** trovato nei file (un indirizzo o un nome):

- **Apparato**: l'apparato della subscription a cui vanno le sue righe, oppure **Non importare**;
- **Orologio dell'apparato**: se l'apparato scriveva l'ora locale senza fuso orario (un router sull'ora italiana, per esempio), scegliete il suo fuso, e le ore vengono lette in quello. **Come scritto nel file** lascia le ore come sono.

Inoltre:

- **Lascia fuori le righe che contengono**: un testo per riga, senza badare alle maiuscole. Serve per lasciare fuori i messaggi di debug inutili;
- **Lascia fuori le righe prima del**: un giorno. Serve per le righe con un'ora sbagliata, come quelle di un router appena acceso con l'orologio al 1° gennaio.

Importa mette l'importazione in coda. Quando è finita, il **Risultato** dice quante righe sono state importate e di quale periodo.

Da sapere

- **Ogni file una volta sola**: un file già importato nella subscription viene rifiutato, anche con un altro nome.
- **Lo spazio**: le righe importate contano nello spazio del piano, non nel volume del mese.
- **Niente avvisi**: i log importati non fanno partire gli avvisi sugli eventi.

Togliere un'importazione

Dalla pagina di un'importazione:

- **Togli le righe di questa importazione** toglie le righe importate; i log ricevuti dal pannello restano;
- **Elimina questa importazione** elimina l'importazione e i suoi file.

Se un'importazione **Non riuscita** si ferma, non viene scritto niente: correggete il problema indicato e ripartite con una nuova importazione.

Archivi e backup dei log

CSP (Central Syslog) protegge i log della subscription in due modi:

- l'**Archivio log** conserva i log più vecchi del periodo consultabile, che non sono più nella pagina **Log**;
- i **Backup** sono copie di sicurezza della subscription, per ripristinarla se qualcosa va storto.

Archivio e copie condividono lo **spazio dei backup** del piano. La pagina mostra quanto ne occupano, per esempio "Spazio dei backup: copie 2 GB e archivio log 5 GB, 7 GB di 50 GB".

L'archivio dei log

Il piano stabilisce per quanto tempo i log restano consultabili nella pagina **Log**. Ogni notte i giorni che escono da quel periodo passano nell'archivio, un file per giorno; un mese archiviato per intero diventa un solo file.

La tessera **Archivio log** elenca gli archivi, con il **Periodo** (**Giorno** o **Mese**) e il numero di **Log**. Nell'archivio i log non si cercano più dal pannello: **Scarica** un archivio per consultarlo o conservarlo altrove.

Aprire un archivio

Un archivio è un file tar compresso con zstd, con un file CSV per ogni giorno. Si apre:

- su Linux, con `tar --zstd -xf <file>`;
- su Windows, con 7-Zip.

I file CSV si aprono con un foglio di calcolo.

Eliminare un archivio

Elimina cancella un archivio per sempre: i suoi log non sono più nel pannello. Fatelo solo dopo averlo scaricato e conservato altrove, per esempio per liberare spazio quando lo spazio dei backup è vicino al limite.

I backup della subscription

La tessera **Backup** contiene le copie di sicurezza di questa subscription. Funziona come il backup dell'organizzazione (vedi I backup della configurazione), ma riguarda solo questa subscription:

- in cima, l'**Ultima copia** con il suo esito, la **Prossima copia** della pianificazione e lo spazio;
- **Fai una copia adesso** ne fa una a mano, **Pianificazione** le fa da sole;
- una copia contiene la **Configurazione (nome, apparati, piano e limiti)**, i **Log consultabili**, o entrambi;
- la cifratura, le destinazioni remote, lo scaricamento e l'eliminazione sono gli stessi del backup dell'organizzazione.

Ripristina apre una pagina guidata: tornano i log mancanti e, se lo scegliete, la configurazione torna com'era nella copia.

Quale usare

Vi serve	Usate
Recuperare log cancellati per errore, o rimettere un apparato rimosso	Il backup della subscription
Riportare indietro utenti, ruoli e tutte le subscription insieme	Il backup dell'organizzazione
Consultare log di molti mesi fa	L'archivio dei log

Vi serve	Usate
Tenere una copia fuori dal server del pannello	Una destinazione remota nella pianificazione, oppure scaricare gli archivi

Lo spazio

Le copie con i log occupano molto spazio. Per restare nel limite:

- usate le copie **incrementali**: dopo una copia completa, le successive contengono solo i log nuovi;
- tenete un numero ragionevole di **Copie da conservare**;
- mandate le copie su una **destinazione remota**: lo spazio remoto non conta nel limite.

Quando lo spazio dei backup è vicino al limite o lo supera, arrivano gli avvisi dei consumi (vedi Le subscription).

La copia fuori sede

1. Introduzione

Che cosa fa il servizio

WFP (Web File) di Esapanel è uno **spazio fuori dalla vostra sede** dove i vostri NAS, i vostri server e i vostri PC mandano i backup e le copie dei file, con i programmi che usate già: Synology Hyper Backup, QNAP Hybrid Backup Sync, Duplicati, il Backup Manager di Plesk, rsync, FileZilla, WinSCP.

Il pannello non si limita a ricevere i file: **sorveglia che le copie arrivino**. Vi dice quando ogni apparato ha caricato l'ultima volta, vi avvisa se uno smette di caricare e compone ogni settimana e ogni mese un report con i giorni in cui le copie sono arrivate, anche come supporto alla documentazione delle misure di sicurezza richieste dalla direttiva NIS2.

WFP è una destinazione per le copie, non un disco di rete: non si monta come unità sui PC e non sostituisce il NAS dell'ufficio.

A chi si rivolge questa guida

Al personale IT dell'azienda, o al fornitore che ne gestisce i sistemi. Serve sapere come si configura un lavoro di backup su un NAS o su un server; non serve conoscere Esapanel.

Che cosa serve

- Una **subscription** WFP attiva.
- Un utente del pannello che possa aprire le pagine della subscription.
- L'accesso amministrativo agli apparati e ai programmi da collegare.
- Che gli apparati possano **uscire verso Internet** verso il server delle copie, sulle porte indicate nel capitolo 3. Non serve aprire nessuna porta in ingresso nella vostra rete.

In questa guida i nomi sono esempi (`copie.example.it`, `ab12c-nas`). I valori veri della vostra subscription sono nelle pagine del pannello.

---

2. Le pagine della subscription

Aprite la subscription nel pannello (**Servizi** › **Subscription**, poi la vostra subscription). Le tessere della copia fuori sede sono cinque:

Tessera	Che cosa contiene
Copia fuori sede	Lo spazio del piano, quello usato, il server e le porte a cui collegarsi
Account	Gli apparati, i programmi e le persone che mandano le copie, con le istruzioni per collegarli
Cartelle condivise	Cartelle della subscription che gli account scelti vedono insieme
Attività	Quando ogni account si è collegato e quanto ha caricato e scaricato
Report	I report settimanali e mensili delle copie arrivate

In ogni pagina il **?** in alto a destra apre la descrizione della pagina.

---

3. Lo spazio e dove collegarsi

La pagina **Copia fuori sede** mostra:

- **Codice**: cinque lettere e cifre date dal pannello, le stesse per tutta la vita della subscription. I nomi degli account cominciano con il codice: se il codice è `ab12c`, l'account `nas` entra come `ab12c-nas`.
- **Spazio del piano** e **Spazio usato**: lo spazio usato si misura ogni ora.
- **Account del piano** e **Cartelle condivise del piano**: quanti ne permette il piano.
- **Dove collegarsi**: il nome del **Server** e la porta di ogni protocollo.

Protocollo	Chi lo usa	Porta di solito
rsync (SSH)	Synology Hyper Backup, server Linux	60022
SFTP	Duplicati, WinSCP, FileZilla	50022
FTPS	Il Backup Manager di Plesk, FileZilla	21, con le porte passive 40000–40999
WebDAV (HTTPS)	QNAP Hybrid Backup Sync	443

Le porte vere sono quelle scritte nella pagina. Se il vostro firewall filtra il traffico in uscita, aprite verso il server solo le porte dei protocolli che usate; per FTPS servono anche le porte passive.

L'**FTP in chiaro non si accetta mai**: ogni collegamento è cifrato.

---

4. Aggiungere un account

Ogni apparato, programma o persona che manda le copie ha un **account**: la sua cartella sul server, la sua password o le sue chiavi SSH, i protocolli che può usare. Un account non entra nel pannello: serve solo a mandare e a rileggere i file. Date a ogni apparato un account suo, così sapete sempre chi ha caricato e potete fermarne uno senza toccare gli altri.

1. Aprite la tessera **Account** e premete **Aggiungi account**.
2. **Che cosa manda le copie?** Scegliete il programma: Synology Hyper Backup, QNAP Hybrid Backup Sync, Duplicati, Plesk, rsync su Linux, FileZilla, WinSCP, oppure **Un altro programma**. La scelta imposta il tipo e i protocolli di partenza e, dopo, le istruzioni.
3. **Nome**: lettere minuscole, cifre e trattini, per esempio `nas`. I programmi entrano con il nome completo, `ab12c-nas`.
4. **Descrizione**: facoltativa, per riconoscerlo ("NAS dell'ufficio").
5. **Tipo**: **Apparato o programma**, oppure **Persona** per chi carica a mano.
6. **Protocolli**: lasciate accesi solo quelli che servono al programma. Ogni protocollo è una porta verso la cartella.
7. **Chiavi pubbliche SSH**: facoltative, per rsync e SFTP, una per riga. L'account entra comunque anche con la sua password.
8. Premete **Crea l'account**.

Il pannello mostra la **password** dell'account. **Copiatela subito nel programma: viene mostrata solo questa volta.** Se si perde, date all'account una nuova password (capitolo 7).

Sotto la password trovate **Come collegarsi**: i passi per il programma scelto e **I valori da inserire** già compilati (server, porta, nome utente, cartella). Con **Istruzioni per** potete vedere le istruzioni di un altro programma.

---

5. Collegare i programmi

Le istruzioni complete, con i valori del vostro account, sono nella pagina dell'account. Qui i punti essenziali.

Synology Hyper Backup

1. In Hyper Backup create una nuova attività di backup dei dati e scegliete **rsync** come destinazione.
2. Tipo di server: **server compatibile rsync**. Nome server, porta, nome utente e password: quelli della pagina dell'account. Accendete la crittografia del trasferimento.
3. **Modulo di backup**: `backup`. **Directory**: un nome a scelta, la cartella di questa attività.
4. Vanno bene sia la versione multipla sia la versione singola; con la versione multipla accendete la crittografia lato client.

QNAP Hybrid Backup Sync

1. In Hybrid Backup Sync aprite **Spazi di archiviazione**, createne uno nuovo e scegliete **WebDAV**.
2. URL del server: l'**Indirizzo (WebDAV)** della pagina dell'account, in HTTPS; nome utente e password dell'account.
3. Create un **lavoro di backup** verso quello spazio, con una cartella a vostra scelta.
4. Tenete accese le versioni e accendete la cifratura lato client.

Verso un server rsync Hybrid Backup Sync fa solo lavori di sincronizzazione, senza versioni: per un vero backup usate WebDAV.

Duplicati

1. Aggiungete un backup; nella destinazione scegliete **SFTP (SSH)**.
2. Server, porta, nome utente e password dell'account. Percorso sul server: `/` o una sottocartella, per esempio `/pc-ufficio`.
3. Verificate la connessione e accettate la chiave del server solo se è una di quelle mostrate nella pagina dell'account (**Chiavi del server**).
4. Tenete la cifratura AES-256 con una frase segreta vostra.

Plesk

1. In Plesk aprite **Strumenti e impostazioni › Gestione backup › Impostazioni dell'archivio remoto › FTP** (per tutto il server), oppure la Gestione backup di una subscription.
2. Nome host del server FTP, nome utente e password dell'account. Directory dei file di backup: `/`.
3. Accendete la **modalità passiva** e **FTPS**.
4. Accendete la protezione con password dei backup.

Plesk lascia nella cartella un file `.ftpaccess`: è normale, e il server lo ignora.

rsync su Linux

1. Mettete la chiave pubblica dell'utente che lancia rsync fra le chiavi SSH dell'account, o usate la password.
2. Mandate con rsync su SSH alla porta di rsync, nella **Cartella (rsync)** dell'account, che è un percorso assoluto. Per esempio:

   ```
   rsync -a -e "ssh -p 60022" /percorso/dei/backup/
   ab12c-nas@copie.example.it:/srv/wfp/ds1/ab12c/accounts/ab12c-nas/
   ```

3. Le opzioni `--inplace` e `--append` sono rifiutate: ogni file arriva come file nuovo, e una copia interrotta non rovina quella di prima.

FileZilla e WinSCP

Per chi carica a mano. In **SFTP** usate la porta di SFTP e accettate la chiave del server solo se è una di quelle della pagina dell'account. In FileZilla potete usare anche **FTP con "Richiedi FTP esplicito su TLS"** sulla porta di FTPS. In SFTP e FTPS la cartella è `/`: l'account vede solo la sua.

Un altro programma

Qualunque programma che manda in SFTP, in FTPS (TLS esplicito, modalità passiva), in rsync su SSH o in WebDAV può usare un account, con i valori della sua pagina.

---

6. Cifrare le copie

Accendete sempre la **cifratura del programma** (Hyper Backup, Hybrid Backup Sync, Duplicati, Plesk), con una password conservata **fuori** dall'apparato e fuori dal server delle copie.

Così le copie restano leggibili solo da voi: chi gestisce il server conserva dati che non può leggere. Attenzione al rovescio: **senza quella password nessuno, nemmeno noi, può ripristinare le copie**.

---

7. Gestire un account

Nella tessera **Account** la lista mostra per ogni account il tipo, i protocolli, l'**Ultimo caricamento** e lo stato. Aprite un account per:

- **Protocolli e chiavi**: cambiare la descrizione, i protocolli, le chiavi SSH e gli avvisi (capitolo 9).
- **Nuova password**: il pannello ne genera una nuova e la mostra una volta. I programmi che usano quella vecchia non entrano più finché non gli date la nuova.
- **Sospendi**: l'account non entra più in nessun protocollo e le sue sessioni finiscono subito; **i file restano**. **Riattiva** lo rimette in funzione.
- **Rimuovi**: l'account e **tutti i file della sua cartella vengono rimossi per sempre**. Non si torna indietro.

Gli stati di un account: **Attivo**, **Sospeso**, **In preparazione**, **Non pronto** (il server non ha accettato l'account: apritelo e premete **Riprova**).

Se un apparato viene compromesso o dismesso, sospendete subito il suo account: gli altri continuano a lavorare.

---

8. Cartelle condivise

Una **cartella condivisa** appartiene alla subscription, non a un account. Gli account che scegliete la trovano come una cartella dentro la loro, e un file caricato da uno può essere letto e modificato dagli altri. Serve, per esempio, a più persone che depositano documenti nello stesso posto.

1. Aprite la tessera **Cartelle condivise** e premete **Aggiungi una cartella condivisa**.
2. **Nome**: gli account vedono una cartella con questo nome dentro la loro.
3. **Account che la vedono**: scegliete gli account.

Regole:

- La vedono solo gli account con **SFTP o FTPS**, e **senza rsync**. Un account che usa rsync non può vedere una cartella condivisa, e un account che ne vede una non può accendere rsync.
- In WebDAV e in rsync le cartelle condivise non si vedono.
- Un account aggiunto la vede alla connessione successiva; un account tolto la perde subito.
- **Rimuovi** cancella la cartella condivisa e tutti i suoi file, per tutti gli account.
- Lo spazio di una cartella condivisa conta nello spazio della subscription.

---

9. Controllare che le copie arrivino

Ultimo caricamento

Nella lista degli account, **Ultimo caricamento** è la fine dell'ultima sessione in cui l'account ha caricato almeno un file. Un account che non ha ancora caricato mostra **Mai**.

Gli avvisi

Nella pagina dell'account, in **Protocolli e chiavi**:

- **Avvisa se non carica da**: 12 ore, 1, 2, 3 o 7 giorni. Passato quel tempo dall'ultimo caricamento ricevete **un** avviso per email, e nella lista l'account è segnato **In ritardo**; quando torna a caricare ricevete l'avviso della ripresa. Un account di tipo **Apparato o programma** nasce con l'avviso acceso a **1 giorno**; uno di tipo Persona senza avviso. Scegliete un tempo un po' più lungo dell'intervallo dei vostri backup: per un backup notturno 1 giorno va bene, per uno settimanale 7 giorni.
- **Avvisa se la copia è molto più piccola del solito**: spento per default. Vi avvisa quando una sessione carica meno della metà di quanto l'account carica di solito: è il caso di un backup che arriva, ma monco.

Un account appena creato non avvisa finché non ha caricato la prima volta. Con la subscription sospesa gli avvisi sono sospesi.

L'attività

La tessera **Attività** elenca le **sessioni**: una riga è tutto quello che un account fa in un protocollo, finché non resta un'ora senza fare niente. Per ogni sessione vedete account, protocollo, indirizzo da cui si è collegato, inizio e fine, file e spazio caricati e scaricati. Il backup di un NAS è di solito una sessione con molti file.

- **In corso**: l'ora di silenzio non è ancora passata, e i numeri crescono ancora.
- **Rifiutati o falliti**: un caricamento interrotto, un file rifiutato perché lo spazio è oltre il limite, un comando non permesso. Una sessione con solo questo numero e niente di caricato merita un controllo sull'apparato.

I singoli file non sono elencati. Il piano dice per quanti giorni le sessioni si conservano.

---

10. I report

La tessera **Report** raccoglie un report per ogni **settimana** (composto il lunedì) e uno per ogni **mese** (composto il primo). Quando un report è pronto ricevete un'email con il collegamento.

Un report dice, per ogni account:

- i **giorni con una copia**: quanti giorni del periodo, e quali, hanno visto arrivare almeno un file;
- i file e lo spazio caricati;
- l'ultimo caricamento.

Seguono i totali e lo spazio usato. Aprite un report per leggerlo e premete **Stampa o salva come PDF** per conservarlo.

Un report **non cambia più** dopo essere stato composto: l'impronta in fondo attesta che i dati sono quelli del giorno in cui è stato fatto. I report si conservano per i giorni in cui il piano conserva l'attività.

In **Le tue scelte** decidete quali report volete (settimanale, mensile).

> Un report prova che le copie **arrivano**, non che si possono **ripristinare**. Quello si verifica solo con una prova di ripristino dall'apparato o dal programma: fatela periodicamente.

11. Quando lo spazio finisce

Quando lo spazio usato supera lo **Spazio del piano**, gli account vanno in **sola lettura**: leggono e cancellano, ma non caricano. Ricevete un avviso per email, e le pagine lo mostrano in rosso.

- Un caricamento già cominciato finisce; i successivi sono rifiutati.
- I programmi di backup segnalano un errore, spesso generico: Hyper Backup scrive solo "Impossibile eseguire l'attività di backup". Se un backup fallisce senza un motivo chiaro, guardate per prima cosa lo spazio.
- Per tornare a caricare liberate spazio (riducete il numero di versioni conservate dal programma, o cancellate copie vecchie) oppure chiedete più spazio. Lo spazio si rimisura ogni ora: quando rientra nel limite la sola lettura si toglie da sola, e ricevete un avviso.

Prima del limite il pannello vi avvisa quando lo spazio supera la soglia di preavviso del piano.

12. Subscription sospesa o eliminata

- **Sospesa o disattivata**: gli account sono bloccati e non entrano; **i file restano**. Quando la subscription torna attiva gli account funzionano di nuovo, con le stesse password.
- **Eliminata**: i file si conservano **30 giorni**, poi vengono cancellati per sempre.

13. Problemi frequenti

Che cosa succede	Che cosa controllare
Il programma non si collega	Server e porta della pagina **Copia fuori sede**; che il vostro firewall lasci uscire verso quella porta; per FTPS anche le porte passive
"Accesso negato"	Il nome utente completo, con il codice (`ab12c-nas`); la password, mostrata solo alla creazione: nel dubbio **Nuova password**; che l'account non sia **Sospeso** e che abbia quel protocollo acceso
Il programma chiede se fidarsi del server	Confrontate la chiave con le **Chiavi del server** nella pagina dell'account, e proseguite solo se è una di quelle
Dopo molti tentativi sbagliati non si collega più nemmeno con la password giusta	Il server blocca per un po' gli indirizzi che sbagliano ripetutamente: aspettate, o chiedete all'assistenza di sbloccare il vostro indirizzo
Il backup fallisce senza un motivo chiaro	Lo spazio: oltre il limite gli account sono in sola lettura (capitolo 11)
Un caricamento FTPS interrotto non riprende	È voluto: un file arriva sempre intero, e la ripresa è rifiutata. Il programma ricarica il file dall'inizio
rsync rifiuta `--inplace` o `--append`	È voluto, per lo stesso motivo: toglietele
L'account non vede la cartella condivisa	Serve SFTP o FTPS, senza rsync; la cartella compare alla connessione

Che cosa succede	Che cosa controllare
	successiva
L'account è segnato **In ritardo** ma il backup gira	Guardate in **Attività** se le sessioni caricano file; se il backup è più raro dell'avviso, allungate **Avvisa se non carica da**
Nell'**Attività** non compare un caricamento appena fatto	Le sessioni si aggiornano ogni pochi minuti

14. Per amministratori e reseller

Chi amministra il server o rivende il servizio trova in più:

- **Verifica**, nella pagina **Copia fuori sede**: ogni notte il pannello confronta quello che il server ha per la subscription (cartelle, proprietari, permessi, utenti, gruppi) con quello che conosce, ed elenca le differenze. **Verifica adesso** lo fa subito; **Repair** riscrive tutto come lo conosce il pannello. Nessun file viene mai cancellato: quello che il server ha e il pannello non conosce viene elencato e lasciato com'è.
- **Il backup della configurazione**: i backup del cliente e del server contengono gli account (con le loro password e chiavi), le cartelle condivise e i report, **non i file**: quelli sono già copie. Dopo un ripristino i programmi dei clienti rientrano con le stesse credenziali.
- **Lo spazio del server**: l'amministratore è avvisato quando il disco delle copie supera l'80% e il 90%; al 95% tutti gli account vanno in sola lettura, finché non si scende sotto il 90%.
- **Le API**: spazio, account, cartelle condivise e attività si gestiscono anche dalle API del pannello, per il provisioning e per i sistemi di monitoraggio.

Host e check

UCP (Uptime Check) controlla di continuo che i vostri server, firewall, siti e servizi rispondano, e vi avvisa quando qualcosa smette di funzionare. Un **host** è una macchina da controllare, come un server, un firewall, una stampante o un sito. Un **check** è un controllo su quell'host, come "il sito risponde", "la porta 443 è aperta" o "il certificato non scade fra poco".

Dove si trova

- Nella subscription, la tessera **Host** elenca gli host di quella subscription. Il numero sulla tessera dice quanti problemi sono aperti.
- Nel menu, il gruppo **Moduli** ha **Host**, **Problemi** e **Downtime**, con gli host di tutte le vostre subscription.

Il piano stabilisce quanti host e quanti check può avere la subscription, e ogni quanto possono girare: la pagina mostra il conteggio, per esempio "4 di 10 host" e "12 di 50 check".

Aggiungere un host

Aggiungi host chiede:

Campo	Che cosa scrivere
Nome	Un nome per voi, come "Firewall sede"
Indirizzo	Un indirizzo IP o un nome DNS. Un nome viene risolto di nuovo a ogni check
Check di host	Il controllo che dice se l'host è **Up** o **Down**: **Ping** per la maggior parte degli host; **Porta TCP**, con una porta sempre aperta, per un host che non risponde al ping
Controlla ogni	Ogni quanto gira il check di host. Il piano stabilisce l'intervallo più breve

Il primo check parte entro un minuto.

Scegliete un check di host che fallisce solo quando tutto l'host è irraggiungibile: quando l'host è down, i suoi altri check non avvisano, avvisa solo l'host.

Aggiungere i check

Aprite l'host e premete **Aggiungi check**. Scegliete il tipo:

Tipo	Che cosa controlla
Ping	L'host risponde, entro i tempi e la perdita di pacchetti che impostate
Porta TCP	Una porta accetta connessioni, e in quanto tempo
HTTP/HTTPS	Una pagina risponde, con il codice di stato e il testo che vi aspettate
DNS	Un nome si risolve, con il valore che vi aspettate
Certificato TLS	Il certificato è valido e non scade entro

Tipo	Che cosa controlla
	i giorni che impostate

Esempi

- **Un sito**: un check **HTTP/HTTPS** con **HTTPS** acceso, il **Nome del sito** se l'host ne serve più di uno, e magari un **Testo nella pagina** che compare solo quando il sito funziona davvero. **Controlla anche il certificato (con HTTPS)** aggiunge insieme un check **Certificato TLS**, che avvisa prima che il certificato scada (conta come un check in più).
- **Un server di posta**: un check **Porta TCP** sulla porta 25, e un check **Certificato TLS** con **SMTP con STARTTLS**.
- **Il nome DNS dinamico di un firewall**: un check **DNS** con il **Valore atteso**, chiedendo **Ai server autorevoli del nome**, che mostrano subito un cambio. In **Indirizzi delle linee di backup** scrivete gli indirizzi di una linea di riserva, come una linea LTE: quando il nome risponde uno di quelli, il check va in **Warning** invece che in **Critical**.

Quando gira un check

In **Quando gira**:

- **Controlla ogni**: l'intervallo normale;
- **Riprova ogni**: dopo un fallimento, il check si ripete più spesso;
- **Tentativi**: quanti fallimenti di seguito confermano il problema.

Con 3 tentativi e una ripetizione ogni minuto, un problema è confermato due minuti dopo il primo fallimento. Così un singolo pacchetto perso non vi sveglia di notte. Un check che torna a rispondere è OK subito.

Gli stati

Stato	Che cosa vuol dire
Up / **Down**	L'host risponde o non risponde al check di host
OK	Il check funziona
Warning	Il check funziona male, per esempio è lento o il certificato scade fra poco
Critical	Il check non funziona
Unknown	Il check non si è potuto eseguire, per esempio perché il nome dell'host non si risolve: leggete l'esito
In attesa	Prima del primo esito
Non controllato	L'host o il check è disattivato

"da confermare" segna un fallimento che ha ancora tentativi.

La pagina di un host

La pagina di un host mostra:

- lo **Stato** e da quando;
- i **Check**, ognuno con il suo stato, l'**Ultimo esito** e quando ha girato. Aprite un check per vedere il suo storico;
- la **Disponibilità dell'host**: la quota di tempo **Up** su 24 ore, 7 giorni, 30 giorni e 12 mesi; la barra de **Gli ultimi 90 giorni**, un segmento al giorno (verde da 99,9 %, giallo da 99 %, rosso sotto, grigio senza dati); il **Tempo di risposta, ultimi 7 giorni**. I downtime non contano. Si aggiorna ogni ora;

- i **Downtime** (vedi Downtime e disponibilità);
- i **Cambi di stato**, i più recenti prima.

Prova adesso esegue subito tutti i check e mostra che cosa rispondono, senza scrivere niente nello storico: è utile dopo aver cambiato un parametro o riparato un servizio.

Modifica cambia nome, indirizzo, nota e check di host. **Disattiva** ferma l'host con tutti i suoi check senza eliminare nulla; **Riattiva** lo fa ripartire. **Elimina** toglie l'host, i suoi check e il loro storico.

I problemi

Moduli › **Problemi** mostra quello che adesso non va:

- **Host down**: gli host il cui check di host ha fallito tutti i tentativi;
- **Check**: i check con uno stato confermato **Warning**, **Critical** o **Unknown**. Un check di un host down è segnato "host down": guardate prima l'host.

Un problema esce dalla pagina quando il check torna OK.

Prendere in carico un problema

Nella pagina del check, **Prendi in carico** dice che qualcuno se ne sta occupando, con una **Nota**: gli avvisi di quel problema non si ripetono più, per nessuno. Il problema resta nella pagina segnato **Preso in carico**.

La presa in carico cade da sola quando il check torna OK, e un problema nuovo avvisa di nuovo. **Annulla la presa in carico** fa ripartire le ripetizioni.

Gli avvisi

Un'email parte quando un problema è confermato, dopo i tentativi del check, e una quando finisce. Chi le riceve lo decide il vostro fornitore nelle notifiche (vedi Le notifiche).

Invia gli avvisi, nella pagina degli host della subscription, dice se gli avvisi si ripetono finché il problema resta:

Scelta	Che cosa succede
Solo al cambio di stato	Un'email quando il problema inizia e una quando finisce
Al cambio di stato e poi ogni ora	Anche un promemoria ogni ora, finché il problema resta
A ogni esecuzione fallita	Un'email ogni volta che il check trova il problema: con un check ogni 5 minuti, 12 email all'ora

Un host può avere una scelta sua, nella sua pagina **Modifica**; **Come impostato per la subscription** segue quella della subscription.

Downtime e disponibilità

Un **downtime** è un periodo in cui UCP (Uptime Check) non manda avvisi su un host o su un check: per esempio una manutenzione che conoscete, un aggiornamento del firewall, o la finestra notturna in cui il vostro provider fa i backup e il server rallenta.

Che cosa succede durante un downtime

- I check continuano a girare e i loro stati cambiano.
- Nessun avviso parte, per nessun utente.
- Il tempo in downtime non conta nella disponibilità.
- Un problema ancora aperto alla fine del downtime viene segnalato al primo giro dopo.

La pagina di un host in downtime lo dice: "In downtime fino al …: nessun avviso parte".

Pianificare un downtime

I downtime si pianificano dalla pagina di ogni host, nella sezione **Downtime**:

Campo	Che cosa scegliere
Su	**Tutto l'host**, oppure un solo check
Ripeti	**Una volta** oppure **Ogni settimana**
Dalle e **Alle**	Per un downtime una tantum, l'inizio e la fine
Giorno, **Alle ore** e **Per (minuti)**	Per un downtime settimanale, il giorno, l'ora di inizio e la durata
Nota	Facoltativa: il motivo, come "manutenzione del provider"

Poi **Pianifica downtime**. Gli orari sono nel vostro fuso orario.

Elimina toglie un downtime: gli avvisi ripartono dal giro successivo. Un downtime una tantum finito sparisce da solo.

Esempi

- **Aggiornamento del firewall sabato sera**: **Tutto l'host**, **Una volta**, dalle 22:00 alle 23:30.
- **Backup notturni del provider**: un check **HTTP/HTTPS** che ogni notte rallenta, **Ogni settimana** per ogni giorno interessato, alle 02:00 per 60 minuti.

Tutti i downtime

Moduli › Downtime elenca i downtime di tutti i vostri host: prima quelli **In corso**, poi i **Prossimi**, con l'host, su che cosa, quando e chi li ha pianificati (**Pianificato da**). Si pianificano e si eliminano dalla pagina di ogni host.

La disponibilità

La disponibilità è la quota di tempo in cui un host è stato **Up**, o un check **OK**. Si vede nella pagina dell'host (dal check di host) e nella pagina di ogni check:

- su **24 ore**, **7 giorni**, **30 giorni** e **12 mesi**;
- **Gli ultimi 90 giorni**, una barra con un segmento al giorno: verde da 99,9 %, giallo da 99 %, rosso sotto, grigio senza dati. Puntate un giorno per leggerne il valore e i minuti in downtime;
- il **Tempo di risposta, ultimi 7 giorni**, ora per ora, con il valore **Medio** e il **Più alto**.

I downtime e l'attesa del primo esito non contano. La disponibilità si aggiorna ogni ora.

È il numero da mostrare a chi vi chiede quanto un servizio è stato disponibile, per esempio per verificare quello che vi promette un fornitore.

I report DMARC

DMARC è il record DNS che dice ai server di posta come trattare i messaggi che usano il vostro dominio come mittente senza esserne autorizzati. Ogni giorno i grandi riceventi della posta (Google, Microsoft, Yahoo e gli altri) mandano all'indirizzo scritto nel record DMARC un **report aggregato**: da quali server è arrivata la posta a nome del vostro dominio, quanta ha passato SPF e DKIM, che cosa ne hanno fatto.

Questi report sono file XML difficili da leggere. DRP (DMARC Report) li raccoglie e li mostra in modo leggibile, così potete vedere:

- se tutta la vostra posta legittima passa DMARC, prima di rendere più severa la politica (da `p=none` a `p=quarantine` o `p=reject`);
- chi manda posta a nome vostro: un servizio di newsletter dimenticato, un gestionale, o qualcuno che si spaccia per voi.

DRP legge i report aggregati (`rua`). I report dei singoli messaggi falliti (`ruf`) non sono compresi.

I domini

La tessera **DMARC** della subscription apre **Domini DMARC**: i domini di cui la subscription segue i report, con il numero di **Report** e l'**Ultimo report**. Il piano stabilisce quanti domini potete seguire.

Aggiungi dominio chiede il **Dominio**, come nel record DMARC, per esempio `example.com`, e una **Nota** facoltativa.

- I sottodomini senza un record DMARC proprio sono nei report del dominio. Un sottodominio con un record proprio riceve report propri: aggiungetelo come dominio per seguirlo a parte.
- Un dominio può essere seguito da una sola subscription del pannello.
- **Togli** smette di seguire un dominio: i suoi riassunti se ne vanno con lui, i suoi report restano fino alla scadenza.

Come arrivano i report

Il riquadro **Come arrivano i report** dice come il pannello riceve i report della subscription. Ci sono due modi.

Una casella di posta

Il pannello legge una casella dove arrivano i report: l'indirizzo scritto nel `rua` del vostro record DMARC, per esempio `rua=mailto:dmarc@example.com`. Ogni 15 minuti prende i messaggi che sembrano report e li legge.

In **Caselle DMARC**, **Aggiungi casella** chiede:

Campo	Che cosa scrivere
Indirizzo	L'indirizzo della casella, come nel `rua`. Facoltativo
Protocollo	**IMAP** o **POP3**
Server, **Porta**, **Sicurezza**	Il server della posta; sempre **TLS** o **STARTTLS**
Utente e **Password**	L'accesso alla casella. La password si conserva cifrata e non si mostra più
Cartella letta	Per IMAP, la cartella dove arrivano i report
Cartella degli elaborati	Per IMAP, dove il pannello sposta i

Campo	Che cosa scrivere
	report presi

Da sapere:

- **Solo i report**: il pannello guarda l'oggetto dei messaggi ("Report Domain: …") e scarica solo quelli; gli altri non vengono letti né segnati come letti. Meglio una casella usata solo per i report.
- Con **IMAP** i report presi si spostano nella cartella degli elaborati: quello che resta nella cartella letta è posta che non è un report. Sui server che tengono tutte le cartelle sotto INBOX il pannello le trova e le crea da solo.
- Con **POP3** i report presi si cancellano dalla casella 7 giorni dopo.
- **Microsoft 365** non accetta IMAP e POP3 con la password: per ora le sue caselle non si possono usare.
- Una casella serve tutti i domini il cui record la nomina: il pannello legge il dominio in ogni report.

Prova la casella entra e dice quanti messaggi ci sono, senza prendere niente. **Leggi ora** legge subito. **Spegni** e **Accendi** fermano e riprendono la lettura. Lo **Stato** dice **Letta**, **Non ancora letta**, oppure **Non si legge dal …** quando qualcosa non va: il motivo è scritto accanto.

Caricare i report a mano

Nella pagina di un dominio, **Carica report** accetta file XML, compressi `.gz` o `.zip`, oppure messaggi salvati come `.eml`. Serve a portare nel pannello lo storico di un dominio i cui report arrivavano a un'altra casella o a un altro servizio: scaricateli da lì, poi caricateli qui.

Per ogni file la pagina dice com'è andata: **Report scritto**, **Già ricevuto** (un report non si scrive due volte), **Non letto**.

Leggere i report

La pagina di un dominio mostra gli **Ultimi 30 giorni**, con i messaggi che i riceventi hanno contato e quanti hanno passato DMARC, e l'elenco dei **Report ricevuti**: **Periodo**, **Ricevente**, **Messaggi**, **Passano DMARC**, **Politica** e come è **Arrivato**.

Un report mostra:

- la **Politica vista dal ricevente**: il vostro record DMARC come l'ha letto il ricevente;
- le **Righe**: per ogni indirizzo di origine (**Fonte**), i **Messaggi**, se **DKIM** e **SPF** sono passati allineati con il dominio del mittente, e che cosa il ricevente ha **Applicato** (**consegnato**, **quarantena**, **rifiutato**). DMARC passa quando almeno uno fra DKIM e SPF passa allineato;
- **Firme e SPF visti**: le firme DKIM e il controllo SPF com'erano, anche quando non allineati.

Scarica XML salva il report originale.

Che cosa guardare

- Una **Fonte** che non riconoscete, con molti messaggi che non passano DMARC, è spesso qualcuno che si spaccia per voi: con una politica `p=reject` quei messaggi vengono rifiutati.
- Una fonte vostra (il vostro server di posta, il servizio di newsletter, il gestionale che manda le fatture) che non passa DMARC va sistemata, aggiungendola al record SPF o configurando DKIM, **prima** di rendere più severa la politica: altrimenti la vostra stessa posta verrebbe rifiutata.