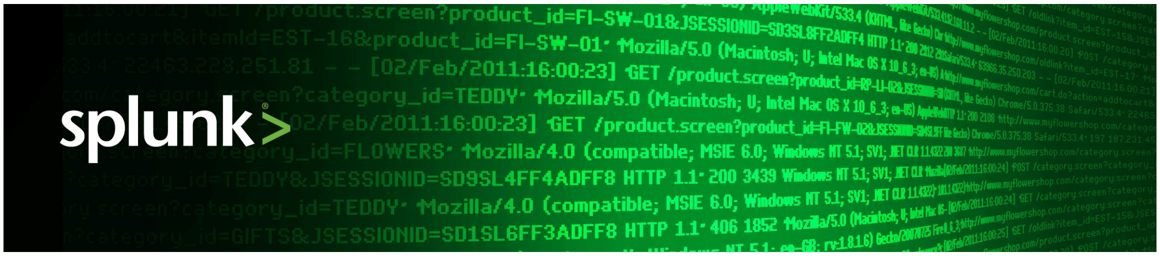

Splunk® Universal Forwarder Forwarder Manual 6.5.0

Troubleshoot the universal forwarder with Splunk Enterprise

Generated: 10/19/2016 9:57 pm

Troubleshoot the universal forwarder with Splunk Enterprise

Receiver doesn't accept new connections on its receiving port

If the internal queue on the receiving indexer gets blocked, the indexer shuts down the receiving/listening (`splunktcp`) port after a specified interval of being unable to insert data into the queue. Once the queue is again able to start accepting data, the indexer reopens the port.

However, sometimes (on Windows machines only) the indexer is unable to reopen the port once its queue is unblocked. To remediate, you must restart the indexer.

If you find you have this issue, you can set the `stopAcceptorAfterQBlock` attribute in inputs.conf on the receiver to a higher value, so that it does not close the port as quickly. This attribute determines the amount of time the indexer waits before closing the port. The default is 300 seconds (five minutes).

If you are using load-balanced forwarders, they will switch their data stream to another indexer in the load-balanced group based to their time-out interval, set in outputs.conf with the `writeTimeout` attribute. This results in automatic failover when the receiving indexers have blocked queues.

Confusing the receiving and management ports

As part of setting up a forwarder, you specify the receiver `hostname/IP_address` and receiving `port`. The forwarder uses these to send data to the receiver. Be sure to specify the port that you designated as the receiving port at the time the receiver was configured. If you mistakenly specify the management port, the receiver will generate an error similar to this:

```
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error =
error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - ACCEPT_RESULT=-1
VERIFY_RESULT=0
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error for fd
from HOST:localhost.localdomain, IP:127.0.0.1, PORT:53075
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error =
error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - ACCEPT_RESULT=-1
VERIFY_RESULT=0
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error for fd
from HOST:localhost.localdomain, IP:127.0.0.1, PORT:53076
splunkd.log:03-01-2010 13:35:28.653 ERROR TcpInputFd - SSL Error =
error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - ACCEPT_RESULT=-1
VERIFY_RESULT=0
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - SSL Error for fd
from HOST:localhost.localdomain, IP:127.0.0.1, PORT:53077
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - SSL Error =
error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
splunkd.log:03-01-2010 13:35:28.654 ERROR TcpInputFd - ACCEPT_RESULT=-1
VERIFY_RESULT=0
```

Receiver indexer closes receiving socket

If a receiving indexer queues become full, it closes the receiver socket to prevent additional forwarders from connecting to it. If a forwarder with load-balancing enabled can no longer forward to that receiver, it sends its data to another indexer on its list. If the forwarder does not employ load-balancing, it holds the data until you resolve the problem.

The receiver socket reopens automatically when the queue gets unclogged.

Typically, a receiver gets behind on the data flow because it can no longer write data due to a full disk or because it is itself attempting to forward data to another Splunk Enterprise instance that is not accepting data.

The following warning message will appear in `splunkd.log` if the socket gets blocked:

```
Stopping all listening ports. Queues blocked for more than N seconds.
```

This message will appear when the socket reopens:

```
Started listening on tcp ports. Queues unblocked.
```