IBM InfoSphere Information Server

DataStage 11.7.1.1 MicroServices Install

DEV Build Book

Abstract This document provides a step-by-step guidance for Installing MicroServices Tier for IIS DataStage Version 11.7.1.1 on Redhat Linux

Creation Date	24-Mar-21
Owner and Technical Advisor	Tariq Mughal System Engineer WSIB – Information Technology Cluster
Author	Tariq Mughal
Participants	Rajasekhar Sajja, Karen Boshyan, Oleg Verbinsky
Source	All snapshots and commands provided in this document were taken from the Installation done during Feb. 5th and Feb. 12th, 2021 (remotely via terminal server) on WSIB DEV Linux Server DLD8AP74.

Revision History			
Version	**Date**	**Author**	**Summary of changes**
0.1	24-Mar-21	Tariq Mughal	Initial Version

Table of Contents

Pre –Requisites

Before starting installation, please make sure that below pre-requisites are completed on the MicroServices Tier server:

1. The server must have a minimum 16 CPUs and 64 GB memory available before commencing the install
2. The following patches have been applied on the server:
    a. bash-completion.noarch
    b. conntrack-tools.x86_64
    c. container-selinux.noarch
    d. libseccomp.x86_64
    e. socat.x86_64
3. The following software has been installed on the server:
    a. Ansible Version: 2.9.5
    b. Corresponding python version
    c. wget
4. The following have been disabled on the server:
    a. SE Status
    b. SWAP
5. Ensure a softlink has been created for dockers from default file system to MicroServices directories
6. Ensure all required binaries have been copied into central library under /temp on the MicroServices Tier (see Appendix 1 for list of binaries)
7. Ensure DB2 client has been installed, port# 25771 to Xmeta DB has been opened and Xmeta DB catalogued under MicroServices Tier (DLD8AP74), see appendix
8. Extend server timeout on MicroServices (DLD8AP74) Tier to ensure connection doesn't timeout during upgrade:
    a. Navigate to directory /etc/ssh logged in as root
    b. Backup file sshd_config under that directory as sshd_config. [backup_date]
    c. Change value of ClientAliveInterval in original file from default 300 to 2300

Note: Databases in development are on the same server as the Services Tier (DLNXAP71), but in all other higher environments databases are installed on separate Linux servers.

It is recommended the install should be done using root ID on the server. On completion of install, the ownership of the subject directories must be changed to [d]wasadm. The prefix [d] varies on each environment.

Run Pre-Requisites for MicroServices Tier Install (DLD8AP74)

Navigate to central library /temp/DS_v11.7.1_code and then sub-directory prereq

1. Unpack archive verify_prereqs_microservicestier.tar with following command

   tar xvf verify_prereqs_microservicestier.tar

   [root@dld8ap74 prereq]# tar xvf verify_prereqs_microservicestier.tar

   UG_WKC_PreReqChk_Package/

   UG_WKC_PreReqChk_Package/pythondir/

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/setup.py

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/ipaddr_test.py

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/README

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/ipaddr.py

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/PKG-INFO

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0/COPYING

   UG_WKC_PreReqChk_Package/pythondir/collisionchk.py

   UG_WKC_PreReqChk_Package/pythondir/get-pip.py

   UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0.tar.gz

   UG_WKC_PreReqChk_Package/pythondir/privatechk.py

   UG_WKC_PreReqChk_Package/pythondir/pip-19.1.1-py2.py3-none-any.whl

   UG_WKC_PreReqChk_Package/pythondir/setuptools-41.0.1-py2.py3-none-any.whl

   UG_WKC_PreReqChk_Package/locationonNode.sh

   UG_WKC_PreReqChk_Package/prechecks_multi.sh

   UG_WKC_PreReqChk_Package/README.txt

   UG_WKC_PreReqChk_Package/uginfo.rsp

   UG_WKC_PreReqChk_Package/prereq_buildinfo.txt

   UG_WKC_PreReqChk_Package/prechecks.sh

2. Copy the uginfo.rsp to /tmp directory

   ```
   cp -p uginfo.rsp /tmp/uginfo.rsp
   ```

3. Edit the /tmp/uginfo.rsp file with highlighted items

   INST_TYPE=INSTALL

   ES_INSTALLDIR=/sys2/iis/v11.7

   NUMBER_OF_NODES=1

   IS_SERVER_HOST=dlnxap71.wsib.on.ca

   MASTER_NODE_HOST= dld8ap74.wsib.on.ca

   WORKER_NODE_HOST2=

   WORKER_NODE_HOST1=

   WEAVE_NET_IP=10.32.0.0/12

   SERVICE_IP_RANGE=10.96.0.0/12

   WKC_DEPLOY_FLAG=true

   UG_LOCAL_STORAGE_DIR=/sys2/iis/v11.7/ugdata

   MASTER_NODE_USER=root

4. Execute the job prechecks.sh under directory /temp/DS_v11.7.1_code/prereq with the following command:

   ./prechecks.sh /tmp/uginfo.rsp

```
[root@dld8ap74 UG_WKC_PreReqChk_Package]# ./prechecks.sh /tmp/uginfo.rsp
/temp/DS_v11.7.1_code/prereq/UG_WKC_PreReqChk_Package/prechecks_multi.sh: line 377:
checkCurrentDir: command not found
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your
Python as Python 2.7 won't be maintained after that date. A future version of pip will drop
support for Python 2.7.
Requirement already satisfied: pip==19.1.1 from
file:///temp/DS_v11.7.1_code/prereq/UG_WKC_PreReqChk_Package/pythondir/pip-19.1.1-py2.py3-none-
any.whl in /usr/lib/python2.7/site-packages (19.1.1)
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your
Python as Python 2.7 won't be maintained after that date. A future version of pip will drop
support for Python 2.7.
Requirement already satisfied: setuptools==41.0.1 from
file:///temp/DS_v11.7.1_code/prereq/UG_WKC_PreReqChk_Package/pythondir/setuptools-41.0.1-py2.py3-
none-any.whl in /usr/lib/python2.7/site-packages (41.0.1)
ipaddr-2.2.0/
ipaddr-2.2.0/setup.py
ipaddr-2.2.0/ipaddr_test.py
ipaddr-2.2.0/README
ipaddr-2.2.0/ipaddr.py
ipaddr-2.2.0/PKG-INFO
ipaddr-2.2.0/COPYING
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your
Python as Python 2.7 won't be maintained after that date. A future version of pip will drop
support for Python 2.7.
Processing /temp/DS_v11.7.1_code/prereq/UG_WKC_PreReqChk_Package/pythondir/ipaddr-2.2.0
Installing collected packages: ipaddr
  Found existing installation: ipaddr 2.1.11
```

```
ERROR: Cannot uninstall 'ipaddr'. It is a distutils installed project and thus we cannot
accurately determine which files belong to it which would lead to only a partial uninstall.
2021-03-01 18:27:40.273 UTC -- ERROR:Unable to pip install ipaddr
/temp/DS_v11.7.1_code/prereq/UG_WKC_PreReqChk_Package/prechecks_multi.sh: line 266: usage_retry:
command not found
installMode singlenode
which: no docker in (/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)
./prechecks.sh: line 228: kubectl: command not found
./prechecks.sh: line 312: chef-server-ctl: command not found
which: no chef-client in (/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)
./prechecks.sh: line 335: salt: command not found
./prechecks.sh: line 344: salt: command not found
./prechecks.sh: line 353: salt: command not found
./prechecks.sh: line 365: puppet: command not found
./prechecks.sh: line 374: puppet: command not found
./prechecks.sh: line 383: puppet: command not found
ansibleVer ************** ansible 2.9.5 config file = /etc/ansible/ansible.cfg configured module
search path = [u'/root/.ansible/plugins/modules', u'/usr/share/ansible/plugins/modules'] ansible
python module location = /usr/lib/python2.7/site-packages/ansible executable location =
/bin/ansible python version = 2.7.5 (default, Aug 13 2020, 02:51:10) [GCC 4.8.5 20150623 (Red Hat
4.8.5-39)]
Loaded plugins: product-id, rhui-lb, search-disabled-repos, subscription-manager

This system is not registered with an entitlement server. You can use subscription-manager to
register.

https://cds2.wshs/pulp/repos///content/dist/rhel/rhui/server/7/7Server/x86_64/custom/repodata/repo
md.xml: [Errno 14] HTTPS Error 404 - Not Found
Trying other mirror.
To address this issue please refer to the below knowledge base article

https://access.redhat.com/articles/1320623

If above article doesn't help to resolve this issue please open a ticket with Red Hat Support.

RHEL7                                                                                    | 2.8 kB
00:00:00
Package matching 32:bind-utils-9.11.4-16.P2.el7.x86_64 already installed. Checking for update.
Nothing to do
bind-utils-9.11.4-26.P2.el7_9.3.x86_64
2021-03-01 18:27:43.273 UTC -- Prechecks complete
 Enterprise Search Install Prechecks failed with ERRORS, please check the log for issues to
address and re-run prechecks script before proceeding with installation

[root@dld8ap74 installer]# ./ansible_check.sh
[INFO]  Ansible version is 2.9.5
[PASS]  Ansible version is supported
[INFO]  Ansible uses python2
[INFO]  Checking for required python2 libraries...
        OK: Module netaddr was found
        OK: Module dns was found
        [PASS]  Required python2 libraries are installed
```

Install MicroServices Tier (DLD8AP74)

Log in as root on Linux server DLD8AP74 and navigate to directory /sys2/iis/v11.7/

1. Create installer directory with following command:

   mkdir installer

2. Copy the MicroServices tier installation bundle to install directory with the following command:

   cp -p /temp/DS_v11.7.1_code/ .

3. Unpack the MicroServices tier installation bundle to the installer directory

   tar zxf is-enterprise-search-11.7.1.1.tar.gz -C installer

4. Upgrade Ansible

   Change directory to installer with the command

   cd installer

   Upgrade the Ansible with the following command

   ./ansible_install.sh -u

   Check the Ansible with the following command

   ./ansible_check.sh

```
[root@dld8ap74 installer]# ./ansible_check.sh
[INFO]  Ansible version is 2.9.5
[PASS]  Ansible version is supported
[INFO]  Ansible uses python2
[INFO]  Checking for required python2 libraries...
        OK: Module netaddr was found
        OK: Module dns was found
[PASS]  Required python2 libraries are installed
```

5. Prepare the Ansible inventory file

   Copy the default inventory file with the following command

   cp defaults/default_inventory.yaml inventory.yaml

   Update the inventory.yaml with required values, see below updated file. Request DS Admin to provide encrypted passwords, generated using application encryption tool:

```
cat installer/inventory.yaml
all:
  hosts:
    deployment_coordinator:
      ansible_host: localhost
      ansible_connection: local
  children:
    kubernetes:
      children:
        masters:
          hosts:
            master-1:
              ansible_host: localhost
              ansible_connection: local
  vars:
    image_registry_host: "{{ hostvars[groups.masters[0]].ansible_nodename|lower }}"
    image_registry_port: 5000
    image_registry_username: "{{ lookup('env', 'REGISTRY_USERNAME') | default('admin', true) }}"
    image_registry_password: "secret!"
    iis_server_host: "dlnxap71.wsib.on.ca"
    iis_server_port: 9446
    iis_admin_user: "isadmin"
    iis_admin_password: "{iisenc}fmp4M4rTqZLSd9d0FgYNhw=="
    iis_db_type: "db2"
    iis_db_host: "dlnxap71.wsib.on.ca"
    iis_db_port: 25771
    iis_db_user: "cddxmt01"
    iis_db_password: "{iisenc}jSQnTN6NjzNaP5HNp1KN/w=="
    iis_db_name: "XMETADEV"
    iis_db_driver: "com.ibm.db2.jcc.DB2Driver"
    iis_db_url: "jdbc:db2://dlnxap71.wsib.on.ca:25771/XMETADEV"
    iis_db_sr_type: "db2"
    iis_db_sr_host: "dlnxap71.wsib.on.ca"
    iis_db_sr_port: 25791
    iis_db_sr_user: "cddstr01"
```

```
iis_db_sr_password: "{iisenc}jSQnTN6NjzNaP5HNp1KN/w=="

iis_db_sr_name: "ddsod011"

iis_db_sr_driver: "com.ibm.db2.jcc.DB2Driver"

iis_db_sr_url: "jdbc:db2://dlnxap71.wsib.on.ca:25791/ddsod011"

ug_local_storage_dir: "/sys2/iis/v11.7/ugdata"

kube_pod_subnet: "10.32.0.0/12"

kube_service_subnet: "10.96.0.0/12"

finley_token: "$Dswiis18"

zookeeper_sasl_enable: "yes"

kafka_zookeeper_sasl_enable: "yes"

kafka_sasl_enable: "yes"

kafka_ssl_enable: "yes"

solr_zookeeper_sasl_enable: "yes"

solr_auth_enable: "yes"

kafka_sasl_users:

  kafka: "{iisenc}fmp4M4rTqZLSd9d0FgYNhw=="

solr_auth_basic_username: "dwasadm"

solr_auth_basic_password: "{iisenc}fmp4M4rTqZLSd9d0FgYNhw=="
```

6. Configure the JWT verification certificate

   To configure the JWT certificate, copy the /sys2/iis/v11.7/lib/iis/tknproperties/tokenservicepublic.cer file from the Information Server services tier into the /sys2/iis/v11.7/files directory on the MicroServices Tier.

7. Run the MicroServices Tier installation by running the following command from directory /sys2/iis/v11.7/ installer

   ./install.sh

```
[root@dld8ap74 v11.7]# cd /sys2/iis/v11.7/installer
[root@dld8ap74 installer]# ./install.sh

[root@dld8ap74 installer]# pwd
/sys2/iis/v11.7/installer
[root@dld8ap74 installer]# ./run_playbook.sh -y
/sys2/iis/v11.7/installer/playbooks/shared_services/kafka_get_ca_crt.yaml -e
kafka_ssl_ca_crt_file=/tmp/kafka_ca.pem
[INFO]  Console log output file:
/sys2/iis/v11.7/installer/logs/kafka_get_ca_crt_2021_03_09_16_00_11.log
[INFO]  Checking for Ansible...
[INFO]  Ansible version is 2.9.5
[PASS]  Ansible version is supported
[INFO]  Ansible uses python2
[INFO]  Checking for required python2 libraries...
        OK: Module netaddr was found
        OK: Module dns was found
[PASS]  Required python2 libraries are installed
```

```
[INFO]  Checking hosts connectivity...
deployment_coordinator | SUCCESS => {"ansible_facts": {"discovered_interpreter_python":
"/usr/bin/python"}, "changed": false, "ping": "dest=localhost"}
master-1 | SUCCESS => {"ansible_facts": {"discovered_interpreter_python": "/usr/bin/python"},
"changed": false, "ping": "dest=localhost"}

PLAY [Load presets]
*********************************************************************************************
***

TASK [Gather basic facts]
*********************************************************************************************
Tuesday 09 March 2021  11:00:15 -0500 (0:00:00.033)       0:00:00.033 *********
ok: [localhost]
ok: [master-1]
ok: [deployment_coordinator]

TASK [Load presets]
*********************************************************************************************
***
Tuesday 09 March 2021  11:00:16 -0500 (0:00:00.752)       0:00:00.786 *********
ok: [deployment_coordinator]

PLAY RECAP
*********************************************************************************************
************
deployment_coordinator     : ok=2    changed=0    unreachable=0    failed=0    skipped=0
rescued=0    ignored=0
localhost                  : ok=1    changed=0    unreachable=0    failed=0    skipped=0
rescued=0    ignored=0
master-1                   : ok=1    changed=0    unreachable=0    failed=0    skipped=0
rescued=0    ignored=0

Tuesday 09 March 2021  11:00:16 -0500 (0:00:00.030)       0:00:00.816 *********
===============================================================================
Gather basic facts ------------------------------------------------------------------------
---------------- 0.75s
Load presets ------------------------------------------------------------------------------
---------------- 0.03s

PLAY [Get Kafka CA certificate]
*********************************************************************************************

TASK [Gathering Facts]
*********************************************************************************************
Tuesday 09 March 2021  11:00:16 -0500 (0:00:00.047)       0:00:00.864 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Get current Kafka SSL secret name]
*************************************
Tuesday 09 March 2021  11:00:16 -0500 (0:00:00.302)       0:00:01.166 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Set current Kafka SSL secret name fact]
**********************************
Tuesday 09 March 2021  11:00:17 -0500 (0:00:00.582)       0:00:01.749 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Search for Kafka SSL secret]
*******************************************
Tuesday 09 March 2021  11:00:17 -0500 (0:00:00.069)       0:00:01.819 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA keystore passphrase from secret]
****************************
Tuesday 09 March 2021  11:00:17 -0500 (0:00:00.329)       0:00:02.148 *********
ok: [master-1]
```

```
TASK [com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA keystore passphrase fact]
***********************************
Tuesday 09 March 2021  11:00:17 -0500 (0:00:00.320)       0:00:02.468 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA keystore content from secret]
*******************************
Tuesday 09 March 2021  11:00:18 -0500 (0:00:00.071)       0:00:02.539 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA keystore content fact]
************************************
Tuesday 09 March 2021  11:00:18 -0500 (0:00:00.316)       0:00:02.856 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Create Kafka SSL CA keystore temporary file]
*****************************
Tuesday 09 March 2021  11:00:18 -0500 (0:00:00.071)       0:00:02.927 *********
changed: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Save Kafka CA keystore to file]
*****************************************
Tuesday 09 March 2021  11:00:18 -0500 (0:00:00.352)       0:00:03.280 *********
changed: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA certificate from CA keystore]
*******************************
Tuesday 09 March 2021  11:00:19 -0500 (0:00:00.258)       0:00:03.538 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Clean Kafka CA certificate]
***********************************************
Tuesday 09 March 2021  11:00:19 -0500 (0:00:00.259)       0:00:03.797 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA certificate fact]
*****************************************
Tuesday 09 March 2021  11:00:19 -0500 (0:00:00.267)       0:00:04.065 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA key from CA keystore]
************************************
Tuesday 09 March 2021  11:00:19 -0500 (0:00:00.070)       0:00:04.136 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Clean Kafka CA key]
*****************************************************
Tuesday 09 March 2021  11:00:19 -0500 (0:00:00.273)       0:00:04.409 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA key fact]
**************************************************
Tuesday 09 March 2021  11:00:20 -0500 (0:00:00.255)       0:00:04.665 *********
ok: [master-1]

TASK [com/ibm/ugi/kubeplatform/shared/kafka : Delete Kafka SSL CA keystore temporary file]
*****************************
Tuesday 09 March 2021  11:00:20 -0500 (0:00:00.074)       0:00:04.739 *********
changed: [master-1]

TASK [Save Kafka CA certificate to file]
*******************************************************************************
Tuesday 09 March 2021  11:00:20 -0500 (0:00:00.475)       0:00:05.214 *********
changed: [master-1 -> localhost]

PLAY RECAP
*************************************************************************************************
************
```

```
deployment_coordinator     : ok=2    changed=0    unreachable=0    failed=0    skipped=0
rescued=0    ignored=0
localhost                  : ok=1    changed=0    unreachable=0    failed=0    skipped=0
rescued=0    ignored=0
master-1                   : ok=19   changed=4    unreachable=0    failed=0    skipped=0
rescued=0    ignored=0

Tuesday 09 March 2021  11:00:21 -0500 (0:00:00.752)       0:00:05.966 *********
===============================================================================
Save Kafka CA certificate to file ---------------------------------------------------------
---------------- 0.75s
Gather basic facts ------------------------------------------------------------------------
---------------- 0.75s
com/ibm/ugi/kubeplatform/shared/kafka : Get current Kafka SSL secret name -----------------
---------------- 0.58s
com/ibm/ugi/kubeplatform/shared/kafka : Delete Kafka SSL CA keystore temporary file -------
---------------- 0.48s
com/ibm/ugi/kubeplatform/shared/kafka : Create Kafka SSL CA keystore temporary file -------
---------------- 0.35s
com/ibm/ugi/kubeplatform/shared/kafka : Search for Kafka SSL secret ------------------------
---------------- 0.33s
com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA keystore passphrase from secret -------
---------------- 0.32s
com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA keystore content from secret ----------
---------------- 0.32s
Gathering Facts ---------------------------------------------------------------------------
---------------- 0.30s
com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA key from CA keystore -----------------
---------------- 0.27s
com/ibm/ugi/kubeplatform/shared/kafka : Clean Kafka CA certificate ------------------------
---------------- 0.27s
com/ibm/ugi/kubeplatform/shared/kafka : Get Kafka CA certificate from CA keystore ----------
---------------- 0.26s
com/ibm/ugi/kubeplatform/shared/kafka : Save Kafka CA keystore to file ---------------------
---------------- 0.26s
com/ibm/ugi/kubeplatform/shared/kafka : Clean Kafka CA key ---------------------------------
---------------- 0.26s
com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA key fact ------------------------------
---------------- 0.07s
com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA keystore content fact -----------------
---------------- 0.07s
com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA keystore passphrase fact --------------
---------------- 0.07s
com/ibm/ugi/kubeplatform/shared/kafka : Set Kafka CA certificate fact ---------------------
---------------- 0.07s
com/ibm/ugi/kubeplatform/shared/kafka : Set current Kafka SSL secret name fact -------------
---------------- 0.07s
        Load presets ------------------------------------------------------------------------
        ----------------------- 0.03s
```

8. You must configure the services Tier to set up the connection to common services that run on the MicroServices Tier, such as Kafka and Solr.

   Before you configure the services Tier, obtain a Kafka CA certificate. Run the following command in the MicroServices Tier shell:

```
[root@dld8ap74 installer]# chmod 644 /tmp/kafka_ca.pem

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/jdk/bin/keytool -import -alias kafka -file
/tmp/kafka_ca.pem -keystore /tmp/ug-host-truststore.jks -storepass
{iisenc}fmp4M4rTqZLSd9d0FgYNhw== -noprompt

Certificate was added to keystore
```

```
[root@dlnxap71 v11.7]# mkdir -p /sys2/iis/v11.7/Kafka

[root@dlnxap71 v11.7]# chmod 755 /sys2/iis/v11.7/Kafka

[root@dlnxap71 v11.7]# ll /tmp/ug-host-truststore.jks

-rw-r--r--. 1 root root 873 Mar  9 11:11 /tmp/ug-host-truststore.jks

[root@dlnxap71 v11.7]# cp /tmp/ug-host-truststore.jks /sys2/iis/v11.7/Kafka

[root@dlnxap71 v11.7]# chmod 644 /sys2/iis/v11.7/Kafka/ug-host-truststore.jks

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key com.ibm.iis.sos.mode -
value remote

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.sos.acceptAllCertificates -value true

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.sdp.zookeeper.connect -value dld8ap74.wsib.on.ca:2181/kafka

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.sdp.kafka.bootstrap.servers -value dld8ap74.wsib.on.ca:9092

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.ug.microservice.indexing.isEnabled -value true

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.truststoreLocation -value /sys2/iis/v11.7/Kafka/ug-host-truststore.jks

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.securityProtocol -value "SASL_SSL"

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.truststorePassword -value {iisenc}l0DqnqBh4tR9+m1X1sJsuA==

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.saslUser -value dwasadm

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.saslPassword -value {iisenc}l0DqnqBh4tR9+m1X1sJsuA==

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.truststoreType -value "JKS"

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.solr.search.connect -value https://dld8ap74.wsib.on.ca/solr

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.solr.search.user -value dwasadm

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.solr.search.password -value {iisenc}l0DqnqBh4tR9+m1X1sJsuA==

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.ug.finley_token -value {iisenc}l0DqnqBh4tR9+m1X1sJsuA==

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.ug.host.name -value dld8ap74.wsib.on.ca

[root@dlnxap71 v11.7]# /sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key
com.ibm.iis.events.kafka.ca.pem -value {iisenc}l0DqnqBh4tR9+m1X1sJsuA==
```

The value of the FINLEY_TOKEN must match the one defined in the inventory file.

The value of the KAFKA_CA_PEM_VAL is the content from generated file kafka_ca.pem on MS tier host /tmp location. Make sure that the

first line (-----BEGIN CERTIFICATE-----), last line (-----END CERTIFICATE-----) and any new line characters/spaces are removed before setting up KAFKA_CA_PEM_VAL value

```
/sys2/iis/v11.7/ASBServer/bin/iisAdmin.sh -set -key com.ibm.iis.events.kafka.ca.pem -
value
MIIDJzCCAg+gAwIBAgIJAPs15FJHMcTEMA0GCSqGSIb3DQEBCwUAMCoxKDAmBgNVBAMMH1VHIEthZmthIENBIGR
sZDhhcDc0LndzaWIub24uY2EwHhcNMjEwMzA5MTUxNzIxWhcNNDgwNzI0MTUxNzIxWjAqMSgwJgYDVQQDDB9VRy
BLYWZrYSBDQSBkbGQ4YXA3NC53c2liLm9uLmNhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxroCR
cqWd+ObUZpXfvsFeKEF0ibd/3Lw/XYOmoKC//e8XYqxdkID3tLi9ulvvHQaSqhJC+yRgOZXypKnzOJ3QBQoI4we
3359acCgBqU+MT+Yp6wGvsqmaxb/GAuBwzuGHxdscngRL4xTr9zAL/axHkscZDMuD3RzqEk0YN/WcSA6GONz1kx
bnvSrW4e9UPNjENzAW8q6jYjskea4GQVeelChzWHRfY4N0ZAs8NGHKrN3OYHA2XFcdmsezVuuX++/u1jgH1e3A2
za7S3Ah1+C1SUmZaKSclKZSLMLiwXVgA8UcZL/cEWZ9fML6iRC2w9o1EWjxz+mUpRgNaitOzdw8QIDAQABo1AwT
jAdBgNVHQ4EFgQU/IgZEY8Q0fE1Hfp5h51M19bXOCwwHwYDVR0jBBgwFoAU/IgZEY8Q0fE1Hfp5h51M19bXOCww
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAQEAcTkMRX/htLnQTehcpxXGhbtjPiUQ+ksGHTO9WH8OkAJ
Nm57VNNe+L96LFlCpmkx4EIHrdCZQ7eMKBI3rLEYT9xSR1I/bYWog8U4rzjd9llTUp1uqIFTl7Pg8hMba+ZCgO5
5H2EdC3JtG/+OCwS34di8+e1It23TPxjs00JxMNnu1WOGXZHX98BYAUgZtUsxNF4cc+ca+ioJd0Hvfex7gyPQXX
lZQ/pkYehMUktxbGvIZbUMQGyRWSxGmdpvIbiGJlU0aVVuuLjhn3qzW79Rj+oDMNfn5iPy1CqVw0aTFLZxq3JHJ
pFUDpjTi4nSZl5h+C6DABc/9b8g1JCO16sJvGQ==
```

Finally, restart WebSphere Application Server for the changes to become effective. Verify that no errors are reported upon startup in the WebSphere system output log.

9. Configure the Engine Tier to connect to the MicroServices tier

   Verify that the following properties exist in the file /sys2/iis/v11.7/ASBNode/conf/odf.properties and the values match the iisAdmin properties in the Services Tier:

   com.ibm.iis.events.kafka.saslPassword=KAFKA_PASSWORD_ENCRYPTED

   com.ibm.iis.events.kafka.saslUser=KAFKA_USERNAME

   com.ibm.iis.events.kafka.securityProtocol=SASL_SSL

   com.ibm.iis.events.kafka.truststoreLocation=/sys2/iis/v11.7/Kafka/ug-host-truststore.jks

   com.ibm.iis.events.kafka.truststorePassword=KAFKA_TRUSTSTORE_PASS_ENCRYPTED

   com.ibm.iis.events.kafka.truststoreType=JKS

   com.ibm.iis.sos.mode=remote

   odf.zookeeper.connect=UG_HOST\:2181/kafka

10. Restart the ODFEngine:

    service ODFEngine stop

    service ODFEngine start

11. Change ownership of /sys2/iis/v11.7 to dwasadm by running the following command

    chown -R dwasadm:dwas /sys2/iis/v11.7

This completes the MicroServices Tier Install.

Appendix

1. DataStage servers in all environments:

Development		**QA SIT/BAT**	
DLNXDE91 (10.49.44.3)	Engine Tier (with NLS)	ALNXDE91 (10.49.47.4)	Engine Tier
DLNXAP71 (10.49.45.5)	Services Tier	ALNXAP81 (10.49.48.9)	Services Tier
DLD8AP74 (10.49.45.10)	MicroServices Tier	ALD8AP81 (10.49.48.53)	MicroServices Tier
N/A	N/A	ALNXDB91 (10.49.47.5)	Xmeta DB
DLNXWB71 (10 49 46 35)	Application Tier	ALNXWB71 (10.49.49.4)	Application Tier
PPD		**Production**	
NLNXDE01 (10.48.22.30)	Engine Tier	PLNXDE01 (10.48.25.29)	Engine Tier
NLNXAP1W (10.48.23.165)	Services Tier	PLNXAP1W (10.48.26.152)	Services Tier
TBD	MicroServices Tier	TBD	MicroServices Tier
NLNXDB07 (10.48.22.29)	Xmeta DB	PLNXDB07 (10.48.25.28)	Xmeta DB
NLNXWB21 (10.48.24.6)	Application Tier	PLNXWB21 (10.48.27.37)	Application Tier

2. Ports for Microservices Tier: Source DLNXAP71, Target DLD8AP74:

Port	**Usage**	**Port**	**Usage**
HTTP 80	Common	TCP 443	ingress-nginx-controller
TCP 5000	docker	TCP 6443*	Kubernetes API Server
TCP 2379-2380	etcd server client API	TCP 10250	Kubelet API
TCP 10251	kube-scheduler	TCP 10248	kubelet
TCP 10249	kube-proxy	TCP 10252	kube-controller-manager
TCP 10255	Read-Only Kubelet API	TCP 30000-32767	NodePort Services
TCP 6783/6784	Weave Services	TCP 9092	Kafka
TCP 2181	zookeeper		

3. Ports for Xmeta DB to Microservices Tier: Source DLD8AP74, Target Xmeta DB:

Environment	Server Name	Xmeta Database	Port Number
Development	DLNXAP71 (10.49.45.5)	DXMED011 (XMETADEV)	25771
SIT/BAT	ALNXDB91 (10.49.47.5)	DXMEB011 (XMETABAT)	25771
PPD	NLNXDB07 (10.48.22.29)	DXMEN011 (XMETAPPD)	25771
PROD	PLNXDB07 (10.48.25.28)	DXMEP011 (XMETAPRD)	25771

Note: The above ports need to be opened if the Services and MicroServices servers are on separate subnets and not within the same zone. In the above install, they were in the same zone so no FW rules were applied.

4. Ports for Terminal Server: Source: PWINTS16, Target: DLD8AP74

TCP: 22, 443, 5578, 8446, 9043, 9060, 9080, 9446