Delphix enables self-monitoring/diagnosability of Delphix Engines by providing native integration with Splunk Enterprise.

Prerequisites

1. The Splunk Host IP address.
2. Enable the HEC Port number on your Splunk instance (default 8088)
3. Enable SSL (this is optional but recommended)
4. Enable the HTTP Event Collector on Splunk, and create a new HEC token with a new Splunk index set as an allowed index for the token. Make sure Enable Indexer Acknowledgement is unchecked for the token.

Configuring Delphix for Splunk

1. Log in to the Delphix Server Setup UI as the sysadmin.
2. From the Preferences menu select Splunk Configuration.
3. In the Splunk Configuration window, enter your Splunk values. To reduce the volume of data that will be sent to Splunk, you can optionally uncheck Enable Metrics.
4. Click Send Test Data to verify your provided values. This will send a test event to the provided token and indexes.
5. Click Save to enable the Splunk configuration and begin sending all new Actions, Job Events, Faults, Alerts, and Metrics to your Splunk instance.

The Delphix Dashboard in Splunk

The customizable default Delphix dashboard provides a single level view of data of all your Delphix Engines. The Delphix Engine and Splunk integration enables the development of a Delphix application that is available through Splunkbase.

Configure dxtoolkit (Optional)

1) Install dxtoolkit2

2) Create directory to generate dxtoolkit output and feed to splunk server.
 mkdir /home/delphix/splunkfeed

3) Schedule dxtoolkit scripts in cron to monitor and generate output files to be consumed by splunk.

Configure Splunk Forwarder
1) Install splunk forwarder on any host
 tar xvfz splunkforwarder-7.2.3-06d57c595b80-Linux-x86_64.tgz -C /opt
 cd $SPLUNK_HOME/bin
 ./splunk start --accept-license

2) Configure receiving indexer
  ./splunk add forward-server <splunk_server>:<receiving_port>
  e.g. ./splunk add forward-server 10.10.10.135:9997

3) Add monitor and forward logfiles to index server
 ./splunk add monitor "/home/delphix/splunkfeed/dx_get_appliance.csv" -sourcetype dx_get_appliance -index delphix_dxtoolkit
 ./splunk add monitor "/home/delphix/splunkfeed/dx_get_db_env.csv" -sourcetype dx_get_db_env -index delphix_dxtoolkit
 ./splunk add monitor "/home/delphix/splunkfeed/dx_get_env.csv" -sourcetype dx_get_env -index delphix_dxtoolkit
 ./splunk add monitor "/home/delphix/splunkfeed/dx_get_audit.csv" -sourcetype dx_get_audit -index delphix_dxtoolkit

4) Restart Splunk Forwarder
 ./splunk restart

ajay.thotangare [12:23 PM]
Splunk Server
1) create 4 source types which will be copy of existing csv types
 dx_get_appliance, dx_get_db_env, dx_get_env, dx_get_audit

2) Enable receiving port
default : 9997

3) Ensure index exists delphix_dxtoolkit. If not create it.

4) create field transformation for csv files received.
dx_get_appliance.csv - timestamp,appliance,status,version,total_GB,used_GB,free_GB,used_PCT,dsource_count,vdb_count,total_objs
dx_get_db_env.csv - timestamp,appliance,hostname_ip,database_name,dlpx_group,obj_type,source_db,parent_snapshot,used_gb,db_status,enabled,unq_name,parent_time,vdb_creation_time
dx_get_env.csv - timestamp,appliance,env_name,os_type,env_status,os_version