```
########################################################################
# Excerpt from Splunkd.log on one of the non working Universal Forwarders:
########################################################################

01-21-2022 08:06:19.370 +1100 WARN  SHCConfig - Default pass4symkey is being used. Please change to a random one.

01-21-2022 08:07:43.381 +1100 INFO  HttpPubSubConnection - Running phone uri=/services/broker/phonehome/connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:07:43.431 +1100 INFO  HttpPubSubConnection - Running phone uri=/services/broker/phonehome/connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:07:43.443 +1100 INFO  DeployedApplication - Checksum mismatch 0 <> 2589272963411924211 for app=indexer_config. Will reload
from='<Indexer_ip>:8089/services/streams/deployment?name=default:Index%20configuration:indexer_config'
01-21-2022 08:07:43.468 +1100 INFO  DeployedApplication - Downloaded url=<Indexer_ip>:8089/services/streams/deployment?name=default:Index%20configuration:indexer_config to file='C:\Program
Files\SplunkUniversalForwarder\var\run\Index configuration\indexer_config-1642570133.bundle' sizeKB=20
01-21-2022 08:07:43.468 +1100 INFO  DeployedApplication - Installing app=indexer_config to='C:\Program Files\SplunkUniversalForwarder\etc\apps\indexer_config'
01-21-2022 08:07:43.490 +1100 INFO  ApplicationManager - Detected app creation: indexer_config
01-21-2022 08:07:43.495 +1100 INFO  DeployedApplication - Checksum mismatch 0 <> 15718042442375535504 for app=Splunk_TA_windows. Will reload
from='<Indexer_ip>:8089/services/streams/deployment?name=default:Windows_clients:Splunk_TA_windows'
01-21-2022 08:07:43.665 +1100 INFO  DeployedApplication - Downloaded url=<Indexer_ip>:8089/services/streams/deployment?name=default:Windows_clients:Splunk_TA_windows to file='C:\Program
Files\SplunkUniversalForwarder\var\run\Windows_clients\Splunk_TA_windows-1642570137.bundle' sizeKB=3420
01-21-2022 08:07:43.674 +1100 INFO  DeployedApplication - Installing app=Splunk_TA_windows to='C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows'
01-21-2022 08:07:43.798 +1100 INFO  ApplicationManager - Detected app creation: Splunk_TA_windows
01-21-2022 08:07:43.803 +1100 INFO  DeployedApplication - Checksum mismatch 0 <> 4613644356142874166 for app=_server_app_Windows_clients. Will reload
from='<Indexer_ip>:8089/services/streams/deployment?name=default:Windows_clients:_server_app_Windows_clients'
01-21-2022 08:07:43.818 +1100 INFO  DeployedApplication - Downloaded url=<Indexer_ip>:8089/services/streams/deployment?name=default:Windows_clients:_server_app_Windows_clients to file='C:\Program
Files\SplunkUniversalForwarder\var\run\Windows_clients\_server_app_Windows_clients-1642570138.bundle' sizeKB=10
01-21-2022 08:07:43.818 +1100 INFO  DeployedApplication - Installing app=_server_app_Windows_clients to='C:\Program Files\SplunkUniversalForwarder\etc\apps\_server_app_Windows_clients'
01-21-2022 08:07:43.827 +1100 INFO  ApplicationManager - Detected app creation: _server_app_Windows_clients
01-21-2022 08:07:43.838 +1100 WARN  DC:DeploymentClient - Restarting Splunkd...

01-21-2022 08:08:52.031 +1100 WARN  SHCConfig - Default pass4symkey is being used. Please change to a random one.

01-21-2022 08:08:52.261 +1100 WARN  X509Verify - X509 certificate (O=SplunkUser,CN=SplunkServerDefaultCert) should not be used, as it is issued by Splunk's own default Certificate Authority (CA). This puts your Splunk
instance at very high-risk of the MITM attack. Either commercial-CA-signed or self-CA-signed certificates must be used; see: <http://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates>
01-21-2022 08:08:52.269 +1100 WARN  FilesystemChangeWatcher - error reading directory "C:\Users\Default User": Access is denied.

01-21-2022 08:08:52.377 +1100 INFO  TcpOutputProc - Connected to idx=<Indexer_ip>:9997, pset=0, reuse=0.
01-21-2022 08:09:04.031 +1100 INFO  DC:DeploymentClient - channel=tenantService/handshake Will retry sending handshake message to DS; err=not_connected
01-21-2022 08:09:06.447 +1100 ERROR TcpOutputFd - Read error. An existing connection was forcibly closed by the remote host.
01-21-2022 08:09:06.657 +1100 ERROR TcpOutputFd - Read error. An existing connection was forcibly closed by the remote host.
01-21-2022 08:09:06.658 +1100 WARN  TcpOutputProc - Applying quarantine to ip=<Indexer_ip> port=9997 _numberOfFailures=2
01-21-2022 08:09:12.225 +1100 WARN  TailReader - Could not send data to output queue (parsingQueue), retrying...
01-21-2022 08:09:16.032 +1100 INFO  DC:DeploymentClient - channel=tenantService/handshake Will retry sending handshake message to DS; err=not_connected

01-21-2022 08:09:23.001 +1100 INFO  HttpPubSubConnection - SSL connection with id: connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:09:23.055 +1100 INFO  HttpPubSubConnection - Running phone uri=/services/broker/phonehome/connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:09:28.032 +1100 INFO  HttpPubSubConnection - Running phone uri=/services/broker/phonehome/connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:09:28.043 +1100 INFO  DC:HandshakeReplyHandler - Handshake done.
01-21-2022 08:09:51.847 +1100 INFO  TcpOutputProc - Removing quarantine from idx=<Indexer_ip>:9997
01-21-2022 08:09:51.847 +1100 INFO  TcpOutputProc - Found currently active indexer. Connected to idx=<Indexer_ip>:9997, reuse=1.
01-21-2022 08:09:55.937 +1100 ERROR TcpOutputFd - Read error. An existing connection was forcibly closed by the remote host.
01-21-2022 08:09:55.958 +1100 ERROR TcpOutputFd - Read error. An existing connection was forcibly closed by the remote host.
01-21-2022 08:09:55.958 +1100 WARN  TcpOutputProc - Applying quarantine to ip=<Indexer_ip> port=9997 _numberOfFailures=2
01-21-2022 08:10:21.741 +1100 INFO  TcpOutputProc - Found currently active indexer. Connected to idx=<Indexer_ip>:9997, reuse=1.
01-21-2022 08:10:28.043 +1100 INFO  HttpPubSubConnection - Running phone uri=/services/broker/phonehome/connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:10:28.106 +1100 INFO  HttpPubSubConnection - Running phone uri=/services/broker/phonehome/connection_<FW_internal_NAT_ip>_8089_<FW_internal_NAT_ip>_<UF_server_hostname>_<UF_server_GUID>
01-21-2022 08:10:38.840 +1100 WARN  TcpOutputProc - The TCP output processor has paused the data flow. Forwarding to host_dest=<Indexer_ip> inside output group default-autolb-group from host_src=<UF_server_hostname> has
been blocked for blocked_seconds=100. This can stall the data flow towards indexing and other network outputs. Review the receiving system's health in the Splunk Monitoring Console. It is probably not accepting data.

01-27-2022 19:30:42.178 +1100 INFO  loader - SAML cert db registration with KVStore failed
01-27-2022 19:30:42.184 +1100 INFO  CertStorageProvider - Updating status from unknown to unknown
01-27-2022 19:30:42.184 +1100 INFO  loader - Auth cert db registration with KVStore failed
01-27-2022 19:30:42.184 +1100 INFO  CertStorageProvider - Updating status from unknown to unknown

01-27-2022 19:30:42.939 +1100 WARN  X509Verify - X509 certificate (O=SplunkUser,CN=SplunkServerDefaultCert) should not be used, as it is issued by Splunk's own default Certificate Authority (CA). This puts your Splunk
instance at very high-risk of the MITM attack. Either commercial-CA-signed or self-CA-signed certificates must be used; see: http://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates


########################################################################
# Excerpt from Health.log on the same non working Universal Forwarder:
########################################################################


02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - product="splunkd" color=red due_to_sub_feature="Data Forwarding" due_to_sub_feature="File Monitor Input" node_type=product node_path=splunkd
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="Data Forwarding" color=red due_to_sub_feature="Splunk-2-Splunk Forwarding" node_type=category node_path=splunkd.data_forwarding
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="Splunk-2-Splunk Forwarding" color=red due_to_sub_feature="TCPOutAutoLB-0" node_type=category node_path=splunkd.data_forwarding.splunk-2-splunk_forwarding
```

```
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="TCPOutAutoLB-0" color=red due_to_stanza="feature:s2s_autolb" due_to_indicator="s2s_connections" node_type=feature
node_path=splunkd.data_forwarding.splunk-2-splunk_forwarding.tcpoutautolb-0
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="TCPOutAutoLB-0" color=red indicator="s2s_connections" due_to_threshold_value=70 measured_value=100 reason="More than 70% of forwarding destinations have
failed.  Ensure your hosts and ports in outputs.conf are correct.  Also ensure that the indexers are all running, and that any SSL certificates being used for forwarding are correct." node_type=indicator
node_path=splunkd.data_forwarding.splunk-2-splunk_forwarding.tcpoutautolb-0.s2s_connections
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="TCPOutAutoLB-1" color=green due_to_stanza="feature:s2s_autolb" node_type=feature
node_path=splunkd.data_forwarding.splunk-2-splunk_forwarding.tcpoutautolb-1
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="File Monitor Input" color=red due_to_sub_feature="TailReader-0" node_type=category node_path=splunkd.file_monitor_input
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="BatchReader-0" color=green due_to_stanza="feature:batchreader" node_type=feature node_path=splunkd.file_monitor_input.batchreader-0
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="TailReader-0" color=red due_to_stanza="feature:tailreader" due_to_indicator="data_out_rate" node_type=feature
node_path=splunkd.file_monitor_input.tailreader-0
02-04-2022 17:01:36.159 +1100 INFO  PeriodicHealthReporter - feature="TailReader-0" color=red indicator="data_out_rate" due_to_threshold_value=2 measured_value=2 reason="The monitor input cannot produce data because
splunkd's processing queues are full.  This will be caused by inadequate indexing or forwarding rate, or a sudden burst of incoming data." node_type=indicator node_path=splunkd.file_monitor_input.tailreader-0.data_out_rate
```