Part XVIII: Connecting to Informix

Tables of Contents

Connecting to Informix

You can connect clients and applications to the Informix server in Red Hat OpenShift.

- Configuring TLS connections with Informix
  Use transport layer security (TLS) to create secure connections from Informix clients to the integrated Informix database server deployed on Red Hat OpenShift.
- Retrieving the Informix port number
  The Informix service exposes the following network communication ports to allow connections from outside of the Red Hat® OpenShift® cluster.
- Configuring the Informix NodePort with an Ingress controller
  If you use an external infrastructure node to route external Informix traffic into the Red Hat® OpenShift® cluster, the cluster might be in a private zone and you need to configure an external-facing Ingress controller to route the traffic to the OpenShift nodes.

Configuring TLS connections with Informix

Use transport layer security (TLS) to create secure connections from Informix clients to the integrated Informix database server deployed on Red Hat OpenShift.

An Informix deployment on Red Hat OpenShift has TLS connections enabled by default. This task outlines how to extract the TLS certificate from the Informix pod.

1. Use one of the following commands to find the namespace for your database deployment.

   ```
   kubectl get ns
   or
   oc get projects
   ```

2. Use the Kubernetes `app.kubernetes.io/name` label selector to find the Informix pod name:

   ```
   oc -n namespace get pods --selector app.kubernetes.io/name=ibm-informix-prod
   ```

3. Run the cp command in the Informix pod with the label to copy the Informix certificate to your local directory:

   ```
    oc -n namespace cp <Informix engine POD name>:/opt/ibm/data/ssl/informix.cert informix.cert
   ```

   Example:

   ```
   [root@js3-inf tmp]# oc -n informix-dev cp server1-ibm-informix-prod-eng-6f9d7965f5-k6qt9:/opt/ibm/data/ssl/informix.cert
   informix.cert
   [root@js3-inf tmp]# ls -la informix.cert
   -rw-r--r-- 1 root root 721 May 13 08:13 informix.cert
   [root@js3-inf tmp]#
   ```

4. Follow the steps as described in Configuring a client for SSL connections.
   Note: If you need to access the keystore and self-signed certificates used for the Informix server, you can find them in the /opt/ibm/data/ssl directory in the Informix pod:

   ```
    $ cd /opt/ibm/data/ssl
   $ ls -l
   rw------. 1 informix informix 87 Dec 10 19:17 client.gpg
   rw-rr-. 1 informix informix 786 Dec 10 19:17 client.jks
   rw------. 1 informix informix 902 Dec 10 19:17 client.p12
   rw------. 1 informix informix 193 Dec 10 19:17 client.sth
   rw------. 1 informix informix 87 Dec 10 19:17 https-keystore.gpg
   rw------. 1 informix informix 2664 Dec 10 19:17 https-keystore.jks
   rw-rr-. 1 informix informix 725 Dec 10 19:17 informix.cert
   rw------. 1 informix informix 87 Dec 10 19:17 informix.gpg
   rw------. 1 informix informix 1441 Dec 10 19:17 informix.p12
   rw------. 1 informix informix 193 Dec 10 19:17 informix.sth
   rw-rr-. 1 informix informix 0 Dec 10 19:17 wl_credentials_status_file
   ```


Retrieving the Informix port number

The Informix service exposes the following network communication ports to allow connections from outside of the Red Hat® OpenShift® cluster.

The following table lists the ports that are exposed by Informix and their usage.

Table 1. Ports exposed by the Informix operand

Port usage	External port	Internal port	C
External client applications to connect to Informix via a DRDA client.	To get the external port run the following command:The external port is the value of the **Port number** field.Optionally, you can run the following command: `oc get svc -n projectservice_name-drda -o jsonpath='{.spec.ports[?(@.name=="http-drda")].nodePort}'` project is the OpenShift project where Informix is deployed. *service_name* is the unique identifier that is assigned to each Informix deployment. The service name always starts with "informix", for example *server1-ibm-informix-prod*.	9089	T

Port usage	External port	Internal port	C
External client applications to connect to Informix via a MONGO client.	To get the external port, run the following command: `oc get svc -n projectservice_name-mongo -o jsonpath='{.spec.ports[?(@.name=="http-mongo")].nodePort}'` project is the OpenShift project where Informix is deployed. *service_name* is the unique identifier that is assigned to each Informix deployment. The service name always starts with "informix", for example *server1-ibm-informix-prod*.	27017	T
External client applications to connect to Informix via a REST client.	To get the external port, run the following command: `oc get svc -n projectservice_name-rest -o jsonpath='{.spec.ports[?(@.name=="http-rest")].nodePort}'` project is the OpenShift project where Informix is deployed. *service_name* is the unique identifier that is assigned to each Informix deployment. The service name always starts with "informix", for example *server1-ibm-informix-prod*.	27018	H
External client applications to connect to Informix via a SQLI client.	To get the external port, run the following command: `oc get svc -n projectservice_name-sqli -o jsonpath='{.spec.ports[?(@.name=="http-sqli")].nodePort}'` project is the OpenShift project where Informix is deployed. service_name is the unique identifier that is assigned to each Informix deployment. The service name always starts with "informix", for example `informix-1597310372757`.	9088	T
External client applications to connect to Informix via a MQTT client.	To get the external port, run the following command: `oc get svc -n projectservice_name-mqtt -o jsonpath='{.spec.ports[?(@.name=="http-mqtt")].nodePort}'` project is the OpenShift project where Informix is deployed. *service_name* is the unique identifier that is assigned to each Informix deployment. The service name always starts with "informix", for example *server1-ibm-informix-prod*.	27833	T

Configuring the Informix NodePort with an Ingress controller

If you use an external infrastructure node to route external Informix traffic into the Red Hat® OpenShift® cluster, the cluster might be in a private zone and you need to configure an external-facing Ingress controller to route the traffic to the OpenShift nodes.

Because Informix is externally exposed through a NodePort, the Ingress controller also needs to expose the NodePort in order to allow traffic into the cluster.

The configuration below is only applicable with an HAProxy Ingress controller. For more detail about configuring networking, see Understanding networking in the OpenShift documentation.

1. On the infrastructure node, open the HAProxy configuration file located at /etc/haproxy/haproxy.cfg.
2. Modify the haproxy.cfg file to include the OpenShift NodePort you want to expose:

```
frontend informix
        bind *:informix NodePort
        default_backend informix_be
        mode tcp
        option tcplog
backend informix_be
        balance source
        mode tcp
        server master0 Master0-privateIP:Informix NodePort check
        server master1 Master1-privateIP:Informix NodePort check
        server master2 Master3-privateIP:Informix NodePort check
```

3. Reload HAProxy:

```
systemctl reload haproxy
```