happy ticket

Monitor del server
Istruzioni per l'uso

Guida sintetica alla pagina di monitoraggio del server 2.29.246.47: stato della macchina, risorse, accessi e tentativi di intrusione, sicurezza, aggiornamenti, servizi, allerte via email pianificate e rapporti periodici.

INDIRIZZO
https://monitor.swred.it

ACCESSO
Utente, password e codice di verifica (2FA facoltativa)

AGGIORNAMENTO DEI DATI
Ogni minuto; controlli lenti ogni 10 minuti

STORICO
Metriche 90 giorni · accessi 180 giorni

Versione 1.0 – novembre 2026

POWERED BY happy ticket

1. Come funziona

- Sul server un **raccoglitore** gira ogni minuto, **solo in lettura**: legge CPU, memoria, dischi, rete, servizi, RAID, sessioni, registri di SSH, fail2ban, firewall e siti web. Ogni 10 minuti esegue i controlli più lenti: aggiornamenti, configurazione di sicurezza, certificati, raggiungibilità dei siti, backup.
- L'applicazione web (senza privilegi di amministratore di sistema) conserva lo storico, valuta le **regole di allerta** e invia le email da `noreply@swred.it`.
- La provenienza geografica degli indirizzi che attaccano si ricava dal servizio pubblico whois di Team Cymru. Gli indirizzi "noti" (esclusi da fail2ban o da cui sono avvenuti accessi riusciti) **non vengono mai inviati all'esterno**.

2. Accesso e ruoli

1. Apri **https://monitor.swred.it**, inserisci nome utente, password e i caratteri del codice di verifica.
2. Al primo accesso (o dopo una reimpostazione) scegli una password personale: almeno 12 caratteri con tre tipi tra minuscole, maiuscole, numeri e simboli.
3. Da **Profilo e sicurezza** puoi attivare la **verifica in due passaggi** con un'app di autenticazione.

> Dopo 8 tentativi errati l'account si blocca per 15 minuti. La sessione si chiude dopo 60 minuti di inattività (l'aggiornamento automatico della pagina non la tiene aperta). Ogni accesso è registrato.

Funzione	Amministratore	Operatore	Sola lettura
Tutte le pagine di stato	✓	✓	✓
"Ricontrolla ora"	✓	✓	—
Regole di allerta e rapporti	✓	✓	vede
Utenti (crea, modifica, elimina)	✓	—	—
Registri di accessi, attività ed email	✓	—	—
Impostazioni e destinatari predefiniti	✓	—	—

3. Le pagine

Pagina	Contenuto
Panoramica	Barra di stato (verde, giallo, rosso) con il riepilogo delle criticità; indicatori di CPU, RAM, carico, disco, swap e rete con l'andamento dell'ultima ora; allerte attive, controlli di sicurezza non superati, accessi delle ultime 24 ore e utenti connessi, aggiornamenti e riavvio richiesto, servizi, siti e certificati, backup e RAID. Si aggiorna da sola ogni 30 secondi. ⟳ Ricontrolla ora ripete subito i controlli lenti.
Grafici	Andamento di CPU (media, massimo, attesa del disco), carico rispetto ai core, memoria e swap, spazio su disco, rete, letture e scritture del disco, connessioni. Periodo: 1 ora, 6 ore, 24 ore, 7, 30 o 90 giorni, oppure **dal … al …** a scelta. Passando il mouse sul grafico si leggono i valori.
Accessi e attacchi	Per il periodo scelto: tentativi SSH falliti, utenti inesistenti provati, scansioni e accessi riusciti (con grafico); indirizzi più attivi con paese, rete di provenienza, utenti provati e stato di blocco; classifica per paese; accessi riusciti con la chiave usata; ban e sblocchi di fail2ban; porte più cercate sul firewall; richieste sospette ai siti (.env, .git, wp-login, phpmyadmin…). Cliccando un indirizzo si apre la sua storia completa.
Sicurezza	Elenco dei controlli con semaforo: SSH solo con chiave, root senza password, chiavi autorizzate, firewall attivo e porte pubbliche attese, fail2ban, aggiornamenti di sicurezza, aggiornamenti automatici, riavvio, certificati, RAID, unità fallite, orologio sincronizzato. Dettaglio di regole del firewall, indirizzi bloccati e porte in ascolto.
Aggiornamenti	Pacchetti aggiornabili (quelli di sicurezza evidenziati), riavvio richiesto e per quali pacchetti, stato degli aggiornamenti automatici, ultime operazioni sui pacchetti.
Sistema e servizi	Macchina, dischi e inode, RAID, interfacce di rete, servizi con stato e riavvii, processi che consumano più CPU e memoria, backup, certificati e siti.

4. Allerte via email

Menu **Allerte**. Il monitor nasce con un insieme di regole già attive; ogni regola si può modificare, spegnere, eliminare o aggiungere (+ Nuova regola).

Regola predefinita	Soglia iniziale	Regola predefinita	Soglia iniziale
Uso della CPU	90% per 10 minuti	Certificati HTTPS	scadenza entro 14 giorni o non validi
Carico del sistema	2 per core per 15 minuti	Siti web	non raggiungibili per 5 minuti
Memoria RAM / Swap	90% / 50%	Backup	fallito o più vecchio di 26 ore
Spazio su disco (e inode)	85%	Tentativi SSH	oltre 300 in un'ora
Servizi e unità fallite	fermi da 2 minuti	Accesso SSH da indirizzo nuovo	mai visto in 30 giorni
RAID	degradato o in ricostruzione	Richieste web sospette	oltre 500 in un'ora
Riavvio richiesto	da più di 72 ore	Configurazione di sicurezza	password SSH, firewall, fail2ban
Aggiornamenti di sicurezza	in attesa da 48 ore	Raccolta dati ferma	nessun dato da 5 minuti

Per ogni regola si impostano:

- **Soglia** e **attesa**: la condizione deve durare almeno i minuti indicati prima di avvisare (evita falsi allarmi); **gravità** critico o avviso.
- **Destinatari**: uno o più indirizzi email. Se vuoto si usano i **destinatari predefiniti** (Impostazioni).
- **Pianificazione**: giorni della settimana e fascia oraria in cui inviare le notifiche (anche a cavallo della mezzanotte, es. 20:00–08:00). Fuori fascia l'allerta resta registrata e la notifica parte all'apertura della fascia successiva.
- **Ripetizione**: promemoria ogni N minuti finché il problema resta (0 = mai) e avviso quando la situazione **rientra**.
- **Elementi da ignorare**: servizi o domini da escludere dalla regola (es. un sito di prova).

> Prova invia subito un'email di prova ai destinatari della regola: serve a verificare che le notifiche arrivino. La pagina mostra le condizioni **in corso** (in osservazione o attive) e lo **storico** per periodo, con l'elenco di chi è stato avvisato.

5. Rapporti periodici

Menu **Rapporti periodici**: riepilogo via email **giornaliero** (ultime 24 ore) o **settimanale** (ultimi 7 giorni) all'ora e nel giorno scelti, con allerte attive, uso delle risorse, tentativi di accesso e indirizzi più attivi, accessi riusciti, ban, firewall, richieste web sospette, aggiornamenti e riavvio, certificati in scadenza, backup. Invia ora lo spedisce subito; l'anteprima mostra il testo che verrà inviato.

6. Amministrazione

- **Utenti**: crea utenti con ruolo amministratore, operatore o sola lettura; la password provvisoria compare una sola volta e va cambiata al primo accesso. Da **Gestisci**: modifica, reimposta la password, sblocca, azzera la 2FA, elimina (il nome resta nello storico). Deve sempre restare almeno un amministratore attivo.

- **Registri**: accessi al monitor (riusciti, falliti, bloccati), attività di chiunque (regole, rapporti, utenti, impostazioni, ricontrolli) ed email inviate con esito.
- **Impostazioni**: destinatari predefiniti, durata delle sessioni, conservazione dei dati, 2FA obbligatoria per gli amministratori.

7. Buone pratiche

- Imposta subito i destinatari predefiniti e usa **Prova** su una regola.
- Per le regole critiche lascia la notifica tutti i giorni a tutte le ore; usa le fasce orarie per gli avvisi meno urgenti.
- Un “accesso SSH da indirizzo nuovo” non atteso va verificato subito.
- Programma il riavvio quando la pagina Aggiornamenti lo richiede.
- Per sbloccare un indirizzo bloccato per errore da fail2ban chiedi all'amministratore di sistema.
- Esci dal monitor (menu utente → Esci) su computer condivisi.