Generate a Self-Signed SSL Certificate

### **Step 1: Generate a Self-Signed SSL Certificate**

1. **Create a directory for the SSL certificate:**

sudo mkdir -p /etc/gitlab/ssl  
sudo chmod 700 /etc/gitlab/ssl

1. **Generate the SSL certificate and private key:** place your\_ip\_address

sudo openssl req -newkey rsa:4096 -nodes -keyout /etc/gitlab/ssl/your\_ip\_address.key -x509 -

### **Create a Certificate Signing Request (CSR)**

### create a CSR using the private key.

sudo openssl req -new -key /etc/gitlab/ssl/gitlab.key -out /etc/gitlab/ssl/gitlab.csr

* You will be prompted to enter details such as: **Country Name**: (e.g., US),**State or Province Name**: (e.g., California), Locality Name,etc.

### **Generate the Self-Signed SSL Certificate**

Now, generate the self-signed SSL certificate using the CSR and the private key.

sudo openssl x509 -req -days 365 -in /etc/gitlab/ssl/ip.csr -signkey /etc/gitlab/ssl/ip.key -out /etc/gitlab/ssl/ip.crt

sudo chmod 600 /etc/gitlab/ssl/10.100.11.68.key

sudo chmod 644 /etc/gitlab/ssl/10.100.11.68.crt

**Verify Certificate Information: Use** openssl to inspect your certificate:

Configure GitLab to Use the SSL Certificate

* **Edit the GitLab configuration file:**

sudo nano /etc/gitlab/gitlab.rb

* **Update the external URL to use HTTPS with your IP address:**

external\_url '<https://10.100.11.68:443>'

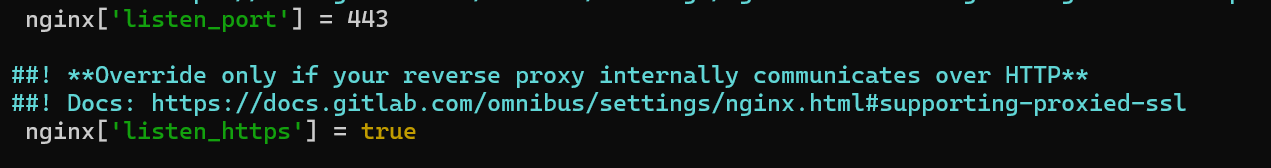
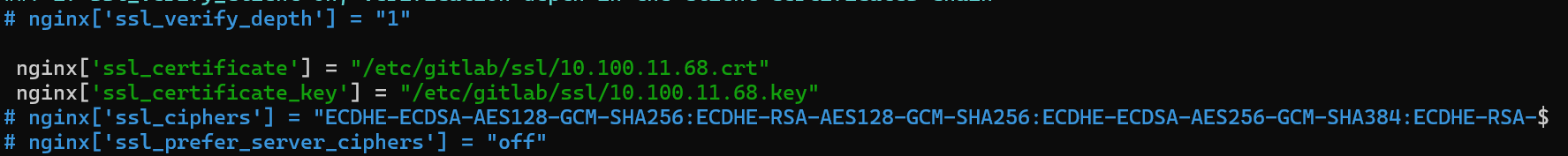


* **Specify the SSL certificate and key paths:**

nginx['ssl\_certificate'] = "/etc/gitlab/ssl/your\_ip\_address.crt"  
nginx['ssl\_certificate\_key'] = "/etc/gitlab/ssl/your\_ip\_address.key"

* **Optionally, disable HTTP access to force HTTPS:**

nginx['redirect\_http\_to\_https'] = true

After making changes in /etc/gitlab/gitlab.rb to ensure it use following commands:

sudo gitlab-ctl reconfigure

sudo gitlab-ctl restart

To check status use: sudo gitlab-ctl status

[root@passionbytes anchors]# sudo cp /etc/gitlab/ssl/10.100.11.68.crt /etc/pki/ca-trust/source/anchors/

[root@passionbytes anchors]# sudo update-ca-trust

[root@passionbytes anchors]# sudo gitlab-ctl reconfigure

Error response from daemon: Get "https://10.100.11.68:5050/v2/": tls: failed to verify certificate: x509: certificate relies on legacy Common Name field, use SANs instead

Steps to debug:

Sudo openssl x509 -req -in /etc/gitlab/ssl/10.100.11.68.csr -signkey /etc/gitlab/ssl/10.100.11.68.key -out /etc/gitlab/ssl/10.100.11.68.crt -days 365 -extensions req\_ext -extfile /etc/gitlab/ssl/san.cnf

Else

sudo openssl req -new -newkey rsa:2048 -sha256 -days 365 -nodes -x509 \

-subj "/C=US/ST=California/L=San Francisco/O=Example Ltd/CN=10.100.11.68" \

-keyout /etc/gitlab/ssl/10.100.11.68.key -out /etc/gitlab/ssl/10.100.11.68.crt \

-addext "subjectAltName=IP:10.100.11.68"

To Verify:

openssl s\_client -showcerts -servername 10.100.11.68 -connect 10.100.11.68:5050

To **Configure CA Trust on CentOS**

1. **Add Certificate to CA Trust**:

sudo cp /etc/gitlab/ssl/10.100.11.68.crt /etc/pki/ca-trust/source/anchors/

sudo update-ca-trust

GitLab and Docker Registry Configuration

### **Gitlab Configuration**

#### **External URL**

Set the external\_url to use port 443 for GitLab’s web interface.

* **File**: /etc/gitlab/gitlab.rb
* **Configuration**:
* external\_url 'https://10.100.11.68:443'  
  

#### **Docker Registry URL**

Set the registry\_external\_url to use port 5050 for the Docker Registry.

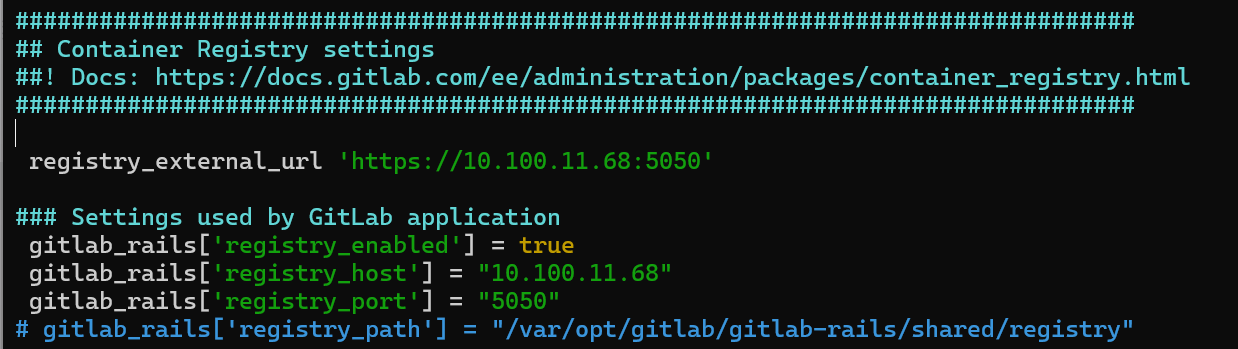
* **File**: /etc/gitlab/gitlab.rb
* **Configuration**:

registry\_external\_url '<https://10.100.11.68:5050>'

#### **Enable Docker Registry**

Ensure the Docker Registry is enabled in GitLab.

* **File**: /etc/gitlab/gitlab.rb
* **Configuration**:
* gitlab\_rails['registry\_enabled']

= true

#### **Nginx Configuration for GitLab and Registry**

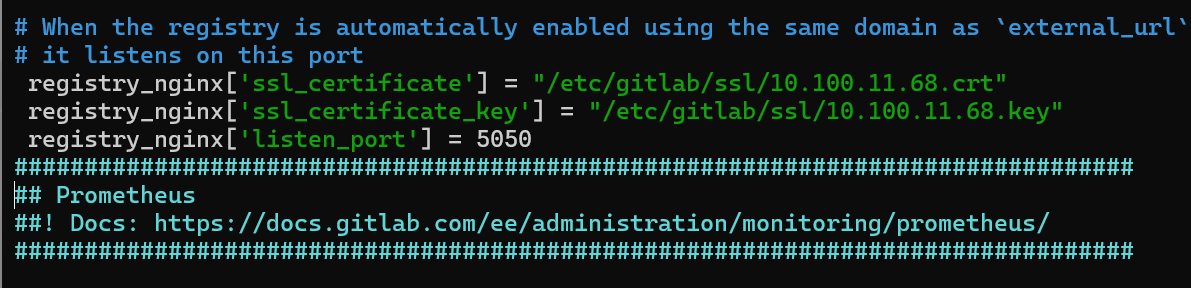
Make sure Nginx is configured to listen on ports 8083 (GitLab) and 5050 (Docker Registry).

* **GitLab Nginx Configuration**:

nginx['listen\_port'] = 443

* **Docker Registry Nginx Configuration:**

registry\_nginx['enable'] = true  
registry\_nginx['listen\_port'] = 5050



* Step to troubleshoot this error

Error response from daemon: Get "https://10.100.11.68:5050/v2/": tls: failed to verify certificate: x509: certificate relies on legacy Common Name field, use SANs instead

* Check for port that we are accessing
* sudo netstat -tulnp | grep 443
* sudo netstat -tulnp | grep 5050
* Copy ssl certificates in docker to get accessing registry
* sudo mkdir -p /etc/docker/certs.d/10.100.11.68:5050/
* sudo cp 10.100.11.68.crt /etc/docker/certs.d/10.100.11.68:5050/
* sudo cp 10.100.11.68.key /etc/docker/certs.d/10.100.11.68:5050/
* Give certificates name as client.crt or client.key to docker can identify it correctly