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6月7日火曜日

Ampere A1インスタンスにKeycloakをインストールする

Oracle APEXのSAML認証を検証するにあたって、IdPを用意する必要がありました。無料で使えるものを探したところ、Keycloakというオープン・ソースのIdPがあったので、それを使うことにしました。

Oracle CloudのAmpere A1インスタンス(ARMのインスタンス)に、Keycloakをインストールした作業の記録になります。Oracle APEXとは直接は関係しません。

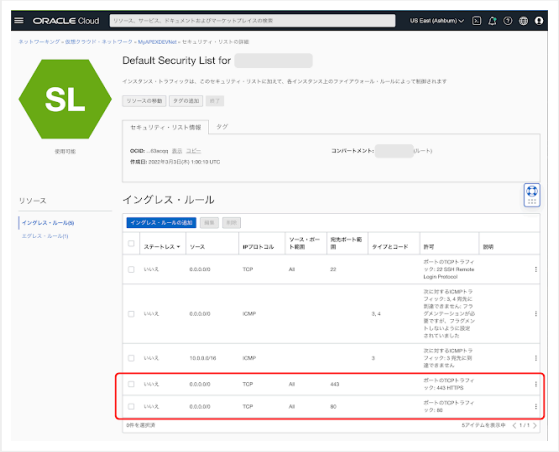
仮想クラウド・ネットワークが構成済み、Always Free枠のAmpere A1インスタンスをひとつ作成した直後の状態から作業を始めます。

作成済みのコンピュート・インスタンスのパブリックIPアドレスは、DNSにホスト名と共に登録済みとします。この作業記録では、Keycloakを稼働させるホスト名を

myidp.mydomain.dev

と記載します。作業を行なう場合は、適時、自分自身で使うホスト名に読み替えてください。

また、パブリック・ネットワークの**イングレス・ルール**として、ポート番号**80(HTTP)**およびポート番号**443(HTTPS)**の通過を許可しておきます。



作成済みのコンピュート・インスタンスに、ユーザーopcにてSSH接続します。

OSを最新にアップデートします。

sudo dnf -y update

```
[opc@idp ~]$ sudo dnf -y update
Failed to set locale, defaulting to C.UTF-8
Ksplice for Oracle Linux 8 (aarch64)                                5.3 MB/s |
270 kB     00:00
MySQL 8.0 for Oracle Linux 8 (aarch64)                               39 MB/s |
2.4 MB     00:00
MySQL 8.0 Tools Community for Oracle Linux 8 (aarch64)              3.3 MB/s |
178 kB     00:00
MySQL 8.0 Connectors Community for Oracle Linux 8 (aarch64)         376 kB/s |
21 kB     00:00
[中略]
  sssd-krb5-2.6.2-4.0.2.el8_6.aarch64                 sssd-krb5-common-2.6.2-
4.0.2.el8_6.aarch64
  sssd-ldap-2.6.2-4.0.2.el8_6.aarch64                 sssd-nfs-idmap-2.6.2-
4.0.2.el8_6.aarch64
  sssd-proxy-2.6.2-4.0.2.el8_6.aarch64
Installed:
  kernel-uek-5.4.17-2136.307.3.5.el8uek.aarch64   kernel-uek-devel-5.4.17-
2136.307.3.5.el8uek.aarch64

Complete!
[opc@idp ~]$
```

ファイアウォールのルールを更新します。

Let's Encryptから証明書を発行する際に、HTTP-01チャレンジを実施できるようにポート番号80での接続を許可します。またKeycloakはポート番号8443で接続を待ち受けますが、HTTPSの標準であるポート番号443で接続を受け付け、それを8443に転送するようにします。

sudo firewall-cmd --add-port=80/tcp
sudo firewall-cmd --add-port=443/tcp
sudo firewall-cmd --add-port=8443/tcp
sudo firewall-cmd --add-forward-port=port=443:proto=tcp:toport=8443
sudo firewall-cmd --runtime-to-permanent
sudo firewall-cmd --reload
sudo firewall-cmd --list-all

```
[opc@idp ~]$ sudo firewall-cmd --add-port=80/tcp
success
[opc@idp ~]$ sudo firewall-cmd --add-port=443/tcp
success
[opc@idp ~]$ sudo firewall-cmd --add-port=8443/tcp
success
[opc@idp ~]$ sudo firewall-cmd --add-forward-port=port=443:proto=tcp:toport=8443
success
[opc@idp ~]$ sudo firewall-cmd --runtime-to-permanent
success
[opc@idp ~]$ sudo firewall-cmd --reload
success
[opc@idp ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: ssh
  ports: 80/tcp 443/tcp 8443/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
        port=443:proto=tcp:toport=8443:toaddr=
  source-ports:
  icmp-blocks:
  rich rules:
[opc@idp ~]$
```

Certbotをインストールするため、EPELのリポジトリを有効にします。

/etc/yum.repos.d/oracle-epel-ol8.repoを開き、ol8_developer_EPELのenabledを0から1に変更します。

sudo vi /etc/yum.repos.d/oracle-epel-ol8.repo

```
[opc@idp ~]$ sudo vi /etc/yum.repos.d/oracle-epel-ol8.repo

[ol8_developer_EPEL]
name=Oracle Linux $releasever EPEL Packages for Development ($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL8/developer/EPEL/$basea
rch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1
```

Certbotをインストールします。

sudo dnf -y install certbot

```
[opc@idp ~]$ sudo dnf -y install certbot
Failed to set locale, defaulting to C.UTF-8
Oracle Linux 8 EPEL Packages for Development (aarch64)                  63 MB/s |
28 MB     00:00
Last metadata expiration check: 0:00:06 ago on Tue Jun  7 13:03:32 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
[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!
[opc@idp ~]$
```

Keycloakの実行に使用するJDK-17をインストールします。

sudo dnf -y install jdk-17

```
[opc@idp ~]$ sudo dnf -y install jdk-17
Failed to set locale, defaulting to C.UTF-8
Last metadata expiration check: 0:01:27 ago on Tue Jun  7 13:03:45 2022.
Dependencies resolved.
================================================================================
=====================
 Package            Architecture        Version                     Repository
               Size
================================================================================
=====================
Installing:
 jdk-17             aarch64             2000:17.0.1-ga
ol8_oci_included             153 M

Transaction Summary
================================================================================
=====================
Install  1 Package
[中略]
Installed:
  jdk-17-2000:17.0.1-ga.aarch64


Complete!
[opc@idp ~]$
```

Let's Encryptよりサーバー証明書を取得します。

sudo certbot certonly --standalone

サーバー証明書を発行するにあたって、以下を入力します。

1. 自分のメールアドレス
2. Terms of Serviceに同意するかどうかという質問への返答（これはYとしないと先に進めません）
3. ニュースやキャンペーンの通知をしてもよいかどうかの同意（これはNでもYでも、どちらでも良い）
4. 証明書を発行するホスト名（ドメイン名）

```
[opc@idp ~]$ sudo 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): 自分自身のE-mailアドレスを入力

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.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 または Yを入力。
Account registered.
Please enter the domain name(s) you would like on your certificate (comma and/or
space separated) (Enter 'c' to cancel): myidp.mydomain.dev
Requesting a certificate for myidp.mydomain.dev

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/myidp.mydomain.dev/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/myidp.mydomain.dev/privkey.pem
This certificate expires on 2022-09-05.
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
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[opc@idp ~]$
```

/etc/letsencrypt/live/myidp.mydomain.dev以下に、

fullchain.pem、**chain.pem**、**cert.pem**、**privkey.pem**

が作成されます。

Keycloakを動作させるユーザー**keycloak**を作成します。

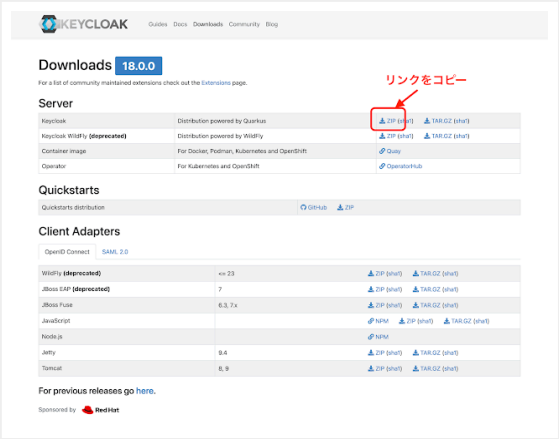
sudo useradd keycloak

```
[opc@idp ~]$ sudo useradd keycloak
[opc@idp ~]$
```

Keycloakは以下のリンクよりダウンロードします。

https://www.keycloak.org/downloads

今回はZIPファイルのリンクをコピーし、コンピュート・インスタンスから直接ダウンロードを実行します。



ユーザー**keycloak**にスイッチし、keycloak（2022年6月7日時点でバージョン18.0.0）をダウンロードします。

```
[opc@idp ~]$ sudo su - keycloak
[keycloak@idp ~]$ curl -OL
https://github.com/keycloak/keycloak/releases/download/18.0.0/keycloak-18.0.0.zip
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
100  164M  100  164M    0     0  88.4M      0  0:00:01  0:00:01 --:--:-- 81.3M
[keycloak@idp ~]$
```

ダウンロードしたファイルを展開します。バージョンに依存しない宛先として、シンボリック・リンクを作成します。

unzip keycloak-18.0.0.zip
ln -s $HOME/keycloak-18.0.0 keycloak

```
[keycloak@idp ~]$ unzip keycloak-18.0.0.zip
Archive:  keycloak-18.0.0.zip
   creating: keycloak-18.0.0/
   creating: keycloak-18.0.0/conf/
   creating: keycloak-18.0.0/themes/
   creating: keycloak-18.0.0/bin/
   creating: keycloak-18.0.0/bin/client/
[中略]
  inflating: keycloak-18.0.0/lib/lib/deployment/org.testcontainers.mariadb-
1.16.3.jar
  inflating: keycloak-18.0.0/lib/lib/deployment/io.quarkus.quarkus-devservices-
mariadb-2.7.5.Final.jar
  inflating: keycloak-18.0.0/lib/lib/deployment/io.quarkus.quarkus-resteasy-
deployment-2.7.5.Final.jar
```

```
  inflating: keycloak-18.0.0/lib/lib/deployment/org.opentest4j.opentest4j-1.2.0.jar

  inflating: keycloak-18.0.0/lib/lib/deployment/org.apache.maven.maven-core-
3.8.4.jar
[keycloak@idp ~]$ ln -s $HOME/keycloak-18.0.0 keycloak
[keycloak@idp ~]$
```

KeycloakにHTTPSで接続できるように、サーバー証明書と秘密キーのファイルを**$HOME/keycloak/conf**以下にコピーします。

一旦、keycloakを抜けてユーザー**opc**に戻ります。

スーパーユーザーに切り替えて、以下のコマンドを実行します。

sudo -s
cp /etc/letsencrypt/live/myidp.mydomain.dev/*.pem /home/keycloak/keycloak/conf/
chown keycloak /home/keycloak/keycloak/conf/*.pem
exit

```
[opc@idp ~]$ sudo -s
[root@idp opc]# cp /etc/letsencrypt/live/myidp.mydomain.dev/*.pem
/home/keycloak/keycloak/conf/
[root@idp opc]# chown keycloak /home/keycloak/keycloak/conf/*.pem
[root@idp opc]# exit
exit
[opc@idp ~]$
```

再度ユーザー**keycloak**にスイッチし、Keycloakを構成します。

sudo su - keycloak

```
[opc@idp ~]$ sudo su - keycloak
Last login: Tue Jun  7 13:17:55 GMT 2022 on pts/0
[keycloak@idp ~]$
```

Keycloakを展開したディレクトリにある**conf**ディレクトリに含まれる、**keycloak.conf**をエディタで開いて、設定を更新します。

vi keycloak/conf/keycloak.conf

```
[keycloak@idp ~]$ vi keycloak/conf/keycloak.conf
```

HTTPS通信に関わる設定を更新します。

https-certificate-file=${kc.home.dir}conf/cert.pem
https-certificate-key-file=${kc.home.dir}conf/privkey.pem
hostname=myidp.mydomain.dev

```
# HTTP

# The file path to a server certificate or certificate chain in PEM format.
https-certificate-file=${kc.home.dir}conf/cert.pem

# The file path to a private key in PEM format.
https-certificate-key-file=${kc.home.dir}conf/privkey.pem
```

```
# The proxy address forwarding mode if the server is behind a reverse proxy.
#proxy=reencrypt

# Do not attach route to cookies and rely on the session affinity capabilities from
reverse proxy
#spi-sticky-session-encoder-infinispan-should-attach-route=false

# Hostname for the Keycloak server.
hostname=myidp.mydomain.dev
```

Keycloakを起動します。初期の管理ユーザーが**admin**、それと**パスワード**を、それぞれ環境変数**KEYCLOAK_ADMIN**、**KEYCLOAK_ADMIN_PASSWORD**に設定します。

```
[keycloak@idp ~]$ export KEYCLOAK_ADMIN=admin
[keycloak@idp ~]$ export KEYCLOAK_ADMIN_PASSWORD=何某かのパスワード
```

Keycloakを開発モードで起動します。

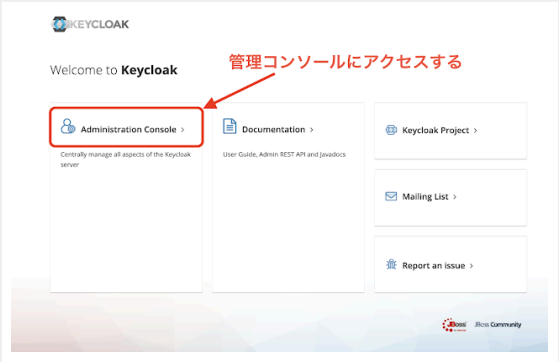
keycloak/bin/kc.sh start-dev

```
[keycloak@idp ~]$ keycloak/bin/kc.sh start-dev
Updating the configuration and installing your custom providers, if any. Please
wait.
2022-06-07 13:40:24,251 INFO  [io.quarkus.deployment.QuarkusAugmentor] (main)
Quarkus augmentation completed in 6278ms
2022-06-07 13:40:26,420 INFO
[org.keycloak.quarkus.runtime.hostname.DefaultHostnameProvider] (main) Hostname
settings: FrontEnd: myidp.mydomain.dev, Strict HTTPS: false, Path: <request>,
Strict BackChannel: false, Admin: <request>, Port: -1, Proxied: false
2022-06-07 13:40:26,959 INFO  [org.infinispan.server.core.transport.EPollAvailable]
(keycloak-cache-init) ISPN005028: Native Epoll transport not available, using NIO
instead: java.lang.UnsatisfiedLinkError: could not load a native library:
netty_transport_native_epoll_aarch_64
2022-06-07 13:40:27,077 WARN  [org.infinispan.CONFIG] (keycloak-cache-init)
ISPN000569: Unable to persist Infinispan internal caches as no global state enabled
2022-06-07 13:40:27,082 WARN  [org.infinispan.PERSISTENCE] (keycloak-cache-init)
ISPN000554: jboss-marshalling is deprecated and planned for removal
2022-06-07 13:40:27,093 INFO  [org.infinispan.CONTAINER] (keycloak-cache-init)
ISPN000556: Starting user marshaller
'org.infinispan.jboss.marshalling.core.JBossUserMarshaller'
2022-06-07 13:40:27,330 INFO  [org.infinispan.CONTAINER] (keycloak-cache-init)
ISPN000128: Infinispan version: Infinispan 'Triskaidekaphobia' 13.0.8.Final
2022-06-07 13:40:28,844 INFO
[org.keycloak.quarkus.runtime.storage.database.liquibase.QuarkusJpaUpdaterProvider]
(main) Initializing database schema. Using changelog META-INF/jpa-changelog-
master.xml
2022-06-07 13:40:31,158 INFO
[org.keycloak.connections.infinispan.DefaultInfinispanConnectionProviderFactory]
(main) Node name: node_907342, Site name: null
2022-06-07 13:40:31,233 INFO  [org.keycloak.services] (main) KC-SERVICES0050:
Initializing master realm
2022-06-07 13:40:33,269 INFO  [org.keycloak.services] (main) KC-SERVICES0009: Added
user 'admin' to realm 'master'
2022-06-07 13:40:33,464 INFO  [io.quarkus] (main) Keycloak 18.0.0 on JVM (powered
by Quarkus 2.7.5.Final) started in 9.127s. Listening on: http://0.0.0.0:8080 and
https://0.0.0.0:8443
2022-06-07 13:40:33,465 INFO  [io.quarkus] (main) Profile dev activated.
2022-06-07 13:40:33,465 INFO  [io.quarkus] (main) Installed features: [agroal, cdi,
hibernate-orm, jdbc-h2, jdbc-mariadb, jdbc-mssql, jdbc-mysql, jdbc-oracle, jdbc-
postgresql, keycloak, narayana-jta, reactive-routes, resteasy, resteasy-jackson,
smallrye-context-propagation, smallrye-health, smallrye-metrics, vault, vertx]
```

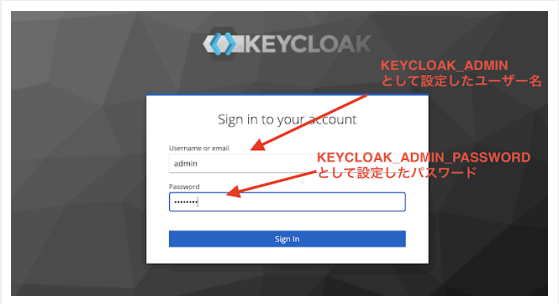
```
2022-06-07 13:40:33,469 WARN  [org.keycloak.quarkus.runtime.KeycloakMain] (main)
Running the server in development mode. DO NOT use this configuration in
production.
```

ブラウザよりKeycloakにアクセスします。

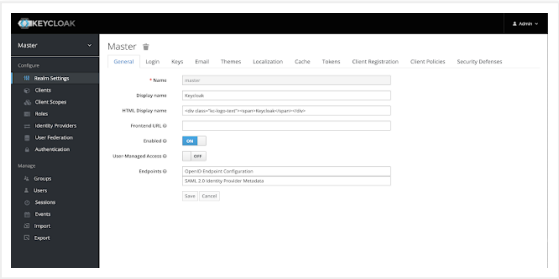
https://myidp.mydomain.dev



Keycloak起動時に環境変数**KEYCLOAK_ADMIN**として設定したユーザー名と、
KEYCLOAK_ADMIN_PASSWORDとして設定したパスワードを入力し、サインインを実行します。



Keycloakの管理画面が開きます。



とりあえず、KeycloakがAmpere A1インスタンスで動作するようになりました。

完

Yuji N. 時刻: 23:00

共有

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