

PRESENTAZIONE TECNICA

IOTLegacy · Architettura

Componenti, reti, sicurezza, dati e flussi operativi.

Architettura logica

Reverse proxy e portale unificato davanti ai servizi applicativi



Il portale autentica gli operatori; i client legacy continuano a usare i percorsi API e i protocolli nativi.

Stack containerizzato

Web

PHP 8.2 + Apache, API legacy, portale, Swagger e monitor.

MQTT

Mosquitto 2.0 e editor Flask con validazione prima del reload.

OpenVPN

Runtime con NET_ADMIN/TUN ed editor Flask separato.

Redis

Telemetria attività e persistenza interna non esposta.

Segmentazione di rete

ui_internal

Connette il portale esclusivamente agli editor MQTT e OpenVPN.

redis_internal

Rete interna dedicata tra web e Redis.

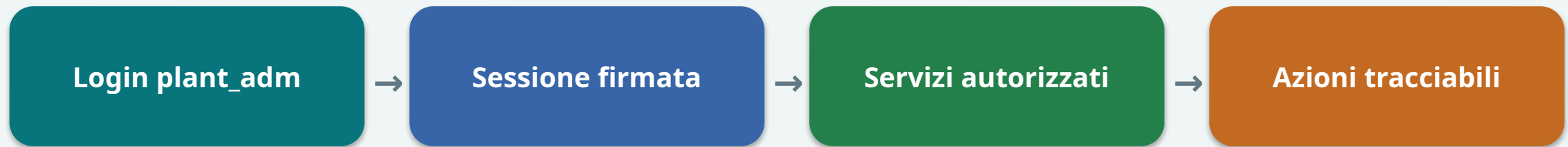
ovpn-internal

Namespace del runtime VPN, forwarding e rotte controllate.

iotgate-private

Rete esterna privata per l'integrazione IOTGate.

Autenticazione e autorizzazione



- Cookie HttpOnly, Secure e SameSite Strict
- Password verificata su AUTHDB e profilo abilitato
- Swagger eredita l'identità del portale per filtrare gli endpoint
- Cambio password protetto da verifica della password corrente e same-origin

OpenVPN: piano dati e controllo

Runtime

OpenVPN, interfacce TUN/TAP, forwarding IPv4 e gestione route.

Configurazione

Server abilitati, CCD, certificati, pacchetti e script montati su volume.

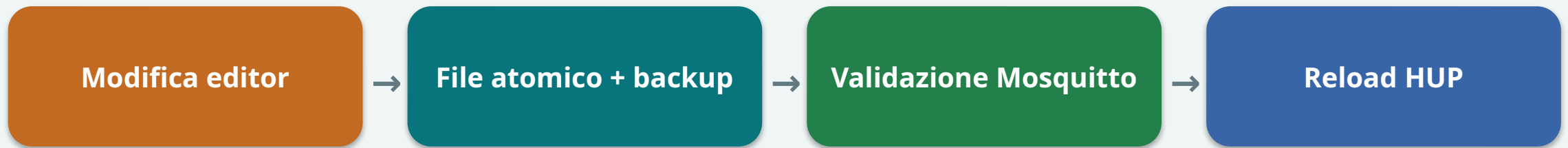
Diagnostica

Client attivi per interfaccia, log strutturati, routing e porte in ascolto.

Sicurezza

Editor separato dal namespace VPN; modifiche applicate tramite comandi controllati.

MQTT: configurazione affidabile



- Listener TCP/TLS/WebSocket e autenticazione configurabili
- Password file e identità PSK gestite dalla console
- Log del broker montati in sola lettura nell'editor
- Dati e log persistenti separati dall'immagine container

Operatività e osservabilità

Health

Verifica web immediata e stato dei componenti essenziali.

Monitor

Richieste, errori, latenza, endpoint e timeline dell'ultima ora.

Log

Popup leggibili con livelli, timestamp e contesto operativo.

Recovery

Volumi persistenti, backup dei file modificati e rebuild ripetibile.

Principi di manutenzione

- Segreti e configurazioni operative esclusi dal repository
- Build mirate: aggiornare solo i servizi coinvolti
- Nessun riavvio del runtime VPN per modifiche alla sola interfaccia
- Validazione sintattica e test HTTP prima del rilascio
- Conservazione della compatibilità con API, porte e profili legacy

Pronti per il prossimo passo

Architettura isolata, compatibile e pronta a evolvere.

hub.somotech.it

Studio Rizzi · IOTLegacy