VERITAS

Running Network Packet Captures using Veritas Quick Assist for Network Troubleshooting

Contents

Introduction

Network diagnostics captures TCP network packets between this computer and one or more target hosts. This tool does not require an installation and does not make any changes to the system. It is necessary to upload the diagnostic data package to the Support Case. The Veritas Engineer will then communicate the results once they have received and analyzed the data package. The following test options can be configured for data collection:

- Packet Size - With an ideal value of 60, which is sufficient for most TCP analysis.
- Bandwidth Capacity - Total bandwidth capacity of the Network where data packet capture is being performed.
- Capture Time - Packet capture duration in hours, minutes, and seconds as per the need.
- IP Addresses - List of the remote IP addresses for data packet capture.
- Ports - List of the remote ports for data packet capture.

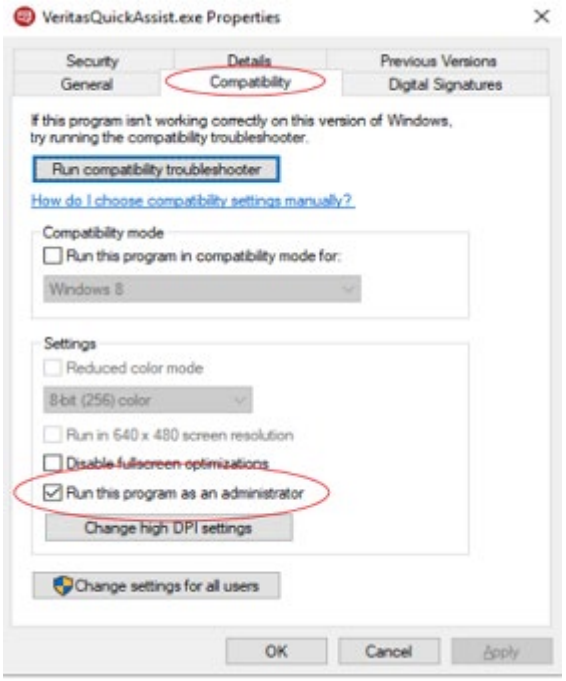
Collecting Network Packet for Windows (2016/2019/2022)

The Veritas Quick Assist (VQA) leverages Windows built-in **netsh** utility. VQA supports Network data collection on

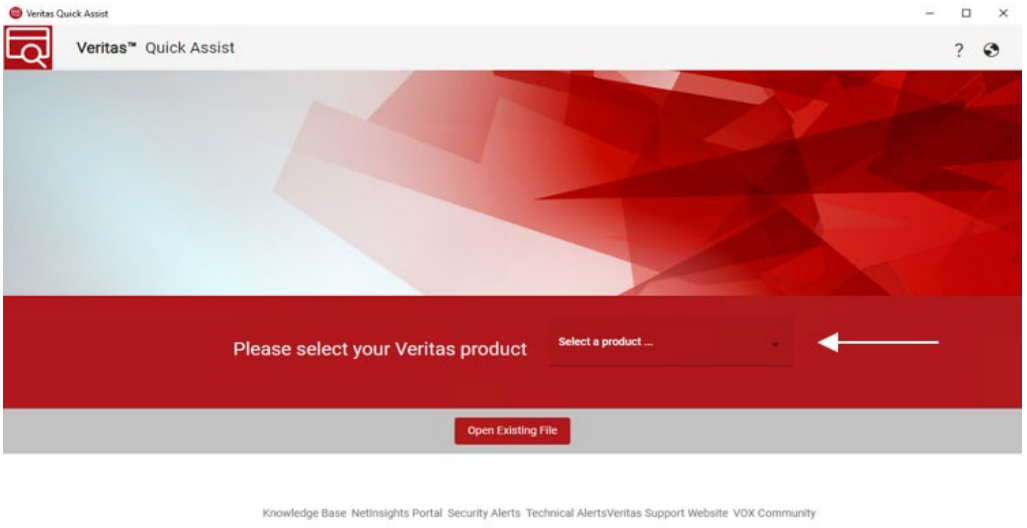
- Windows Server 2016, Windows Server 2019, Windows Server 2022
- Windows 10 22H2
- Windows 11 23H2, 11 22H2

Perform the following steps:

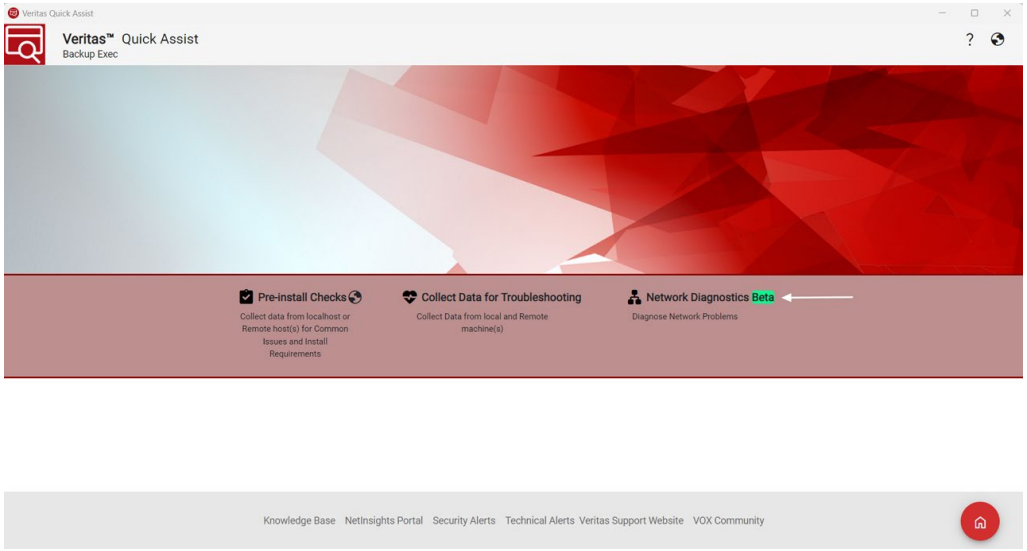
1. Download and run Veritas Quick Assist (VQA) as Administrator.
2. Alternatively, enable **Run this program as an administrator** under the **Compatibility** tab of VQA Properties.



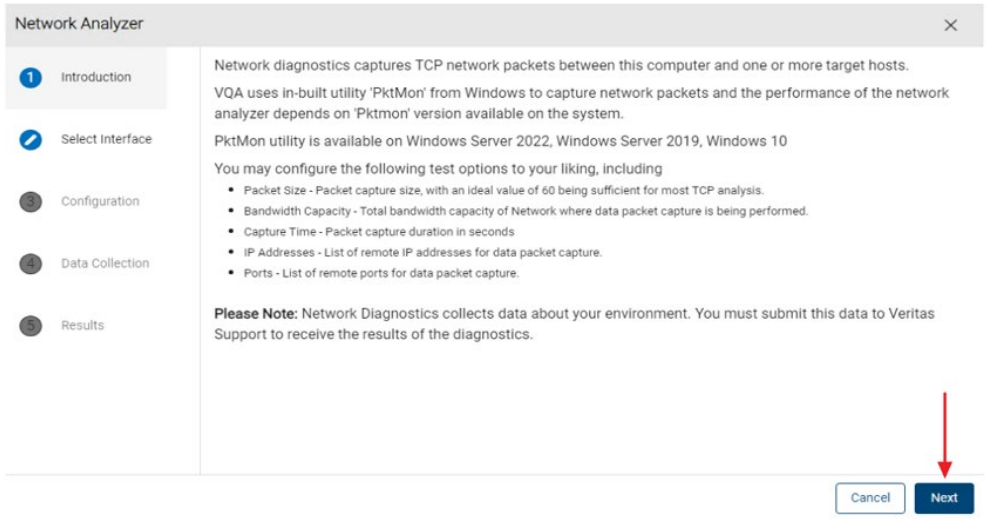
3. Accept the EULA.
4. Select the Product



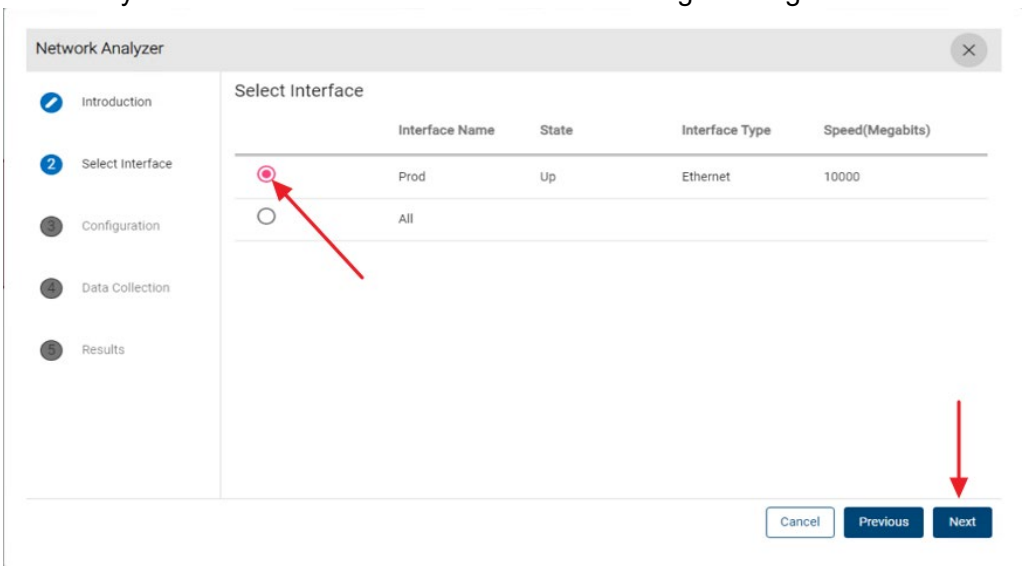
5. Click Network Diagnostics.



6. Read the Network Diagnostics introduction, then click Next



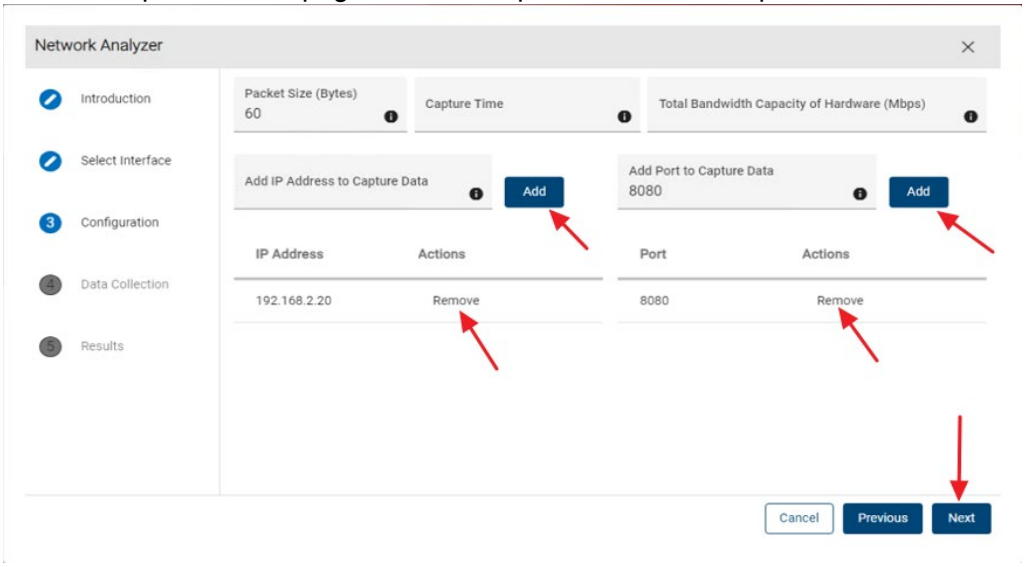
7. Select any one or all the interfaces to use when running the diagnostics.



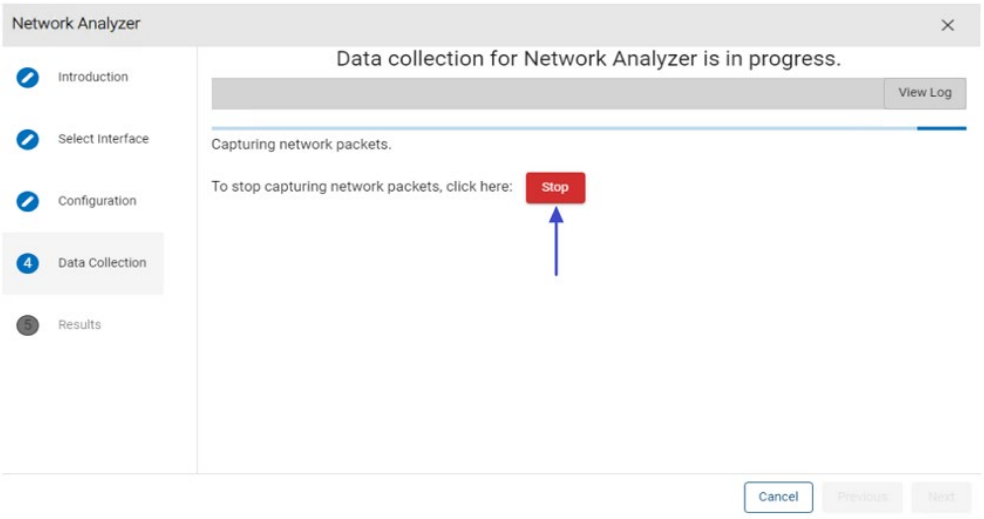
8. Enter the configuration parameters.
   Add one or more target hosts and ports on which the packets need to be captured. The diagnostics will be

run between the current system running VQA and each of the target hosts.

For most collection, Packet size of 60 bytes is sufficient. If the capture time is not entered, then the user must click on stop in the next page. Once the options are entered, please click on next to continue.



9. Click on the **Stop** button, in case the Capture time is not entered in the previous screen.



10. Once the file is collected, attach the same to the support case.

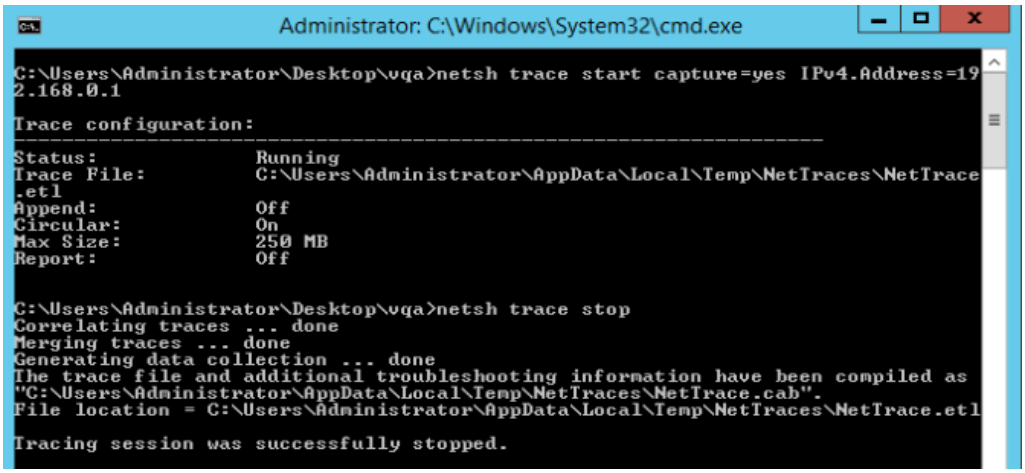
Collecting Network Packet for Windows 2012/2012R2

Windows Server 2012/2012R2 contains a built-in packet capture tool through the netsh utility. As it is included with the OS, it can be preferable to other packet sniffing/capturing tools such as Wireshark or NetMon.
To start a packet capture with netsh trace, first launch an administrative command prompt window. Then enter the following command:

netsh trace start capture=yes IPv4.Address=192.168.0.1

The packet capture will begin. To stop the packet capture, use the following command:
netsh trace stop

After the capture is stopped, netsh will output two files (NetTrace.cab and NetTrace.etl) in the current user's %temp% folder.



The etl files can be converted into pcap files using etl2pcapng (or any other 3rd party utility) and uploaded to a Support Case.

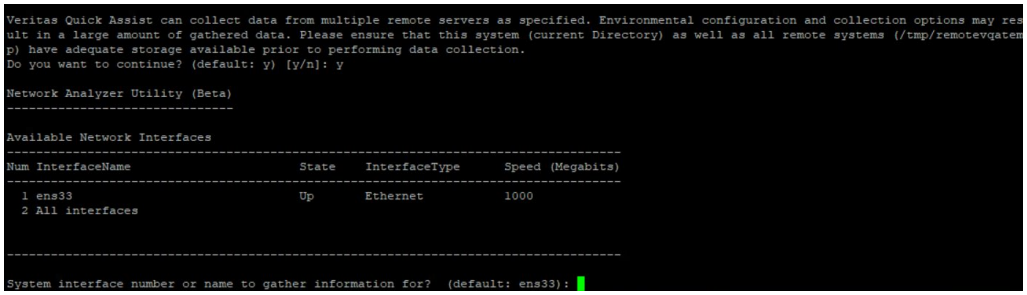
Collecting network packets for Linux

The following operating systems are supported by Veritas Quick Assist Data Collector:

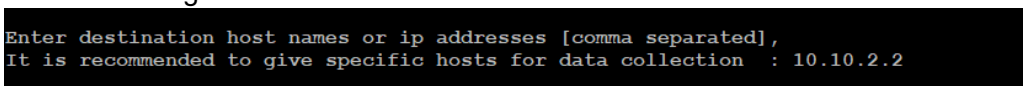
Operating System	Version
CentOS Stream	9
RHEL	8.x, 9.x
SUSE Enterprise Linux	12.5, 15.5, 15.6

Guided Experience

1. Download and extract the Linux data collector.
2. Run *./vqacollector networkanalyzer* and accept the EULA.
3. Choose any one or all interfaces to use when running the diagnostics. You may enter the interface number or its name.

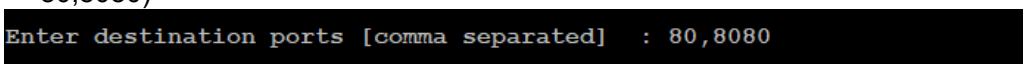


4. Enter one or more target IP addresses. It is recommended to enter the specific IP address for which the network diagnostics needs to be done.



Network packet captures will be run between the system running the VQA Data Collector and each of the target hosts. Multiple target hosts can be specified by listing them separated with a comma (ex. 10.10.10.2,10.10.10.5,10.10.10.9)

5. Enter one or more ports. Multiple target hosts can be specified by listing them separated with a comma (ex. 80,8080)



6. Enter Snaplength. Packet capture size, with an ideal value of 60 being sufficient for most TCP analysis.

7. Enter Capture Time in seconds.
   If no value is entered, VQA DC collects the packets till the user presses Ctrl+C.
8. Wait for the packet captures to be completed.

Command Line Experience
Use the following command line options to run the network packet capture.

```
Usage: vqacollector [options] NetworkAnalyzer [netanalyzer-options]

Run Network Analyzer Utility.

Note: This command requires TcpDump installed on the system.

Options:
    -ch|--capturehosts <hosts>      Capture packets for the specified host. Comma separated list of hosts
                                    Default: All -- packets going and coming from all host captured.

    -cp|--captureports <ports>      Capture npackets for the specified port.Comma separated list of ports
                                    Default: All -- packets going and coming from all ports captured.
                                    Supported only on Linux platform

    -ct|--capturetime <time>        Capture network packets for <time> seconds.

    -i|--interfaces <interfaces>    Required. An interface number or name (Any one or All interfaces)
                                    Default: First system interface..

    -l|--list                       Lists interfaces for capturing packets

    -s|--snaplength <size>          Captures <size> bytes for every packet.
                                    Default: 60 -- Packet length.

    -h|--help                       Show command line help

Example:
./vqacollector NetworkAnalyzer  -i ens92 -ch "x.x.x.x, y.y.y.y"
./vqacollector NetworkAnalyzer  -i ens92 -cp "10, 20"
```

Example:

```
[root@[redacted] VQA]# ./vqacollector networkanalyzer -i ens192 -ch "192.168.1.100" -s 100

Veritas Quick Assist can collect data from multiple remote servers as specified. Environmental configu
ration and collection options may result in a large amount of gathered data. Please ensure that this s
ystem (current Directory) as well as all remote systems (/tmp/remotevqatemp) have adequate storage ava
ilable prior to performing data collection.
Do you want to continue? (default: y) [y/n]:

Starting data collection. Waiting for data collection completion.

Collecting Network Information...

Capturing network packets...

Press 'Ctrl + C'  to stop collection.

Packaging data. Please wait, this may take some time.

Completed data collection.

Status: dalsgsswebdin01 : RunOk

The data is saved to : dalsgsswebdin01__2024-09-23__07-23-09.vqa
```

For those servers, that VQA doesn't support, use the following commands:

tcpdump -w <fileName.pcap> -i <interfaces> -n '(host <IP_Addr1> or host <IP_Addr2>) and (port <Port1> or port <Port2>)' -s <CaptureBytes>

For example:
tcpdump -w Server.pcap -i 'ens192' -n '(host 1.1.1.1 or host 2.2.2.2) and (port 8080 or port 8081)' -s 60