Ingesting External Data Feeds

Before beginning this procedure, you'll need the URL to an open-source data feed. Illustrations on this page use https://ransomwaretracker.abuse.ch/feeds/csv/ to serve as a representative example.

Process

1. Open the open-source data feed.
2. Identify the column heads and separation symbol.

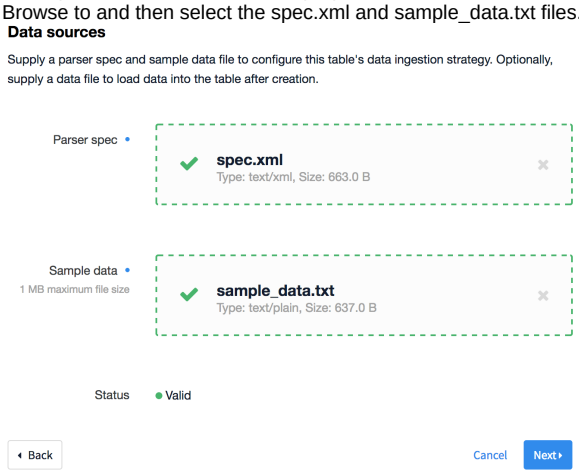
Column Heads:	Separation Symbol:
Firstseen (UTC), Threat, Malware, Host, URL, Status, Registrar, IP address(es), ASN(s), Country	comma

3. In your favorite text-edit application, update spec.xml to contain the column heads you need. Your updated xml file should look similar to this:

```
<specification xmlns="http://www.xl5software.com/schemas/pds/1.0">
  <pipeline name="ransomware">
    <delimited-parser field-separator="," quote="&quot;" skip-header-rows="1" escape="\">
      <fields>
<field name="firstseen" type="string"/>
<field name="threat" type="string"/>
<field name="malware" type="string"/>
<field name="host" type="string"/>
<field name="url" type="string"/>
<field name="status" type="string"/>
<field name="registrar" type="string"/>
<field name="ip_address" type="string"/>
<field name="asn" type="string"/>
<field name="country" type="string"/>
</fields>
</delimited-parser>
</pipeline>
</specification>
```

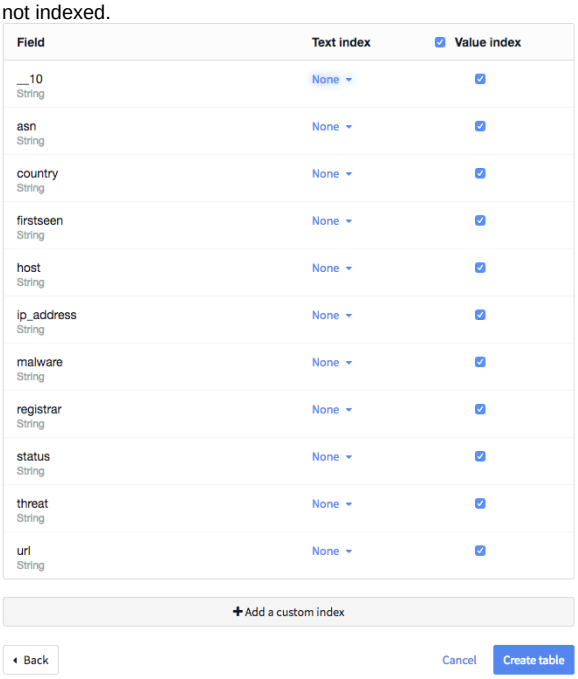
Still in your text-edit application, create a sample_data.txt file like this one that contains one or more rows of data from the feed.

1. Log in to Asset Manager Command Center via your browser interface.
2. Navigate to **Settings >Tables > Add Table.**
3. In the Name field, enter a descriptive name for the table you are creating such as ransomware_tracker_feed.
4. In the Table Type field, select **Managed Primary Table**.
5. At your option, you can add Tags to help other Asset Manager users to find the table and a Description to let others know the purpose of the table.
6. Browse to and then select the spec.xml and sample_data.txt files.



7. Click **Next**.
   The column headings for your table display, ordered alphabetically. Review the values listed in the Field column to confirm that they match your spec.xml.

8. Click the **Value Index** checkbox for those fields you want to HDFS to index immediately. If you do not check any items in the Value Index column, your table with still be created–just not indexed.



9. Click **Create Table**.
   The table structure is created in the Asset Manager's HDFS data store.

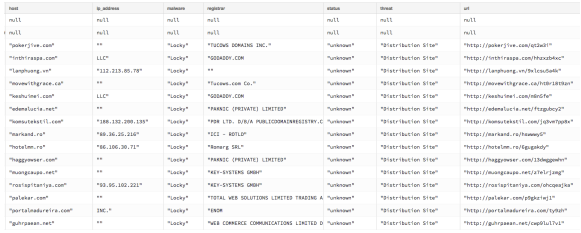
1. Log in to the CLI of your Asset Manager Command Center.
2. At the command-line prompt, enter **`support db`**.
   You now have access to Asset Manager's PostgreSQL database.
3. Insert the feed details into Asset Manager's PostgreSQL database using the Insert command. The labels will remain the same from feed to feed. The values for each label will need to be customizer for your feed. Here's a sample entry:
   `insert into system.feed(name, shortname, enabled, overwrite, url, key, filename, tablename, pipelinename, pollinterval) values ('ransomware-tracker', 'ransomware', true, true, 'https://ransomwaretracker.abuse.ch', '','/feeds/csv/', 'Asset Manager.public.ransomware_tracker_feed', 'ransomware',1440);`
4. Make sure the insertion was received by entering
   `select * from system.feed where name ='ransomware-tracker';`
   A response similar to this one indicates that Asset Manager's database has received the insertion.

5. To validate the connection, restart the Asset Manager-api service by entering:
   `support service api restart`

The feed will begin to populate and records will very soon be available in the Asset Manager GUI.

1. In the Asset Manager GUI, browse to **Settings** > **Tables**.
2. Select the **ransomware_tracker_feed** table.
3. Check the number of records present to confirm that the database has been populated.

4. Click **View**.



host	ip_address	malware	registrar	status	threat	url
null	null	null	null	null	null	null
null	null	null	null	null	null	null
"jokerjive.com"	""	"Locky"	"TUCOWS DOMAINS INC."	"unknown"	"Distribution Site"	"http://jokerjive.com/qt2w3t"
"inthirsapa.com"	LLC"	"Locky"	"GODADDY.COM	"unknown"	"Distribution Site"	"http://inthirsapa.com/hhxxubk4xc"
"lanphuong.vn"	"112.213.89.78"	"Locky"	""	"unknown"	"Distribution Site"	"http://lanphuong.vn/9xlcou5w4k"
"movewithgrace.ca"	""	"Locky"	"Tucows.com Co."	"unknown"	"Distribution Site"	"http://movewithgrace.ca/ht0r18t9xn"
"woshuine1.com"	LLC"	"Locky"	"GODADDY.COM	"unknown"	"Distribution Site"	"http://woshuine1.com/n6nGfe"
"edemalucia.net"	""	"Locky"	"PANAIC (PRIVATE) LIMITED"	"unknown"	"Distribution Site"	"http://edemalucia.net/ftzgubcy2"
"womusteksti1.com"	"188.132.209.135"	"Locky"	"PDR LTD. D/B/A PUBLICDOMAINREGISTRY.C	"unknown"	"Distribution Site"	"http://womusteksti1.com/jq3vm7pp8x"
"markand.ro"	"69.16.25.216"	"Locky"	"ICI - ROTLD"	"unknown"	"Distribution Site"	"http://markand.ro/hawwwyG"
"hotelmn.ro"	"86.106.30.71"	"Locky"	"Bonarg SRL"	"unknown"	"Distribution Site"	"http://hotelmn.ro/EguguHoV"
"haggzmwser.com"	""	"Locky"	"PANAIC (PRIVATE) LIMITED"	"unknown"	"Distribution Site"	"http://haggzmwser.com/1hdwggpwhv"
"nuungzaupa.net"	""	"Locky"	"KEY-SYSTEMS GMBH"	"unknown"	"Distribution Site"	"http://nuungzaupa.net/z7mlrjaag"
"roktaptarya.com"	"93.95.102.221"	"Locky"	"KEY-SYSTEMS GMBH"	"unknown"	"Distribution Site"	"http://roktaptarya.com/dhcqeqjwa"
"palekar.com"	""	"Locky"	"TOTAL WEB SOLUTIONS LIMITED TRADING A	"unknown"	"Distribution Site"	"http://palekar.com/p0gkaiwjl"
"portalnadurelra.com"	INC."	"Locky"	"ENOM	"unknown"	"Distribution Site"	"http://portalnadurelra.com/ty9zh"
"guhrpaean.net"	""	"Locky"	"WEB COMMERCE COMMUNICATIONS LIMITED D	"unknown"	"Distribution Site"	"http://guhrpaean.net/cwp9lulTvi"

Congratulations! The table displays. Asset Manager has ingested an external data feed.

Hooray! You now have Asset Manager to ingest a feed of external data.