Redmine4.2(Redmine 5.x)?SSL??

??????????

- ???????????Redmine?SSL??????
- ??SSL???????????

????????

- Redmine?SSL???????
- SSL???????????

??

??????????????

- Ubuntu 20.04? / Ubuntu 22.04??Redmine 5.x)
- Apache2.4
- ?????Redmine?????????????????
- ?????SSL?????????????

????

??????SSL???????????????

- ??????????????????????
- Let's Encrypt??????????

??

?????????

1. ??????????????????????
2. ??SSL???????????????????????????
3. Apache??????????SSL?????????
4. Redmine??????????
5. [??????]??????????Redmine?????????????

??????

?SSL?????????????????????????????(Let's Encrypt?????3??)

????????????Apache?????????????????????????/?????????????????????

?????????????

```
sudo mkdir /etc/certs
```

???????????????

```
sudo mkdir /etc/private
```

???????????????

??????????????????????

- SCP?SFTP?????????????????????
- Let's Encrypt?????????????????????????????/????

??????????????

????Let's Encrypt?2023?1???????hoge.sample.com (/etc/letsencrypt/live/?????/?????????)??

- hoge.sample.com.crt.202301 (???:/etc/certs???)
- hoge.sample.com.key.202301 (???:/etc/private???)

???????

?????????????

hoge.sample.com.crt.CA.202301

???????????????

??????????????????????

```
cd /etc/certs && pwd
```

`/etc/certs` ????????

```
sudo ln -sf hoge.sample.com.crt.202301 hoge.sample.com.crt
```

```
ls -l hoge.sample.com.crt
```

????????hoge.sample.com.crt.202301???????????

- ?????????????

```
sudo ln -sf hoge.sample.com.crt.CA.202301 hoge.sample.com.CA.crt
```

???????Global Sign, Sectigo, GeoTrust??????????????????????????(Let's Encrypt????chain.pem???)

??????????????????

```
cd /etc/private && pwd
```

`/etc/private`????????

```
sudo ln -sf hoge.sample.com.key.202301 hoge.sample.com.key
```

```
ls -l hoge.sample.com.key
```

????????hoge.sample.com.crt.202301???????????

?????????????

```
openssl x509 -noout -dates -subject -in /etc/certs/hoge.sample.com.crt
```

- notBefore=
- notAfter=

????????????????????????????

- subject=CN =

??????????????????????????????hoge.sample.com ?????????????? *.sample.com

- ?????????????????

```
openssl x509 -pubkey -in /etc/certs/hoge.example.com.crt -noout | openssl md5
```

```
openssl pkey -pubout -in /etc/private/hoge.example.com.key | openssl md5
```

??????????????????????????????????2???????((stdin)= ?????)????????????????????????????

- ???????????? (Let's Encrypt??????????????????)

```
openssl crl2pkcs7 -nocrl -certfile /etc/certs/hoge.example.com.crt | openssl pkcs7 -print_certs -outform PEM | awk 'BEGIN {c=0;} /BEGIN CERTIFICATE/ {c++} { print > "cert" c ".pem"}' && openssl verify -CAfile cert2.pem cert1.pem
```

> openssl verify -CAfile cert2.pem cert1.pem
> cert1.pem: OK

???????

- ????????????? (??????????????????????)

```
openssl verify -CAfile /etc/certs/hoge.sample.com.CA.crt /etc/certs/hoge.example.com.crt
```

> /etc/certs/hoge.example.com.crt: OK

???????

??SSL??????????????????

????????

```
cat /etc/apache2/mods-available/rewrite.load
```

```
cat /etc/apache2/mods-available/ssl.load
```

```
cat /etc/apache2/mods-available/headers.load
```

????????

```
sudo a2enmod rewrite
```

```
sudo a2enmod ssl
```

```
sudo a2enmod headers
```

???????

```
sudo systemctl restart apache2
```

Apache?????????

http??????????????????????????

```
sudo mkdir -p /etc/apache2/old
```

```
cd /etc/apache2/sites-available && pwd
```

```
sudo a2dissite redmine.conf
```

```
sudo systemctl restart apache2.service
```

http????????????????????????

```
sudo mv redmine.conf ../old/redmine.conf.$(date +%Y%m%d)
```

???http??????????????????????????????

??SSL??????????

- ??
- cat ? __EOF__????????????????????? ? ??????(??????????????) ? ?????????????????????

```
cat <<- __EOF__ | sudo tee -a /etc/apache2/sites-available/redmine.conf
<VirtualHost *:80>
    servername 【hoge.example.com】
    # ドメイン名を指定します
    RewriteEngine On
        RewriteCond %{HTTPS} off
        RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
# HTTPアクセスを強制的にHTTPSにリダイレクトします
</VirtualHost>

<VirtualHost *:443>
    ServerName 【hoge.example.com】
    # ドメイン名を指定します
    DocumentRoot 【/home/www-data/redmine/public】
    # 自身の環境に合わせます
    <Directory 【/home/www-data/redmine/public】>
    # 自身の環境に合わせます
        Options -MultiViews
        AllowOverride All
        Require all granted
    </Directory>

#SSL設定
  SSLEngine on
    Protocols h2 http/1.1
  # SSLを有効化します
```

```
SSLCertificateFile 〔/etc/certs/hoge.example.com.crt〕
# SSL証明書を指定します
SSLCertificateKeyFile 〔/etc/private/hoge.example.com.key〕
# 秘密鍵を指定します

# SSLCACertificateFile 〔/etc/certs/hoge.example.com.CA.crt〕
# 中間証明書が発行元から別ファイルで提供されている場合は、この直上をコメントアウトして中間証明書を指定します

#セキュリティヘッダー付与

    Header always set Strict-Transport-Security "max-age=63072000"
    Header set X-Content-Type-Options "nosniff"
    Header always append X-Frame-Options "SAMEORIGIN"
    Header set X-XSS-Protection "1; mode=block"

</VirtualHost>

SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1 -TLSv1.2
SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:EC6-GCM-SHA384
SSLHonorCipherOrder     off
SSLSessionTickets       off

SSLUseStapling On
SSLStaplingCache "shmcb:logs/ssl_stapling(32768)"
# これらのセクションはSSL暗号化強度を高めるための記述です
# </VirtualHost>の外側に書くことにご注意ください
__EOF__
```

????????

```
sudo a2ensite redmine
```

?????redmine??????????

```
sudo apache2ctl configtest
```

`Syntax OK` ??

```
sudo systemctl restart apache2.service
```

??????????????redmine?????????????

- https????????
- ??????????
- ??????????????

???????

Redmine??????????

1. Redmine????????????
2. ?? ? ????????
3. ??????????????????????(hoge.example.com)
4. ????????HTTP?HTTPS????

????Redmine???SSL???????????

???????Redmine????SSL????????????

????????????????????????????

- Redmine?????????????????????
- Let's Encrypt?????????????????????????

SSL?????????????????

https://www.ssllabs.com/ssltest/

?????????????????

1. Hostname:Redmine?URL
2. ?Do not show the results on the boards??????(????????????)
3. ?Submit??????????

2023?1????????Apache?????????????A?????????????????????????????

Revision #8
Created 1 April 2024 11:00:38 by manualmaton
Updated 11 October 2024 06:41:35 by manualmaton