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。

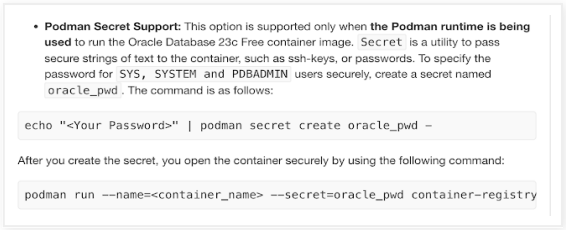
2024年3月19日火曜日

Oracle Datababase 23c Freeのコンテナ作成時に与えるパスワードについて

Oracle Container RegistryにあるOracle Database 23c Freeのコンテナ・イメージを使ってコンテナを作成する際に、与えるパスワードを秘匿する方法について調べた内容を記録します。

コンテナ・イメージのドキュメントは以下です。
https://container-registry.oracle.com/ords/ocr/ba/database/free

ドキュメントに記載があるように、Podman Secretがサポートされています。



- **Podman Secret Support:** This option is supported only when **the Podman runtime is being used** to run the Oracle Database 23c Free container image. `Secret` is a utility to pass secure strings of text to the container, such as ssh-keys, or passwords. To specify the password for `SYS`, `SYSTEM` and `PDBADMIN` users securely, create a secret named `oracle_pwd`. The command is as follows:

```
echo "<Your Password>" | podman secret create oracle_pwd -
```

After you create the secret, you open the container securely by using the following command:

```
podman run --name=<container_name> --secret=oracle_pwd container-registry
```

このシークレットの処理は/opt/oracle/checkDBStatus.shの78行から始まる以下の部分で、Podman Secretの値を環境変数**ORACLE_PWD**に設定しています。

```
# Setting up ORACLE_PWD if podman secret is passed on
if [ -e '/run/secrets/oracle_pwd' ]; then
   export ORACLE_PWD="$(cat '/run/secrets/oracle_pwd')"
fi
```

シークレット名が**oracle_pwd決め打ち**なので、それ以外の名前のシークレットを--secretで渡しても無視されます。環境変数ORACLE_PWDが-eオプションで渡されていないと、パスワードがランダムに設定されます。

RedHad社の以下のドキュメントを参照し、パスワードの秘匿方法を試してみます。

Storing sensitive data using Podman secrets: Which method should you use?
https://www.redhat.com/sysadmin/podman-kubernetes-secrets

シークレット**my-pasword**を作成します。

printf MyOraclePass1234 | podman secret create my-password -

```
[oracle@apex ~]$ printf MyOraclePass1234 | podman secret create my-password -
cefd6e98d323872508371e87f
[oracle@apex ~]$
```

RedHatのドキュメントにある手順に従って、シークレット**my-password**が環境変数**ORACLE_PWD**に渡せることを確認します。

**podman run --secret=my-password,type=env,target=ORACLE_PWD **
**registry.access.redhat.com/ubi9:latest **
printenv ORACLE_PWD

```
[oracle@apex ~]$ podman run --secret=my-password,type=env,target=ORACLE_PWD \
> registry.access.redhat.com/ubi9:latest \
> printenv ORACLE_PWD
MyOraclePass1234
[oracle@apex ~]$
```

シークレットの指定を入れ替えて、コンテナを作成します。

podman run -d --name apex-db --privileged --secret=my-password,type=env,target=ORACLE_PWD container-registry.oracle.com/database/free:latest

```
[oracle@apex ~]$ podman run -d --name apex-db --privileged --secret=my-
password,type=env,target=ORACLE_PWD container-
registry.oracle.com/database/free:latest
36a54cad61ff8e943079fce7c1a8fc92fd7120e785a0cf66265459bcf9ce9584
[oracle@apex ~]$
```

上記で作成したコンテナには環境変数**ORACLE_PWD**に値が渡っていないようで、シークレット**my-password**で設定したパスワードを使って接続することができませんでした。

コンテナ・イメージにより受け付けられる--secretオプションに違いがあるのかもしれません。

YAML形式の構成ファイルからポッドを作成する場合、データベースのコンテナ作成時に--secretオプションを与える方法を見つけることができませんでした。

RedHatのドキュメントを参照すると、podman kube playでYAML形式の構成ファイルを使う場合はKubernates secretを使うとのことなので、試してみました。

パスワードをBASE64でエンコードします。

printf MyOraclePass1234 | base64

```
[oracle@apex ~]$ printf MyOraclePass1234 | base64
TXlPcmFjbGVQYXNzMTIzNA==
[oracle@apex ~]$
```

secret.yamlを作成します。

```
apiVersion: v1
data:
  password: TXlPcmFjbGVQYXNzMTIzNA==
kind: Secret
metadata:
  creationTimestamp: null
  name: oracle_pwd
```

podman kube playコマンドを実行して、このファイルをpodman secretとして保存します。シークレットの名前は**oracle_pwd**になります。

podman kube play secret.yaml

```
[oracle@apex ~]$ podman play kube secret.yaml
Secrets:
ac8274cba0f17e9caa58f4e8c
[oracle@apex ~]$
```

シークレット**oracle_pwd**の内容を確認します。

**podman run --secret=oracle_pwd,type=env,target=ORACLE_PWD **
**registry.access.redhat.com/ubi9:latest **
printenv ORACLE_PWD

secret.yamlの内容がそのまま保存されていることが分かります。

```
[oracle@apex ~]$ podman run --secret=oracle_pwd,type=env,target=ORACLE_PWD \
> registry.access.redhat.com/ubi9:latest \
> printenv ORACLE_PWD
apiVersion: v1
data:
  password: TXlPcmFjbGVQYXNzMTIzNA==
kind: Secret
metadata:
  creationTimestamp: null
  name: oracle_pwd
```

ポッドを作成し保存されたシークレットを参照します。

```
apiVersion: v1
kind: Pod
metadata:
  name: kube-secret-print
spec:
  restartPolicy: Never
  containers:
  - name: alpine
    image: docker.io/library/alpine:latest
    env:
    - name: ORACLE_PWD
      valueFrom:
        secretKeyRef:
          name: oracle_pwd
          key: password
    command:
    - printenv
    args:
    - ORACLE_PWD
```

以下のコマンドを実行します。

podman kube play pod.yaml
podman logs kube-secret-print-alpine

シークレットが参照できていることが確認できます。

```
[oracle@apex ~]$ podman kube play pod.yaml
Pod:
fe1619c0c8a52f9f64334038fc9e58e2dde1add16e5fdc894e7f5f875a723fd7
Container:
5b0bcfa097be13c707fa55c15183c59df44889b62c8ea96f2352d56699f2b971

[oracle@apex ~]$ podman logs kube-secret-print-alpine
MyOraclePass1234
[oracle@apex ~]$
```

残念なことに**podman generate kube kube-secret-print**を実行すると、パスワードがYAMLファイルにそのまま出力されるようです。

```
[oracle@apex ~]$ podman generate kube kube-secret-print
# Save the output of this file and use kubectl create -f to import
# it into Kubernetes.
#
# Created with podman-4.6.1
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: "2024-03-19T02:44:48Z"
  labels:
    app: kube-secret-print
  name: kube-secret-print
spec:
  containers:
  - args:
    - ORACLE_PWD
    command:
    - printenv
    env:
    - name: ORACLE_PWD
      value: MyOraclePass1234
    image: docker.io/library/alpine:latest
    name: kube-secret-print-alpine
  restartPolicy: Never

[oracle@apex ~]$
```

以下のYAMLファイルよりポッドapexとOracle Database 23c Freeのコンテナを作成します。

```
apiVersion: v1
kind: Pod
metadata:
  labels:
    app: apex
  name: apex
spec:
  containers:
  - env:
    - name: ORACLE_PWD
      valueFrom:
        secretKeyRef:
          name: oracle_pwd
          key: password
    image: container-registry.oracle.com/database/free:latest
    name: db
    ports:
    - containerPort: 1521
      hostPort: 1521
    - containerPort: 8181
      hostPort: 8181
```

```
    - containerPort: 8443
      hostPort: 8443
    securityContext:
      privileged: true
```

ポッド**apex**を作成します。

podman kube play apex.yaml

```
[oracle@apex ~]$ podman kube play apex.yaml
Pod:
6d88cd9b6e23252f41460e34ea53e77ec5d4ce6ef2d06b652c37400af8d071f3
Container:
2c6a0c055f59b092495e559b17dcb88abb21a611582109928227b16a5c29d463

[oracle@apex ~]$
```

このポッドもYAMLファイルを出力すると、パスワードがそのまま出力されます。

podman generate kube apex

```
[oracle@apex ~]$ podman generate kube apex
# Save the output of this file and use kubectl create -f to import
# it into Kubernetes.
#
# Created with podman-4.6.1
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: "2024-03-19T02:51:13Z"
  labels:
    app: apex
  name: apex
spec:
  containers:
  - env:
    - name: ORACLE_PWD
      value: MyOraclePass1234
    image: container-registry.oracle.com/database/free:latest
    name: apex-db
    ports:
    - containerPort: 1521
      hostPort: 1521
    - containerPort: 8181
      hostPort: 8181
    - containerPort: 8443
      hostPort: 8443
    securityContext:
      privileged: true
  restartPolicy: Always

[oracle@apex ~]$
```

このYAMLファイルから作成したデータベースには、指定したパスワードで接続することができました。シークレットが環境変数**ORACLE_PWD**に渡されているようです。

```
[oracle@apex ~]$ podman exec -it apex-db sh
sh-4.4$ sqlplus sys/MyOraclePass1234@localhost/freepdb1 as sysdba

SQL*Plus: Release 23.0.0.0.0 - Production on Tue Mar 19 02:55:11 2024
```

```
Version 23.3.0.23.09

Copyright (c) 1982, 2023, Oracle.  All rights reserved.


Connected to:
Oracle Database 23c Free Release 23.0.0.0.0 - Develop, Learn, and Run for Free
Version 23.3.0.23.09

SQL>
```

しかしgenerate kubeでパスワードが出力されるのであれば、このような手順を踏むよりインストール終了後に以下のコマンドを実行してパスワードを変更する方が安全のように思います。

```
podman exec <oracle-db> ./setPassword.sh <your_password>
```

完

Yuji N. 時刻: 12:10

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