

WORK
SHOP
GARR
2023

NET
MAKERS

Il servizio eduVPN



Lorenzo Fava
GARR

Intro



www.eduvpn.org

Overview



Multiprotocollo

Overview



Multiprotocollo



Client cross-platform



Overview

Supporto IPv4 e IPv6



Multiprotocollo



Client cross-platform

Overview

Supporto IPv4 e IPv6



Singolo login



Multiprotocollo



Client cross-platform



Profili

Institute Access: Accesso remoto sicuro alle risorse interne dell'istituto/organizzazione.



Secure Access: Navigazione sicura anche attraverso reti pubbliche offrendo un gateway sicuro.



Opzioni di personalizzazione del profilo:

- Default gateway
- Scelta del protocollo
- Server DNS
- Definire rotte specifiche o escluderle

Autenticazione e Autorizzazione

AuthN:

- LDAP



- SAML



- OIDC



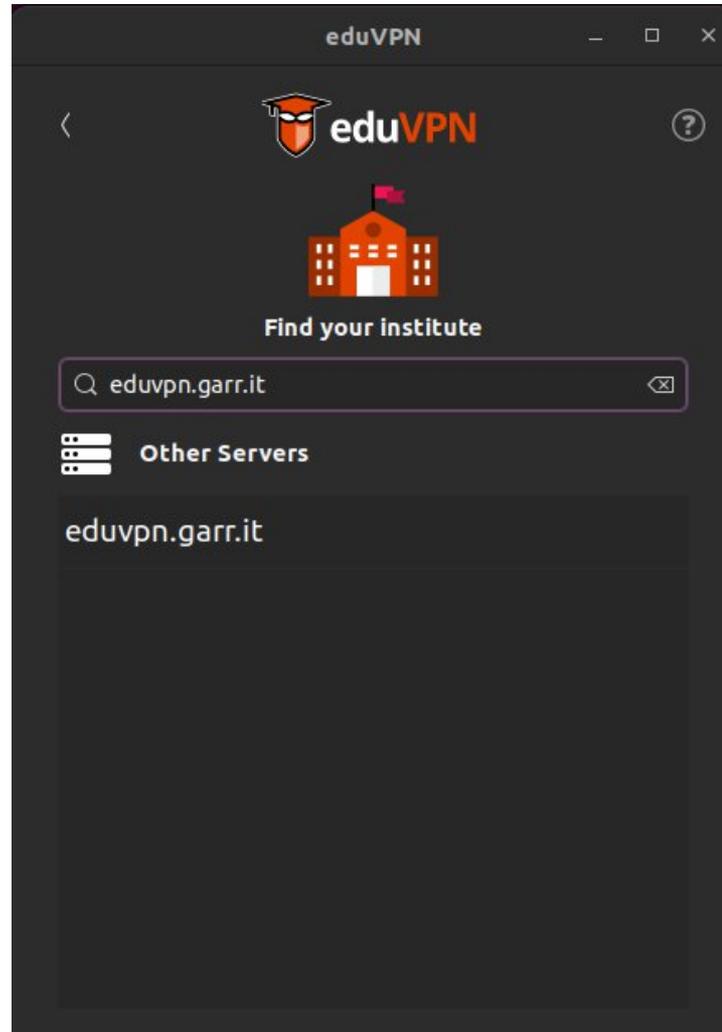
- Radius

- Local DB

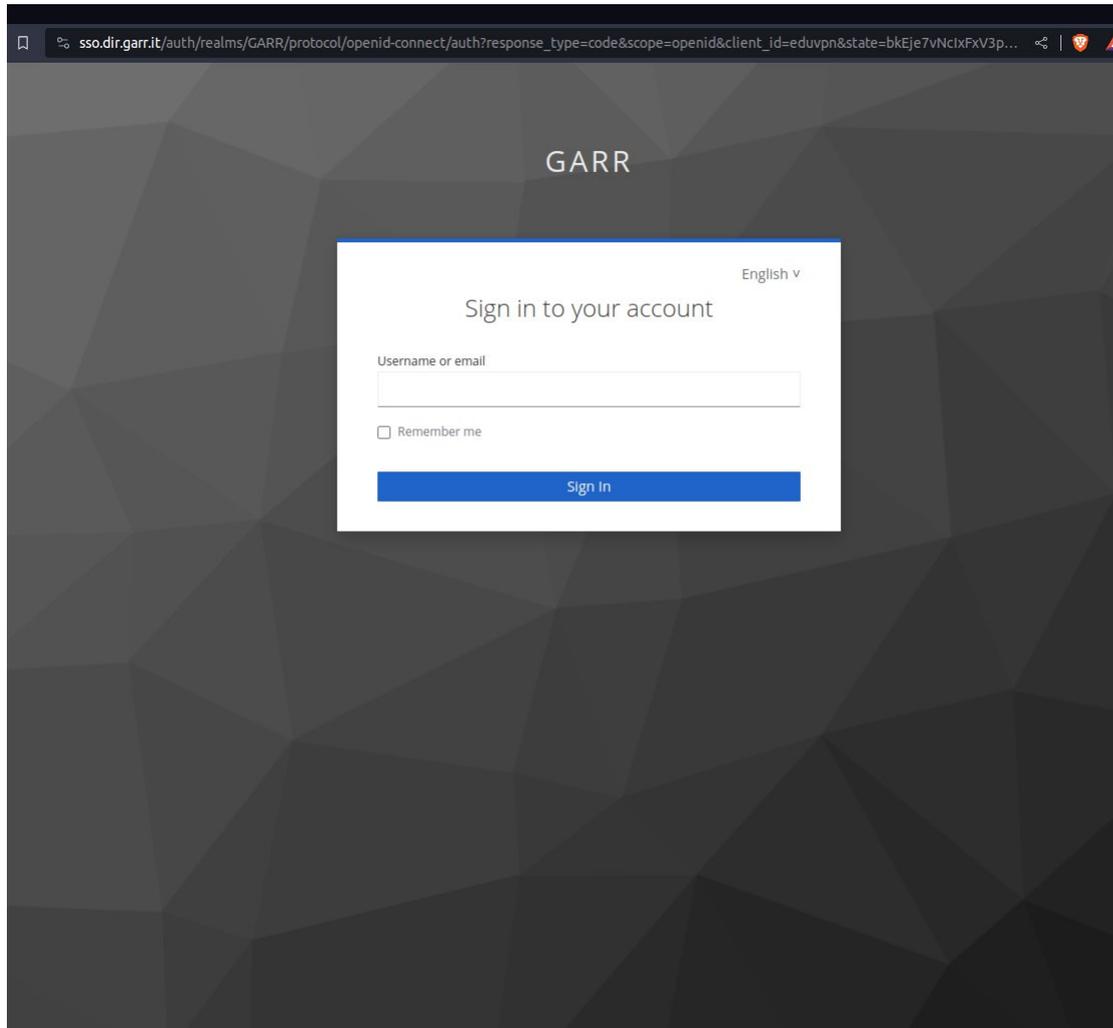
AuthZ:

- Restrizione di accesso al servizio
- Restrizione di accesso ai profili

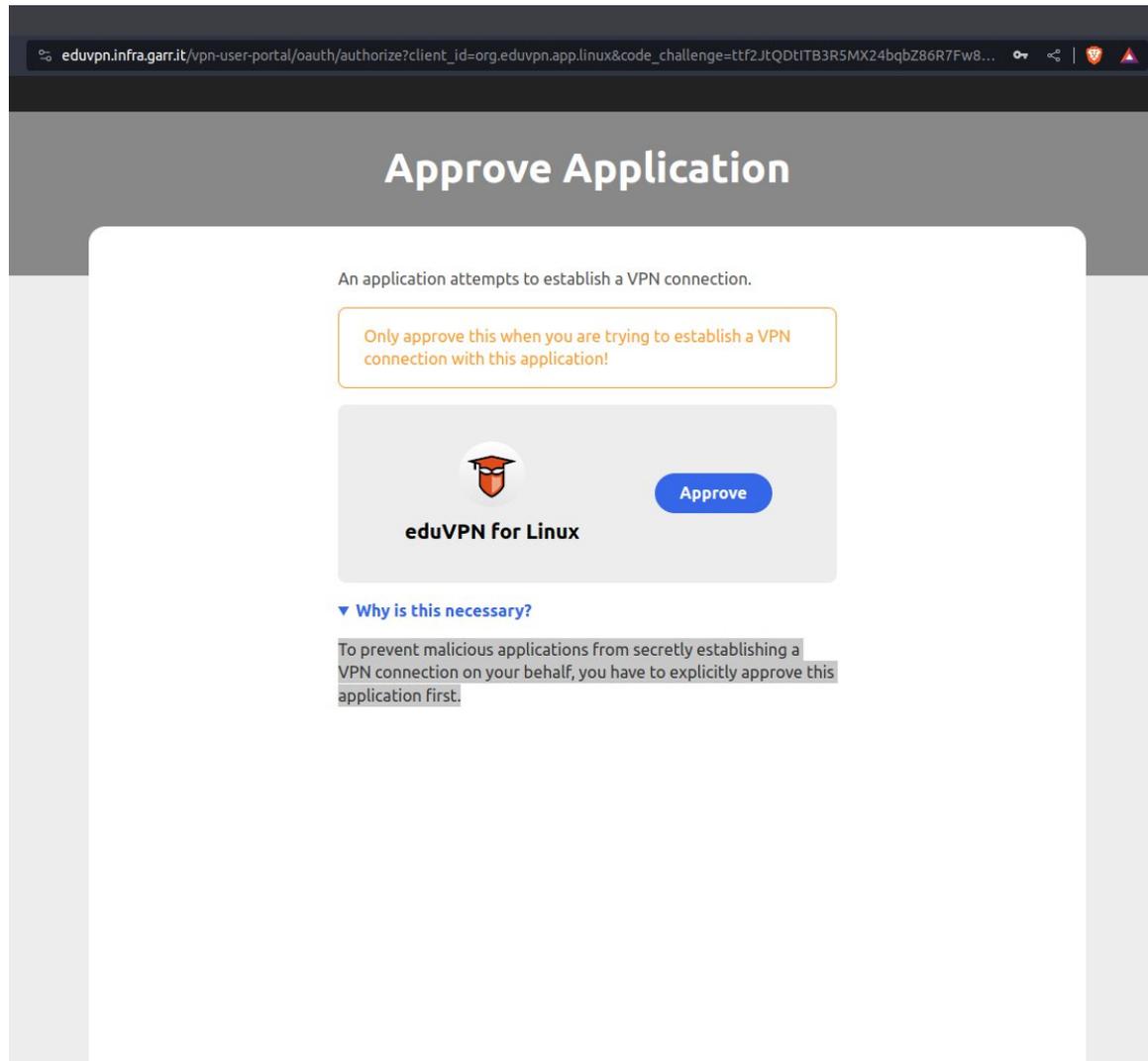
Flusso di Autenticazione e Autorizzazione



Flusso di Autenticazione e Autorizzazione



Flusso di Autenticazione e Autorizzazione



eduvpn.infra.garr.it/vpn-user-portal/oauth/authorize?client_id=org.eduvpn.app.linux&code_challenge=ttf2JtQDtTB3R5MX24bqbZ86R7Fw8...

Approve Application

An application attempts to establish a VPN connection.

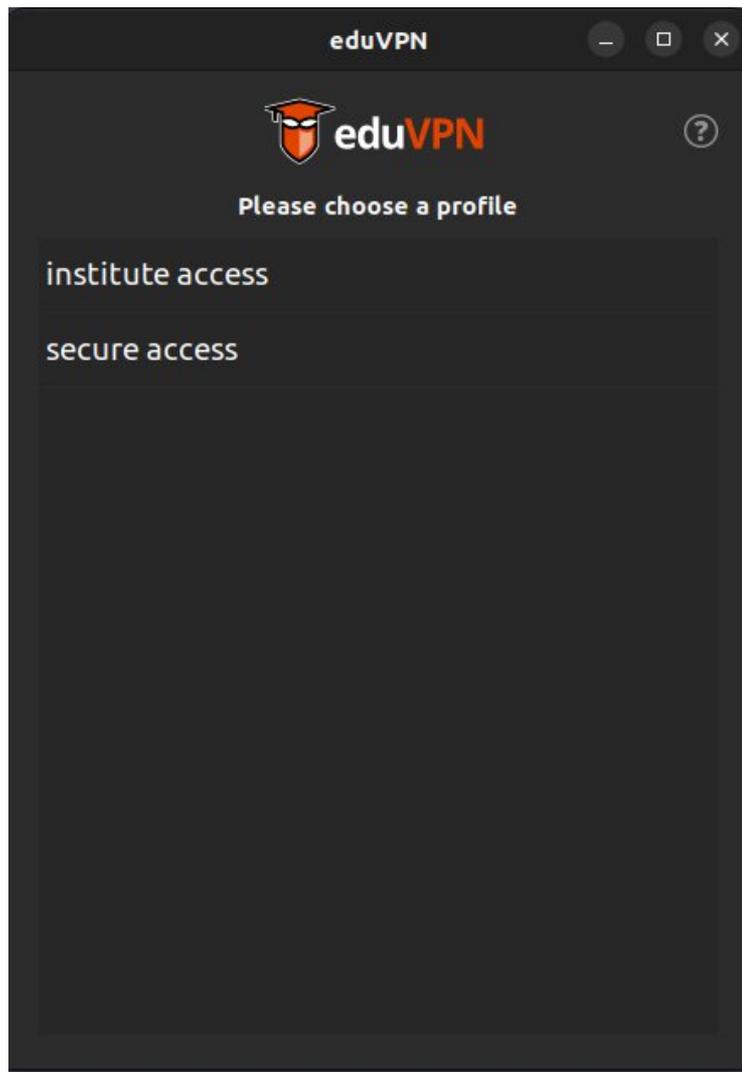
Only approve this when you are trying to establish a VPN connection with this application!

 **eduVPN for Linux** [Approve](#)

▼ Why is this necessary?

To prevent malicious applications from secretly establishing a VPN connection on your behalf, you have to explicitly approve this application first.

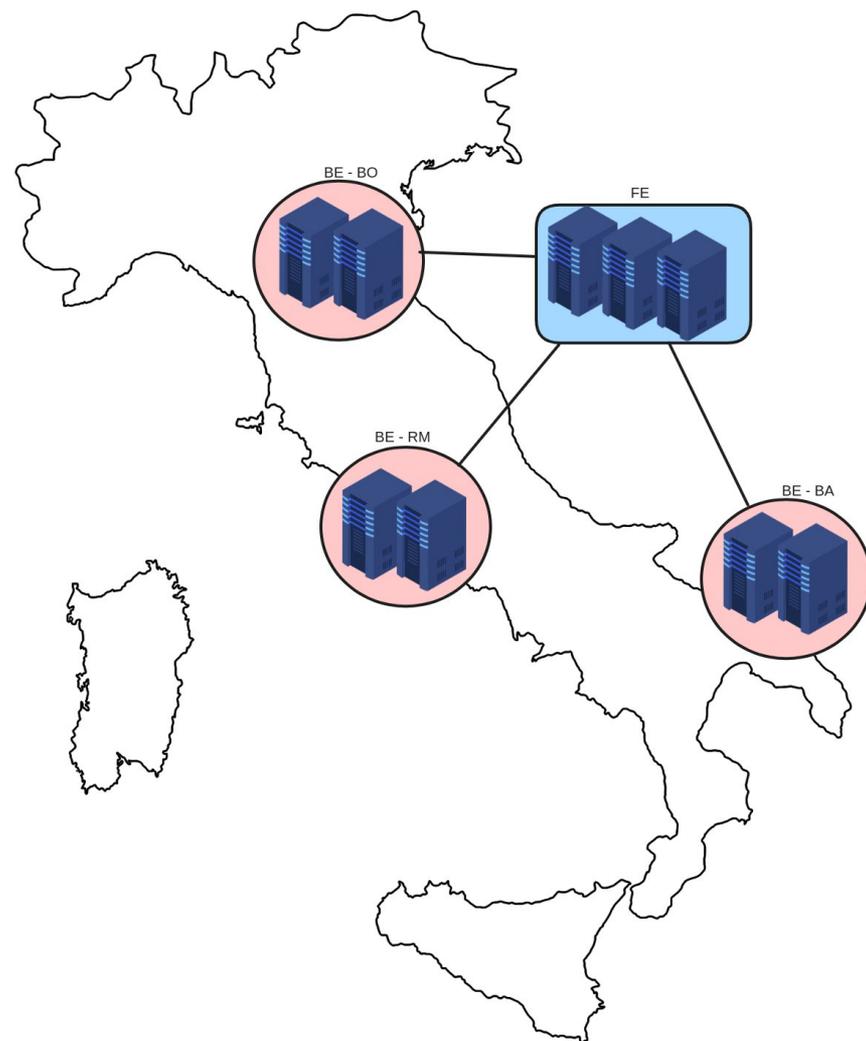
Flusso di Autenticazione e Autorizzazione



Architettura

Il servizio si basa su un'architettura distribuita su 3 regioni geografiche che garantisce resilienza al servizio

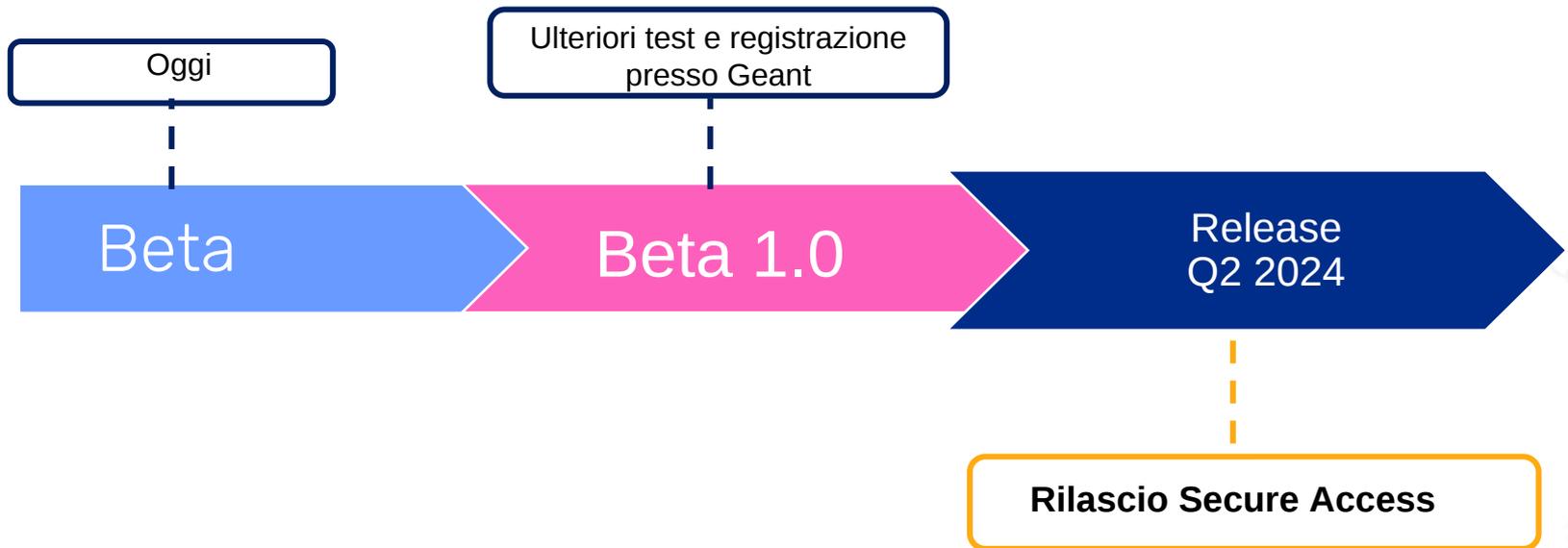
Componenti	Dettagli
Frontend	Gestiscono l'autenticazione degli utenti tramite OIDC (OpenID Connect).
Backend	Gestiscono le richieste dei client e forniscono il servizio VPN.
Database (Postgres)	Memorizza le informazioni degli utenti, le sessioni VPN, le configurazioni del server, le autorizzazioni e i log.



Prestazioni

PRESTAZIONI	DETTAGLI
Numero Massimo di Client per Singolo Nodo	~1000, assumendo ≥ 16 core CPU con AES-NI e prestazioni di rete adeguate, ad es. interfaccia/e da 10+ Gbit.
Limiti del Software del Server	Il software supporta 64 processi OpenVPN per ogni core e può gestire fino a 64 core. Questo permette a un singolo nodo con 64 core di gestire ~4096 client connessi.

Considerazione finali



WORK
SHOP
GARR
2023

**NET
MAKERS**

Grazie per
l'attenzione

www.garr.it/domande
codice: 2318 9129

Contributors:

- Funicello A.
- Giardino S.
- Marzulli G.
- Viola G.