日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2022年11月25日金曜日

Customer Managed ORDSの構成(2) - Let's Encryptを使ったSSL化

自己署名証明書の代わりに、Let's Encryptによって発行された証明書に置き換えます。

DNSにコンピュート・インスタンスのホスト名とパブリックIPアドレスが登録され、どこからでもホスト名からIPアドレスが解決できる状態になっていることが前提条件です。

firewalldの構成

httpのサービスで接続できるようにします。

firewall-cmd --add-service=http
firewall-cmd --runtime-to-permanent
firewall-cmd --reload
firewall-cmd --list-all

ORDSを実装したコンピュート・インスタンスにログインし、ユーザーrootにて上記のコマンドを実行します。

```
[root@cmords ~]# firewall-cmd --add-service=http
success
[root@cmords ~]# firewall-cmd --runtime-to-permanent
success
[root@cmords ~]# firewall-cmd --reload
success
[root@cmords ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dhcpv6-client http https ssh
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
        port=443:proto=tcp:toport=8443:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:
[root@cmords ~]#
```

Certbotのインストール

以下のコマンドを実行し、Certbotをインストールします。

dnf --enablerepo=ol8_developer_EPEL -y install certbot

```
[root@cmords ~]# dnf --enablerepo=ol8_developer_EPEL -y install certbot
Failed to set locale, defaulting to C.UTF-8
Last metadata expiration check: 0:01:48 ago on Fri Nov 25 07:53:52 2022.
Dependencies resolved.
================================================================================
 Package                    Arch    Version              Repository          Size
================================================================================
Installing:
 certbot                    noarch  1.22.0-1.el8         ol8_developer_EPEL  55 k
Installing dependencies:
 python3-acme               noarch  1.22.0-1.el8         ol8_developer_EPEL  97 k
 python3-certbot            noarch  1.22.0-1.el8         ol8_developer_EPEL 427 k
 python3-configargparse     noarch  0.14.0-6.el8         ol8_developer_EPEL  37 k
 python3-distro             noarch  1.4.0-2.module+el8.3.0+7694+550a8252
                                                         ol8_appstream       37 k
 python3-josepy             noarch  1.9.0-1.el8          ol8_developer_EPEL 104 k
 python3-parsedatetime      noarch  2.5-1.el8            ol8_developer_EPEL  80 k
 python3-pyrfc3339          noarch  1.1-1.el8            ol8_developer_EPEL  20 k
 python3-requests-toolbelt noarch  0.9.1-4.el8          ol8_developer_EPEL  92 k
 python3-zope-component     noarch  4.3.0-8.el8          ol8_developer_EPEL 314 k
 python3-zope-event         noarch  4.2.0-12.el8         ol8_developer_EPEL 211 k
 python3-zope-interface     aarch64 4.6.0-1.el8          ol8_developer_EPEL 159 k

Transaction Summary
================================================================================
Install  12 Packages

[中略]

Installed:
  certbot-1.22.0-1.el8.noarch
  python3-acme-1.22.0-1.el8.noarch
  python3-certbot-1.22.0-1.el8.noarch
  python3-configargparse-0.14.0-6.el8.noarch
  python3-distro-1.4.0-2.module+el8.3.0+7694+550a8252.noarch
  python3-josepy-1.9.0-1.el8.noarch
  python3-parsedatetime-2.5-1.el8.noarch
  python3-pyrfc3339-1.1-1.el8.noarch
  python3-requests-toolbelt-0.9.1-4.el8.noarch
  python3-zope-component-4.3.0-8.el8.noarch
  python3-zope-event-4.2.0-12.el8.noarch
  python3-zope-interface-4.6.0-1.el8.aarch64

Complete!
[root@cmords ~]#
```

Certbotのインストールは以上で完了です。

Let's Encryptからの証明書取得

Certbotを実行し、Let's Encryptにより署名されたサーバー証明書を取得します。

最初にホスト名からIPアドレスが解決できるか、hostコマンドを実行して確認します。

host ホスト名

ホスト名とIPアドレスの部分は、DNSに登録した値になります。

```
[root@cmords ~]# host ホスト名
ホスト名 has address IPアドレス
[root@cmords ~]#
```

certbotを実行し、証明書を取得します。

certbot certonly --standalone

最初に緊急のリニューアルとセキュリティに関する通知を受け取る**メール・アドレス**を入力します。

使用許諾について確認されるので、**Y**を入力します。

Electronic Frontier Foundationと入力したメール・アドレスを共有して良いかどうか聞かれるので、YまたはNのどちらかを入力します。

最後に証明書に含めるドメイン名（ホスト名）を聞かれるので、**ホスト名**を入力します。

以上を入力すると**/etc/letsencrypt/live/ホスト名**以下に、サーバー証明書として**cert.pem**、秘密キーのファイルとして**private.pem**が作成されます。

/etc/letsencrypt/live/ホスト名/cert.pem
/etc/letsencrypt/live/ホスト名/privkey.pem

```
[root@cmords ~]# certbot certonly --standalone
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): メール・アドレスの入力

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: Y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: N
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): ホスト名
```

```
Requesting a certificate for ホスト名

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/ホスト名/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/ホスト名/privkey.pem
This certificate expires on 2023-02-23.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the
background.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[root@cmords ~]#
```

生成されたファイルを使うように、ORDSの構成を変更します。

ORDSの構成変更

cert.pemを/etc/ords/config/global/standaloneにコピーし、ユーザーoracleでアクセスできるようにします。

cp /etc/letsencrypt/live/ホスト名/cert.pem /etc/ords/config/global/standalone/cert.pem
chown oracle /etc/ords/config/global/standalone/cert.pem
chmod 600 /etc/ords/config/global/standalone/cert.pem

```
[root@cmords ~]# cp /etc/letsencrypt/live/ホスト名/cert.pem
/etc/ords/config/global/standalone/cert.pem
[root@cmords ~]# chown oracle /etc/ords/config/global/standalone/cert.pem
[root@cmords ~]# chmod 600 /etc/ords/config/global/standalone/cert.pem
[root@cmords ~]#
```

秘密キーのファイルであるprivkey.pemは、PKCS#8形式に変換した上でコピーします。

openssl pkcs8 -topk8 -in /etc/letsencrypt/live/ホスト名/privkey.pem -nocrypt -outform PEM -out /etc/ords/config/global/standalone/server.key
chown oracle /etc/ords/config/global/standalone/server.key
chmod 400 /etc/ords/config/global/standalone/server.key

```
[root@cmords ~]# openssl pkcs8 -topk8 -in /etc/letsencrypt/live/ホスト名/privkey.pem
-nocrypt -outform PEM -out /etc/ords/config/global/standalone/server.key
[root@cmords ~]# chown oracle /etc/ords/config/global/standalone/server.key
[root@cmords ~]# chmod 400 /etc/ords/config/global/standalone/server.key
[root@cmords ~]#
```

/etc/ords/config/global/settings.xmlに、standalone.https.cert、standalone.https.cert.keyの２行を含めます。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Saved on Fri Nov 25 06:07:43 UTC 2022</comment>
```

```
<entry key="database.api.enabled">false</entry>
<entry key="standalone.context.path">/ords</entry>
<entry key="standalone.doc.root">/etc/ords/config/global/doc_root</entry>
<entry key="standalone.https.port">8443</entry>
<entry key="standalone.static.context.path">/i/22.2.0/</entry>
<entry key="standalone.static.path">/home/oracle/i</entry>
<entry
key="standalone.https.cert">/etc/ords/config/global/standalone/cert.pem</entry>
<entry
key="standalone.https.cert.key">/etc/ords/config/global/standalone/server.key</entr
y>
</properties>
```

変更を反映させるためにORDSを再起動します。

```
[root@cmords opc]# systemctl restart ords
[root@cmords opc]#
```

以上でLet's Encryptにて発行されたサーバー証明書を使うようになりました。

Hostsファイルに残っているエントリがあれば削除します。また、自己署名証明書が手元のPCに信頼する証明書として登録されたままであれば、それも削除しておきます。

完

Yuji N. 時刻: 17:33

共有

‹ ホーム ›

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示