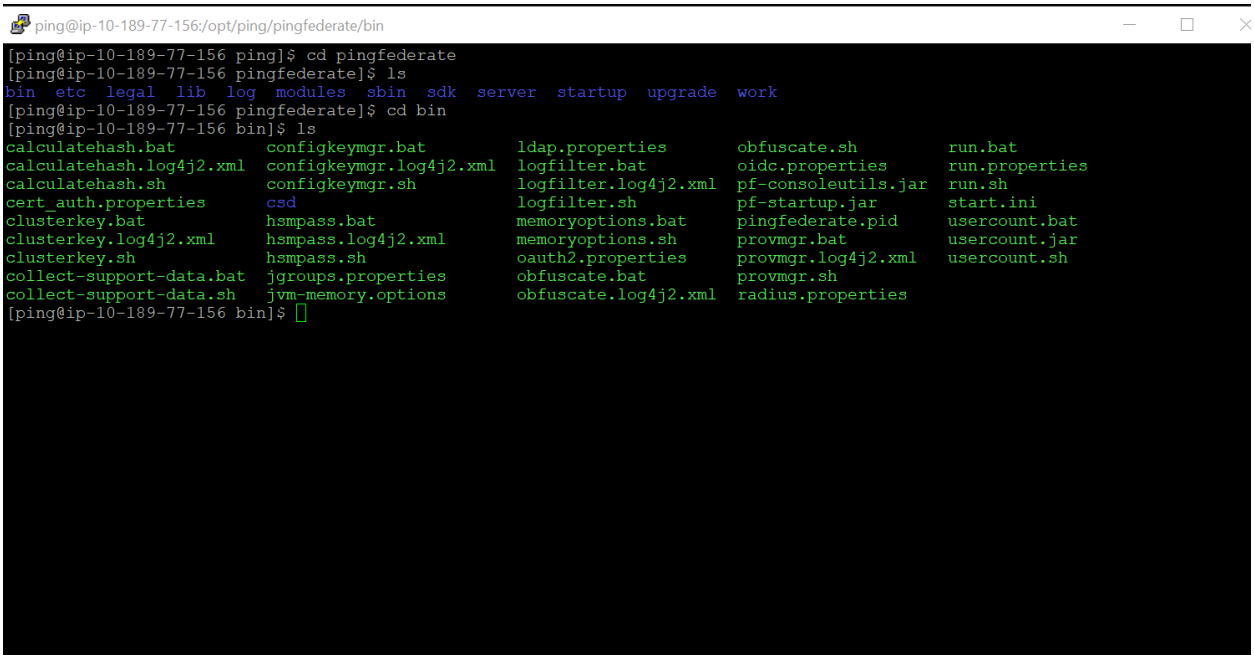
Scenario 5: Configuring PingFederate as a Cluster Environment

For additional redundancy, administrators can configure PingFederate in a cluster environment. In this configuration you will assign one node as the Console node (on which you'll make changes through the UI), and one or more nodes as engine nodes.

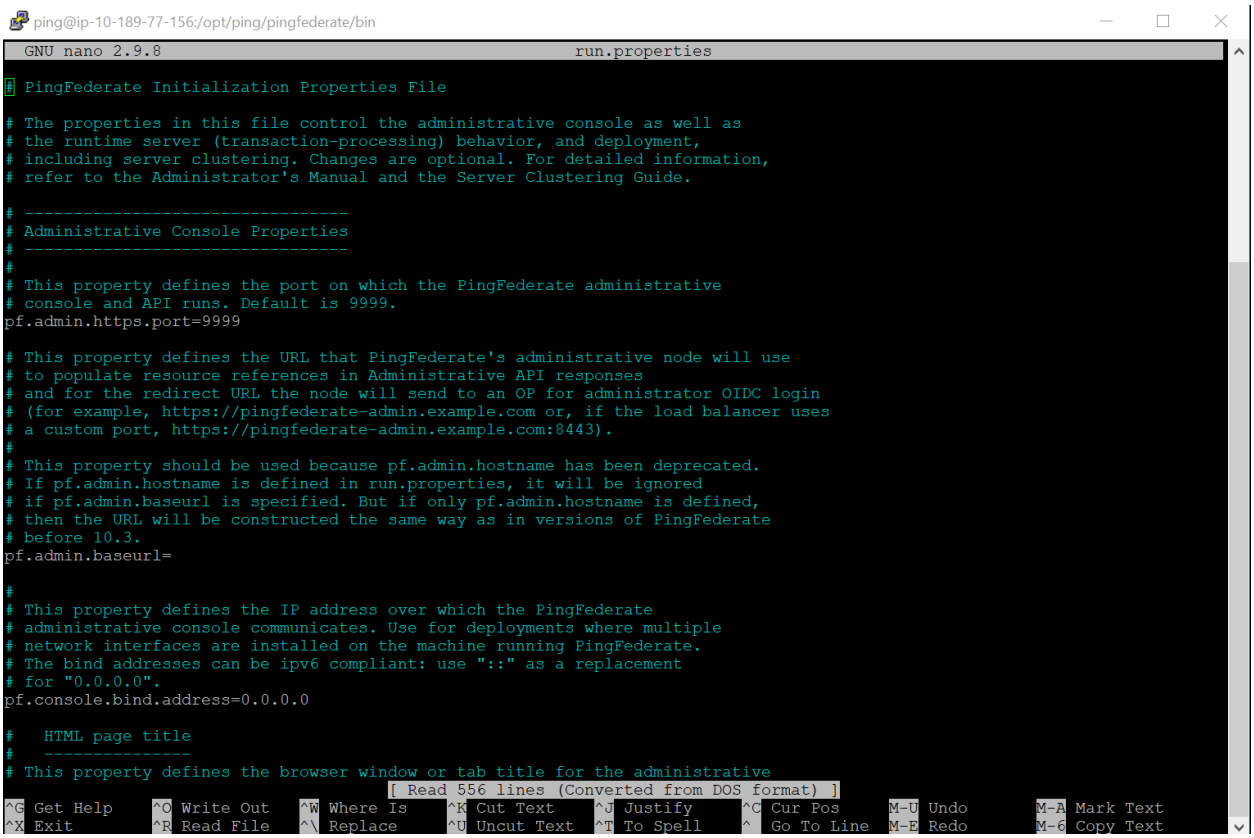
Note: you should shut down your PingFederate sever before making any of these changes.

Modifying the Existing Node

Start by navigating to the folder of your existing ping install (/opt/ping/pingfederate in our case) and then go to **bin.**

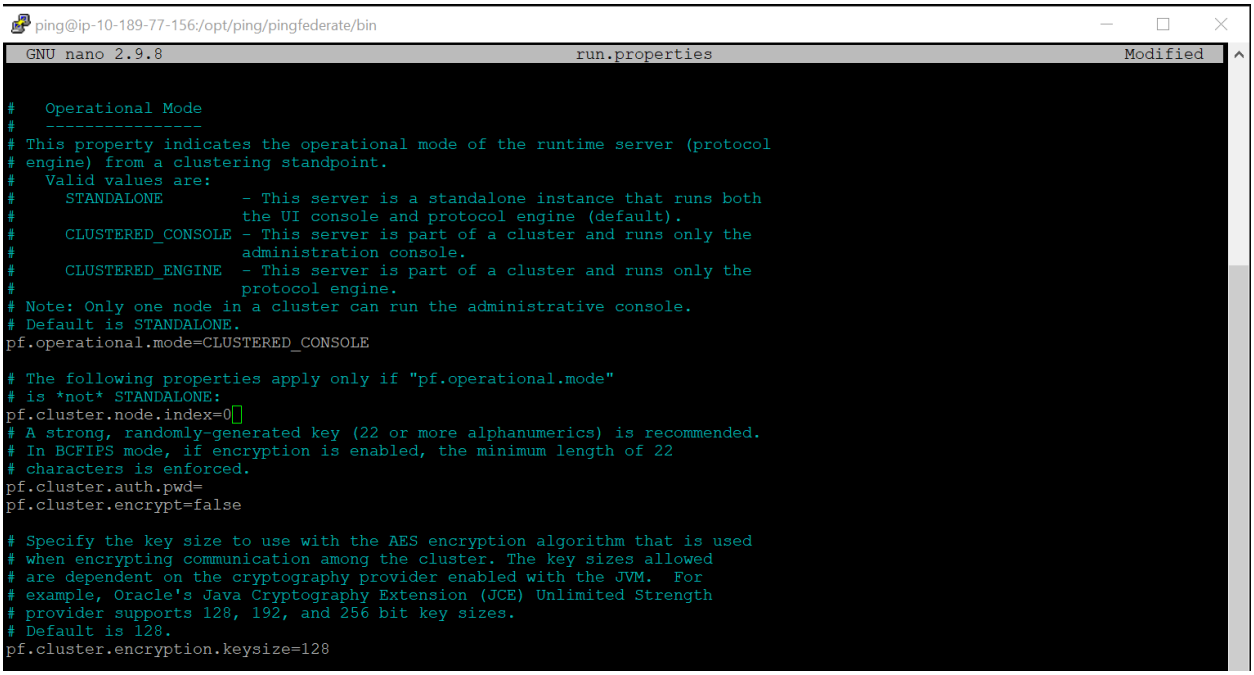


Open **run.properties**

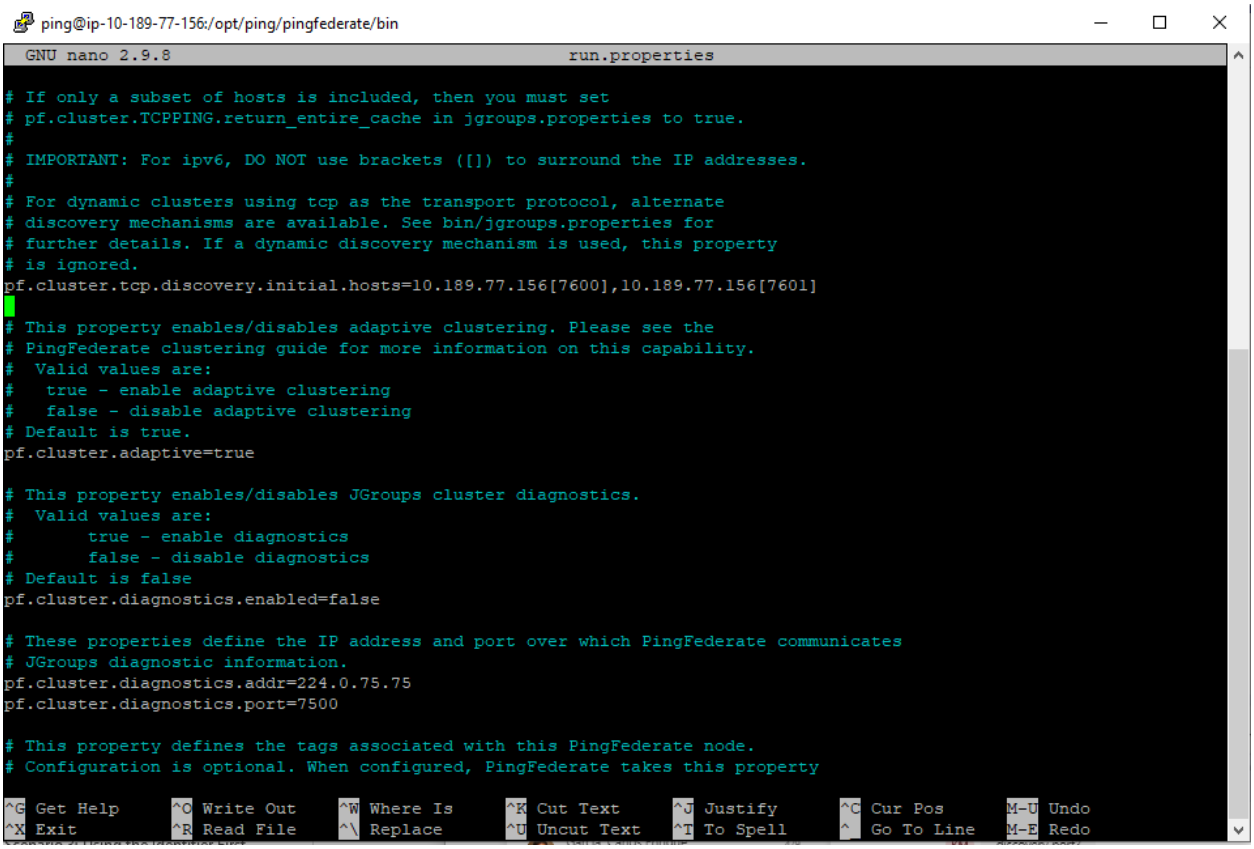


Set the **pf.operational.mode** equal to **CLUSTERED_CONSOLE.**

Set the **pf.cluster.node.index** equal to **0**



Set the **pf.cluster.tcp.discovery.initial.hosts** equal to **firstHostIP[7600],secondHostIP[7601]**



Write the data out and exit.

Creating the Engine Node

Start by making a copy of your already configured instance into the same directory (/opt/ping in this example)

```
ping@ip-10-189-77-156:/opt/ping
[ping@ip-10-189-77-156 ping]$ ls
java              PingDataSync     PingDirectory-3       start_ping_demo.sh
jdk-17.0.2        PingDirectory-1  pingfederate          status_ping_demo.sh
pingaccess-8.0.0  PingDirectory-2  restart_ping_demo.sh  stop_ping_demo.sh
[ping@ip-10-189-77-156 ping]$ cp -R pingfederate pingfederate-engine
[ping@ip-10-189-77-156 ping]$
```

Go to the newly copied install folder, and open **run**.**properties** from the **bin** directory.

```
ping@ip-10-189-77-156:/opt/ping/pingfederate-engine/bin
  GNU nano 2.9.8                                  run.properties

# PingFederate Initialization Properties File

# The properties in this file control the administrative console as well as
# the runtime server (transaction-processing) behavior, and deployment,
# including server clustering. Changes are optional. For detailed information,
# refer to the Administrator's Manual and the Server Clustering Guide.

# ---------------------------------
# Administrative Console Properties
# ---------------------------------
#
# This property defines the port on which the PingFederate administrative
# console and API runs. Default is 9999.
pf.admin.https.port=9999

# This property defines the URL that PingFederate's administrative node will use
# to populate resource references in Administrative API responses
# and for the redirect URL the node will send to an OP for administrator OIDC login
# (for example, https://pingfederate-admin.example.com or, if the load balancer uses
# a custom port, https://pingfederate-admin.example.com:8443).
#
# This property should be used because pf.admin.hostname has been deprecated.
# If pf.admin.hostname is defined in run.properties, it will be ignored
# if pf.admin.baseurl is specified. But if only pf.admin.hostname is defined,
# then the URL will be constructed the same way as in versions of PingFederate
# before 10.3.
pf.admin.baseurl=

#
# This property defines the IP address over which the PingFederate
# administrative console communicates. Use for deployments where multiple
# network interfaces are installed on the machine running PingFederate.
# The bind addresses can be ipv6 compliant: use "::" as a replacement
# for "0.0.0.0".
pf.console.bind.address=0.0.0.0

#   HTML page title
#   ---------------
# This property defines the browser window or tab title for the administrative
                        [ Read 556 lines (Converted from DOS format) ]
^G Get Help   ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo      M-A Mark Text
^X Exit       ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo      M-6 Copy Text
```

Scroll down until you see the **pf.https.port** field. Set it to **9032**, since 9031 is already being used by our runtime console node.

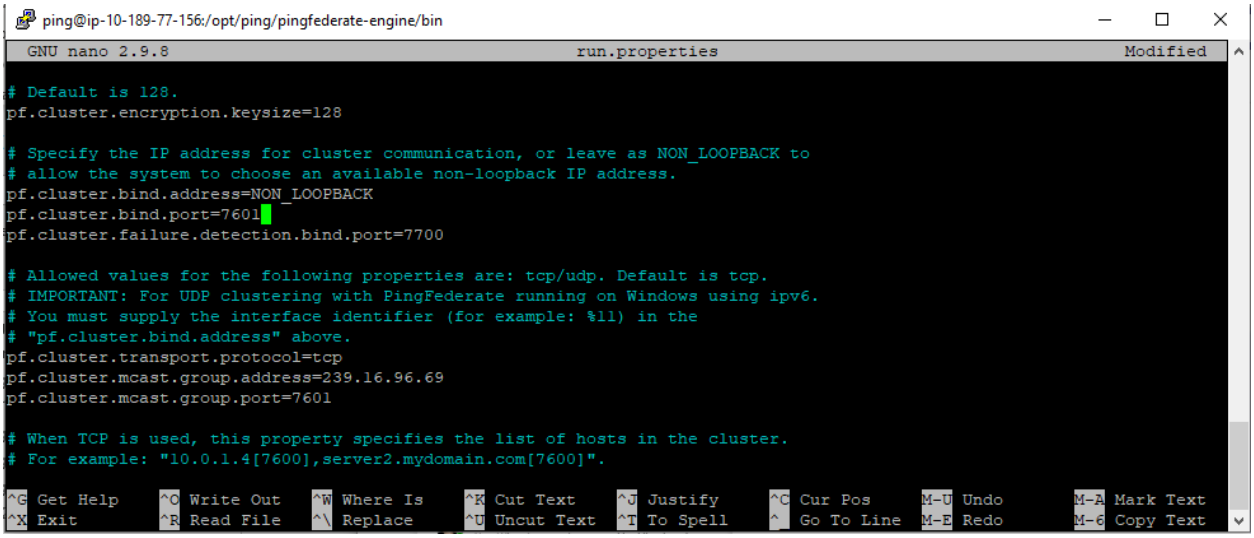
```
# -------------------------
# Runtime Server Properties
# -------------------------
#
# To turn off an HTTP listener, set the port to a value of less than zero.
# You should always use SSL. Turning on "pf.http.port" is not recommended.
# If you do want to turn on "pf.http.port" for testing purposes, you will
# need to update data/config-store/session-cookie-config.xml
# to turn off the secure cookie.
pf.http.port=-1

#
# This property defines the port on which PingFederate listens for
# encrypted HTTPS (SSL/TLS) traffic.
# Default is 9031.
pf.https.port=9032

# This property defines a secondary HTTPS port that can be used for mutual SSL/TLS
# (client X.509 certificate) authentication for both end users and protocol
# requests (SAML, WS-Trust and OAuth). Set its value to the desired inbound
# listening TCP port.
# A value of -1 disables this feature.

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text
```

Set the **pf.operational.mode** equal to **CLUSTERED_ENGINE.**

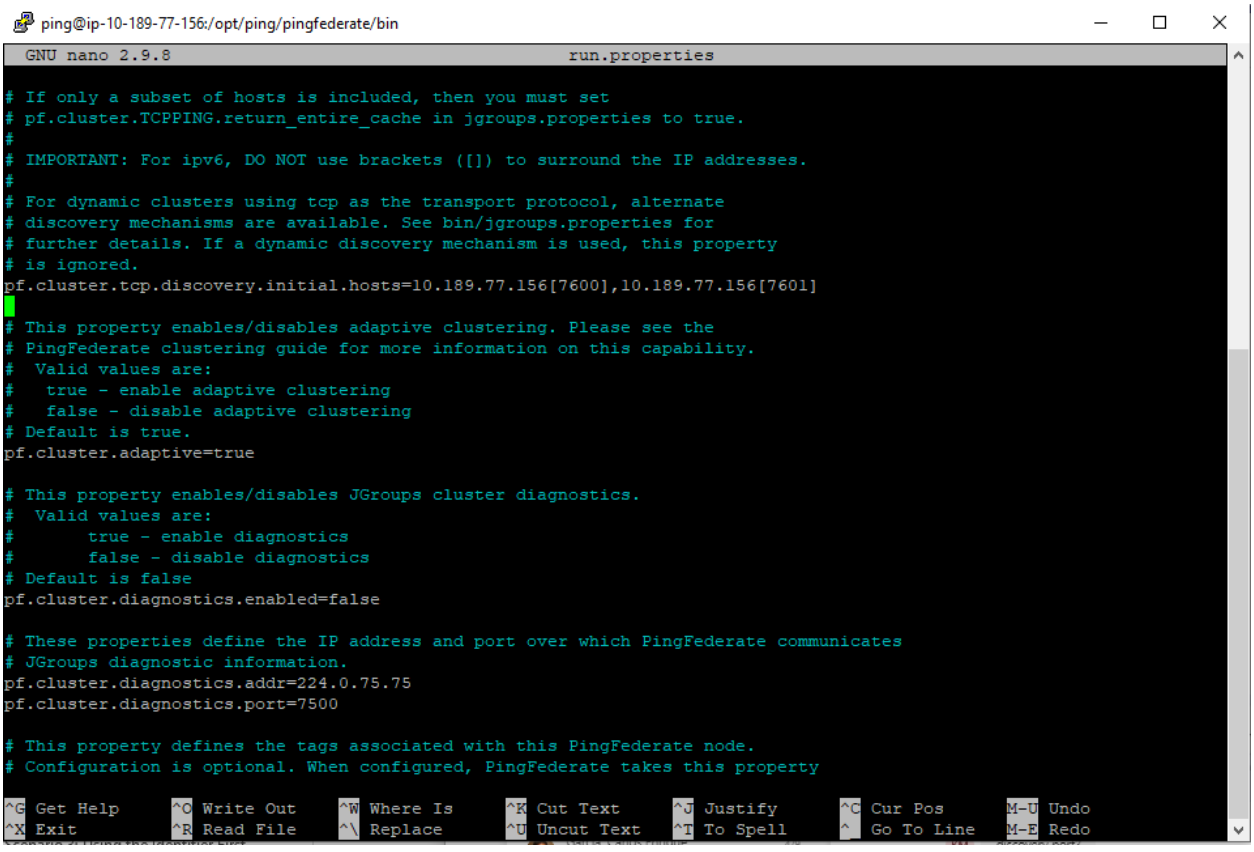
Set the **pf.cluster.node.index** equal to **1**

```
ping@ip-10-189-77-156:/opt/ping/pingfederate-engine/bin
  GNU nano 2.9.8                          run.properties                          Modified


#   Operational Mode
#   ----------------
# This property indicates the operational mode of the runtime server (protocol
# engine) from a clustering standpoint.
#   Valid values are:
#     STANDALONE        - This server is a standalone instance that runs both
#                         the UI console and protocol engine (default).
#     CLUSTERED_CONSOLE - This server is part of a cluster and runs only the
#                         administration console.
#     CLUSTERED_ENGINE  - This server is part of a cluster and runs only the
#                         protocol engine.
# Note: Only one node in a cluster can run the administrative console.
# Default is STANDALONE.
pf.operational.mode=CLUSTERED_ENGINE

# The following properties apply only if "pf.operational.mode"
# is *not* STANDALONE:
pf.cluster.node.index=1
# A strong, randomly-generated key (22 or more alphanumerics) is recommended.
# In BCFIPS mode, if encryption is enabled, the minimum length of 22
# characters is enforced.
pf.cluster.auth.pwd=
pf.cluster.encrypt=false

# Specify the key size to use with the AES encryption algorithm that is used
# when encrypting communication among the cluster. The key sizes allowed
# are dependent on the cryptography provider enabled with the JVM.  For
# example, Oracle's Java Cryptography Extension (JCE) Unlimited Strength
# provider supports 128, 192, and 256 bit key sizes.
# Default is 128.
pf.cluster.encryption.keysize=128

# Specify the IP address for cluster communication, or leave as NON_LOOPBACK to
# allow the system to choose an available non-loopback IP address.
pf.cluster.bind.address=NON_LOOPBACK
pf.cluster.bind.port=7600
pf.cluster.failure.detection.bind.port=7700


^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text
```

Set the **pf.cluster.bind.port** to **7601**



Set the **pf.cluster.tcp.discovery.initial.hosts** equal to **firstHostIP[7600],secondHostIP[7601]**



Write the data out and exit.