**SSL Configuration**

## Available SSL Configuration Tasks

Omnibus-GitLab supports several common use cases for SSL configuration.

1. Allow https connections to GitLab instance services
2. Configure public certificate bundles for external resource connections

Add the following entries to /etc/gitlab/gitlab.rb to enable **Let’s Encrypt** support for the primary domain:

letsencrypt['enable'] = true # GitLab 10.5 and 10.6 require this option

external\_url "https://gitlab.example.com" # Must use https protocol

letsencrypt['contact\_emails'] = ['foo@email.com'] # Optional

#### GitLab Components

Introduced in GitLab 11.0.

[Follow the steps to enable basic **Let’s Encrypt** integration](https://docs.gitlab.com/omnibus/settings/ssl.html#lets-encrypt-integration) and modify /etc/gitlab/gitlab.rb with any of the following that apply:

registry\_external\_url "https://registry.example.com" # container registry, must use https protocol

mattermost\_external\_url "https://mattermost.example.com" # mattermost, must use https protocol

#registry\_nginx['ssl\_certificate'] = "path/to/cert" # Must be absent or commented out

The **Let’s Encrypt** certificate is created with the GitLab primary instance as the primary name on the certificate. Additional services such as the registry are added as alternate names to the same certificate. Note in the example above, the primary domain is gitlab.example.com and the registry domain is registry.example.com. Administrators do not need to worry about setting up wildcard certificates

#### Automatic Let’s Encrypt Renewal

[Introduced](https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/2433) in [GitLab](https://about.gitlab.com/pricing/) 10.7.

Administrators installing or upgrading to GitLab 12.1 or later and plan on using their own **Let’s Encrypt** certificate should set letsencrypt['enable'] = false in /etc/gitlab/gitlab.rb to disable automatic renewal. **Otherwise, a gitlab-ctl reconfigure may attempt to renew the certificates, and thus overwrite them.**

Default installations schedule renewals after midnight on every 4th day. The minute is determined by the value in external\_url to help distribute the load on the upstream Let's Encrypt servers.

Explicitly set renewal times by adding the following to /etc/gitlab/gitlab.rb:

# This example renews every 7th day at 12:30

letsencrypt['auto\_renew\_hour'] = "12"

letsencrypt['auto\_renew\_minute'] = "30"

letsencrypt['auto\_renew\_day\_of\_month'] = "\*/7"

Disable automatic renewal with the following in /etc/gitlab/gitlab.rb:

letsencrypt['auto\_renew'] = false

#### Manual Let’s Encrypt Renewal

Renew **Let’s Encrypt** certificates manually using **one** of the following commands:

sudo gitlab-ctl reconfigure

sudo gitlab-ctl renew-le-certs

<VirtualHost gitlabdev.statebanktimes.in:443>

SSLEngine on

SSLProtocol all -SSLv2 -SSLv3

SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA

ProxyPreserveHost On

ProxyPass / http://10.191.159.50:8083/

ProxyPassReverse / http://10.191.159.50:8083/

SSLCertificateFile /opt/ssl\_cert/29122020/devopsdev.statebanktimes.in.crt

SSLCertificateKeyFile /opt/ssl\_cert/29122020/devopsdev.statebanktimes.in.key

</VirtualHost>

<VirtualHost nagiosdev.statebanktimes.in:443>

SSLEngine on

SSLProtocol all -SSLv2 -SSLv3

SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA

SSLCertificateFile /opt/ssl\_cert/29122020/devopsdev.statebanktimes.in.crt

SSLCertificateKeyFile /opt/ssl\_cert/29122020/devopsdev.statebanktimes.in.key

</VirtualHost>