Setting up Basic User Authentication in Drill

NOTE This is a continuation of my series on the deployment of Apache Drill on Azure (https://blogs.msdn.microsoft.com/data_otaku/2016/05/27/deploying-apache-drill-on-azure/). That said, there is nothing in this post that is specific to an Azure deployment though I will assume you are familiar with my topology (https://blogs.msdn.microsoft.com/data_otaku/2016/05/27/an-overview-of-an-apache-drill-topology-in-azure/)when I reference servers by name.

With my Drill cluster deployed, I want to setup some kind of authentication. Out of the box, Drill is wide-open which means that without ring-fencing the application, any anonymous user could login to the Web Console to not only query my data but see the Storage Plugin configurations, some of which contain passwords for authenticating against data sources. Not good.

To implement basic authentication, I need to take four actions:

1. Create user logins
2. Identify users to serve as Drill admins
3. Enable user authentication
4. Restart Drill and test user authentication

Create User Logins

On each of the Linux servers that make up my Drill cluster, I need to create a consistent set of identities for my users. I can do this using adduser with appropriate substitutions:

```
sudo /usr/sbin/useradd myusername
sudo passwd myusername
```

It is important that the user name and passwords for these users are perfectly identical on each of the servers.

Identify Users to Serve as Drill Admins

The Drill documentation does a good job of covering all the steps in both setting up user authentication and establishing Drill admins. However, the order of the pages in the documentation implies an order to these operations that will leave you with a cluster with no admins. Before enabling user authentication, be sure to configure Drill to recognize its administrative users.

To do this, you will simply connect to the Drill service using sqlline and alter the security.admin.users setting. I'm doing this while SSH'ed into one of my Drill VMs. I have an ensemble of ZooKeeper nodes but have elected to leverage just one of these nodes, *i.e.* zk001, to establish my Drill connection:

```
/drill/current/bin/sqlline
!connect jdbc:drill:zk=zk001:2181
alter system set security.admin.users = 'sudo, myusername';
!quit
```

NOTE In my cluster, I installed Drill to /drill/current as documented here. The location of sqlline on your servers may vary.

In the ALTER SYSTEM statement, I assigned a comma-delimited list of users on my Drill servers to the admin role. In this example, those users are sudo and *myusername*.

Enable User Authentication

With my users created and a few of these identified as admins, I can now enable basic authentication. I do this by first installing the basic authentication PAM on each of my Drill servers:

```
cd ~
wget
http://liquidtelecom.dl.sourceforge.net/project/jpam/jpam/jpam-
1.1/JPam-Linux_amd64-1.1.tgz
tar -xzvf JPam-Linux_amd64-1.1.tgz
sudo mkdir /opt/pam
sudo cp ~/JPam-1.1/libjpam.so /opt/pam/
```

NOTE I am running a 64-bit OS which is why I have downloaded this particular version of the PAM.

I've placed the PAM under /opt/pam per the Drill documentation. Now I need to modify the drill-env.sh script to reflect this location:

```
sudo vi /drill/current/conf/drill-env.sh
```

Within the vi editor, I add this line somewhere towards the top of the script:

```
export DRILLBIT_JAVA_OPTS="-Djava.library.path=/opt/pam/"
```

I then save the changes to the script and close vi.

Finally, I need to modify the drill-override.conf file to enable basic authentication with Drill startup. I first open this file using vi:

```
sudo vi /drill/current/conf/drill-override.conf
```

I then modify the value for drill.exec to include the security.user.auth settings as highlighted in red (including the comma on the end of the value for zk.connect:

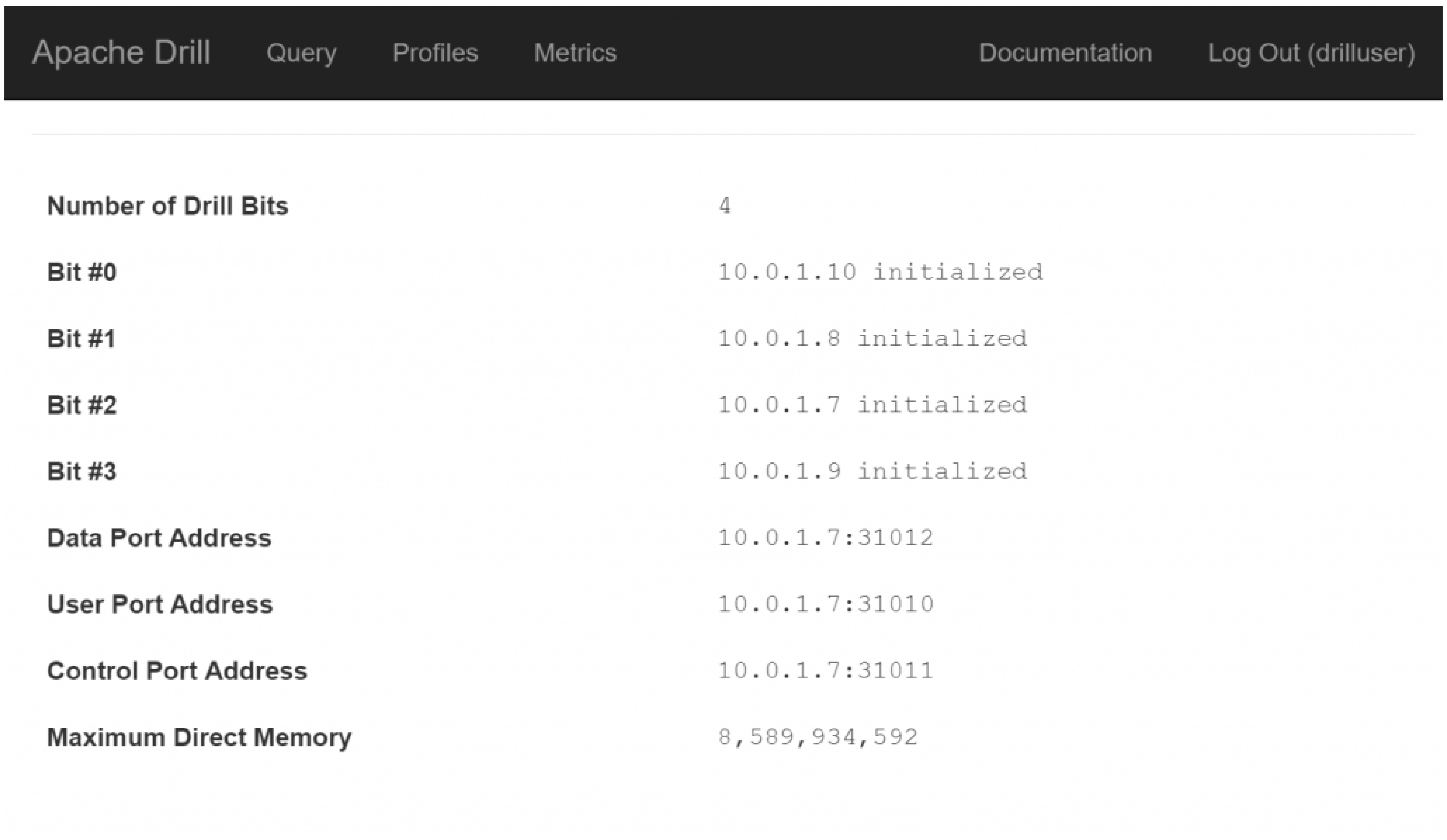
```
drill.exec: {
cluster-id: "drillcluster001",
zk.connect: "zk001:2181,zk002:2181,zk003:2181",
security.user.auth: {
enabled: true,
packages += "org.apache.drill.exec.rpc.user.security",
impl: "pam",
pam_profiles: [ "sudo", "myusername" ]
}
}
```

The array assigned to pam_profiles is worth a quick note. This should be a comma-delimited list of all users on your Drill servers to whom you would like to grant Drill access. Your administrators should be in here as well.

Restart Drill & Test User Authentication

With authentication configured on each of my Drill servers, I now must restart Drill for it to go into effect. The easiest way I have found to do this is simply to restart my Drill servers.

With my Drill servers now restarted, I can go to the Drill Web Console where I should be prompted to enter a username and password. If I login as an admin, I should be able to see the full range of functionality available in the Web Console including the Storage page. If I login as a non-admin user, I should see the home, Query, Profiles and Metrics pages only. Note that you will not be prompted to login by the home page but the other pages will trigger a login request:



Number of Drill Bits	4
Bit #0	10.0.1.10 initialized
Bit #1	10.0.1.8 initialized
Bit #2	10.0.1.7 initialized
Bit #3	10.0.1.9 initialized
Data Port Address	10.0.1.7:31012
User Port Address	10.0.1.7:31010
Control Port Address	10.0.1.7:31011
Maximum Direct Memory	8,589,934,592

(https://msdnshared.blob.core.windows.net/media/2016/06/2016-06-10_15-04-21.png)