Installing Soffid on Kubernetes

Guide to show le installation process os Soffid IAM in Kubernetes

- Installing IAM Console
- Installing Sync server
- How to copy to Kubernetes Secrets?
- How to copy Sync Server Kube Conf to Database table?

Installing IAM Console

Guide to install IAM Console on Kubernetes.

Prerequisites

- Kubernetes
- 8GB RAM
- > 10GB disk space
- Supported database installed

Video Tutorial

Linux

https://www.youtube.com/embed/kcMO1DZeD4w?rel=0

Installation

You can use the docker image described at Installing IAM console using Docker. Here you have a sample Kubernets YAML descriptor to deploy it.

Mind that any certificate present in the folder /opt/soffid/iam-console-4/trustedcerts is considered as a trusted certificate. It is important to include the root syncserver certificate or any other certificate the console must connect with.

Another aspect to be aware of is the DNS resolution cache implemented by the java virtual machine. Because pods and service names often change its IP address, it suggested to disable the DNS cache adding the **-Dsun.net.inetaddr.ttl=-1** parameter.

```
apiVersion: v1
kind: Secret
metadata:
  name: trusted-certs
data:
  syncserver:
MIIC+TCCAeGgAwIBAgIGAWwFI+dWMA0GCSqGSIb3DQEBCwUAMDMxDzANBgNVBAMMBlJvb3RDQTEPMA0GA1UE
CwwGbWFzdGVyMQ8wDQYDVQQKDAZTb2ZmaWQwHhcNMTkwNzE3MTMwMjE0WhcNMjkwNzE4MTMwMjE0WjAz
MQ8wDQYDVQQDDAZSb290Q0ExDzANBgNVBAsMBm1hc3RlcjEPMA0GA1UECgwGU29mZmlkMIIBIjANBgkqhkiG9w
0BAQEFAAOCAQ8AMIIBCgKCAQEArkRq5/Kq1a/WlI00xzuxj0CDaH/L3G01dN5tXEFMXnm4VgDaaQXEjxGL0HEO47fl
DWGvJckLxIHSgEtRaHTquLRYLfHwHw3S0CC/DqdYcMZGG7QkCHDfdGunIoRGvWOAYOaV0pSiqBsfXhqG/7R4Ux7kx
7mWoRXHnTyWXZl6tlNl9k2fC47foI5uMsblB3bybNnzLw2JvdwC6I8bbzf1j38r98WevdzQMVYxn10CQjLz2ZN7irYpgH
zaBPoZlwKNVBhf7Tke9TDWuGO5G2UXTpys3euyTFw82TeetNTydcVK8SpdGKMlN95Cj2pgwzzz9d+qaMbN0tJu2Cu
GO+TROwIDAQABoxMwETAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQApbPFO3fMlLOdvgx+
O8w7JJyxOJNG+ogV7QH+ipxM6eyCWLI7euJbRSc7skR61Hw0H6Ka+ExFjHOqe0u/ysIg/ITlWTV6olaD8OpT3GKsZqhi
QpBO6dKqPs8JcwMt4gBbQ7YxfYefk3OER6PUG9sk8OPMmdeF+jQu1bWijUNPB0qEPio+NWXc+SF0/lj1DQF2sW9yD
b5LvsbgrkQXewvp6eUJPpwHh+pGqNKKuHkwTCfu5cUtNBMAC6CQjjCm6CUy4BYxRcF3zfzjV2nK3zTeshF7wlK95ZM
aC8IGYbYwZ86qT/x/PxX/qYOjRftSr6/Y58heYvfXLFM1pceQYVW9v
  star_soffid_com:
MIIGcDCCBVigAwIBAgIRAOFY+IkZ+FTddCqKixlQEIMwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAkdCMRswGQ
YDVQQIExJHcmVhdGVyIE1hbmNoZXN0ZXIxEDAOBgNVBAcTB1NhbGZvcmQxGDAWBgNVBAoTD1NlY3RpZ28gTGlt
aXRlZDE3MDUGA1UEAxMuU2VjdGlnbyBSU0EgRG9tYWluIFZhbGlkYXRpb24gU2VjdXJlIFNlcnZlciBDQTAeFw0xOTA2
MTgwMDAwMDBaFw0yMTA2MTcyMzU5NTlaMFkxITAfBgNVBAsTGERvbWFpbiBDb250cm9sIFZhbGlkYXRlZDEdMBs
GA1UECxMUUG9zaXRpdmVTU0wgV2lsZGNhcmQxFTATBgNVBAMMDCouc29mZmlkLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAKnDKURLcT1XfaMjmIU8QtxdhVe1XG1Oo4LrrEyUVBaAA/5RPcWrvkClf2Kq6/JTBB
xbwvJP1pHAninwTGLam2lNTL2jvlyYXC/oA0hqbRxDCBjkq7e7fj6R2rcFJcAx0jUiyzlfgZmP/QX+ju7KrJ33sR4DPAG47X
nz8XgWJMuXdoSvQ8NeaWNAUjK7Pt3vHB/QD40MAAisXuOq1w11R3MzEJv0nHgNPvxqGvVdHTDX5RwHoVEMEHF7l
QY0Mh2oIejQgN+VPOJNJh6vd7HiVUlVLXop8qhjJQgy2DQS2VGTUBObTFTgD81UPKzZgRzlziU3RWimZMVgHjzDn9M
mzkcCAwEAAaOCAvowggL2MB8GA1UdIwQYMBaAFI2MXsRUrYrhd+mb+ZsF4bgBjWHhMB0GA1UdDgQWBBTPiYcz
qwQVFTogNEQydqg0WGGnwzAOBgNVHQ8BAf8EBAMCBaAwDAYDVR0TAQH/BAIwADAdBgNVHSUEFjAUBggrBgEF
BQcDAQYIKwYBBQUHAwIwSQYDVR0gBEIwQDA0BgsrBgEEAbIxAQICBzAlMCMGCCsGAQUFBwIBFhdodHRwczovL3N
lY3RpZ28uY29tL0NQUzAIBgZngQwBAgEwgYQGCCsGAQUFBwEBBHgwdjBPBggrBgEFBQcwAoZDaHR0cDovL2NydC
5zZWN0aWdvLmNvbS9TZWN0aWdvUlNBRG9tYWluVmFsaWRhdGlvblNlY3VyZVNlcnZlckNBLmNydDAjBggrBgEFBQ
cwAYYXaHR0cDovL29jc3Auc2VjdGlnby5jb20wIwYDVR0RBBwwGoIMKi5zb2ZmaWQuY29tggpzb2ZmaWQuY29tMII
BfgYKKwYBBAHWeQIEAgSCAW4EggFqAWgAdgC72d+8H4pxtZOUI5eqkntHOFeVCqtS6BqQlmQ2jh7RhQAAAWtpdk
7pAAAEAwBHMEUCIQCyc83CoGLtckCrDEtAph3U/+XMqwkEPwqEgi9bu7xNBgIgKachYG2OED40K9pd9byRWUjy+B
eV+5tVeN+I8JD48XoAdQBElGUusO7Or8RAB9io/ijA2uaCvtjLMbU/0zOWtbaBqAAAAWtpdk7+AAAEAwBGMEQCIFqju
u2Q/TTq48nkobC87nRfgE9FQmlUp4PI98U90ygJAiBoFsiy0kz2ZDNz+BeAVjqAj7UsnrNIv8vwG3V7rh6kxgB3AG9Tdq
wx8DEZ2JkApFEV/3cVHBHZAsEAKQaNsgiaN9kTAAABa2l2Tv4AAAQDAEgwRgIhAMLmnVu4rduXSiaC5pfbk6uQsceV
6zEx1fgNjQXNupDwAiEAtCh5VG2IC6iWy0chA/PfC5ejmlgBAmHbYLxsr9uiOWwwDQYJKoZIhvcNAQELBQADggEBAB
```

```
qZ8Stnzkk/abCQTMjOhNsSswSZZ74mszAGrd+emh7/VhLeJ29AaoMiCF5j0uphx/t9id5UmKbqwuapo9E1NuAVQqDO
V1N0wV4Awa2nEivbDcuDCTMX6VtOK3DnCnE9yLMdD6GF9xcwzsgz5wKXu2Dxwt4vw05KIM+4Myy91sEpifa62+q
dzR/Vfbv6SqeL1IzTDyHMzEtBu/4jL189VeSkTVvdKGT1g6eAMHTX562z7jJgTH23c2zolCEj9YPd+KUbt6/OO+Pljsj0Me
TzO1QImj2syqCE/O4tYyHOHOdHJcrVSP951nCu0bkH6MBUhFvgk8a6rjI8tcnZCpsdcNU=
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: soffid-console
  labels:
    app: soffid
    type: console
spec:
  replicas: 1
  selector:
    matchLabels:
      app: soffid
      type: console
  template:
    metadata:
      labels:
        app: soffid
        type: console
    spec:
      containers:
      - name: soffid-console
        image: soffid/iam-console:4.0.0-beta-8
        imagePullPolicy: Always
        resources:
          limits:
            memory: 4Gi
          requests:
            memory: 2Gi
        volumeMounts:
        - name: trusted-certs-volume
          mountPath: /opt/soffid/iam-console-4/trustedcerts
        ports:
        - containerPort: 8080
        env:
          - name: DB_USER
```

```
            value: soffid
          - name: DB_PASSWORD
            value: 5uper5ecret
          - name: JAVA_OPT
            value: "-Xmx4048m -Dsun.net.inetaddr.ttl=1"
          - name: DB_URL
            value: jdbc:mariadb://mariadb-service:3306/soffid
      imagePullSecrets:
      - name: regcred
      volumes:
      - name: trusted-certs-volume
        secret:
          secretName: trusted-certs
---
apiVersion: v1
kind: Service
metadata:
  name: iam-console-service
spec:
  selector:
      app: soffid
      type: console
  type: loadBalancer
  ports:
  - name: web
    protocol: TCP
    port: 8080
    targetPort: 8080
```

Linux commands

Apply the YAML file with the defining Kubernetes resources

```
kubectl apply -f syncserver.yaml
```

Check deployments

```
kubectl get deployments
```

Check pods: you can check pods and their status

```
kubectl get pods
```

View the IAM console log

```
kubectl logs <your-pod-iamconsole-name>
```

> When the console is created, the password for the user *admin* will be *changeit* and it will be valid for 24 hours.

> Now you can connect to Soffid Console http://<Node-Ip>:<publish-port>/soffid The first thing you must do is to change the admin user password.

> Next Step: Installing Sync server

Installing Sync server

Guide to install Sync server on Kubernetes.

Prerequisites

Soffid IAM sync server requires the following requirements:

- Supported database installed
- Soffid Console Installed

Video Tutorial

Linux

https://www.youtube.com/embed/XZFMLQ0OkAA?rel=0

Installation

You can use the docker image described at Installing Sync server using Docker. Here you have a sample Kubernets YAML descriptor to deploy it.

```
# Secrets to store syncserver configuration
apiVersion: v1
kind: Secret
metadata:
  name: syncserver
type: Opaque
data:
```

```
  config: c3Nva20=
---
# Service account for sync server
apiVersion: v1
kind: ServiceAccount
metadata:
  name: syncserver
---
# Role to access the sync server
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: syncserver
rules:
  - verbs:
      - get
      - update
    apiGroups:
      - ''
    resources:
      - deployments
      - pods/attach
      - secrets
      - secrets/syncserver
---
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: syncserver
  namespace: default
subjects:
  - kind: ServiceAccount
    name: syncserver
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: syncserver
---
apiVersion: apps/v1
kind: Deployment
```

```
metadata:
  name: syncserver01
  labels:
    app: soffid
    type: syncserver
spec:
  replicas: 1
  selector:
    matchLabels:
      app: soffid
      type: syncserver
  template:
    metadata:
      labels:
        app: soffid
        type: syncserver
    spec:
      serviceAccountName: syncserver
      containers:
        - name: syncserver
          image: soffid/iam-sync:4.0.0-beta-2
          ports:
            - containerPort: 760
              name: syncserver-port
          readinessProbe:
            initialDelaySeconds: 5
            failureThreshold: 1
            httpGet:
              path: /diag
              scheme: HTTPS
              port: 760
          livenessProbe:
            initialDelaySeconds: 5
            timeoutSeconds: 3
            failureThreshold: 3
            httpGet:
              path: /diag
              scheme: HTTPS
              port: 760
          env:
```

```
            - name: DB_USER
              value: soffid
            - name: DB_PASSWORD
              value: 5uper5ecret
            - name: SOFFID_HOSTNAME
              value: syncserver01.cloud.soffid.com
            - name: SOFFID_MAIN
              value: "yes"
            - name: KUBERNETES_CONFIGURATION_SECRET
              value: "syncserver"
            - name: DB_URL
              value: jdbc:mariadb://mariadb-service/soffid
---
apiVersion: v1
kind: Service
metadata:
  name: syncserver
spec:
  externalTrafficPolicy: Local
  type: LoadBalancer
  selector:
    app: soffid
    type: syncserver
  ports:
  - name: syncserver
    protocol: TCP
    port: 760
    targetPort: 760
```

If the syncserver pod is not available in 5 seconds, probably it will restart constantly and it will not be available. To solve this, change the sample Kubernetes YAML descriptor showed above like this:

```
livenessProbe:
        failureThreshold: 3
        httpGet:
          path: /diag
          port: 761
          scheme: HTTP
        initialDelaySeconds: 360
        periodSeconds: 10
```

```
    successThreshold: 1
    timeoutSeconds: 3
  name: syncserver
  ports:
    - containerPort: 760
      name: syncserver-port
      protocol: TCP
  readinessProbe:
    failureThreshold: 1
    httpGet:
      path: /diag
      port: 761
      scheme: HTTP
    initialDelaySeconds: 300
    periodSeconds: 10
    successThreshold: 1
    timeoutSeconds: 1
```

Linux commands

Apply the YAML file with the defining Kubernetes resources

```
kubectl apply -f syncserver.yaml
```

Check deployments

```
kubectl get deployments
```

Chek pods: you can check pods and their status

```
kubectl get pods
```

View Sync server log

```
kubectl logs <your-pod-syncserver-name>
```

> Now you can connect to the IAM console http://<Node-Ip>:<publish-port>/soffid and chek if Console and Syncserver are connected.

How to copy to Kubernetes Secrets?

When making any manual changes to the Sync server configuration files, it will be necessary to copy these changes to the Kubernetes secrets.

Command example:

```
java -cp "/opt/soffid/iam-sync/bin/bootstrap.jar" com.soffid.iam.sync.bootstrap.KubernetesSaver
```

> Since Soffid version 3.x, the certificates are automatically updated when the certificate end date is close and no manual actions are required.

How to copy Sync Server Kube Conf to Database table?

When you install soffid Sync server in kubernetes, a properties file is generated. If this file is not saved in a permanent storage, it could be lost during the Syns Server upgrade process.

Here you are the steps to copy your Kube config to a data base table

1.-

```
unset KUBERNETES_CONFIGURATION_SECRET
```

2.-

```
export DB_CONFIGURATION_TABLE=syncserver
```

3.-

```
java -cp "/opt/soffid/iam-sync/bin/bootstrap.jar:/opt/soffid/iam-sync/lib/mariadb-java-client-1.8.0.jar:/opt/soffid/iam-sync/lib/ojdbc10-19.18.0.0.jar:/opt/soffid/iam-sync/lib/postgresql-42.2.5.jre7.jar:/opt/soffid/iam-sync/lib/sqljdbc4-3.0.jar" com.soffid.iam.sync.bootstrap.KubernetesSaver
```