

# Docker Commands

- [Build and Run a Container](#)
- [Reverse Proxy with Nginx](#)
- [Enter a Container as Root](#)

# Build and Run a Container

## Build the Docker image

```
docker build -t <image-name> .
```

## Run the container:

```
docker run -d --name <container-name> <image-name>
```

You can verify it's working by checking the logs with:

```
docker logs <container-name>
```

Or by viewing the cron log specifically:

```
docker exec -it <container-name> tail -f /var/log/cron.log
```

# Reverse Proxy with Nginx

To install and configure Nginx with HTTPS support (SSL/TLS) on your Linux server, follow these steps. I'll outline the process assuming you're setting up Nginx on a Debian/Ubuntu system. Adjust commands and paths as needed for other distributions.

## Step 1: Install Nginx

First, ensure your package lists are up-to-date, then install Nginx:

```
sudo apt update
sudo apt install nginx
```

## Step 2: Obtain SSL/TLS Certificates

You can obtain SSL/TLS certificates for your domain using Let's Encrypt, which provides free certificates. Here's how to set it up with Certbot, a tool for automatically managing Let's Encrypt certificates:

### Install Certbot

```
sudo apt install certbot python3-certbot-nginx
```

## Step 3: Configure Nginx for HTTPS

### 1. **Configure Nginx**

Create a new configuration file for your domain under Nginx's sites-available directory:

```
sudo nano /etc/nginx/sites-available/<domain>
```

Example Nginx configuration for HTTPS:

```
server {
    listen 80;
    server_name <domain>;
```

```
location / {  
    proxy_pass http://localhost:<port>;  
    proxy_http_version 1.1;  
    proxy_set_header Upgrade $http_upgrade;  
    proxy_set_header Connection 'upgrade';  
    proxy_set_header Host $host;  
    proxy_cache_bypass $http_upgrade;  
}  
}
```

Replace `<domain>` with your actual domain name and adjust `proxy_pass` to point to your BookStack Docker container.

## 2. Enable the Site

Create a symbolic link to enable the site in Nginx:

```
sudo ln -s /etc/nginx/sites-available/<domain> /etc/nginx/sites-enabled/
```

## 3. Test Nginx Configuration

Verify the Nginx configuration for syntax errors:

```
sudo nginx -t
```

## 4. Reload Nginx

Apply the new configuration:

```
sudo systemctl reload nginx
```

# Step 4: Obtain SSL/TLS Certificates with Certbot

Run Certbot to obtain SSL certificates for your domain (`<domain>`):

```
sudo certbot --nginx -d <domain>
```

Follow the prompts to set up HTTPS for your domain. Certbot will automatically configure Nginx with SSL/TLS settings and handle certificate renewal.

# Step 5: Verify HTTPS Setup

Access `https://<domain>` in your web browser to verify that Nginx is correctly serving your BookStack application over HTTPS.

# Notes:

- **Firewall:** Ensure ports 80 (HTTP) and 443 (HTTPS) are open in your firewall.
- **Security:** Regularly update Nginx and renew SSL certificates before expiry.
- **Backup:** Maintain backups of your Nginx configurations and SSL certificates.

This setup ensures secure access to your BookStack application with HTTPS, enhancing data security and user trust.

# Enter a Container as Root

```
docker exec -u 0 -it <container_name_or_id> /bin/bash
```