AuthS

Authentication Service

Microservizio dedicato per la registrazione e per l'autenticazione. Nello specifico al suo interno vengono gestite: la registrazione, l'autenticazione (login) e il cambio password.

Istruzioni per l'utilizzo

- Se necessaria, la pwd del DB è nella cartella DB
- Per avviare questo servizio:
  1. Posizionarsi con un terminale aperto in VisualStudio nella cartella AuthS\Code (deve essere disponibile il main.py)
  2. Attivare il virtualenv che include tutte le librerie necessarie per questo progetto
     Per attivarlo ……\Configs\AuthS\venv-AuthS\Scripts\activate
     Per disattivarlo deactivate
  3. Startare il server per le api
     uvicorn main:app –reload –host 0.0.0.0 –port 8001
  4. Per debuggare:
     Andare sul debugger ed eseguire sul main.py così ogni breakpoint potrà essere provato e controllato
  5. TEST AUTOMATICI: per eseguire test automatici già preparati, aprire un cmd, posizionarsi nella cartella Test ed eseguire 'pytest –html=report_test1.html' (ovviamente avendo già attivato: la virtual machine, il db e l'api del servizio)
- Per disabilitare la documentazione per API di questo servizio basta indicare un url per la documentazione oppure impostarlo a None per disabilitarlo.

Checklist delle schermate

1. VM
2. cmd (vs code)
   - ssh verso la VM
   - test : ‘pytest –html=report_test1.html’
   - rebuild della documentazione : ‘.\make clean’ e poi ‘.\make html’
   - debugger in python
3. VS code
   - service documentation page
4. Brave browser
   - documentazione
   - risultati testing
5. Insomnia
   - api testing

Specifiche dettagliate

1. **Registrazione**
   Questo applicativo verrà utilizzato solo dai partner (i miei clienti) e dal loro staff. Per tale motivo la loro registrazione non si potrà fare in autonomia, ma verrà effettuata dagli utenti amministratori. Sulla base di un elenco di utenti da registrare, verrà creata un'utenza per ciascuno di essi (se non è già presente).
2. **Autenticazione**
   Ciascun utente registrato può effettuare l'operazione di login indicando email / username e password. Per questioni di sicurezza, ad ogni accesso verrà inviata un'e-mail per indicare dell'accesso avvenuto e non sarà possibile accedere da più dispositivi contemporaneamente. Nel caso di tentativi di accesso sbagliati, la mail verrà inviata dopo il 5° e ultimo tentativo.
   Attenzione: Le varie utenze si contraddistinguono con un campo specifico chiamato userType (0-utente normale, 1-admin, 2-partner, 3-admin collaboratore, …)
   Attenzione: Gli admin sono gli amministratori supremi. Gli admin collaboratori sono amministratori che però avranno una libertà di potere più limitata rispetto a quelli supremi.
   Attenzione: Nel caso di utenze di amministratore e utenze di direzione del partner, l'operazione di login potrà avvenire in qualsiasi momento. Per quanto riguarda le utenze del gruppo staff, potranno essere vincolate a specifici orari e giornate per poter accedere al sistema.
   Riassumendo:
   - Esito OK -> viene restituito un token jwt con cui l'utente potrà usare per usare le varie funzionalità utilizzabili solo da utenti registrati;
   - Esito KO -> se l'utente sbaglia più di 5 volte l'accesso, la sua utenza viene disattivata. Per poterla riattivare sarà necessario reimpostare la password o inviare richiesta esplicita via mail alla mail degli amministratori.
3. **Cambio password**
   Nel caso di utenze nuove, l'utente dovrà procedere alla modifica immediata, perchè la password associata all'utenza sarà corretta, ma scaduta. Quest'operazione potrà essere richiesta anche esplicitamente :
   - dalla pagina dei dati personali dell'utente loggato
   - senza dover effettuare la login, ma indicando la casella postale associata alla propria utenza. Dunque verrà inviata un'e-mail con un link valido per 1 giorno. Se il link dovesse risultare ancora valido, allora si potrà procedere alla modifica effettiva, altrimenti si potrà richiedere un re-invio. Al completamento dell'operazione di modifica si riceverà un'e-mail di conferma e l'utenza verrà riattivata, nel caso si fosse disabilita per numerosi tentativi errati.

Esempio
Una persona potrebbe essere autorizzata ad entrare:

- in un orario specifico: (8-12;12:30-18:00) o qualsiasi orario (0-24). Esempio di salvataggio: 08:30-12:30;18:30-23:30 oppure all= 00:00-23.59
- giorni specifici: Lun;Gio;Sab;Dom o all (qualsiasi giorno). Esempio di salvataggio: 0;1;2;3;4;5;6 oppure 7 tutti i giorni

Endpoints

[P] - endpoint pubblico
[PNV] - endpoint pubblico ma non visibili all'esterno - usato per operazioni di controllo / operazioni interne
[L] - endpoint per utenti loggati
[IC] - endpoint per la comunicazione interna - richiamabile solo da altri microservizi - pubblico
[ICL] - endpoint per la comunicazione interna - richiamabile solo da altri microservizi - richiede l'autenticazione dell'utente che ha originato la request
[ICLA] - Internal communication logged administrator (userType= 1 o 3)- endpoint per la comunicazione interna - richiamabile solo da altri microservizi - richiede l'autenticazione dell'utente che ha originato la request - solo admin
[ICLP] - Internal communication logged partners ((userType= 1,2,3)) - endpoint per la comunicazione interna - richiamabili solo da altri microservizi - richiede l'autenticazione dell'utente che ha originato la request - per administrator e partner
[A] - endpoint solo per admin

- **[PNV] | checkS**
  permette agli amministratori di controllare lo stato del servizio -> se tutto ok allora si riceverà un esito HTTP con status code = 200
- **[PNV] | checkSDB**
  permette agli amministratori di controllare se il servizio riesce ad accedere correttamente al DB -> verrà eseguita una semplice query e se risulta tutto ok allora si riceverà un esito HTTP con status code = 200
- **[P] | login**
  permette di effettuare il login
  - esito OK entro il 5° tentativo: viene ritornato un token JWT + si riceverà una mail che conferma l'accesso
  - esito KO : ritorna un errore opportuno. Se si ha raggiunto il 5° tentativo errato -> l'utenza viene disabilitata per i numerosi tentativi sbagliati + si riceverà una mail di avviso
- **[P] | sendChangePwdLink**
  permette di ricevere una mail con il link per cambiare la password - Il link che si riceverà conterrà un token valido per 1gg e contenente informazioni interne (email e userId dell'utente che sta tentando di effettuare la modifica della password)
- **[P] | changePwd**
  permette di cambiare la password agli utenti che forniscono un token JWT valido, in cui sono riportate le informazioni come email e username dell'utente che intende cambiare password. Come conferma si riceverà un token JWT aggiornato + si riceverà una mail che conferma il cambio della password
- **[IC] | ICcheckS**
  richiesta proveniente dagli altri servizi - verifica lo stato del servizio

- **[ICLA] | ICRegisterUsers**
  richiesta proveniente dal servizio UserS solamente da utenti di tipo amministratore - registra nuovi utenti
- **[ICLP] | ICReactivateUsers**
  richiesta proveniente dal servizio UserS - riattiva le utenze degli utenti indicati, sia dal punto di vista del campo userDisabledPwd che userDisabled
- **[ICLP] | ICDisableUsers**
  richiesta proveniente dal servizio UserS - disattiva le utenze degli utenti indicati, agendo sul campo userDisabled
- **[ICL] | ICChangeUserData**
  richiesta proveniente dal servizio UserS - permette di cambiare username, email, password e UsabilityTD (tutti questi campi o solo alcuni) per un utente specifico

Tabelle

In questa sezione vengono descritte le tabelle gestite in questo microservizio:

- **Users** (id, username, email, userType, pwd, lastPwd, pwdExpired, dtPwdChanged, tokenChgPwd, dtRegistration, userDisabledPwd, userDisabled, usabilityTime, usabilityDays, token, userID_OP)
  Note particolari:
  1. userType è necessario per indicare la tipologia di utente (0-utente normale, 1-admin, 2-partner, 3-admin collaboratore, ecc…)
  2. lastPwd è necessario per obbligare l'utente ad utilizzare una pwd diversa da quella precedente
  3. pwdExpired sarà un campo booleano per indicare che la password è scaduta e per obbligare l'utente a cambiarla. (Grazie a dei job automatici da far girare ogni giorno, si controllerà se è passato un mese dalla precedente modifica della password, e in tal caso si attiverà e obbligherà l'utente alla modifica della stessa non appena proverà ad effetuare il login)
  4. tokenChgPwd token dalla validità di 1gg, che verrà inviato via mail all'utente per consentirgli di cambiare la password
  5. userDisabledPwd indica se l'utente è stato disabilitato in seguito a numerosi tentativi di accesso errati
  6. userDisabled indica che l'utente è stato disabilitato da un amministratore o un utente autorizzato a gestire quell'utenza
  7. usabilityTime e usabilityDays indicano gli orari in cui quell'utente può accedere e usare il sistema. Esempio usabilityTime (08:30-15:00;19:00-20.25 | se vuoto = l'utente non può accedere), usabilityDays (0;2;5;5 oppure 7=tutti i giorni; se vuoto = l'utente non può accedere)
  8. token memorizza il token che viene emesso in fase di login. Questo dato ha una durata massima prefissata, ma se l'utente effettua l'accesso da un altro dispositivo, allora questo campo verrà sovrascritto, e il token precedente anche se ancora valido, non sarà più utilizzabile.
  9. userID_OP è l'id dello User che ha eseguito l'ultima operazione di creazione / modifica. Questo campo sarà presente in tutte le tabelle in cui l'utente può andare ad aggiungere / modificare i vari record.

- **LogLoginActivities** (id, userId, loginResult, dtLogin, attemptNum, token)
  Note particolari:
  1. lastPwd è necessario per obbligare l'utente ad utilizzare una pwd diversa da quella precedente
  2. userDisabledPwd indica se l'utente è stato disabilitato in seguito a numerosi tentativi di accesso errati
  3. userDisabled indica che l'utente è stato disabilitato da un amministratore o un utente autorizzato a gestire quell'utenza
  4. usabilityTime e usabilityDays indicano gli orari in cui quell'utente può accedere e usare il sistema
  5. userID_OP è l'id dello User che ha eseguito l'operazione. Questo campo sarà presente in tutte le tabelle in cui l'utente può andare ad aggiungere / modificare i vari record.