ChatGPT

חיבור Cloud Run ל־Cloud SQL – הרשאות ודרישות

1. הרשאות IAM נדרשות לחשבון השירות של Cloud Run

כדי שיישום ב־Cloud Run יוכל להתחבר ל־Cloud SQL באמצעות ספריית ה־Cloud SQL Connector, יש להעניק לחשבון השירות (Service Account) שה־Cloud Run משתמש בו את ההרשאות המתאימות. ההרשאה המומלצת היא **תפקיד Cloud SQL Client** (`roles/cloudsql.client`), אשר כולל את ההרשאות הנדרשות *cloudsql.instances.connect* ו־*cloudsql.instances.get* [1]. תפקיד זה מאפשר לחשבון השירות לפתוח חיבור מאובטח אל אינסטנס ה־Cloud SQL. (תפקידי **Cloud SQL Editor** או **Cloud SQL Admin** הרחבים יותר גם כוללים הרשאות אלה, אך השימוש ב־Cloud SQL Client מממש את עקרון ההרשאות המינימליות הדרושות [1]).

> **הערה:** במידה ואתה משתמש באימות באמצעות סיסמה *(Password Auth)* בלבד ולא ב-IAM Database Authentication, **אין צורך** בתפקיד כמו **Cloud SQL Instance User**. תפקיד Instance User נחוץ רק בתרחישים שבהם משתמשים באימות IAM מול מסד הנתונים, דבר שלא חל במקרה זה כאשר משתמשים בשם משתמש וסיסמת מסד נתונים רגילים.

2. וידוא הפעלת Cloud SQL Admin API

יש לוודא ש־**Cloud SQL Admin API** (ממשק הניהול של Cloud SQL) מופעל בפרויקט. שירות ה־Cloud SQL Connector וכן חיבורי Cloud Run ל־Cloud SQL דורשים ש־API זה יהיה פעיל לצורך ניהול החיבור [2]. כדי לבדוק ולהפעיל את ה־API:

- היכנס למסוף Google Cloud (Console) אל **APIs & Services** ובדוק ברשימת ה-APIs אם *Cloud SQL Admin API* (נקרא גם "Cloud SQL Administration API") **מופעל**. אם לא, לחץ על "Enable" כדי להפעיל אותו.
- לחלופין, ניתן להשתמש בפקודת gcloud:

```
gcloud services enable sqladmin.googleapis.com
```

פקודה זו תפעיל את ה־Cloud SQL Admin API בפרויקט הנוכחי.

במידה וחשבון השירות של Cloud Run נמצא בפרויקט שונה מזה של אינסטנס ה-Cloud SQL, **יש להפעיל את ה-API בשני הפרויקטים** – גם בפרויקט שבו רץ השירות וגם בפרויקט שבו נמצא מסד הנתונים [3]. למעשה, בעת הוספת חיבור Cloud SQL דרך מסוף Cloud Run, הממשק יציג כפתור "Enable the Cloud SQL Admin API" שאותו יש ללחוץ אם ה-API טרם הופעל [4]. הקפד לבצע שלב זה כדי למנוע שגיאות *"Cloud SQL Admin API not enabled"* או שגיאות הרשאה בזמן החיבור.

3. הענקת הרשאות ברמת הפרויקט לעומת ברמת האינסטנס

בפועל, **אין צורך להגדיר הרשאות IAM ישירות על אינסטנס Cloud SQL יחיד אם החשבון מורשה ברמת הפרויקט**. כאשר מעניקים לחשבון השירות את תפקיד Cloud SQL Client ברמת הפרויקט שבו נמצא אינסטנס מסד הנתונים, הדבר מקנה לו גישה לכל אינסטנסי Cloud SQL באותו פרויקט [5]. גישה ברמת הפרויקט היא השיטה הנפוצה והפשוטה: יש לגשת לעמוד IAM & Admin של הפרויקט המארח את מסד הנתונים, ולהעניק לחשבון השירות את התפקיד **Cloud SQL Client** (או תפקיד מתאים אחר) ברמת הפרויקט. תפקיד זה כבר יאפשר גישה לכל המסדים בפרויקט זה. אין חובה להגדיר הרשאות נוספות ברמת האינסטנס עצמו.

עם זאת, אם רוצים לאכוף עקרון **Least Privilege** באופן הדוק יותר, Google Cloud מאפשר גם להעניק תפקידי IAM ברמת משאב האינסטנס הבודד. כלומר, ניתן לפתוח את עמוד ה־Cloud SQL Instance עצמו (במסוף תחת Cloud SQL > שם האינסטנס > Permissions) ולהגדיר שמותאם לחשבון שירות תפקיד **Cloud SQL Client** רק על האינסטנס המסוים. בצורה זו ההרשאה תוגבל לאותו אינסטנס בלבד. זהו צעד אבטחה נוסף אפשרי, אך שוב – **אינו נדרש טכנית** אם הענקת את התפקיד ברמת הפרויקט ומדובר באותו פרויקט [3] . ברירת המחדל ו"הדרך הפשוטה" היא להגדיר ברמת הפרויקט, מה שמכסה את כל המקרים הרלוונטיים.

> **חשוב:** אם Cloud Run וה-Cloud SQL נמצאים בפרויקטים שונים, עליך להוסיף את תפקיד ה-Cloud SQL Client (או ההרשאות *cloudsql.instances.connect* ו-*cloudsql.instances.get*) **בפרויקט שבו נמצא אינסטנס ה-Cloud SQL** עבור חשבון השירות הרלוונטי [3] . זאת בנוסף להרשאות שייתכן ונתת לו בפרויקט שמריץ את Cloud Run. באופן דומה, ודא שה-Cloud SQL Admin API מופעל בכל אחד מהפרויקטים המעורבים.

4. עקיפת הקריאה ל־Cloud SQL Admin API בעת שימוש בסיסמה בלבד

ספריית ה-**Cloud SQL Connector** (וגם proxy החיבור המשולב של Cloud Run) **תמיד משתמשת ב־Cloud SQL Admin API ברקע** כדי לנהל את החיבור, גם כאשר החיבור למסד הנתונים עצמו מתבצע עם שם משתמש וסיסמה. הקריאה ל-API דרושה לקבלת פרטי אינסטנס, אימות הרשאות IAM של חשבון השירות, והגדרת חיבור TLS מאובטח (לרבות השגת אישורים זמניים (ephemeral certificates) עבור ההצפנה) [2] . לכן, כאשר אתה משתמש בספרייה עם `authType: PASSWORD`, משמעות הדבר היא **שאינך משתמש באימות IAM מול מסד הנתונים עצמו**, אך עדיין מתבצעות קריאות ל־SQL Admin API לצורך הקמת החיבור. **אין אפשרות מובנית לבטל את השימוש ב-API זה בספריית ה-Connector** – תנאי מוקדם להפעלתה הוא שה-API פעיל ולחשבון השירות יש הרשאות מתאימות, אחרת תקבל שגיאת הרשאה כדוגמת *"Not authorized to access resource... missing permission cloudsql.instances.get"* כפי שחווית.

הדרך היחידה לעקוף לחלוטין את השימוש ב-SQL Admin API היא **לא** להשתמש כלל בספריית ה-Cloud SQL Connector או בחיבור המשולב, אלא להתחבר באופן ישיר למסד הנתונים. גישה זו דורשת ניהול ידני יותר של התקשורת והאבטחה:

- **חיבור ישיר באמצעות כתובת IP פרטית:** ניתן להגדיר ל־Cloud SQL אינסטנס כתובת IP פרטית (ב-VPC) ולצרף לשירות Cloud Run מחבר VPC Serverless . לאחר מכן, באפליקציה שלך תוכל להתחבר ישירות לכתובת ה־IP הפרטית של מסד הנתונים (למשל x.x.x.10) על פורט 5432 עם שם המשתמש והסיסמה של מסד הנתונים. במקרה זה, התקשורת מתבצעת בתוך הרשת הפרטית, וניתן לעקוף את ה-Cloud SQL Proxy/Connector – **אין קריאות ל-Cloud SQL Admin API בעת החיבור** כי אתה מתחבר ישירות לשרת PostgreSQL עצמו. עם זאת, תהיה אחראי לוודא שהחיבור מאובטח (למשל, לשקול שימוש ב-SSL בין Cloud Run למסד הנתונים, אם כי בחיבור פרטי בתוך VPC ייתכן שזה פחות קריטי) ולנהל את הזכות גישה לרשת (באמצעות חוקי חומת אש או IAM על המחבר).

- **חיבור ישיר באמצעות כתובת IP ציבורית:** לחלופין, אם אינסטנס Cloud SQL שלך מוגדר עם כתובת IP ציבורית, תוכל **לנסות להתחבר ישירות ל-IP הציבורי** עם שם משתמש וסיסמה. אולם, כדי ש-Cloud Run יוכל לגשת אליו, יהיה עליך לפתור את נושא ה-IP המשתנה של Cloud Run. בד"כ משתמשים ב-VPC egress או Cloud NAT כדי להקצות יציאת תעבורה עם IP ידוע, ואז מוסיפים את ה-IP הזה ל"רשימת היתרים" (Authorized Networks) של Cloud SQL. פתרון זה עוקף את הצורך ב-Proxy וב-Admin API, אך הוא מורכב ולא תמיד מומלץ. כמו כן, יש לוודא הצפנת התעבורה (Cloud SQL מאפשר SSL Certificates לחיבור ישיר) והגבלת הגישה רק לכתובות המורשות.

חשוב להדגיש שפתרונות העוקפים את ה-Cloud SQL Admin API **מגיעים עם פשרה** : הם מדלגים על השכבה שה-Google Cloud מספק לניהול מאובטח ופשוט של החיבור. השימוש ב-Cloud SQL Connector או Cloud SQL Auth Proxy מומלץ כיוון שהוא **מטפל עבורך באבטחה, בהצפנה, ובניהול התעבורה** ללא צורך בניהול כתובות IP או אישורים

ידנית [2] . רק במקרים מיוחדים בהם אין אפשרות להפעיל את ה-API או להעניק את ההרשאות (או דרישות ארגוניות אחרות), ניתן לשקול חיבור ישיר כאמור – אך אז האחריות על האבטחה והתחזוקה היא עליך.

לסיכום: כדי לפתור את השגיאה שקיבלת ולחבר את Cloud Run ל-Cloud SQL בהצלחה: ודא ש-**Cloud SQL Admin API פעיל**, תן לחשבון השירות של Cloud Run את **תפקיד Cloud SQL Client** (ברמת הפרויקט של מסד הנתונים) כך שיש לו את ההרשאות *cloudsql.instances.get* ו-*cloudsql.instances.connect* [1] , וודא שהגדרת **חיבור Cloud SQL מנוהל** (דרך ה-Connector/Proxy) כראוי. כך, ספריית ה-Connector תוכל לבצע את הקריאות הנדרשות ל-API ולקבל גישה למסד הנתונים באופן מאובטח. במידה ואתה מעדיף שלא להשתמש ב-API, יהיה עליך לחבר את השירות באופן ישיר כפי שתואר, אם כי פתרון זה פחות נפוץ ומצריך תכנון קפדני של אבטחה וחיבורי רשת.

מקורות: ההנחיות והתצורה דלעיל התבססו על התיעוד הרשמי המעודכן של Google Cloud, כולל דפי ההרשאות של Cloud SQL [1] [5] , מדריכי חיבור Cloud Run ל-Cloud SQL [6] [4] , ונתוני הספריות הרשמית של Cloud SQL Connector [2] .

---

[1] GitHub - GoogleCloudPlatform/cloud-sql-proxy: A utility for connecting securely to your Cloud SQL instances
https://github.com/GoogleCloudPlatform/cloud-sql-proxy

[2] google-cloud/cloud-sql-connector - npm@
https://www.npmjs.com/package/@google-cloud/cloud-sql-connector

[3] [4] [6] Connect from Cloud Run | Cloud SQL for SQL Server | Google Cloud
https://cloud.google.com/sql/docs/sqlserver/connect-run

[5] Roles and permissions | Cloud SQL for MySQL | Google Cloud
https://cloud.google.com/sql/docs/mysql/roles-and-permissions