Deployment Error Analysis: Secret Manager Permissions

What Happened?

Your Cloud Run deployment failed at two stages:

1. Build Failed

The build process failed (you can check the build logs for specific details).

2. Routing Traffic Failed - CRITICAL ERROR

The deployment failed with multiple “Permission denied” errors when trying to access secrets:

```
Permission denied on secret: projects/143559442445/secrets/nextauth-secret/versions/
latest
Permission denied on secret: projects/143559442445/secrets/smtp-password/versions/
latest
Permission denied on secret: projects/143559442445/secrets/database-url/versions/
latest
```

Why Did This Happen?

When you deploy to Cloud Run from a Git repository, Google Cloud Run creates a **service account** that runs your application. This service account needs explicit permission to access secrets stored in Google Secret Manager.

The Problem: By default, the Cloud Run service account does NOT have permission to read secrets from Secret Manager. You need to manually grant this permission.

The Root Cause

In the deployment checklist, you configured secrets in Secret Manager (Step 5), but you likely didn’t grant the Cloud Run service account permission to access those secrets. This is a **separate step** that must be done.

Technical Details

Your Cloud Run service uses a service account with an email like:

```
143559442445-compute@developer.gserviceaccount.com
```

This account needs the **“Secret Manager Secret Accessor”** role for each secret (or at the project level).

How to Fix This - Complete Instructions

Option A: Grant Access at Project Level (Recommended - Simpler)

This gives the service account access to ALL secrets in the project:

1. **Open Google Cloud Console IAM Page:**
   - Go to: https://console.cloud.google.com/iam-admin/iam
   - Make sure you're in the correct project

2. **Find the Service Account:**
   - Look for an account ending with `@developer.gserviceaccount.com`
   - It's usually named "Compute Engine default service account"
   - The full email is: `143559442445-compute@developer.gserviceaccount.com`

3. **Grant the Role:**
   - Click the **pencil icon** (Edit) next to that service account
   - Click **"+ ADD ANOTHER ROLE"**
   - Search for and select: **"Secret Manager Secret Accessor"**
   - Click **SAVE**

4. **Retry the Deployment:**
   - Go back to your Cloud Run service
   - Click **"EDIT & DEPLOY NEW REVISION"**
   - You don't need to change anything
   - Click **DEPLOY**

Option B: Grant Access to Individual Secrets (More Secure)

This gives access only to specific secrets:

1. **Open Secret Manager:**
   - Go to: https://console.cloud.google.com/security/secret-manager
   - Make sure you're in the correct project

2. **For EACH secret (`nextauth-secret`, `smtp-password`, `database-url`):**

a. Click on the secret name

b. Click the **PERMISSIONS** tab

c. Click **"+ GRANT ACCESS"**

d. In "New principals", enter: `143559442445-compute@developer.gserviceaccount.com`

e. In "Select a role", choose: `Secret Manager Secret Accessor`

f. Click **SAVE**

g. Repeat for all three secrets

1. **Retry the Deployment:**
   - Go back to your Cloud Run service
   - Click **“EDIT & DEPLOY NEW REVISION”**
   - You don’t need to change anything
   - Click **DEPLOY**

About the Build Failure

You also had a build failure. Common causes:

1. **Missing Dependencies:** The Dockerfile might be missing some build dependencies
2. **Environment Variables:** Some build-time environment variables might be missing
3. **Build Timeout:** The build might have taken too long

To investigate:
- Click on “Details: Build failed; check build logs for details” in the Cloud Run interface
- Or go to: https://console.cloud.google.com/cloud-build/builds
- Look at the most recent build and check the logs

Common build issues and fixes:

If Prisma-related:

The build might fail if Prisma can’t generate the client. Add to your Dockerfile before the build step:

```dockerfile
# Make sure DATABASE_URL is available at build time
ARG DATABASE_URL
ENV DATABASE_URL=$DATABASE_URL
RUN npx prisma generate
```

If dependency-related:

Make sure all peer dependencies are installed. Check the build logs for missing packages.

Prevention: Update Your Deployment Checklist

Add this as a new step between Step 5 and Step 6 in `DEPLOYMENT_CHECKLIST.md`:

Step 5.5: Grant Secret Access to Service Account

Before deploying, grant the Cloud Run service account permission to read secrets:

```
# Get your project number
PROJECT_NUMBER=$(gcloud projects describe YOUR_PROJECT_ID --format="value(projectNumber)")

# Grant Secret Manager Secret Accessor role
gcloud projects add-iam-policy-binding YOUR_PROJECT_ID \
  --member="serviceAccount:${PROJECT_NUMBER}-compute@developer.gserviceaccount.com" \
  --role="roles/secretmanager.secretAccessor"
```

Or do it manually via the Cloud Console as described above.

Summary

What you need to do RIGHT NOW:

1. ✅ Grant “Secret Manager Secret Accessor” role to service account `143559442445-compute@developer.gserviceaccount.com`
   - Use Option A (project level) for simplicity

2. ✅ Check the build logs to see why the build failed
   - Go to Cloud Build history in GCP Console

3. ✅ After fixing permissions, click “Edit & Deploy New Revision” to retry

4. ✅ Update your deployment checklist to include the permission step

Expected outcome:
After granting the permissions, your deployment should succeed and your app will be accessible at the Cloud Run URL.

Need More Help?

If you continue to have issues:

1. Share the **build logs** from Cloud Build
2. Verify that all three secrets exist in Secret Manager
3. Double-check that the secret names in your Cloud Run configuration exactly match the names in Secret Manager (case-sensitive)
4. Ensure your database is accessible from Cloud Run (check firewall rules if using Cloud SQL)

Quick Reference: Your Project Details

- **Project Number:** 143559442445
- **Service Account:** 143559442445-compute@developer.gserviceaccount.com
- **Region:** us-central1
- **Service Name:** hotel-shift-log
- **Secrets Needed:** nextauth-secret, smtp-password, database-url

This document was created to help you understand and resolve the Cloud Run deployment error related to Secret Manager permissions.