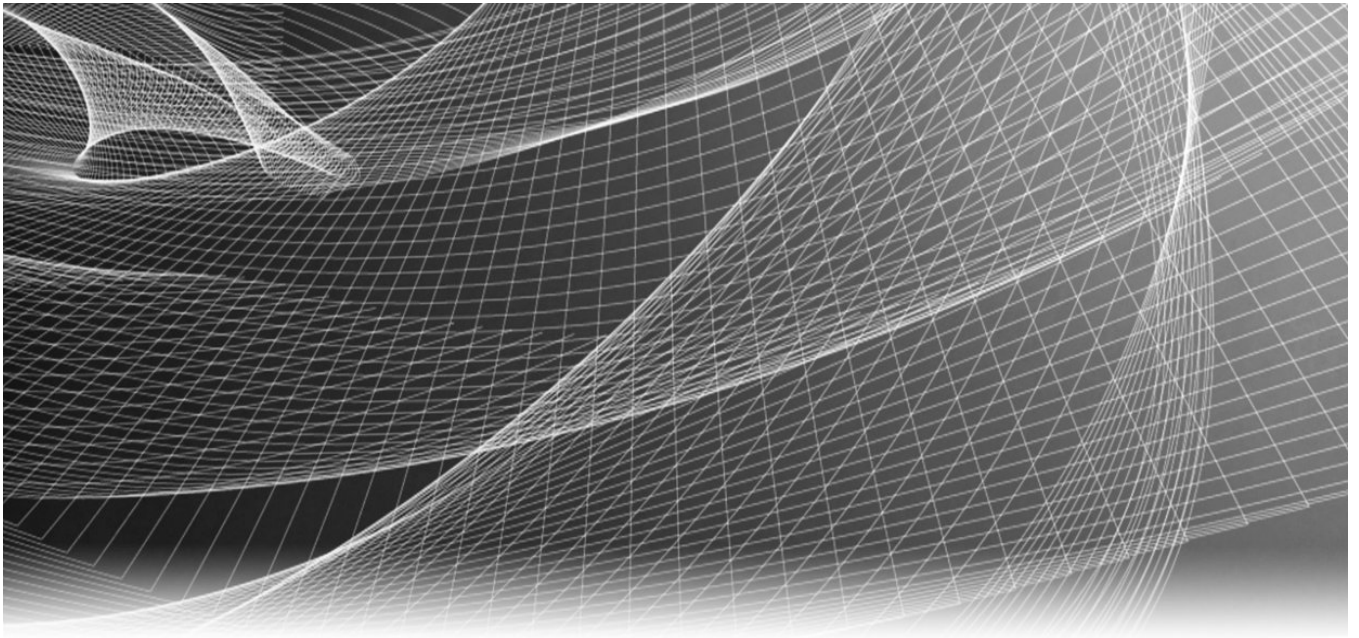




EMC® Watch4net®

SolutionPack for Traffic Flows: Administration Guide

EMC²

TABLE OF CONTENTS

1	Introduction	3
1.1	Document Purpose	3
1.1	Document Scope	3
2	Pre-Requisites	3
3	Features	3
4	Architecture and Scalability	4
4.1	Architecture	4
4.2	Flow Processing	5
4.3	Minimum Specification	5
5	Installation	6
6	Upgrading	10
7	Known Issues	14

1 Introduction

1.1 Document Purpose

This document is to serve as a guide to installing and making operational the EMC Watch4Net SolutionPack for Traffic Flows.

1.1 Document Scope

- Pre-requisites for installation
- Installation and upgrade procedure
- Known Issues

2 Pre-Requisites

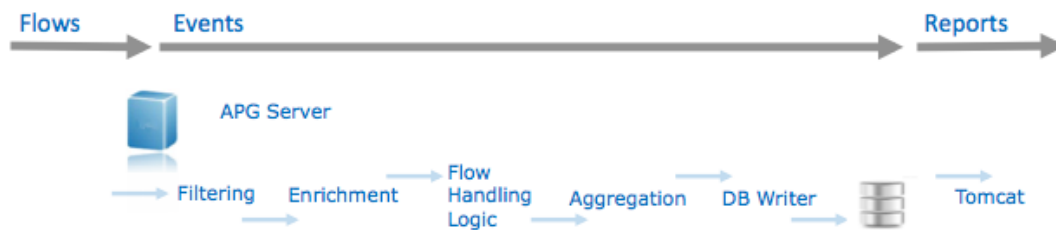
- APG 6.4: Incremental features in the platform have been leveraged and so this is the minimum build recommended for this SolutionPack.
- Valid SolutionPack and flow listener licenses
- Known port that flows will be sent to: This can be configured both at install time and easily corrected later if not known up front by editing the configuration file.
- Exporter devices managed in APG as Routers: These must be managed as device type of 'Router' for the solution to function properly.
- W4N Health SolutionPack installed: To obtain statistics on the number of traffic flows that are seen at the interface, this external solution pack is required.

3 Features

The Solution Pack for Traffic Flows currently supports the following;

- Support for Netflow v5 and v9
- IPFIX (v10) Support
- NSEL Support
- Exporter and interface search
- Managed host search
- Spatial aggregation: per IP address by default and also configurable
- Temporal aggregation:
 - 5 minute – Event based aggregation for (protocol, application, source/destination, conversation, host)
 - 5 minute – Time Series for the following metrics (nbFlows, nbBytes, nbPackets)
- TopN at the collection layer where N is configurable at installation time
- Flow stats (applications) for managed hosts (via ICMP/SNMP/other protocols)

4.2 Flow Processing



4.3 Minimum Specification

The minimum Specification for 10,000 flows/sec solution

- 3 GHz Dual-processor server
- 32GB Ram
- 100GB (OS and Application) Disk
- Separate 1TB Flow storage

5 Installation

- Add the license from “Centralised Management” within APG
- There are 3 Solution Pack Blocks to be configured as part of the installation of Flow Solution Pack;
 - Events
 - Database
 - Reports
- Install the solution pack from the Solution Pack Centre in APG
- Enter requisite details for the configuration of the Solution Pack making sure to enter “Default” for the value of Datastore web instance
- Proceed with the installation once all inputs have been given

Browse and Install SolutionPacks

SAP Traffic Flows v0.10

Flow Collection v0.10
Collection and processing of traffic flows from the defined collection port

Data collection
Select options for the collected data, including destination for storage.

- * Hostname or IP address to send data to: localhost
- * Network port to send data to: 2020
- * Please select the Gateway: localhost:48443
- * Datastore Web-Service Instance: -Custom instance- Default

APG Property Store configuration
Selection configuration option for the APG Property Store.

- * APG WebService hostname or IP address: localhost
- * APG WebService port number: 50080
- * APG WebService username: admin
- * APG WebService password: *****

Traffic Flow SolutionPack
Traffic Flow SolutionPack covering Netflow and Sflow

Listener configuration
Port must be unique, and available. Default for NetFlow is 2055 (or sometimes 9555, 9556), sFlow is 6343. If using a privileged port on Unix systems, make sure to run the service as root. See documentation for more details.

Back Next

Post-Installation steps

Following the installation of the Flow Solution Pack, the following steps must be undertaken in this order.

1. Start the Flow Database
2. Create Flow Tables
3. Start EPM service
4. Edit Common front-end files
5. Restart Tomcat



Note: Assuming the installation path is **/opt/APG**, otherwise replace command strings with appropriate APG installation path.

1. Start The Flow Database

Execute the following;

```
/opt/APG/bin/manage-modules.sh service start datastore Default
```

2. Create Flow Tables



Note: The instance name was chosen during the installation of the solution pack and if not changed manually, will default to “**generic-traffic-flow**”

Execute the following;

(WINDOWS) Navigate to **APG\Event-Processing\APG-Datastore-Writer\<instance name>\ddl** and edit the file **flow-setup-db.ddl** in notepad+ or similar. Highlight all text and copy, either from the menu or by using CTRL+C.

Navigate to **APG\Databases\APG-Datastore\Default\bin** and run the script to connect to the datastore.

```
datastore-client.cmd
```

At the “SQL>” prompt, paste the contents of the buffer by using CTRL+V.

(LINUX) Navigate to **/opt/APG/Event-Processing/APG-Datastore-Writer/<instance name>/ddl/**

```
/opt/APG/Databases/APG-Datastore/Default/bin/datastore-client.sh < flow-setup-db.ddl
```

You can check that this process was successful by executing the following

```
/opt/APG/Databases/APG-Datastore/Default/bin/datastore-client.sh
```

This should provide a SQL prompt like the following.

```
Welcome to APG-Datastore 5.0 CLI (Ctrl+D to exit).  
Connected to jdbc:x100://localhost:50358/ !  
sql>
```

To test if the database tables were correctly installed, you can execute the following command: **.tables;**

```
|
```

Connected to idbc:x100://localhost:50678/ !

```
sql> .tables;
```

[illegible]

Note: Starting the EPM service will start flow data collection. If the exporters are not already managed in the APG Time-series performance database, then they will **only** appear in the reports as unmanaged, in a small section of the product reserved for counting flows from routers not currently being managed by SNMP.

It is therefore best practice to discover the flow exporters into APG via SNMP first, before starting the EPM service.

At this stage, to start flow data collection, execute the following.

```
/opt/APG/bin/manage-modules.sh service start event-processing-manager <instance>
```



Note: Log files are located in the following path: **/opt/APG/Event-Processing/Event-Processing-Manager/<instance name>/logs** and it can be a good idea to tail the most recent log file (processing-0-0.log) to check that the service has started.

```
INFO    -- [2013-12-16 08:13:55 EST] -- HttpServer$Service::publish(): Publishing
com.watch4net.events.processing.manager.webservice.impl.EventProcessingManager@46f0bf3d at /...
INFO    -- [2013-12-16 08:13:55 EST] -- RuntimeModeler::getRequestWrapperClass(): Dynamically
creating request wrapper Class com.watch4net.events.processing.manager.webservice.jaxws.GetComponents
INFO    -- [2013-12-16 08:13:55 EST] -- RuntimeModeler::getResponseWrapperClass(): Dynamically
creating response wrapper bean Class
com.watch4net.events.processing.manager.webservice.jaxws.GetComponentsResponse
INFO    -- [2013-12-16 08:13:55 EST] -- HttpServer::start(): Starting web service server at
/127.0.0.1:59064 (http)...
INFO    -- [2013-12-16 08:13:55 EST] -- HttpServer::start(): Writing service identification in
/opt/APG/Event-Processing/Event-Processing-Manager/flow/.webservice
INFO    -- [2013-12-16 08:13:55 EST] -- Bootstrap::start(): Processing manager started !
```

The following warnings can be ignored.

```
WARNING -- [2013-12-16 08:13:50 EST] -- ComponentClassLoader::init(): Component type
EventPropertyTagger is deprecated, please update your Event-Processing-Manager configuration to use
Event-Property-Tagger instead !
```

5. Edit the Front-End files

Navigate to **/opt/APG/Web-Servers/Tomcat/Default/conf** and edit the file `server.xml` and uncomment the following section by removing the quotes in yellow.

```
<!-- Defines the connection to the APG Traffic Flow database for APG Datastore. -->
<!--
    <Resource name="jdbc/FLOW-TF-DATA" auth="Container" type="javax.sql.DataSource"
maxActive="10"
    maxIdle="10" validationQuery="SELECT 1" testOnBorrow="false" testWhileIdle="true"
timeBetweenEvictionRunsMillis="10000" minEvictableIdleTimeMillis="60000"
maxWait="10000"
    username="admin" password="changeme" driverClassName="com.watch4net.x100.jdbc.Driver"
removeAbandoned="true" removeAbandonedTimeout="60" logAbandoned="true"
url="jdbc:x100://localhost:48443/Databases/APG-Datastore" />
-->
```

Navigate to **/opt/APG/Web-Servers/Tomcat/Default/conf/Catalina/localhost** and edit the file `APG.xml` and uncomment the following section by removing the quotes in yellow.

```
<!-- Gives access to the Traffic Flow data. -->
<!--
    <ResourceLink name="jdbc/FLOW-TF-DATA:{ mapping=FLOW-TF-DATA.xml,
table=FLOW_RAW_DATA_SEQ_0_4 }" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
```

```

<ResourceLink name="jdbc/FLOW-TF-PROTO:{ mapping=FLOW-TF-PROTO.xml,
table=FLOW_PROTOCOL_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-TF-APP:{ mapping=FLOW-TF-APP.xml,
table=FLOW_APPLICATION_TOPN_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-TF-SRCADDR:{ mapping=FLOW-TF-SRCADDR.xml,
table=FLOW_SRCADDR_TOPN_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-TF-DSTADDR:{ mapping=FLOW-TF-DSTADDR.xml,
table=FLOW_DSTADDR_TOPN_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-TF-CONV:{ mapping=FLOW-TF-CONV.xml,
table=FLOW_CONVERSATION_TOPN_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-TF-HOSTS:{ mapping=FLOW-TF-HOSTS.xml,
table=FLOW_HOSTS_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />
<ResourceLink name="jdbc/FLOW-TF-NOSNMP:{ mapping=FLOW-TF-NOSNMP.xml,
table=FLOW_NOSNMP_SEQ_0_4__}" global="jdbc/FLOW-TF-DATA" type="javax.sql.DataSource" />

```

-->

6. Restart Tomcat

Execute the following;

```
/opt/APG/bin/manage-modules.sh service restart tomcat Default
```

6 Upgrading

Summary of steps

To migrate from the SolutionPack for Traffic Flows v1.0 to v2.0

- Stop the EPM service
- Navigate to datastore Default instance CLI and connect using datastore-client.sh
- Modify tables.
- Load new v2.0 package from centralised management if not part of core build
- Update each solution pack block starting with the database, reports then collection
- Restart EPM
- Restart tomcat



Note: DSCP data from previous installation cannot be kept as part of this migration

1. Stopping the EPM Service

Execute the following;

```
/opt/APG/bin/manage-modules.sh service stop event-processing-manager <instance>
```



Note: <instance> will be either “generic-traffic-flow” or whatever was specified at installation time.

2. Starting the Datastore CLI

Execute the following;

Navigate to **APG\Databases\APG-Datastore\Default\bin** and run the script to connect to the datastore.

```
WIN
datastore-client.cmd

LINUX
Datastore-client.sh
```

You should have a “SQL>” prompt with no errors

3. Modify Flow Data in Datastore

Copy and paste the following SQL commands into the Datastore client window and ensure return is pressed and the prompt returns to “SQL>”

```
CREATE TABLE `FLOW_ALLPORTS__SEQ_0_4__` (  
  `TMSTMP` INTEGER,  
  `FLOWID` BIGINT,  
  `PKTSIN` BIGINT,  
  `PKTSOUT` BIGINT,  
  `PKTS` BIGINT,  
  `BYTESIN` BIGINT,  
  `BYTESOUT` BIGINT,  
  `BYTES` BIGINT,  
  `ROUTER_SRC` BIGINT,  
  `INTERFACE` INTEGER,  
  `PROTOCOL` SMALLINT,  
  `L4_SRC_PORT` INTEGER,  
  `L4_DST_PORT` INTEGER,  
  `PORT` INTEGER,  
  `IF_NAME` VARCHAR(128),  
  `IF_DESC` VARCHAR(128),  
  `APPLICATION_NAME` VARCHAR(128),  
  `APPLICATION_DESC` VARCHAR(128),  
  `ROUTER_SRC_NAME` VARCHAR(128),  
  `SNMP_NAME` VARCHAR(128),  
  `IP_TOS` SMALLINT,  
  `DSCP` SMALLINT,  
  `DSCP_ECN` SMALLINT  
);  
  
ALTER TABLE `FLOW_PROTOCOL__SEQ_0_4__` DROP `IP_TOS`;  
ALTER TABLE `FLOW_PROTOCOL__SEQ_0_4__` DROP `DSCP`;  
ALTER TABLE `FLOW_PROTOCOL__SEQ_0_4__` DROP `DSCP_ECN`;  
  
ALTER TABLE `FLOW_APPLICATION_TOPN__SEQ_0_4__` ADD `IP_TOS` SMALLINT;  
ALTER TABLE `FLOW_APPLICATION_TOPN__SEQ_0_4__` ADD `DSCP` SMALLINT;  
ALTER TABLE `FLOW_APPLICATION_TOPN__SEQ_0_4__` ADD `DSCP_ECN` SMALLINT;  
  
ALTER TABLE `FLOW_CONVERSATION_TOPN__SEQ_0_4__` ADD `IP_TOS` SMALLINT;  
ALTER TABLE `FLOW_CONVERSATION_TOPN__SEQ_0_4__` ADD `DSCP` SMALLINT;  
ALTER TABLE `FLOW_CONVERSATION_TOPN__SEQ_0_4__` ADD `DSCP_ECN` SMALLINT  
;
```

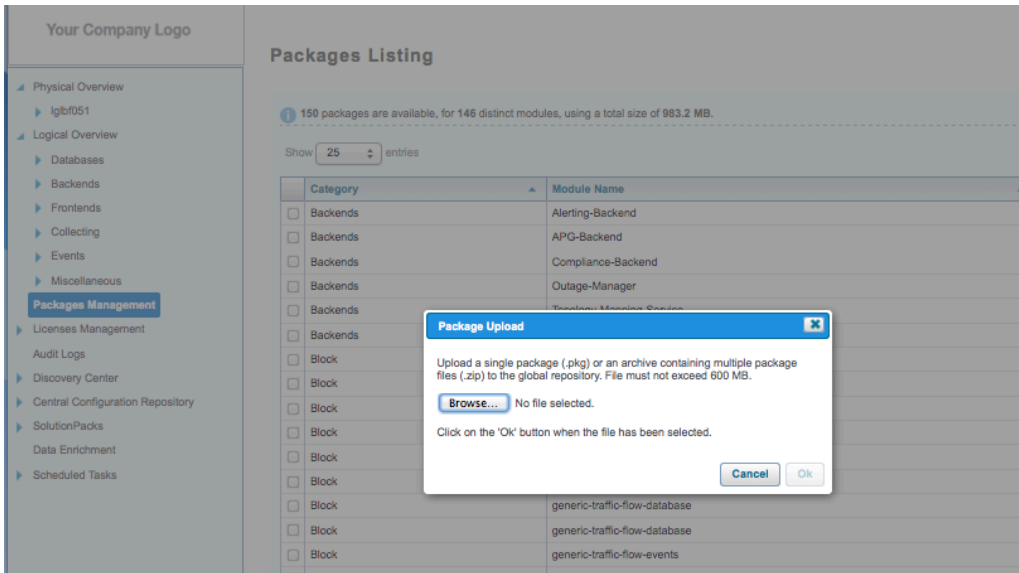
You should have a “SQL>” prompt with no errors



Note: This text is shipped in a migration file called “migrate-flow-db.ddl” with the v2.0 build and can be found in the ddl folder described above.

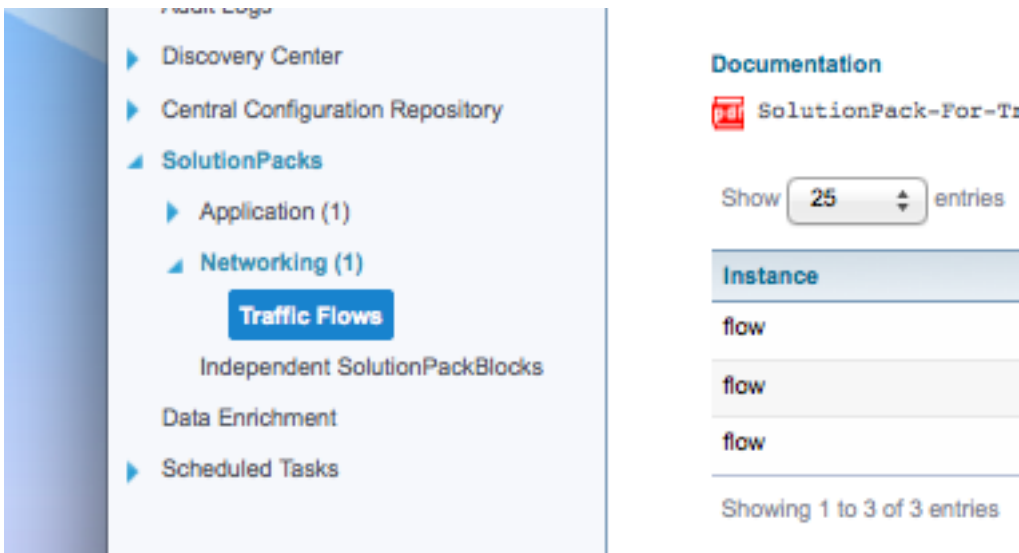
4. Load new package

From packages management load the new v2.0 package if not shipped with the version of w4n.



5. Update the SolutionPack to v2.0

Select the “update” icon from within the SolutionPack section of centralised management, and first update the database, then the reports and last the flow collection block.



6. Start EPM Service



Note: Starting the EPM service will start flow data collection.

At this stage, to start flow data collection, execute the following.

```
/opt/APG/bin/manage-modules.sh service start event-processing-manager <instance>
```



Note: Log files are located in the following path: **APG/Event-Processing/Event-Processing-Manager/<instance name>/logs** and it can be a good idea to tail the most recent log file (processing-0-0.log) to check that the service has started.

```
INFO    -- [2013-12-16 08:13:55 EST] -- HttpServer$Service::publish(): Publishing
com.watch4net.events.processing.manager.webservice.impl.EventProcessingManager@46f0bf3d at /...
INFO    -- [2013-12-16 08:13:55 EST] -- RuntimeModeler::getRequestWrapperClass(): Dynamically
creating request wrapper Class com.watch4net.events.processing.manager.webservice.jaxws.GetComponents
INFO    -- [2013-12-16 08:13:55 EST] -- RuntimeModeler::getResponseWrapperClass(): Dynamically
creating response wrapper bean Class
com.watch4net.events.processing.manager.webservice.jaxws.GetComponentsResponse
INFO    -- [2013-12-16 08:13:55 EST] -- HttpServer::start(): Starting web service server at
/127.0.0.1:59064 (http)...
INFO    -- [2013-12-16 08:13:55 EST] -- HttpServer::start(): Writing service identification in
/opt/APG/Event-Processing/Event-Processing-Manager/flow/.webservice
INFO    -- [2013-12-16 08:13:55 EST] -- Bootstrap::start(): Processing manager started !
```

6. Restart Tomcat

To restart tomcat execute the following then restart any browsers open with a connection to w4n.

```
/opt/APG/bin/manage-modules.sh service restart tomcat
```

7 Known Issues

- Installation database provisioning: The Flow database must be provisioned manually as described in this document. It is not the desired solution and will be addressed in a future release.
- Distribution of flow SP components: This is not supported yet as part of the automated installer
- Data Migration from v1.0 of the SolutionPack to v2.0 is supported but only following the steps listed here but DSCP data will not be migrated as part of the process. DSCP data will start collecting automatically once the EPM is restarted though.