# Setting Up a Cron Job for PostgreSQL Backup and Secure SCP Transfer

## 1. Create the cron\_job.sh File

1. Navigate to the desired directory:

cd /home/boss/Support\_Tools

2. Create the script file:

touch cron\_job.sh

3. Open the file in an editor:

nano cron\_job.sh

4. Add the following backup script:

#!/bin/bash

# Variables

PGUSER="postgres" # PostgreSQL username

PGDATABASE="flowtest" # Database name

PGHOST="localhost" # Database host (default is localhost)

BACKUP\_DIR="/home/boss/Music/Backup" # Directory where you want to store the backup

DATE=$(date +"%Y%m%d%H%M%S") # Timestamp for unique backup filename

BACKUP\_FILE="$BACKUP\_DIR/$PGDATABASE-$DATE.sql"

SECOND\_MACHINE\_USER="cloud"

SECOND\_MACHINE\_IP="10.0.0.1"

SECOND\_MACHINE\_DIR="/home/cloud/Videos/testbackup"

# Command to dump the database

pg\_dump -U $PGUSER -h $PGHOST $PGDATABASE > $BACKUP\_FILE

# Optional: Clean up backups older than 30 days

find $BACKUP\_DIR -type f -name "\*.sql" -mtime +30 -exec rm {} \;

# Sending backup to second machine

scp $BACKUP\_FILE $SECOND\_MACHINE\_USER@$SECOND\_MACHINE\_IP:$SECOND\_MACHINE\_DIR

# Unset password

unset PGPASSWORD

5. Save the file and exit the editor.

6. Provide execute permissions:

chmod +x cron\_job.sh

## 2. Schedule the Cron Job

1. Open the crontab editor:

crontab -e

2. Add the following entry to run the script daily at 18:26:

26 18 \* \* \* export PGPASSWORD="12345" && /home/boss/Support\_Tools/cron\_job.sh

3. Save and exit the editor.

4. Restart the cron service:

sudo systemctl restart cron

## 3. Secure SCP Transfer Without Password

To securely transfer the backup file to another machine without a password:

1. Navigate to the SSH directory:

cd ~/.ssh

2. Generate an SSH key pair:

ssh-keygen -t rsa -b 2048

- Press Enter to save the key in the default location.

- Press Enter twice to skip the passphrase.

3. Copy the public key to the target machine:

ssh-copy-id cloud@10.0.0.1

4. Set proper permissions on the target machine:

chmod 700 ~/.ssh

chmod 600 ~/.ssh/authorized\_keys

5. Restart the SSH service on the target machine:

sudo systemctl restart sshd