



KUBERNETES - SFTP SERVICE

Cognitive Assistant for Networks (CAN) Release 5.5



JULY 16, 2021

AVANSEUS TECHNOLOGY PVT. LTD.

Revision History

Version	Date	Change description	Created by	Updated by	Reviewed by
V 1.0	July, 2021	Initial Release	Sunil	Sandeep Singh	Chiranjib

Table of Contents

1. Aim	3
2. Prerequisites	3
3. SFTP on kubernetes	3
3.1. Storage Space.....	3
3.2. Password Encryption	4
3.3. YAML Configuration	4
4. Test SFTP	8

1. Aim

The aim of this document is to configure, setup and run SFTP server on any Kubernetes based platform.

Many customers ask for SFTP service. SFTP service is used to transfer the data files like Alarms, Tickets, Performance counters etc. on a daily basis to feed the CAN tool to predict the faults. Since, CAN Release 5.5 deployment is entirely moved to Kubernetes platform, we have two options to expose SFTP service to customers.

- a. Traditional SFTP service on a VM (Virtual Machine)
- b. SFTP service on Kubernetes

This document completely focuses on Option (b). SFTP on Kubernetes helps both cloud based and on-premises based deployment to avoid procuring a new VM just for SFTP purpose.

2. Prerequisites

Before moving forward with the installation of SFTP service on Kubernetes platform, there should be load balancer which must be procured separately. This load balancer IP or host must be used to expose the SFTP Kubernetes service with a service type as "LoadBalancer".

In case of cloud based deployment, there are load balancers which are available for a small cost on Cloud service providers like AWS, Azure, and GCP etc.

In case of on-premise deployment, the vendor's IT team need to internally setup a load balancer and provide us the IP or Host name of that load balancer.

3. SFTP on kubernetes

3.1.Storage Space

Before setting up SFTP, we would need a storage space for files being uploaded. For this, we need a PersistenceVolumeClaim (PVC) of whatever size desired for that project. A sample of PVC configuration which creates a PVC named "sftp-storage" is mentioned below:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: sftp-storage
  namespace: <namespace>
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: <pvc_disk_size>
  storageClassName: <storage_class>
```

Fill up the placeholders in <> with the appropriate values:

- a. <namespace> - Replace this with the namespace or project name
- b. <pvc_disk_size> - PVC disk size

- c. <storage_class> - Storage class name available in the deployment

3.2. Password Encryption

SFTP needs a user and password for file upload. This needs to be created beforehand. The command to generate encrypted password which the SFTP server can use and authenticate the user who logs in is given below. Please make sure that docker command line client is available on that machine.

```
echo -n "<string_escaped_password>" | docker run -i --rm atmoz/makepasswd --crypt --clearfrom=-
```

Example: (If password is Avanseus\$0)

```
echo -n "Avanseus$0" | docker run -i --rm atmoz/makepasswd --crypt --clearfrom=-
```

The above mentioned command would print out the encrypted password.

3.3. YAML Configuration

A YAML configuration creates three things:

- a. Secrets with SSH keys & initial user information for login.
- b. Deployment configuration which runs SFTP process as a pod.
- c. Service configuration which exposes SFTP as a service over a Load balancer.

```
kind: Secret
apiVersion: v1
metadata:
  name: sftp-secrets
stringData:
  ssh_host_ed25519_key: "-----BEGIN OPENSSH PRIVATE KEY-----\n
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACDhdLIBSuLFMXG8oXTkyk0T983KHN1pXXOxEERHFZlg0AAAAALjSy/hs0sv4
bAAAAAtzc2gtZWQyNTUxOQAAACDhdLIBSuLFMXG8oXTkyk0T983KHN1pXXOxEERHFZlg0A
AAAEBCvV8F+X72Y24Bg3fhtf/HnklQxGAIB4uocfzU9xJEIOF0sgFK4sUxcbyhdOTKTRP3
zcoc3Wldc7EQSScVkiDQAAAAMGF2YW5zZXVzdGVjaG5vbG9naWVzQEF2YW5zZXVzcy1NYW
NCb29rLVByby5sb2NhbaECAwQF\n-----END OPENSSH PRIVATE KEY-----\n"
  ssh_host_rsa_key: "-----BEGIN OPENSSH PRIVATE KEY-----\n
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAACFwAAAAAdzc2gtcn
NhAAAAAwEAAQAAAEAE4yir0gpPpcseFmHZMYEPJclxhdx/X0m2pYTImIGgc1MKYJLQD4AT
C4xkblj/l0qI4AXeHs225/3P2YvaYHuM7wdabzG/yEwSouehkTA8zKG8MuFUvZOZhKiVwb
iyZP+YwwPf/1kdfvPtO2XgPaY9/drjFtM2inz9JxZ3jYZoaOqL2jOgRFtdlOrkuhIR8zZS
Kw6tqaGBN+vWPCQnkpmNUyJiQBhKUHvQ1v4UMSLvrndkQbErfsjaQVYAqZYI2+82XtZ+eO
Qb1Dumkvblbmm01k51PHCC8wjDXQppONTzgZZ474XhtnpyoSyk1BI6iS1sqvPLQbb0t5DU
9Klb7X8QbYNogwfU6sXZafGDG5EV3pwLK/y8VWUo5E1vle6/WG3bNR2k5UGCjLasmhoSC1
1I2mHtjto5iOevlpCaD3pij1CrbJHCi/MRpUIf0Y+YWERZqUTaPNd9LHxyVukMvxC3+ELI
r9godwpl3TbpoG1lIkpes+IngMWMK9raxcLEXE6cn7x7L12ndobT31A8Y5XGOu/zSd/MC
z2fjbcMnBOGcsP7a3OYh1q7Ye7PnGpCrt+ngJlZDABTSZR05tqV8oD/FIPvBbafJoMkb7R
0cE9dNarOF1FIURNqliggNLY1vNDbS+CqvyaRKV4dF2moBB1kJYttlyufQYmvxW9r8vg6U
sAAAdojkdI/45HSP8AAAAHc3NoLXJzYQAAAEAE4yir0gpPpcseFmHZMYEPJclxhdx/X0m2
```

```
pYTImlGgc1MKYJLQD4ATC4xkblj/l0ql4AXeHs225/3P2YvaYHuM7wdabzG/yEwSouehkT
A8zKG8MuFUVZOZHkiVwbiyZP+YwwPf/1kdfvPtO2XgPaY9/drjFtM2inz9JxZ3jYZoaOqL
2jOgRFtdlOrkuhIR8zZSKw6tqaGBN+vWPCQnkpnmNUyJiQBhKUHvQ1v4UMSLvrndkQbErfs
jaQVYAqZYI2+82XtZ+eOQb1Dumkvblbmm01k51PHCC8wjDXQppONTzgZZ474XhtnpyoSyk
1Bl6iS1sqvPLQbb0t5DU9Klb7X8QbYNogwfu6sXZafGDG5EV3pwLK/y8VWUo5E1vle6/WG
3bNR2k5UGCjLasmhoSC11I2mHtjto5iOevlpCaD3pij1CrbJHCi/MRpUlf0Y+YWERZqUTa
PNd9LHxyVukMvxC3+ELlr9godwpl3TbpoG1llKpes+llngMWMK9raxcLEXE6cn7x7L12nd
obT31A8Y5XGOu/zSd/MCz2fjbcMnBOGcsP7a3OYh1q7Ye7PnGpCrt+ngJlZDABTSZR05tq
V8oD/FIPvBbafJoMkb7R0cE9dNarOF1FIURNqliggNLY1vNDbS+CqvyaRKV4dF2moBB1kJ
YttlyufQYmvxW9r8vg6UsAAAADAQABAAACAA+5zBNRZWwr4JxaD8gukBbkmDhVKHg3SS6y
P5TXPH1fXVOMNI0sV6UwBe/BmDgoD8u6fEMTqLrsxkvgM7EEPKB7mNYj0owSQCQI9xVvCn
Z8J+Q51zz8j98wMJXlrGvziebOSN6Lk9ArINxA1EJQVPBTC++Tla4GsxxWoVYp3OaOfjoP
4uN4k8TwcF8zqxw0UUHr1TfuF10AtacaNacffDoqljUfuV1TBQUtN8ajDYa9ezJVCpbPXt
SxGICIA13+dHwiS0UhPY/2xTRdY0jJhpxjeBhEDby3eZbiVqB5lZX+Dcc/NH4GghMIXSzV
Sjoe6+v1zrdw7AYdP7DkXJnXdxKMZXDFq5xfwwCod0121FhjN2JsuKtAaJ/on1ZY26Brir
JXVGYHb/J7srjTnvU6FWvyWZ2GRwLGVWS1qCan/mFEijVY403eK3POLRINT33JMHEoED+Z
137Zg7myy+gRVegdarUlKwIKNnOj/TfOYDMP4MBmp+c9HfAdE6OkzvKZFzo7zJ8oRsySVn
IDfXyJbX5ZiscAlqv1aEBCBKw14DE2J0kWvRpeFtBTJuG2fbkhiXpDmHGmeIZ2OsqmwCCI
NzjaHNRws5Dwdby+hVOqEdwZXclJC6tWkzYPUTdeLpQ1DRtFChQcbw8ZtnmOmD7Qo/5Y3
xvXBoyLKNJWV2J0MRAAABAQCiqExXF/j2PI3qmSp4RAuY1LuQ2XcX68i6/y1eVvEUNCWG
+ePmh2nmL88kxNSqB8u2zdSNUkdFNW2zphBNlat9XAQHHevGHnZ3tD2UxjFJM6PWC71q
en3KwGLsquj5Tp/EvDrvvQCHFrSb1dWx/45X8FVNUZayewVFaw6jnT8agWhtlQf0luq21T
gf5KWc8vLSVZLQ1JQ6E5QV4PN4Kwf9OSW1WRYsHnjJl6KOWNO/ayBBX0goDWMh9FNKAb+T
lz1uYYRo0XlZjXYf3Ti3iYD9aC57YU9zYWxtIDNotad+7GDNDjkO8tp6TeQ09+WscFzMBp
R766zFHZdM9JHGnpAAABAQD21rmkb6Xx8m9I2icnK5T0wJKx5570aAH7gBFCsTw9lc2D9n
IE3byciRLxH/OFZ13WiR+anoPuxpIVUg1aNfYtJMHuo1wxexJoSls507uADkfrAlBw7CBCr
qKH4pMM4UXhFbvSZr/TB24LRExkD2kGODQ43QA0JCz8RU9LUTTOLNSXLq0BvtBFK9fhe8f
ZAcYKYW9tkPlOj6HqrYICY1H/dK9+XvZAX0VoSPCrq3MUzW2iOy4a0Na+Pa0YqGyEyh6
tuaSn/8X+3bAbm5Sxa3zVALPuAoK80dDYdOW/OnTtBYqjl3Z3DqGXuS5sTa0V4Go0JY6iy
h9V4juv6yVCrazAAABAQDrlvZouoZCeVJfirQd+ltlZcJrjVYs0yXYxo3BVCyZRXe8gqTm
bYVb6y+uknYghQEzfrXUvBTdXYhYBgelrHFAOC+RplaMxBjq+/qseckD4nbL95pQj3n8/h
0R8eTd4AOOCNcaNuUMPH9Uzj78TiKjIO/JWT7vB6h9b6lqjpaEcY+P9IONIDuU5naM/Gy+
7GeW+vaexZshLk7M8KaVCKUaYdAEc0akM0EummTB6BxFPVhC+q0wSfRw9/6ZuOGYsCRPrV
PSbt9116AH1d07CQFU38b4MtjoS7rmYQA2Y4zFNLQOTusO0JK9Mr+XE/tocZxGQ3R9jg4L
RfQ0JqkhBA8JAAAAMGF2YW5zZXVzdGVjaG5vbG9naWVzQEF2YW5zZXVzcy1NYWNkb29rLV
Byby5sb2NhbaECn-----END OPENSSH PRIVATE KEY-----\n"
```

`users.conf`: "testuser:PXG4dAmHQ0FRM:e:1001:100:alarms\n"

`kind`: Deployment

`apiVersion`: apps/v1

`metadata`:

`name`: sftp

```

labels:
  app: sftp
spec:
  replicas: 1
  selector:
    matchLabels:
      app: sftp
  template:
    metadata:
      labels:
        app: sftp
    spec:
      serviceAccountName: <service_account_name>
      volumes:
        - name: sftp-container-key
          secret:
            secretName: sftp-secrets
            defaultMode: 0400
        - name: sftp-host-key
          secret:
            secretName: sftp-secrets
            defaultMode: 0400
        - name: sftp-user-conf
          secret:
            secretName: sftp-secrets
        - name: sftp-store
          persistentVolumeClaim:
            claimName: sftp-storage
    containers:
      - name: sftp
        ports:
          - containerPort: 22
            protocol: TCP
        volumeMounts:
          - name: sftp-container-key
            readOnly: true
            mountPath: /etc/ssh/ssh_host_ed25519_key
            subPath: ssh_host_ed25519_key
          - name: sftp-host-key
            readOnly: true
            mountPath: /etc/ssh/ssh_host_rsa_key
            subPath: ssh_host_rsa_key
          - name: sftp-store
            mountPath: /home/testuser/

```

```

    subPath: testuser
  - name: sftp-user-conf
    mountPath: /etc/sftp/users.conf
    subPath: users.conf
  image: 'atmoz/sftp:latest'

```

```

kind: Service
apiVersion: v1
metadata:
  name: sftp
  labels:
    app: sftp
spec:
  type: "LoadBalancer"
  loadBalancerIP: <Loadbalancer_IP>
  ports:
  - name: "ssh"
    port: 22
    targetPort: 22
  selector:
    app: sftp

```

Fill up the information in <> with the appropriate values:

- d. <Loadbalancer_IP> - IP or hostname of the load balancer
- e. <service_account_name> - Service account name where permission is available to run your pods.

The above mentioned YAML configuration when run in Kubernetes would create:

- a. Secrets

This YAML content mentioned above has 3 secrets. The first two secrets are related to SSH RSA keys to be stored in the Pod. Even if the Pod restarts, the users who all had logged in previously, will not have the SSH key changed or would not get a warning of MITM attacks. Last secret by name "users.conf" content must be list of users line by line with their necessary information. The format of the content is as follows:

```
<username>:<encrypted_password>:e:<uid>:<gid>:<initial_directory>\n
```

Example:

```
testuser1:xyxyxyxyxy:e:1001:100:alarms\n
```

```
testuser2:mnsosbsuss:e:1001:100:tickets\n
```

- b. SFTP Deployment

This part of the YAML configuration creates the SFTP pod and mounts all the secrets and PVC to load data.

- c. SFTP service using Load balancer

As mentioned in the pre-requisites section, once Load balancer IP or Host information is received, this can be used in the SFTP service configuration to expose the SFTP service outside the Kubernetes.

In the YAML configuration, <Loadbalancer_IP> must be replaced with appropriate Load balancer IP.

4. Test SFTP

The SFTP can be tested by using the username & password configured in “users.conf” and also the Loadbalancer IP configured in Service YAML.

Example: `sftp testuser@10.2.1.187`