monitor failed: software caused connection abort: recv failed

This error message indicates a general network connectivity error between the Monitoring Station and the monitored agent servers. It has only been seen on Windows Monitoring Stations and is generally resolved using one of the following methods:

Disable TCP Offload Engine (TOE)

If your monitoring station server has a TOE-enabled network card, you may need to disable it. TOE is intended to accelerate long-running TCP connections. Because Uptime Infrastructure Monitor uses many short-lived connections to contact agents, its process can be mismanaged by the TOE. Please perform the following commands on the monitoring station to disable TOE:

- Go to Control Panel > Network Connections.
- Right click on the active NIC card and select Properties.
- Click the Configure button and select the Advanced tab.
- Locate TCP/IP Offload in the list and set it to Disabled.
- If you don't see the 'TCP/IP Offload' Property in that list another common name for it is 'Large Send Offload (IPv4)'

If the TCP/IP Offload setting is not found by using the previous steps, you may need to disable the TCP Offload setting within another program or Windows service with an advanced network card configuration. For example:

HP Network Configuration Utility

- Click Advanced.
- Set TCP Offload Engine (TOE) to disabled.

Broadcom Advanced Control Suite

- Click on the Primary Adapter.
- Click on the Resource Allocations tab on the right.
- If TOE is enabled, click the Configure button and disable it.

Windows TCP Stack is overloaded

If Uptime Infrastructure Monitor is monitoring more than 500 services, you may find that the default Windows TCP stack options are not sufficient to maintain the outbound Uptime Infrastructure Monitor connections. In this case, we recommend adjusting registry settings on the monitoring station to relieve some common TCP bottlenecks:

Under the :HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Tcpip\\Parameters registry key, create the following new keys:

- Value Name: MaxUserPort
- Value Type: REG_DWORD
- Value data: 65534
- Valid Range: 5000-65534 (decimal)
- Default: 0x1388 (5000 decimal)

Description: this parameter controls the maximum port number that is used when a program requests an available user port from the system.

Typically, ephemeral (short-lived) ports are allocated between the values of 1024 and 5000 inclusive.

- Value Name: TcpTimedWaitDelay
- Value Type: REG_DWORD—time in seconds
- Value data: 30
- Valid Range: 30-300 (decimal)
- Default: 0xF0 (240 decimal)

Description: this parameter determines the length of time that a connection stays in the TIME_WAIT state when being closed. While a connection is in the TIME_WAIT state, the socket pair cannot be re-used.

This is also known as the 2MSL state because the value should be twice the maximum segment lifetime on the network. See RFC 793 for further details.

How to Disable TCP Chimney Offload

TCP Chimney Offload is a networking technology that helps transfer the workload from the CPU to a network adapter during network data transfer. In Windows Server 2008, TCP Chimney Offload enables the Windows networking subsystem to offload the processing of a TCP/IP connection to a network adapter that includes special support for TCP/IP offload processing.

Please review - Information about the TCP Chimney Offload for detailed explanation of what the TCP Chimney Offload is and instructions (including an option to run a wizard) to guide you through this change.

Related KB - Increasing Windows TCP socket limits