(U//FOUO) DEEPDIVE Configuration Read Me

(U) Overview

(C) The purpose of this document is to provide procedures to configure an XKEYSCORE server as a DEEPDIVE server. DEEPDIVE can be defined as featuring a filter in front of the traditional XKEYSCORE processor (back-end). It is a Federated Query system that has a rolling buffer of all unfiltered data processed by XKEYSCORE. One query scans all sites.

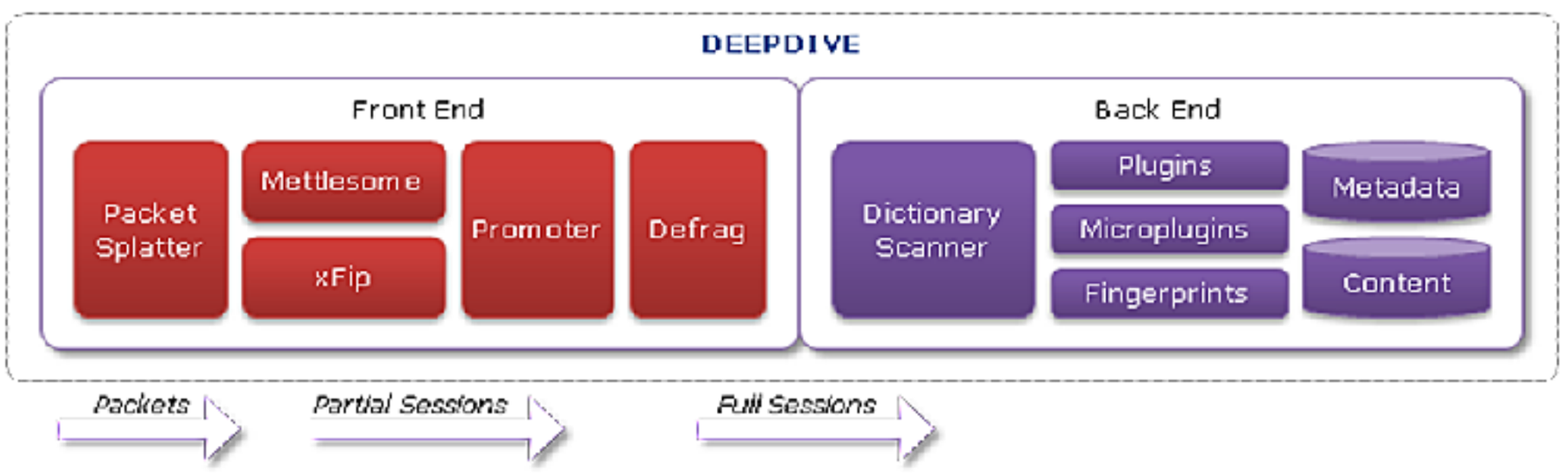
(U//FOUO) DEEPDIVE has two distinct functions. The Front End ingests various input types (e.g., .pcap, .sff, Ethernet, sdh, and sotf packets), sessionizes the data and promotes the data to the Back End. The backend can also ingest different input types and uses tools such as packet_splatter, xks_xfip (a Fast IP sessionizer), METTLESOME, PROMOTER (optional), defrag, and sotf_output.

(C) The DEEPDIVE Back End performs strong (e-mail) and soft (content) selection and provides real-time tipping. It uses GENESIS Appid/Fingerprints which are updated hourly to all accessible field sites. An appid identifies a specific protocol and details of a session. Fingerprints flag sessions that meet specific criteria.

(U//FOUO) DEEPDIVE Dataflow

(U//FOUO) Data packets "enter" DEEPDIVE's front-end, are processed and are fully sessionized before being passed to the back-end. The data is then analyzed, processed and released or stored as the mission dictates.

(C)



(C)

(U//FOUO) XKS Deep Dive can be configured differently at each site depending on the priorities of your mission.

(U//FOUO) Configuring DEEPDIVE for MINUTEMAN in *xks.config*

(U//FOUO) Use these configurations if your front-end system is outputting SOTF packets only to an XKS DEEPDIVE. If this is the case, then follow these steps to configure DEEPDIVE for the MINUTEMAN program only after XKEYSCORE software has been installed:

1. (U) Logon as the user `oper`.
2. (U//FOUO) At the command line from within any directory, type `viconfig` and then press `Enter`. The *xks.config* file will open.
3. (U//FOUO) In the *Signal Acquisition configuration* section of *xks.config*, confirm:

   a. `signal_acquisition_enable = yes` **:** By setting this option to yes, signal_acquisition processes and any associated configurations will be added to proc_resources.

   b. `signal_acquisition_on_master = yes` **:** This creates a `signal_acquisition_base` on the Master.

   c. `have_promoter = false` **:** This indicates no promoter is configured for the system.

   d. splatter_hosts = [master_hostname]

   In this case, `master_hostname` is the actual hostname of the Master server. Setting `splatter_hosts` equal to `master_hostname` indicates that the master is the only back-end host to receive the SOTF file (e.g., xks01, xks02, etc.).

4. (C) In the *[signal acquisition]* section of *xks.config,* type:

   ```
   signal_acquisition[%:base] = sigad = US-XXX, config =
   signal_acquisition.config, front_end_only = False
   ```

   (C) In this case, the commas separate three options:

   - `[%:base] = sigad = US-XXX` : This creates a `signal_acquisition_base` process on each host in the XKS cluster and configures each to the US SIGAD (XXX) that is carrying the data.

     Important: (U//FOUO) On each host, do not forget to change `master_hostname` to the appropriate Master server hostname.

   - `Config = signal_acquisition.config` : Sets the configuration file to $XSCORE_DIR/config/signal_acquisition/signal_acquisition.config

   - `front_end_only = False` **:** Indicates the host will act as both a front-end and a back-end host.

5. (U//FOUO) Type `:wq!` and then press `Enter` to save and exit *xks.config*. You will now configure *signal_acquisition.config*.

(U//FOUO) Completing the Configuration of DEEPDIVE for MINUTEMAN

(U//FOUO) To complete the configuration of DEEPDIVE for MINUTEMAN, be sure to configure *signal_acquisition.config*:

1. (U//FOUO) At the command line from within any directory, type `sa-config` and then press `Enter`. This will take you to $XSCORE/config/signal_acquisition.

2. (U//FOUO) Open *signal_acquisition.config,* or create a file by that name if it does not already exist. This file will be used to configure several front-end processes for ingesting, sessionizing, and reassembling data. Each process is described in the following table.

   (U//FOUO)

Front-End Processes		
What It's Called	**What It Does**	**What It Means**
Packet Splatter	Ingests packets (from files, from the network, from a capture card) in a variety of formats.	If it's a packet stream, it can probably be fed into a DEEPDIVE.
xFip	Fast reassembly of TCP/IPv4 and UDP/IPv4 streams*.	DEEPDIVE sessionizes **everything** before making a keep/drop decision.
METTLESOME	Reassembly of streams from less common protocol stacks.	
Promoter	Rule-based filtering of reassembled sessions, based on keyword, country code or appid/fingerprint.	DEEPDIVE intelligently chooses the most useful traffic for retention.
Defrag	Fully rebuilds sessions**	Enough content available to do full decoding/document descent at the Back End
*up to a 256K limit **up to a 10MB limit		

   (U//FOUO)

   Note: (U//FOUO) In this Read Me, we will not address the Promoter.

3. (U//FOUO) In the *signal_acquisition.config*, type/edit the following configurations for the processes identified in step 2:

   a. `packet_splatter,-p 23000 --casenotation_source in_channel_sri -i 22000 -t sotf --stats_topic ps_stats -v -n 4 ,isCritical=True,asRoot=True`

   b. `xks_xfip, -f %{SEQ($XSCORE_DIR/config/misc/xfip_auto_inc#.cf)},count=4`

c. `Mettle_tcmalloc, -f %{SEQ($XSCORE_DIR/config/misc/mettle#.cf)},count=4`

d. `xks_defrag,-i %{PORT_IN_INC(24000)} -o 5040,count=4`

4. (U//FOUO) Type `:wq!` and then press `Enter` to save and exit *signal_acquisition.config*.

5. (U//FOUO) Perform the following commands only after making changes to both *signal_acquisition.config* and *xks.config*:

6. (U//FOUO) At the command prompt, type `xks setup processes` and then press `Enter`. This will create signal_acquisition_base on each host in the cluster.

7. (U//FOUO) At the command prompt, type `xks proc start` and then press `Enter`. This will start the newly created processes.

(U//FOUO) Configuring DEEPDIVE for FORNSAT

(U//FOUO) Use these configurations if your front-end system is a TURNWEALTHY and outputting packets, packet bundles, and sessions to an XKS DEEPDIVE. If this is the case, then follow these steps to configure DEEPDIVE for FORNSAT:

1. (U) Logon as the user `oper`.

2. (U//FOUO) At the command line from within any directory, type `viconfig` and then press `Enter`. The *xks.config* file will open.

3. (U//FOUO) In the *#[signal acquisition]* section of *xks.config,* set the following configurations:

   a. `signal_acquisition_enable = yes` : By setting this option to `yes`, `signal_acquisition` processes and associated configurations will be added to `proc_resources`.

   b. `signal_acquisition_on_master = no` : This will not create a `signal_acquisition_base` on the Master.

   c. `have_promoter = false` : This indicates no promoter is configured for the system.

   d. `signal_acquisition[%:base] = casenotation=dynamic,config=generic_packet_to_bundle.config`

(U/FOUO) In the case, the comma separates two options:

- `[%:base] = casenotation=dynamic :` This configures the multiple `signal_acquisition_base` process on all the hosts in the cluster (%).
- `Config = generic_packet_to_bundle.config :` This sets the configuration file to $XSCORE_DIR/config/signal_acquisition/generic_packet_to_bundle.config

  Important: (U/FOUO) If it does not already exist, you must create and configure `generic_packet_to_bundle.config`. See below, *Configuring generic_packet_bundle.config,* for configuration insructions.

4. (U//FOUO) Type `:wq!` and then press `Enter` to save and exit *xks.config*.

Configuring generic_packet_bundle.config

Configuring DEEPDIVE for FORNSAT also requires that you setup the *generic_packet_bundle.config* file:

1. (U//FOUO) At the command line from within any directory, type `sa-config` and then press `Enter`. This will take you to $XSCORE/config/signal_acquisition.
2. (U//FOUO) Open *generic_packet_bundle.config,* or create a file by that name if it does not already exist.
3. (U//FOUO) In the *generic_packet_bundle.config*, type/edit the following configurations for the processes identified in step 2:

   a. `sotf_mux_2,-i 5038 -o 34000 -s 5010,isCritical=True`

   b. `xks_xfip, -f %{SEQ($XSCORE_DIR/config/misc/xfip_generic_packet_to_bundle_auto_inc#.cf)},isCritical=True`

   c. `Mettle tcmalloc,-f %{SEQ($XSCORE_DIR/config/misc/mettle_generic_packet_to_bundle_auto_inc#.cf)},isCritical=True`

   d. `xks_defrag_2,-i 5039 -o 5040,isCritical=True`

4. (U//FOUO) Type `:wq!` and then press `Enter` to save and exit *generic_packet_bundle.config*.

(U) Additional Processes

(U//FOUO) Run these additional processes only after making changes to the configurations in *xks.config*,:

1. (U//FOUO) At the command prompt, type `xks rsync push_config` and press `Enter`. This sets pushes configuration changes out to the slaves.

2. (U//FOUO) At the command prompt, type `xks setup processes` and press `Enter`. This creates the `signal_acquisition_base` process.

3. (U//FOUO) At the command prompt, type `xks proc start` and press `Enter`. This will ensure all of the running processes pick up any configuration changes.