Manuale dell’amministratore

Esapanel

Esalogica

15/11/2026

Indice

L'installazione....4
Prima di cominciare....4
Installare....4
Dopo l'installazione....5
Eseguire di nuovo esapanel-setup....5
La sicurezza di partenza....5
La licenza....6
Attivare la licenza....6
Il controllo giornaliero....6
La scadenza....6
Un'altra macchina....6
Aggiornamenti, riavvio e spegnimento....7
Gli aggiornamenti di Esapanel....7
Riavvio e spegnimento....7
Rete e sicurezza....9
Gli indirizzi IP....9
La panoramica della sicurezza....9
Il firewall....9
I ban IP....10
Gli scanner di Internet....10
Certificati, posta e DNS....11
Il certificato del pannello....11
La posta....11
Il DNS....12
I reseller....13
Creare un reseller....13
I piani reseller....13
Le risorse del reseller....13
Il resto....13
Statistiche e notifiche....14
Le statistiche del server....14
Le notifiche....14
Disaster recovery....16
Che cosa contiene....16
Fare i backup....16
La chiave del server....16
Ripristinare su questo server....16
Ricostruire il server su un server nuovo....16

Una prova ogni tanto....17
CSP: la ricezione dei log....18
Lo stato della ricezione....18
I log che non arrivano al database....18
Le porte senza risposta....18
Le porte nel firewall....18
Il certificato....18
UCP: le impostazioni dei check....19
Tutti gli host....19
I check verso indirizzi privati....19
Il resolver....19
Il firewall in uscita....19
WFP: i datastore e la rilocazione....20
I datastore....20
La rilocazione....20
La copia remota....20
Verifica e repair....21
LSP: il server delle licenze....22
Una licenza è una subscription....22
Le licenze....22
La pagina di una licenza....22
I trasferimenti....22
Un server delicato....23

Come installare Esapanel e gestire il server: la licenza, gli aggiornamenti, la rete e la sicurezza, i reseller, il backup del server e le impostazioni dei moduli. Per le pagine che vedono anche reseller e clienti, vedi i loro manuali.

L'installazione

Esapanel si installa su un server Debian 13 appena installato, fisico o virtuale (VMware, Hyper-V, Proxmox e gli altri ambienti KVM), anche un VPS. Uno script aggiunge il repository dei pacchetti, installa il pacchetto `esapanel` e lancia `esapanel-setup`, che configura il server e il pannello.

Prima di cominciare

- **Debian 13** appena installato, architettura **amd64** o **arm64**, con accesso da **root**.
- Il **nome completo definitivo** del server, come `log.example.com`, e il suo **indirizzo definitivo**: il pannello li usa per il suo certificato e per la licenza. Il nome deve risolversi nell'indirizzo.
- **Accesso a Internet** in uscita: il repository dei pacchetti in HTTPS (porta 443) e il server delle licenze (`license.esalogica.com`, porta 9444). Un server senza Internet non può attivare né controllare la licenza.
- Il **codice di attivazione** della licenza, se lo hai già: si può inserire anche dopo, nel pannello.
- Per i moduli che conservano molti dati (i log di CSP, le copie fuori sede di WFP), un disco o una partizione a parte, montata prima dell'installazione.

Installare

Come root:

```
wget -qO install.sh https://repo.esalogica.com/install.sh && bash install.sh --modules=csp
```

Su un Debian minimale senza `wget`, prima: `apt-get install -y wget ca-certificates`.

Lo script controlla il sistema, il nome e l'architettura, aggiunge la chiave e il repository dei pacchetti, installa `esapanel` e lancia `esapanel-setup`. Se mancano i dati dell'amministratore, li chiede.

Le opzioni

Le opzioni di `install.sh` passano a `esapanel-setup`:

Opzione	Che cosa fa
`--channel=stable`	Il canale dei pacchetti: `stable` (predefinito) o `testing`, per i server di prova. Solo di `install.sh`
`--modules=csp,ucp`	I moduli da installare: `csp`, `ucp`, `drp`, `wfp`, `lsp`, anche insieme
`--license=ESAP-XXXX-XXXX-XXXX-XXXX`	Il codice di attivazione
`--company=`, `--name=`, `--username=`, `--email=`	L'azienda e l'amministratore del pannello
`--sender=panel@example.com`	Il mittente della posta del pannello; senza, `panel@` seguito dal nome del server
`--ssh-port=22`	La porta SSH che il firewall lascia aperta
`--backups-path=/var/lib/esapanel/backups`	La cartella dei backup, meglio su un disco a parte
`--wfp-datastore=/srv/wfp/ds1`	Il primo datastore di WFP (Web File), meglio il mount di un disco suo

La password dell'amministratore viene chiesta, oppure letta dalla variabile d'ambiente `ESAPANEL_ADMIN_PASSWORD`: mai sulla riga di comando.

I moduli

Modulo	Che cosa installa
`csp`	CSP (Central Syslog): la ricezione dei log
`ucp`	UCP (Uptime Check): i plugin dei check e il database dei risultati
`drp`	DRP (DMARC Report): il database dei report DMARC
`wfp`	WFP (Web File): FTPS e SFTP, rsync sulla porta 60022, WebDAV sulla 443, il datastore delle copie
`lsp`	LSP (License Server): il server delle licenze, sulla porta 9444. Serve solo a chi vende le licenze

Un modulo si può aggiungere dopo: esegui di nuovo `esapanel-setup` con tutti i moduli, quelli di prima e quello nuovo. Il modulo deve essere anche nella licenza.

Dopo l'installazione

Alla fine `esapanel-setup` mostra l'indirizzo del pannello:

```
https://log.example.com:9943
```

1. Apri l'indirizzo. Il pannello parte con un **certificato autofirmato**: il browser lo segnala, ed è normale. Sostituiscilo subito con uno di Let's Encrypt (vedi Certificati, posta e DNS).
2. Entra con l'amministratore creato dall'installazione.
3. Se non l'hai dato con `--license`, inserisci il **codice di attivazione** (vedi La licenza).
4. Conferma il **mittente** della posta in **Server › Posta**: finché non lo fai, ogni pagina te lo ricorda.
5. Attiva il **secondo fattore** sul tuo account.
6. Controlla il **firewall**: per esempio apri SSH solo dal tuo ufficio (vedi Rete e sicurezza).
7. Imposta il **backup del server** su una destinazione remota (vedi Disaster recovery).

Eseguire di nuovo esapanel-setup

`esapanel-setup` si può eseguire di nuovo quando vuoi: quello che è già configurato resta (la password del database, la chiave dell'applicazione, il certificato), il resto viene riscritto, e il pannello si installa una volta sola. Serve per aggiungere un modulo, aggiungere un datastore di WFP o riscrivere gli indirizzi IP aggiunti dal pannello.

Non modificare a mano i file che `esapanel-setup` scrive: eseguilo di nuovo.

La sicurezza di partenza

- Il **firewall** del pannello è attivo dall'installazione: aperti il pannello, SSH e le porte dei moduli.
- **fail2ban** protegge SSH, l'accesso al pannello e il server web.
- Gli **aggiornamenti di sicurezza di Debian** sono automatici.

La licenza

Il pannello funziona con una licenza rilasciata da Esalogica per il tuo server. La licenza dice quali moduli puoi usare e con quali limiti, per esempio quante subscription.

La pagina è **Server › Licenza**.

Attivare la licenza

Scrivi il **codice di attivazione** che hai ricevuto, nella forma `ESAP-XXXX-XXXX-XXXX-XXXX`. Il pannello lo invia al server delle licenze di Esalogica, che lega la licenza a questo server.

Un codice nuovo sostituisce la licenza attuale. Per aggiungere un modulo alla licenza non serve un codice nuovo: lo porta **Controlla ora**. Se il modulo non è ancora installato sul server, la pagina lo dice: installalo con `esapanel-setup` (vedi L'installazione).

Senza una licenza valida entra nel pannello solo l'amministratore, in questa pagina. I servizi già configurati, come la ricezione dei log, continuano a funzionare.

Il controllo giornaliero

Ogni giorno il pannello controlla la licenza con Esalogica, e riceve da solo rinnovi e modifiche. **Controlla ora** lo fa subito, per esempio dopo un rinnovo.

Se il controllo non riesce, per esempio senza Internet, non si ferma niente: la licenza resta valida fino alla scadenza, e dopo 7 giorni ricevi un avviso. Controlla che il server raggiunga `license.esalogica.com` sulla porta 9444.

La scadenza

- Gli amministratori ricevono un'email 7, 3 e 1 giorni prima della scadenza, il giorno stesso, 5 e 10 giorni dopo, e quando il pannello si è fermato. Dopo l'accesso la vedono da 7 giorni prima.
- Dopo la scadenza il pannello funziona per altri **10 giorni**, con un avviso a tutti. Una licenza **Trial** si ferma subito.
- Un rinnovo arriva al pannello da solo e ferma le email.

Un'altra macchina

La licenza è legata a questo server da un'**impronta**, che cambia quando il server viene ripristinato su un'altra macchina o copiato. Dopo un ripristino su un altro server, o su una copia del server, la licenza appartiene alla macchina di prima: il pannello funziona per 10 giorni.

Trasferisci la licenza su questo server con il pulsante della pagina. Una licenza si sposta da sola fino a 2 volte in 30 giorni; oltre, il trasferimento aspetta l'approvazione di Esalogica.

La pagina mostra l'impronta: Esalogica può chiedertela per emettere una licenza a mano o per seguire un trasferimento.

Aggiornamenti, riavvio e spegnimento

Gli aggiornamenti di Esapanel

Le versioni nuove arrivano dal repository dei pacchetti, che il pannello controlla ogni ora. La pagina è **Server › Aggiornamenti**: mostra la versione installata, l'ultima del canale e l'elenco degli aggiornamenti fatti con il loro esito.

Il canale

- **Stabile**: le versioni provate. È la scelta per i server in produzione.
- **Prova**: le versioni nuove prima degli altri, per i server di prova.

Passare da Prova a Stabile non riporta a una versione più vecchia: il server resta sulla versione che ha finché Stabile non la raggiunge.

Aggiornare da solo o a mano

Con **Aggiorna Esapanel da solo** acceso, il pannello installa una versione nuova nella fascia oraria e nei giorni che scegli, dopo i giorni di **Aspetta (giorni)** (contati da quando questo pannello ha visto la versione la prima volta). Spento, il pannello ti avvisa soltanto che c'è una versione nuova, e la installi tu dalla pagina.

Durante l'aggiornamento il pannello non risponde per un minuto o due mentre riparte.

Per un server da cui dipendono molti altri, come il server delle licenze, aspetta qualche giorno e scegli le mattine dei giorni feriali: una versione arriva dopo che altri server l'hanno provata, e un errore si vede quando qualcuno può intervenire.

Che cosa fa un aggiornamento

1. Conserva una copia del database del pannello e il pacchetto della versione installata.
2. Aggiorna il solo pacchetto `esapanel`, non tutto il sistema.
3. Controlla che il pannello risponda e che i suoi servizi siano attivi.

L'esito arriva per email. Un aggiornamento non riuscito dice come tornare alla versione di prima.

Gli aggiornamenti di sicurezza di Debian

Con **Aggiornamenti di sicurezza di Debian da soli** acceso, le correzioni di sicurezza del sistema si installano ogni giorno da sole. Esapanel non è fra queste: segue le impostazioni qui sopra. Spegnerli lascia il sistema senza le sue correzioni di sicurezza finché qualcuno non lo aggiorna a mano.

Il server non si riavvia mai da solo: la pagina dice quando serve un riavvio, per esempio dopo un aggiornamento del kernel.

Riavvio e spegnimento

Server › Riavvio e spegnimento riavvia o spegne il server dal pannello, senza terminale.

Quando: tra un minuto, oppure a un'ora del giorno nel tuo fuso orario (oggi se non è ancora passata, altrimenti domani). Per esempio di notte, dopo gli aggiornamenti di sicurezza, quando la pagina degli aggiornamenti dice che il server va riavviato. Fino ad allora la programmazione si può annullare, dalla pagina o dall'avviso in cima a ogni pagina.

Finché il server è fermo non funziona niente: il pannello, la ricezione dei log, i controlli degli host. Gli apparati che inviano i log in UDP perdono quelli dei minuti del riavvio; gli agenti li tengono e li inviano dopo. La ricezione dei log registra l'interruzione, e i clienti la vedono nei loro log.

Spegnimento: il pannello non può riaccendere il server. Dopo uno spegnimento si riaccende dalla console del provider o a mano. Per questo la pagina chiede di scrivere il nome del server: un controllo per non spegnere il server sbagliato.

Scegli per i riavvii un'ora in cui i clienti ne risentono poco, e avvisali se hanno apparati che inviano solo in UDP.

Rete e sicurezza

Questa pagina riguarda gli indirizzi IP del server e le sue protezioni: il firewall, i ban di fail2ban, il blocco degli scanner di Internet e la panoramica della sicurezza.

Gli indirizzi IP

Server › Indirizzi IP elenca gli indirizzi del server.

- **Rileva gli indirizzi** legge quelli configurati sul server, che restano in sola lettura. La prima volta che apri la pagina lo fa da sola.
- **Aggiungi un indirizzo** mette un indirizzo secondario su un'interfaccia: il pannello lo configura subito e a ogni avvio. Resta **In corso** finché il server non lo conferma.
- **Indirizzo pubblico** serve solo quando il server è dietro NAT: è l'indirizzo con cui il server si vede da Internet.

Un indirizzo è **Condiviso**, se serve tutti i clienti, o **Dedicato**, se appartiene a un reseller o a un cliente, nei limiti delle sue subscription. Un indirizzo dedicato serve, per esempio, a far ricevere a una subscription di CSP (Central Syslog) i log sulle porte standard 514 e 6514. Gli indirizzi condivisi che un reseller dà ai suoi clienti vengono dal suo pool.

Un indirizzo aggiunto viene scritto nella configurazione di rete del server, così torna a ogni avvio. A ogni avvio il pannello lo controlla: se manca diventa **Non riuscito**. Esegui di nuovo `esapanel-setup` per riscrivere gli indirizzi; se resta non riuscito, la sua interfaccia non esiste più oppure la rete del server è stata cambiata a mano.

La panoramica della sicurezza

Sicurezza › Panoramica mostra le protezioni del server in un colpo d'occhio:

- **Firewall**: se le regole del pannello sono attive, e se ci sono modifiche in attesa di essere applicate;
- **Ban IP**: gli indirizzi che fail2ban blocca adesso, e quelli bloccati nell'ultimo giorno;
- **Scanner di Internet**: quante reti e quanti indirizzi ferma il firewall;
- **Accessi falliti**: password e codici del secondo fattore sbagliati nell'ultimo giorno;
- **Certificato del pannello**: quanto dura ancora;
- **Secondo fattore**: quante persone attive lo hanno acceso.

Ogni riquadro porta alla sua pagina.

Il firewall

Sicurezza › Firewall: il traffico in ingresso è chiuso, tranne quello che le regole aprono.

- **Regole di Esapanel**: proteggono il server e servono i moduli, per esempio le porte di ricezione di CSP e la porta 514 degli indirizzi dedicati. Le scrive il pannello e sono in sola lettura.
- **Le tue regole**: controllate nel loro ordine, decide la prima che corrisponde. Vengono dopo le connessioni già stabilite e prima delle aperture dei moduli: una regola che scarta una rete la blocca anche sulle porte dei moduli. Le regole **SSH** e **Pannello** le ha create l'installazione e puoi modificarle.
- **Accesso SSH**: da qualsiasi indirizzo, oppure solo dagli indirizzi e dalle reti che elenchi, come l'ufficio e la casa dell'amministratore. La pagina ti avvisa quando l'indirizzo che usi adesso non è nell'elenco. Il pannello resta raggiungibile: si chiude solo SSH.

Applicare le modifiche senza chiudersi fuori

Le modifiche sono una **bozza**: il server tiene il suo firewall finché non le rivedi e applichi.

1. Fai le modifiche e apri l'anteprima: mostra il firewall completo che verrà caricato, con le righe aggiunte e tolte.

2. **Applica il firewall**: il server lo carica subito.
3. Torna alla pagina **Firewall** e **conferma** entro 60 secondi. La conferma arriva al server solo se raggiungi ancora il pannello.

Se una regola ti ha chiuso fuori, non riesci a confermare, e il server torna da solo al firewall di prima.

Anche quando SSH è chiuso al tuo indirizzo, la console del provider funziona comunque.

I ban IP

Sicurezza › Ban IP mostra i ban applicati da fail2ban.

- **Ban attivi**: gli indirizzi bloccati ora, da fail2ban dopo i loro tentativi falliti o a mano, con la scadenza. **Sblocca** toglie subito un ban.
- **Banna un indirizzo**: blocca un indirizzo per un certo tempo o per sempre, per esempio uno che scandisce il server. Un ban a mano finisce da solo alla sua scadenza.
- **Jail**: per SSH, per l'accesso al pannello e per il server web (bot malevoli, ricerche di applicazioni vulnerabili, accessi falliti), quanti tentativi falliti entro quanti minuti bannano un indirizzo, e per quanto tempo. Con WFP (Web File) installato, una riga sorveglia anche FTPS, SFTP, rsync e WebDAV; un tentativo lì banna l'indirizzo su tutte le porte.
- **Mai bannati**: indirizzi e reti che fail2ban non banna mai. Mettici la rete del tuo ufficio, così una password sbagliata non ti chiude fuori. Le voci di sistema evitano che il server banni se stesso.

Il registro dei ban si aggiorna ogni minuto.

Gli scanner di Internet

Servizi come Censys, Modat o Shodan sondano tutti gli indirizzi di Internet e catalogano i servizi che rispondono. Da soli non fanno danni, ma riempiono la quarantena di CSP e dicono a chiunque legga i loro cataloghi che cosa espone il server.

Sicurezza › Scanner: il firewall li ferma prima che raggiungano qualsiasi cosa del server, pannello e SSH compresi:

- le **reti** che gli scanner pubblicano, elencate in **Scanner noti**;
- gli **indirizzi trovati**: ogni pochi minuti il pannello cerca il nome inverso dei mittenti non autorizzati di CSP, e quelli con il nome di uno scanner vengono bloccati per 30 giorni. Una sorgente autorizzata, un indirizzo del server e un indirizzo mai bannato non vengono mai bloccati.

Sblocca toglie un indirizzo; se ritorna con il nome di uno scanner, viene bloccato di nuovo.

Gli scanner di ricerca, come Shadowserver, avvisano i CERT nazionali e i proprietari delle reti dei servizi esposti per errore o vulnerabili. Bloccandoli, quegli avvisi su questo server non arrivano più: pensaci prima di farlo.

Certificati, posta e DNS

Il certificato del pannello

Server › Certificati SSL gestisce il certificato che il pannello usa per l'HTTPS sul nome del server. Lo stesso certificato serve anche la porta TLS di CSP (Central Syslog): un certificato valido permette agli apparati e agli agenti di verificare il server.

Tipo	Quando usarlo
Let's Encrypt	La scelta normale: gratuito, accettato dai browser, rinnovato dal pannello 30 giorni prima della scadenza
Carica un certificato	Un certificato di un'altra autorità, per esempio quello aziendale
Certificato autofirmato	Generato dal server, valido 10 anni. Cifra la connessione, ma ogni browser lo segnala. L'installazione parte con uno di questi

Let's Encrypt

Let's Encrypt verifica il nome in HTTP sulla **porta 80**:

- il nome del server deve puntare al server nel DNS;
- la porta 80 deve essere raggiungibile da Internet. Il firewall del pannello la apre; anche un router o un provider davanti al server devono lasciarla passare.

La richiesta richiede un minuto; il pannello tiene il suo certificato finché il nuovo non è installato. Se la richiesta fallisce, la pagina mostra il motivo: correggilo e richiedi di nuovo. Quando un rinnovo fallisce, gli amministratori ricevono un solo messaggio e il pannello riprova ogni giorno.

Caricare un certificato

Incolla, in formato PEM:

- il **certificato** del server;
- i **certificati intermedi** dell'autorità: senza, alcuni client rifiutano il certificato;
- la **chiave privata**, senza password. Viene salvata cifrata e non viene più mostrata.

Il pannello controlla che la chiave appartenga al certificato, che copra il nome del server, che non sia scaduto e che porti a un'autorità attendibile. Un certificato caricato non viene rinnovato: il pannello avvisa 30 e 7 giorni prima della scadenza e il giorno in cui scade.

La posta

Server › Posta: la posta che il pannello invia (notifiche, inviti, esiti dei backup) passa da postfix su questo server. postfix si limita a spedire: non accetta posta dall'esterno.

Impostazione	Che cosa contiene
Mittente	L'indirizzo e il nome da cui arriva la posta; vuoto, `panel@` seguito dal nome del server. Salvare la pagina lo conferma: fino ad allora ogni pagina te lo ricorda
Destinatario della posta di sistema	Dove va la posta del server per root e postmaster, e quella non consegnata. Imposta un indirizzo che leggi

Impostazione	Che cosa contiene
Consegna	**Diretta: postfix consegna ai server dei destinatari**, oppure **Tramite un relay: postfix passa tutto a un altro server SMTP**, come quello della tua azienda, Microsoft 365 o un servizio di invio

La posta ai clienti di un reseller mantiene il mittente del server, ma porta il nome del marchio del reseller, e le risposte vanno all'indirizzo di assistenza del suo marchio.

Usa un **relay** quando il fornitore del server blocca la porta 25, o quando la posta finisce nello spam.

Perché la posta arrivi

Per la consegna diretta, i server dei destinatari si fidano della posta quando:

- il **nome inverso** di ogni indirizzo da cui il server spedisce, IPv4 e IPv6, è il nome del server. Lo imposta il fornitore dell'indirizzo;
- il **record SPF** del dominio del mittente autorizza il server. Con il mittente predefinito basta il record `v=spf1 a -all` sul nome del server.

Se l'SPF non autorizza il server, la pagina mostra il record da pubblicare e la politica DMARC del dominio, che dice che cosa succede alla posta nel frattempo; ogni pagina te lo ricorda finché non è a posto. Con un relay, l'SPF riguarda il fornitore del relay.

La **Coda** mostra la posta che postfix non ha ancora potuto consegnare: riprova da solo per alcuni giorni. Il **Messaggio di prova** verifica che un messaggio esca e arrivi.

Il DNS

Server › DNS imposta, in **Come trova i nomi**, il resolver del server, che trova gli indirizzi dei nomi per il pannello, la posta, i certificati e i moduli. Tiene le risposte nella sua cache e risponde solo al server stesso.

Modo	Quando usarlo
Da solo, a partire dai server radice, controllando le firme DNSSEC	La scelta normale: il resolver chiede direttamente ai server di ogni dominio e controlla le firme DNSSEC. Non dipende dal DNS del fornitore, e le liste antispam, che rifiutano le domande dei resolver pubblici, gli rispondono
Chiedendo ad altri resolver, ad esempio quelli del fornitore	Quando il fornitore blocca il DNS verso Internet: il resolver chiede ai resolver che indichi, di solito quelli del fornitore. Le firme non vengono controllate

Domini privati: i domini che esistono solo nella tua rete, come `azienda.lan`, non sono noti su Internet: indica il DNS della rete che li conosce. Servono, per esempio, ai check di UCP (Uptime Check) verso macchine interne.

Il cambio di modo svuota la cache: per un momento i nomi vengono cercati di nuovo. Se il resolver non risponde, l'installazione mantiene il resolver che il server aveva.

I reseller

Un **reseller** è un cliente che rivende i servizi a clienti propri, con il proprio marchio, nei limiti del suo **piano reseller**. Che cosa fa un reseller nel pannello è descritto nel manuale del reseller.

Servizi › Reseller elenca i reseller. Tu, come amministratore, gestisci anche i clienti diretti, cioè quelli senza reseller: in **Servizi › Clienti** il filtro **Appartiene a** mostra i clienti di un reseller o i **Diretti**.

Creare un reseller

Nuovo reseller chiede, come per un cliente, i dati aziendali, l'account principale e, se vuoi, una prima subscription di un **piano reseller**.

Il piano reseller decide quanti clienti e subscription può avere il reseller e quali servizi può rivendere. Un reseller senza piano reseller non può avere clienti: puoi assegnarglielo dopo, dalla sua pagina.

Un cliente esistente può diventare reseller: nella sua pagina, **Converti in reseller**. Mantiene le sue subscription.

I piani reseller

I piani reseller si creano in **Servizi › Service plan**, come gli altri piani, scegliendo **Per**: **Reseller**. Oltre ai servizi da rivendere, comprendono il servizio di rivendita, con i suoi limiti: quanti clienti, quante subscription, e quante risorse il reseller può distribuire in totale. Esistono anche gli **Addon per reseller**.

Le risorse del reseller

La pagina di un reseller mostra **Risorse del reseller**: per ogni risorsa, quanto ha **Assegnato ai clienti** (la somma dei limiti delle loro subscription non disattivate), il **Consumo misurato** e quanto consente il **Piano reseller**. Una riga rossa supera il piano.

Con l'**Overselling** i limiti assegnati possono superare in totale il piano: il reseller vende più di quello che ha, contando sul fatto che non tutti i clienti usano tutto. Il consumo misurato dice quanto è prudente.

Clienti e subscription elenca i clienti del reseller, con **Apri il cliente**.

Il resto

Le altre sezioni della pagina di un reseller funzionano come per un cliente: dati aziendali, account principale, stato, backup, indirizzi IP ed eliminazione (vedi il manuale del reseller, "I clienti").

- **Sospendere** o **disattivare** un reseller vale per le sue subscription.
- Un reseller si può **eliminare** solo quando non ha più clienti: spostali o eliminali prima.
- Gli indirizzi **Dedicati** di un reseller o di un cliente li assegni tu (vedi Rete e sicurezza).

Statistiche e notifiche

Le statistiche del server

Server › Statistiche mostra come sta il server: il pannello misura CPU, RAM, rete e dischi ogni minuto.

Grafico	Che cosa mostra
CPU	La parte in uso, con la media e il minuto più alto di ogni punto, e il carico dell'ultimo minuto
RAM	La parte in uso, senza la cache che il sistema libera da solo quando un programma ne ha bisogno
Rete	Il traffico ricevuto e inviato dalla scheda di rete principale, in byte al secondo
Dischi	Quanto è pieno il disco del sistema, e quelli dei database e dei dati del pannello quando sono separati

Scegli il periodo in alto: le ultime 24 ore mostrano un punto ogni 10 minuti, gli ultimi 7 giorni uno all'ora, gli ultimi 30 giorni uno ogni 6 ore, gli ultimi 12 mesi uno al giorno. I minuti restano 2 giorni, le ore 3 mesi, i giorni 2 anni. Passa il mouse su un punto per leggerne ora e valore.

La pagina iniziale mostra le ultime 24 ore, con **Tutte le statistiche**.

Guarda soprattutto i dischi: un disco dei log o delle copie fuori sede che si riempie va allargato, o i dati vanno spostati, prima che sia pieno.

Le notifiche

Server › Notifiche sceglie chi riceve le email che il pannello invia quando succede qualcosa, e con quale testo. Funziona come per i reseller (vedi il manuale del reseller, "Le notifiche"), con queste differenze:

- c'è anche la colonna **Amministratore**;
- le tue scelte valgono per tutta l'installazione; un reseller può cambiarle per i propri clienti, e dove non cambia nulla valgono le tue;
- gli eventi dell'installazione li configuri solo tu.

Gli eventi dell'installazione

Riguardano il server e arrivano a te:

Gruppo	Eventi
Certificato	Il certificato caricato scade a breve, è scaduto; il rinnovo di Let's Encrypt è fallito; il rinnovo del certificato del nome del pannello di un reseller è fallito
Licenza	La licenza scade a breve, oggi, è scaduta; il pannello si è fermato; la licenza non si può controllare
Aggiornamenti	È disponibile una versione nuova; il

Gruppo	Eventi
	pannello è stato aggiornato; l'aggiornamento non è riuscito
Ricezione dei log (CSP)	La ricezione è ferma, ripartita; i log non arrivano al database, arrivano di nuovo; il servizio di ricezione non ascolta su alcune porte, ascolta di nuovo
Copia fuori sede (WFP)	Il datastore si sta riempiendo, ha di nuovo spazio; la verifica ha trovato differenze; una rilocazione è finita, è fallita
License Server (LSP)	Un trasferimento di licenza attende l'approvazione

Assicurati che questi avvisi arrivino a un indirizzo letto: in **Indirizzi email** puoi aggiungere quello del gruppo che segue i server.

Le notifiche inviate

Notifiche inviate negli ultimi 90 giorni elenca ogni notifica inviata, con gli indirizzi raggiunti e quelli a cui non è stato possibile inviarla. Un indirizzo indicato come inviato è stato passato alla posta del server; se non è arrivato, guarda la coda in **Server › Posta**. L'elenco viene dal registro attività.

Disaster recovery

Il backup di tutto il server serve a ricostruirlo se va perso: un disco guasto, un server cancellato, un provider che chiude. È diverso dai backup che clienti e reseller fanno delle loro organizzazioni e subscription.

La pagina è **Server › Disaster recovery**.

Che cosa contiene

- Sempre la **configurazione**: il database del pannello, la configurazione del server, i dati di ogni cliente.
- Per ogni modulo quello che scegli: per CSP (Central Syslog) i **log consultabili** e gli **archivi dei log**.

I backup che clienti e reseller tengono sul server non sono inclusi.

Fare i backup

Fai una copia adesso ne fa una a mano, in background; l'email dice l'esito.

Soprattutto, imposta una **Pianificazione** con una **destinazione remota** (un server SFTP o FTP, o uno storage S3): un backup tenuto solo su questo server si perde con lui. La pianificazione funziona come quella dei backup dei clienti: frequenza, ora, copie da conservare, incrementali. Con i backup incrementali sono incrementali solo i log; il resto è completo in ogni backup.

Scarica (file unico) dà un file con tutto dentro, cifrato come hai scelto.

La chiave del server

I backup sono cifrati con la **chiave del server**, oppure con la tua chiave personale age. In **Chiave del server**, **Scarica la chiave** (con la tua password) e tienila lontano dal server, per esempio in un gestore di password: senza di lei, o senza la tua chiave personale, i backup non si aprono se il server va perso.

Ripristinare su questo server

Ripristina riporta, su questo server, una parte del backup:

- i clienti che scegli (un reseller con i suoi clienti; nessuno scelto vuol dire tutti);
- la loro configurazione, i loro log consultabili, gli archivi non più presenti;
- entro un periodo.

Il ripristino si esegue in background; l'email e la lista ne dicono l'esito. Per un singolo cliente o una singola subscription, di solito basta il backup del cliente o della subscription.

Ricostruire il server su un server nuovo

1. Prepara un server nuovo come per l'installazione (vedi L'installazione), con lo stesso nome e indirizzo se puoi.
2. Installa il pacchetto `esapanel`, della versione del backup o più recente.
3. Copia i file del backup in una cartella del server.
4. Come root:

```
esapanel-setup --restore=/root/backup --key=<chiave del server>
```

oppure, con la tua chiave personale, `--identity=<chiave privata>`.

La configurazione torna completa e il pannello riparte con i suoi clienti, utenti, certificati e chiavi. I log si ripristinano poi da **Server › Disaster recovery**, tutti o a scelta.

Se il server nuovo ha un altro nome o indirizzo

`esapanel-setup` te lo chiede:

- se il nome o l'indirizzo principale saranno cambiati come quelli di prima, si ferma: cambiali e rilancialo;
- con `--host=adapt` il pannello prende il nome e l'indirizzo del server nuovo.

Per gli indirizzi aggiunti dal pannello che il server nuovo non ha: `--addresses=apply` li sposta qui, `--addresses=skip` li lascia **Non riuscito**.

Ricorda che apparati e agenti dei clienti inviano al nome e alle porte di prima: se il nome cambia, vanno riconfigurati.

La licenza

Dopo un ripristino su un'altra macchina, la licenza appartiene alla macchina di prima: il pannello funziona per 10 giorni, e la trasferisci dalla pagina **Server › Licenza** (vedi La licenza).

Una prova ogni tanto

Un backup che non è mai stato ripristinato non è un backup sicuro. Ogni tanto prova a ricostruire il server su una macchina di prova, con la chiave che hai conservato: è l'unico modo di sapere che, quando serve, funziona.

CSP: la ricezione dei log

CSP (Central Syslog) riceve i log degli apparati dei clienti sulle porte delle loro subscription. Se la ricezione si ferma, i log inviati in UDP in quel momento sono persi. **Moduli › Ricezione log** è la pagina con cui la tieni d'occhio.

Lo stato della ricezione

In cima la pagina dice com'è la ricezione adesso: "Il server sta ricevendo i log (controllato alle …)", oppure il problema in corso. Il controllo avviene ogni minuto.

Sotto, l'elenco delle **interruzioni**, con **Dalle**, **Alle**, **Durata** e **Causa**:

- **Ricezione fermata (riavvio o spegnimento)**: un riavvio del servizio di ricezione o uno spegnimento del server; inizio e fine sono precisi al secondo;
- **Server fermato senza preavviso**: un guasto o una mancanza di corrente. L'inizio è l'ultimo controllo prima, approssimato al minuto.

I clienti vedono ogni interruzione fra i loro log, nel punto in cui cade, e nei report. Quando la ricezione resta ferma per qualche minuto ricevi una notifica, e un'altra quando riparte.

I log che non arrivano al database

Il servizio di ricezione (rsyslog) può essere in funzione e non scrivere comunque i log, per esempio quando il database rifiuta un messaggio e rsyslog lo riprova all'infinito. Ogni minuto il pannello invia un messaggio di prova lungo la strada dei log: quando non arriva per qualche minuto, la pagina lo mostra e ricevi una notifica.

Nel frattempo i log aspettano nella coda di rsyslog, fino a 1 GB, e arrivano ai clienti quando il problema è risolto; gli avvisi degli apparati silenziosi sono sospesi.

Guarda il log di rsyslog sul server, per esempio con `journalctl -u rsyslog`.

Le porte senza risposta

rsyslog può anche essere in funzione e non ascoltare su alcune porte della ricezione, quando non è riuscito ad avviarle. Ogni minuto il pannello confronta le porte su cui rsyslog ascolta con tutte le porte della ricezione: quando ne mancano per qualche minuto, la pagina dice quante sono e ricevi una notifica con le prime.

Gli apparati che inviano a quelle porte perdono i loro log finché rsyslog non viene riavviato: guarda il suo log e riavvialo con `systemctl restart rsyslog`.

Le porte nel firewall

Le porte di ricezione delle subscription, e la 514 e la 6514 degli indirizzi dedicati, le apre il pannello fra le **Regole di Esapanel** del firewall: non devi aprirle a mano (vedi Rete e sicurezza). Se il server è dietro un firewall esterno o un NAT, lì le porte vanno aperte a mano.

Il certificato

La porta TLS e la porta degli agenti usano il certificato del pannello: con un certificato autofirmato gli apparati non possono verificarlo, e gli agenti non inviano su TLS. Usa un certificato valido, di Let's Encrypt o caricato (vedi Certificati, posta e DNS).

UCP: le impostazioni dei check

UCP (Uptime Check) esegue i check dei clienti da questo server: i ping, le connessioni, le richieste HTTP e DNS partono da qui e raggiungono gli indirizzi che i clienti scrivono. Come si usano host e check è descritto nel manuale del cliente.

Tutti gli host

Moduli › Host elenca gli host di tutte le subscription, con lo **Stato**, i **Check** in ogni stato e da quando (**Da**). In testa, gli **Host down** e i **Check con un problema**: entrambi aprono **Moduli › Problemi**. Puoi cercare per nome o indirizzo e filtrare per stato e per cliente.

I check verso indirizzi privati

Moduli › Impostazioni check ha una scelta sola, importante: **Consenti i check verso indirizzi privati**.

Scelta	Quando
Accesa	Il pannello è installato nella rete dell'azienda che lo usa: i clienti possono controllare le macchine della rete interna, come `192.168.x.x` e `10.x.x.x`
Spenta	Il pannello ospita clienti che non si conoscono fra loro: sono accettati solo indirizzi pubblici, e non quelli di questo server

Su un pannello che ospita più clienti lasciala spenta: accesa, un cliente potrebbe usare i suoi check per sondare la rete interna del server.

Il pannello stesso (`127.0.0.1`) non è mai una destinazione. Spegnendo la scelta, gli host già salvati non vengono eliminati: i loro check rispondono **Unknown** con la ragione.

Il resolver

I check DNS "al resolver del pannello", e i nomi degli host, usano il resolver del server. Per far controllare ai clienti nomi che esistono solo nella rete interna, aggiungi i **Domini privati** in **Server › DNS** (vedi Certificati, posta e DNS).

Il firewall in uscita

I check partono dal server: se il server sta dietro un firewall che limita il traffico in uscita, i check verso le porte bloccate falliscono. Controlla le regole in uscita prima di dare UCP ai clienti.

WFP: i datastore e la rilocazione

WFP (Web File) conserva le copie fuori sede dei clienti in uno o più **datastore**: cartelle del server, meglio ciascuna su un disco suo, che contengono i file delle subscription. La pagina è **Moduli › Datastore fuori sede**.

I datastore

Il primo datastore nasce con il modulo, nella cartella data con `--wfp-datastore` all'installazione (vedi L'installazione).

Per aggiungerne uno, monta il nuovo disco ed esegui sul server, come root:

```
esapanel-setup --modules=csp,wfp --wfp-add-datastore=/mnt/disco2/wfp
```

con in `--modules` tutti i moduli installati. Il datastore compare nella pagina entro cinque minuti. La cartella non può stare sotto `/home`, `/root` o `/run`. Il pannello non sceglie mai da solo una cartella del server.

Per ogni datastore la pagina mostra la **Cartella**, quanto è **In uso** e **Libero** il suo disco, e quante **Subscription** contiene.

- All'80% e al 90% ricevi un avviso.
- Al 95% i suoi account vanno in sola lettura, finché non scende sotto il 90%.
- "Non trovato sul server: il suo disco è montato?" vuol dire che la cartella non c'è più: controlla il mount.

Nuove subscription: il datastore dove nascono le subscription create da ora in poi (**Falle nascere qui**). Quelle che esistono restano dove sono: spostale con **Riloca**.

La rilocazione

Riloca sposta i file su un altro datastore, per esempio per svuotare un disco da sostituire o per bilanciare lo spazio. In **Che cosa rilocare** scegli **Una subscription**, **Un cliente, o un reseller con i suoi clienti** oppure **Tutte le subscription di un datastore**, e **Verso il datastore**.

Le subscription si spostano una alla volta, in tre passi:

1. **In copia, account al lavoro**: i file sono copiati mentre gli account continuano a lavorare, per tutto il tempo che serve;
2. **Ultima copia, account fermi**: l'ultima copia si fa con gli account fermi, così trova i file immobili. Dura il tempo di rileggere l'elenco dei file, di solito pochi minuti; un backup che parte in quei minuti fallisce e si rifà al giro successivo;
3. la subscription passa al nuovo datastore e viene verificata. Account, password, chiavi e indirizzi non cambiano: sui dispositivi dei clienti non c'è niente da cambiare.

Ricevi un avviso quando una rilocazione finisce e quando fallisce. Una rilocazione che fallisce lascia la subscription dov'era, funzionante. **Annulla** ferma una rilocazione in corso e toglie la sua copia.

La cartella vecchia

Dopo una rilocazione la cartella vecchia resta nel datastore che ha lasciato, e ne occupa lo spazio. **Togli la cartella vecchia** quando hai visto che le copie arrivano nel nuovo datastore: non si può annullare. Fino ad allora la stessa subscription non può essere rilocata di nuovo.

La copia remota

Le copie fuori sede delle subscription con il servizio **Copia remota** possono essere mandate ogni notte a un secondo server Esapanel in un altro luogo, anche lui con WFP.

Questo server può solo aggiungere. Sull'altro server ogni subscription ha un suo account, che conserva quello che viene sostituito o cancellato per i giorni scelti lì. Chi prendesse il controllo di questo server non potrebbe distruggere le copie remote.

Per impostarla:

1. Sull'altro server crea una subscription della copia fuori sede e, dentro, **un account per ogni subscription da mandare**, con soltanto rsync. Nella pagina dell'account incolla la **Chiave pubblica di questo server** e scegli per quanti giorni conserva quello che viene sostituito o cancellato.
2. Qui, in **Copie remote**, scrivi il **Server delle copie remote** e salva. Confronta le **Impronte del server** mostrate con quelle nella pagina dell'account sull'altro server: se sono diverse, a quell'indirizzo risponde qualcos'altro.
3. Dai il servizio **Copia remota** a una subscription, nel suo piano o come addon, e scrivi qui il suo **Account sull'altro server**.

Gli invii cominciano all'ora scelta, una subscription alla volta, e mandano solo quello che è cambiato; puoi limitare la **Banda, in KB al secondo**. **Manda ora** ne avvia uno senza aspettare la notte. Quando un invio fallisce ricevi un avviso; il successivo si prova la notte dopo.

Verifica e repair

Ogni notte il pannello confronta quello che il server ha per ogni subscription con quello che conosce. Le differenze, e il **Repair** che le corregge, sono nella pagina **Copia fuori sede** di ogni subscription (vedi il manuale del reseller, "I moduli per il reseller"). Quando la verifica trova differenze ricevi un avviso.

LSP: il server delle licenze

LSP (License Server) è il modulo che rilascia le licenze di Esapanel: serve solo a chi vende le licenze del pannello, come Esalogica. Su un pannello che non vende licenze non è installato, e questa pagina non ti riguarda.

Con LSP installato, il server risponde ai pannelli dei clienti sulla porta **9444**, dove attivano e controllano ogni giorno la loro licenza.

Una licenza è una subscription

Ogni licenza venduta è una **subscription** di un piano con il servizio **Licenza**:

- il **piano** stabilisce il modulo, il livello, se è una Trial e i limiti;
- la **subscription** stabilisce la validità e lo stato.

Per vendere una licenza, quindi, crei una subscription del piano giusto per il cliente, come per qualsiasi servizio.

Le licenze

Moduli › Licenze vendute elenca le licenze, con:

- **Codice**: il codice di attivazione che il cliente inserisce nella pagina **Licenza** del suo pannello;
- **Stato**: attiva, sospesa o cessata, come lo stato della subscription. Il pannello del cliente lo riceve al controllo giornaliero;
- **Server**: il server a cui è legata la licenza, oppure "Non attivata";
- un eventuale **trasferimento in attesa**.

Puoi cercare per codice, nome del server o cliente.

La pagina di una licenza

Nella subscription, la tessera **Licenza** mostra:

- il **Codice di attivazione**: la licenza si lega al primo server che la attiva, e il pannello del cliente riceve la licenza firmata;
- lo **Stato**: sospendi, riattiva o cessa la licenza con lo stato della subscription. Una licenza sospesa o cessata ferma il pannello del cliente al prossimo controllo giornaliero; i servizi già configurati continuano a funzionare;
- il **Server** legato alla licenza, con il suo ultimo controllo giornaliero;
- **Rinnovo e condizioni**: l'ultimo giorno di validità, il modulo, il livello e i limiti. I limiti vuoti di clienti e reseller sono quelli del livello. Il server del cliente riceve ogni modifica al prossimo controllo giornaliero;
- **Attivazioni e trasferimenti**: quando la licenza è stata attivata e spostata su altri server, da sola o con approvazione.

I trasferimenti

Un cliente sposta la licenza su un altro server, per esempio dopo un ripristino su un hardware nuovo, dalla pagina **Licenza** del suo pannello.

- Una licenza si sposta da sola fino a **2 volte in 30 giorni**: il pannello del cliente la riceve subito.
- Oltre, il trasferimento attende in **Moduli › Trasferimenti licenze**. **Approva** sposta la licenza: il nuovo server la riceve al prossimo controllo giornaliero, e il server di prima si ferma al suo. **Rifiuta** lascia la licenza dov'è.
- Una nuova richiesta del cliente sostituisce quella in attesa.

Ricevi una notifica per ogni trasferimento in attesa.

Un server delicato

Da questo server dipendono i pannelli di tutti i clienti. Tienilo aggiornato con prudenza: aggiornamento automatico con qualche giorno di attesa, nelle mattine dei giorni feriali (vedi Aggiornamenti, riavvio e spegnimento). Un pannello che non riesce a controllare la licenza continua a funzionare fino alla scadenza, ma i suoi amministratori ricevono un avviso dopo 7 giorni.