Installation Instructions For Splunk BlackLynx App

BlackLynx technology combines high performance heterogeneous computing (accelerated CPUs, GPUs, and FPGAs) with standard applications and protocols to achieve high performance analytics

Prerequisites
The user ID running all commands in these instructions needs sudo privilege.
Splunk Enterprise is already installed on the Splunk server.
BlackLynx software products (ryftx, ryft-server, ryft-pcap) are already installed on the BlackLynx server.

Firewall requirements
BlackLynx Server
Allow incoming requests to TCP ports 8765, 8080

Splunk Server (or Splunk Search Head in Distributed Splunk Enterprise deployment)
Allow outgoing requests to BlackLynx server's TCP ports 8765, 8080

Unless indicated, all steps are performed on the Splunk Search Head platform (or Splunk standalone instance).

BlackLynx App Install

1. wget https://s3.amazonaws.com/ryft-product-installers/latest/splunk_blacklynx_1.0.3_installer.tgz
2. tar xvzf splunk_blacklynx_1.0.3_installer.tgz
3. If any of the following defaults are different in your situation, edit install_blacklynx_app.sh and modify the script variables as necessary, then save your edits.

Variable Name	Description	Default value
SPLUNK_HOME	Splunk home directory	/opt/splunk
SPLUNK_USERNAME	Splunk home directory owner	splunk
SPLUNK_GROUPNAME	Splunk home directory group name	splunk

4. ./install_blacklynx_app.sh
   Expected final message: "Splunk BlackLynx App installed successfully"

5. Copy rm-tmp-splunk-files onto the **BlackLynx server's** /etc/cron.daily directory (**NOT the Splunk server**).

/etc/hosts

If you do not want to add the BlackLynx server hostname in your Splunk server's /etc/hosts file, skip this section.

1. Edit /etc/hosts
2. Add an entry for the IP address and hostname of the BlackLynx server, then save your edits.

   Example: 10.13.1.12 blsvr1

BlackLynx App Dashboards and Saved Searches
The BlackLynx App installs sample dashboards and saved searches for triggered alerts.
The following steps will point those samples to your BlackLynx server and verify the communications link.

Dashboards & Saved Searches Host Modification

1. Edit mod_search_dash_host.sh

2. Set **BLACKLYNX_HOST** to the hostname or IP address of the BlackLynx server

   Examples:
   a. If BlackLynx server hostname in /etc/hosts is blsvr1
      BLACKLYNX_HOST=blsvr1

   b. BLACKLYNX_HOST=10.13.1.12

3. If any of the following defaults are different in your situation, modify the variables as necessary, then save your edits.

Variable Name	Description	Default value
SPLUNK_HOME	Splunk home directory	/opt/splunk
SPLUNK_USERNAME	Splunk home directory owner	splunk

4. ./mod_search_dash_host.sh
   Expected final message: "Splunk BlackLynx App Saved Searches & Dashboards modified successfully“

Splunk to BlackLynx server Communication Test

1. Edit ck_blsvr_comm.sh

2. Set BLACKLYNX_HOST to the hostname or IP address of the BlackLynx server

3. Save your edits.

4. ./ck_blsvr_comm.sh
   Expected message: "Communications to BlackLynx Server REST interfaces successful"

BlackLynx Server Demo Data
The steps below will install demo data onto the BlackLynx server.
These data sets will allow you to use the sample Splunk BlackLynx App dashboards and Alerts.

BlackLynx Server demo data load

1. Login to the **BlackLynx server** (NOT the Splunk server) as ryftuser

2. wget https://s3.amazonaws.com/ryft-product-installers/latest/splunk_blacklynx_1.0.2_demodata_installer.tgz

3. tar xvzf splunk_blacklynx_1.0.2_demodata_installer.tgz

   WARNING
   The install script will download **6 GB** of demo data from the Amazon S3 repository located in Virginia.
   The total download time depends on the data transfer rate between S3 and the BlackLynx server.

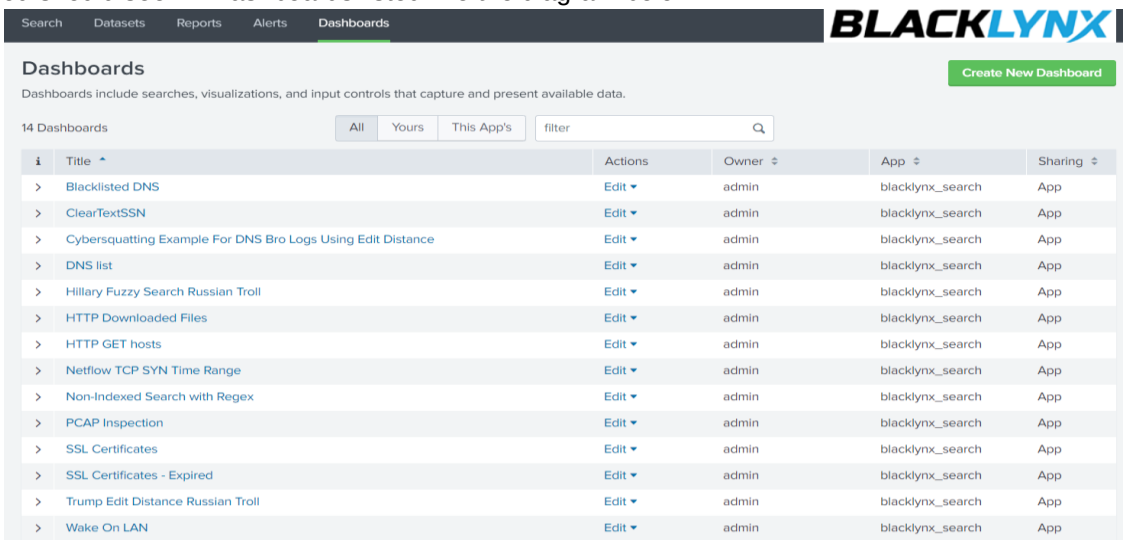
4. ./install_splunk_demodata.sh
   Expected result: "Splunk BlackLynx App Demo Data Sucessfully Installed"

5. ./test_splunk_demodata.sh
   Expected Result: "Number of Tests Run: 13, PASSED: 13"

Dashboards and Alerts
This section tests the sample BlackLynx App Dashboards and Alerts

Dashboard Tests

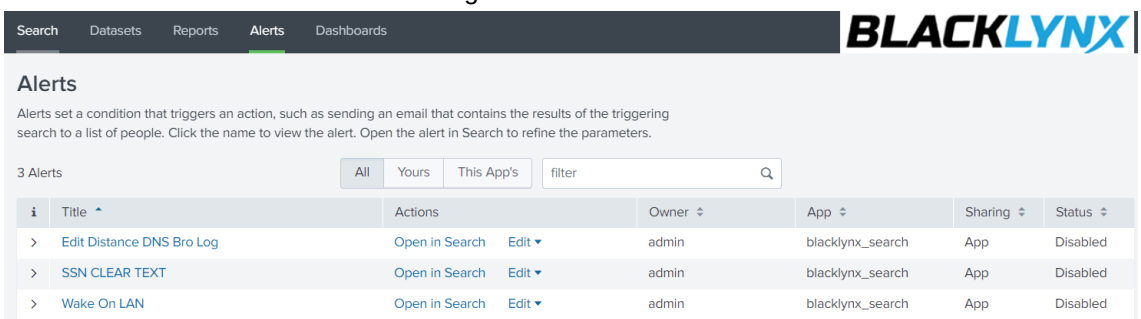
1. Login to the Splunk Web interface (e.g. <Splunk server IP>:8000)
2. Navigate to the BlackLynx search App.
3. Navigate to the BlackLynx search App Dashboards page.
   You should see 14 Dashboards listed like the diagram below.



4. Click each dashboard. Verify that query results appear. NOTE: The **Pcap Inspection** dashboard requires pressing the **Submit** button.

Alerts Tests

1. From the Splunk Web interface, navigate to the BlackLynx search App Alerts page.
   You should see 3 alerts listed like the diagram below.



2. Enable the “Edit Distance DNS Bro Log”, "SSN CLEAR TEXT" and "Wake On LAN" alerts.
3. Wait 5 minutes.
4. Navigate to the Triggered Alerts page for the BlackLynx search App.
5. A Triggered alert should appear for “Edit Distance DNS Bro Log”, “SSN CLEAR TEXT” and “Wake On LAN”.
6. **NOTE:** These alerts are scheduled to run every minute via cron. Disable these alerts if so desired.