Usage instructions:

1. **Launch the product via 1-click. Please wait until the instance passes all status checks and is running.**

2. **You can connect using your Amazon private key and 'ubuntu' login via your SSH client.**

   - **To update software, use:** `sudo apt-get update`

3. **Initialize Appwrite (containers).** Everything is preinstalled. Start the stack:

   ```
   sudo su
   cd /srv/appwrite/appwrite
   docker compose up -d --remove-orphans
   docker compose ps
   ```

4. Open a browser to:

   https://YOUR_INSTACE_PUBLIC_IP

   Now you can **create a new account** (this becomes the first admin) or log in with your credentials.

   • For additional documentation: https://appwrite.io/docs

3) (Optional) Point a domain & enable Let's Encrypt

Create an A record from app.yourdomain.com → your instance's Public IPv4.

Reconfigure Appwrite for a proper certificate:

```
sudo su
cd /srv/appwrite/appwrite

# Stop the stack
docker compose down

# Run the installer to set hostname & Let's Encrypt email

docker run -it --rm \
```

```
  -v /var/run/docker.sock:/var/run/docker.sock \
  -v "$PWD:/usr/src/code/appwrite:rw" \
  --entrypoint=install \
  appwrite/appwrite:1.8.0
```

For prompts:

- HTTP port: 80 (default)
- HTTPS port: 443 (default)
- Secret API key: choose & save it securely
- Appwrite hostname: app.yourdomain.com
- Custom domains CNAME (can match hostname): app.yourdomain.com
- Email for SSL: you@yourdomain.com

Bring the stack back up:

```
docker compose up -d --remove-orphans
```

Visit:

https://app.yourdomain.com

and create/login to your admin account.

4) Useful commands

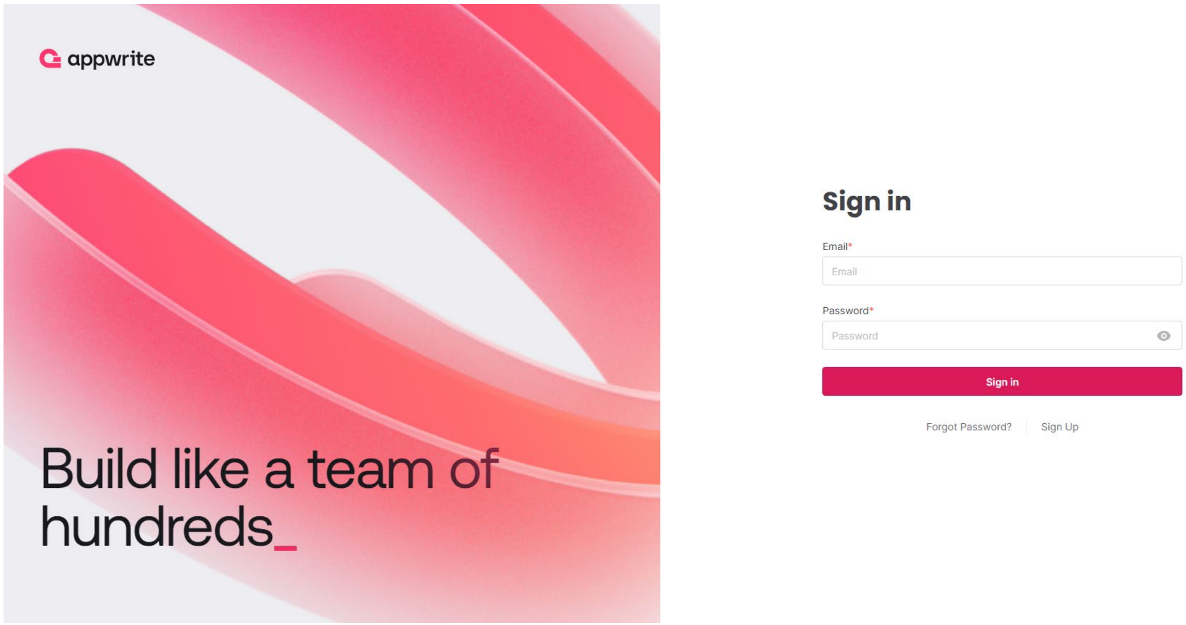
```
# Check status
docker compose ps

# Show logs (follow)
docker compose logs -f

# Stop stack (keeps data)
docker compose down

# Stop & remove data volumes (factory reset)
docker compose down --volumes

# Update images, then restart
docker compose pull
docker compose up -d --remove-orphans
```



AWS Data

- Data Encryption Configuration: This solution does not encrypt data within the running instance.
- User Credentials are stored: /root/.ssh/authorized_keys & /home/ubuntu/.ssh/authorized_keys
- Monitor the health:
  - Navigate to your Amazon EC2 console and verify that you're in the correct region.
  - Choose Instance and select your launched instance.
  - Select the server to display your metadata page and choose the Status checks tab at the bottom of the page to review if your status checks passed or failed.

Extra Information: **(Optional)**

Allocate Elastic IP

To ensure that your instance keeps its IP during restarts that might happen, configure an Elastic IP. From the EC2 console:

1. **Select ELASTIC IPs.**
2. **Click on the ALLOCATE ELASTIC IP ADDRESS.**
3. **Select the default (Amazon pool of IPv4 addresses) and click on ALLOCATE.**
4. **From the ACTIONS pull down, select ASSOCIATE ELASTIC IP ADDRESS.**
5. **In the box that comes up, note down the Elastic IP Address, which will be needed when you configure your DNS.**
6. **In the search box under INSTANCE, click and find your INSTANCE ID and then click ASSOCIATE.**
7. **Your instance now has an elastic IP associated with it.**