Splunk Stream™ Installation and Configuration Manual 7.2.0

Configure 10Gbps network capture

Generated: 12/25/2019 10:57 am
Configure 10Gbps network capture

To ensure efficient data capture with minimal packet loss over high-volume 10Gb network interfaces, Splunk Stream lets you deploy an alternate Stream forwarder, which supports 10Gbps data capture on compatible network interfaces. Stream uses 18.11.1 version of dpdk library.

This page shows you how to optimize your Linux environment and configure Stream forwarder to enable 10Gbps data capture on compatible devices.

Operating system and permissions requirements

- Dedicated 10Gb capture mode is supported on 64-bit Linux platforms (kernel version 3.10.0 or later). For information on supported NICS, see http://dpdk.org/doc/nics.
- You must be a root user of your Splunk platform deployment to run streamfwd in dedicated capture mode.

Dedicated 10Gb capture mode has been tested on CentOS/RHEL only.

Optimize Linux environment

For best results with dedicated capture mode, update your kernel boot parameters for hugepages, as follows:

1. Edit /etc/grub.conf.
2. Add these parameters to your kernel boot line to configure sixteen 1GB hugepages: default_hugepagesz=1G hugepagesz=1G hugepages=16. You may need to adjust the number of hugepages to fit your hardware configuration. For example, after adding these parameters, your kernel boot line might look like this:

   ```
   kernel /vmlinuz-2.6.32-573.3.1.el6.x86_64 ro
   root=/dev/mapper/vg_cmload02-lv_root
   rd_LVM_LV=vg_cmload02/lv_root rd_NO_LUKS LANG=en_US.UTF-8
   rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto
   rd_LVM_LV=vg_cmload02/lv_swap KEYBOARDTYPE=pc KEYTABLE=us
   rd_NO_DM default_hugepagesz=1G hugepagesz=1G hugepages=16 rhgb
   quiet
   ```
3. Reboot your linux machine.

Updating kernel boot parameters for dedicated capture mode is optional, though highly recommended.
Configure 10Gb dedicated capture mode

The following configuration steps apply to independent stream forwarder (streamfwd) deployments only. You must be a root user to run streamfwd in dedicated capture mode.

**Step 1: Enable dedicated capture mode in streamfwd.conf**

1. Edit `local/streamfwd.conf`.  
2. Add `dedicatedCaptureMode = 1`. For example:

   ```
   [streamfwd]
   port = 8889
   ipAddr = 127.0.0.1
   dedicatedCaptureMode = 1
   ```
3. Restart Splunk.

**Step 2: Identify compatible interfaces**

Use the `streamfwd --iflist` command to identify the interface on which you want to capture 10Gbps traffic. You can capture packets at 10Gbps on any interface listed under `Dedicated capture mode compatible devices`. For example:

   ```
   # ./linux_x86_64/bin/streamfwd --iflist
   Dedicated capture mode compatible devices
   ================================
   0000:04:00.0 driver=uio_pci_generic if=
   0000:04:00.1 driver=uio_pci_generic if=
   0000:05:00.0 driver=uio_pci_generic if=
   0000:05:00.1 driver=uio_pci_generic if=
   
   Dedicated capture mode non-compatible devices
   ================================
   0000:02:00.0 driver=tg3 if=eth4 *Active*
   0000:02:00.1 driver=tg3 if=eth5
   0000:02:00.2 driver=tg3 if=eth6
   0000:02:00.3 driver=tg3 if=eth7
   ```

**Step 3: Specify network address in streamfwd.conf**

1. Edit `local/streamfwd.conf`.  
2. Specify the network address of the 10Gbps-compatible device. For example:
[streamfwd]
port = 8889
ipAddr = 127.0.0.1
dedicatedCaptureMode = 1
streamfwdcapture.0.interface = 0000:04:00.0

Dedicated capture mode requires specifying network device(s) using the PCI bus address notation.

**Step 4: Specify UIO driver in streamfwd.conf**

1. Edit `local/streamfwd.conf`.

2. Specify the UIO driver to use. For example:

   ```
   [streamfwd]
   port = 8889
   ipAddr = 127.0.0.1
dedicatedCaptureMode = 1
   uioDriverModuleName=igb_uio
   streamfwdcapture.0.interface = 0000:04:00.0
   ```

3. Restart the Splunk Platform.

Note: Dedicated capture mode supports binding to any of the following three UIO drivers:

- `uio_pci_generic`
- `vfio-pci`
- `igb_uio`

If a driver name is not specified in `streamfwd.conf`, then Stream uses the `uio_pci_generic` driver. Before restarting the Splunk Platform, make sure the UIO driver you are using is loaded. The UIO driver can be loaded either using the `modprobe` or `insmod` commands.

**Supported network interface controllers**

- For supported network interface controllers see http://dpdk.org/doc/nics.
- Stream has been tested on the following network interface controllers:
  - Intel(R) 82599ES 10 Gigabit Ethernet Controller
  - Intel Corporation Ethernet Controller X710