GigaStor Software Edition 18.1.0.0

User Guide

1 Jul 2020

Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and VIAVI reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Copyright

© Copyright 2020 VIAVI Solutions Inc. All rights reserved. VIAVI and the VIAVI logo are trademarks of VIAVI Solutions Inc. (“VIAVI”). All other trademarks and registered trademarks are the property of their respective owners. No part of this guide may be reproduced or transmitted, electronically or otherwise, without written permission of the publisher.

Copyright release

Reproduction and distribution of this guide is authorized for Government purposes only.

Terms and conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to VIAVI standard terms and conditions, available at www.viavisolutions.com/terms.

Specifications, terms, and conditions are subject to change without notice. All trademarks and registered trademarks are the property of their respective companies.

Federal Communications Commission (FCC) Notice

This product was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this product in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

The authority to operate this product is conditioned by the requirements that no modifications be made to the equipment unless the changes or modifications are expressly approved by VIAVI.

Laser compliance

This device is a class 1 laser product.

Industry Canada Requirements

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

WEEE and Battery Directive Compliance

VIAVI has established processes in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive, 2002/96/EC, and the Battery Directive, 2006/66/EC.

This product, and the batteries used to power the product, should not be disposed of as unsorted municipal waste and should be collected separately and disposed of according to your national regulations. In the European Union, all equipment and batteries purchased from VIAVI after 2005-08-13 can be returned for disposal at the end of its useful life. VIAVI will ensure that all waste equipment and batteries returned are reused, recycled, or disposed of in an environmentally friendly manner, and in compliance with all applicable national and international waste legislation.

It is the responsibility of the equipment owner to return equipment and batteries to VIAVI for appropriate disposal. If the equipment or battery was imported by a reseller whose name or logo is marked on the equipment or battery, then the owner should return the equipment or battery directly to the reseller.

Instructions for returning waste equipment and batteries to VIAVI can be found in the Environmental section of VIAVI web site at . If you have questions concerning disposal of your equipment or batteries, contact VIAVI WEEE Program Management team at WEEE.EMEA@viavisolutions.com.

Technical Support

North America	1.844.GO VIAVI / 1.844.468.4284
Latin America	+52 55 5543 6644
EMEA	+49 7121 862273
APAC	+1 512 201 6534
All Other Regions	viavisolutions.com/contacts
email	customer.care@viavisolutions.com

Support hours are 7:00 A.M to 7:00 P.M. (local time for each office).

Table of Contents

Chapter 1: Getting started....4
How to set up the GigaStor Software Edition....4
Differences between GigaStor Software Edition and GigaStor....6
Minimum and recommended system specifications....6
Installing Observer software....9
How to license Observer and GigaStor....9
Running Observer with reserved memory....10
How to allocate the reserved RAM....11
How to configure the capture buffer settings....11
How to install a version of GigaStor....13
How to change the GigaStor storage directory or drive....13
How to change the monitored network adapter....13
Understanding GigaStor protocol and port settings....14
Setting a schedule for when data captures should occur....14
Scheduling your network trending data collection....15
Index....16

1

Chapter 1: Getting started

How to set up the GigaStor Software Edition

The GigaStor Software Edition is configurable in the same way a GigaStor hardware appliance is.

To set up the GigaStor Software Edition:

1. (Optional) Learn about the differences between the GigaStor Software Edition (GSE) and a GigaStor hardware appliance.

   (Optional) Differences between GigaStor Software Edition and GigaStor (page 6)
2. Review the minimum and recommended system specifications.

   Minimum and recommended system specifications (page 6)
3. Review the supported operating systems.

   Supported Operating Systems (page 8)
4. Install the Observer Analyzer software.

   Installing Observer software (page 9)
5. Transform your Observer installation into a full GigaStor Software Edition by applying your license.

   How to license Observer and GigaStor (page 9)
6. Reserve some of your available RAM for the GigaStor Software Edition to use exclusively.

   Running Observer with reserved memory (page 10)
7. Allocate the reserved RAM to the capture and statistical buffers.

   How to configure the capture buffer settings (page 11)

   How to allocate the reserved RAM (page 11)
8. Update your Observer installation to the latest available build.

   How to install a version of GigaStor (page 13)

9. (Optional) Change the hard disk or directory where your GigaStor stores network traffic.

   (Optional) How to change the GigaStor storage directory or drive (page 13)

10. Ensure the correct network adapter is selected for your GigaStor probe instance.

    How to change the monitored network adapter (page 13)

11. Decide to use—or not use—features designed to lower the GigaStor resource consumption on your computer or virtual machine.

    Understanding GigaStor protocol and port settings (page 14)

12. Set a schedule for when the GigaStor should collect network traffic.

    Setting a schedule for when data captures should occur (page 14)

13. (Optional) Set a schedule for when network trending should

    (Optional) Scheduling your network trending data collection (page 15)

Differences between GigaStor Software Edition and GigaStor

The GigaStor Software Edition (GSE) is identical in most ways to a hardware GigaStor purchased from VIAVI. However, there are differences that exist due to GSE naturally lacking GigaStor hardware components like the capture card and high-performance RAID card(s).

Capability	GigaStor Software Edition	GigaStor as Appliance
Mining & Analysis Interface	X	X
Packet Capture	X	X
Real-Time Statistics	X	X
Trending	X	X
Triggers and Alarms	X	X
Data-at-Rest Security		X
Capture card		X
Hardware Acceleration		X
Hardware Filtering		X
Packet Deduplication		X
Physical Port Indexing		X
Precision Time Stamping		X
Virtual Adapters		X
High-performance RAID card		X

Minimum and recommended system specifications

If you are installing the software on your own hardware or a virtual machine, these are the minimum and recommended specifications for a production environment.

Table 1. Observer Expert Console Only (ECO)

	Minimum	Recommended
Processor / CPU	Dual core Pentium class processor	Quad core Pentium class processor
RAM[1]	2 GB RAM	8 GB RAM
Operating system[2]	64-bit Operating System Windows 7 or newer	64-bit Operating System Windows 7 or newer
Network Card	Server-class	Intel server-class

1. If your system has 4 GB of RAM, you cannot reserve any memory for Observer. This is a limitation of Windows known as the BIOS memory hole. Either add more RAM or take some out.

2. See Supported Operating Systems (page 8) for a full list of supported operating systems.

Table 2. Observer or GigaStor Software Edition in a virtual server

	Minimum	Recommended
Processor / CPU	Four core	Six core Intel
RAM[1]	Minimum 16 GB (8 GB for Observer and 8 GB for the operating system)	64 GB
Storage	Packet capture - Hardware: Determined by your product	Same

	Minimum	Recommended
	Packet capture - GigaStor Software Edition: Determined by your license. Network trending: See How to determine disk space requirements for network trending (page 9).	
Operating system[2]	64-bit Operating System Windows 7 or newer	64-bit Operating System Windows 7 or newer
Network Card	Virtualized network adapter	Intel server-class
Capture Card[3]	Virtualized network adapter	Server-class onboard network adapter

1. If your system has 4 GB of RAM, you cannot reserve any memory for Observer. This is a limitation of Windows known as the BIOS memory hole. Either add more RAM or take some out.

2. See Supported Operating Systems (page 8) for a full list of supported operating systems.

3. A second network card that acts solely as a capture card is required (and must be in “promiscuous mode”). Alternatively, a dual-port NIC can be used.

Current compatibility and incompatibly of virtual machines with the GigaStor Software Edition (GSE) is described in this list:

- VMWare ESXi Server
  - ESXi 5.0 and higher is *compatible* with GSE.
- VMWare Workstation Pro is not supported with GSE
- Microsoft Hyper-V may function but is not supported with GSE

Supported Operating Systems

Your product must be installed on one of these operating systems to receive assistance from Technical Support.

Product name	64-bit Windows	32-bit Windows
	Windows 7 (SP1 or higher) or newer	Not supported
	Windows Server 2008 R2 Enterprise, Standard, Web (SP1 or higher) or newer	
	Windows 7 (SP1 or higher) or newer	

Storage limits of packet capture for GigaStor Software Edition (GSE)

The disk storage capacity usable for packet capture and of GigaStor Software Edition (GSE) is governed by your GSE license. This allows flexible cost options when considering the storage available to the computer, or virtual machine, that you are installing GSE on.

GSE licenses are available at these maximum storage sizes:

256 GB

1 TB

4 TB

16 TB

32 TB

48 TB

64 TB

Maximum storage size is a measure of how much network data (in the form of packets) can be retained by the GigaStor Software Edition before the oldest GigaStor data is removed in a first-in first-out (FIFO) storage scheme. The maximum storage size is not an indication of how much disk space the GigaStor Software Edition will consume on your hard disk. For example, the program files and libraries, storage of network trending data (not packets), and other executables are not governed by your GSE license and do not count towards the maximum storage capacity.

Network trending storage is a separate issue from packet capture storage and they are not connected in any way except both require writing data to the hard drive. When estimating file size, retention, and system maintenance, you may want to look at the system holistically and consider both simultaneously. Read more about network trending in Configuring your network trending settings.

How to determine disk space requirements for network trending

Because network trending can consume a lot of disk space, you need to know how much disk space to reserve.

Network trending data consumes hard disk space. Depending on where you store trending data and your storage requirements for network trending data, the network trending data could fill that drive to full capacity—this is a problem. Therefore, determine your typical 24-hour data rate and how many days of trending data you want to retain. The result indicates how much storage space is required.

To determine the amount of space required to store your desired amount of trending data:

1. Determine your typical 24-hour data rate.

   Example: 15 MB or 20 GB.

   The *data rate* is amount of trending data collected in one 24-hour period.
2. Multiply your typical 24-hour data rate by the number of days you want to retain.

   Example: 15 MB x 365 days = 5.475 GB

   Example: 20 GB x 30 days = 600 GB

The result is the amount of hard drive space required to retain the trending data.

You can use the numbers you calculated to inform your decisions when deleting network trending data.

Installing Observer software

Prerequisite(s):

See Supported Operating Systems (page 8) for a list of supported operating systems.

To install the Observer software, follow these steps:

1. Download the latest installation image from our website. Start the installation program.

   http://update.viavisolutions.com/latest/ObserverSetupx64.exe
2. When the setup program runs, follow the onscreen instructions.

How to license Observer and GigaStor

To license and activate a compatible GigaStor, Observer, or Probe:

1. Install and launch the application.
2. After launching the application in DEMO mode, click the **Help** menu and select **License Observer**.
3. Click the **Enter Name** button in the lower left corner.
4. Type into the **Contact/Department** and **Company** boxes exactly what is listed in your license document.
5. Click **OK**, and then click **Accept** on the confirmation dialog.
6. Ensure the **Identification Number** matches the number on your license document. If they do not match, click **Re-Type Name?** to correct any mistakes.
7. Type the license number, from your license document, into the **License Number** box.
8. Click **OK**.

You successfully licensed and activated your product.

If licensing and activating your product remains unsuccessful, please contact Technical Support.

Running Observer with reserved memory

Reserved memory helps Observer run more efficiently by dedicating memory for its exclusive use.

Prerequisite(s):

- Observer Expert
- Observer Suite
- Expert Probe software
- Multi Probe software

Observer uses reserved memory for packet capture and the statistics queue buffer. It is highly-recommended that you use reserved memory. (GigaStor appliances running Observer are preconfigured this way.) You must determine how you want Observer to be configured for your system.

> **Tip!** If you need more RAM for the statistics queue buffer, you may need to lower the amount of RAM dedicated to packet capture so that it is freed and available to add to the statistics queue.

Reserving memory allows Observer to allocate RAM for its exclusive use. This ensures that Observer has the necessary memory to store packets for statistical analysis, or for capturing large amounts of data for decoding. The more memory you reserve for Observer, the larger the packet capture and statistical queue buffers can be.

If the memory buffer for the statistics queue buffer is too small, you may end up with inaccurate statistical data because some data may get pushed out before it can be processed. Observer processes packets on a first-in, first out (FIFO) basis, so it is important that the buffer be large enough to allow for processing.

When reserving RAM for Observer you are taking RAM away from the operating system. Table 3 (page 10) shows how much memory is required by the operating system. Anything beyond this amount may be reserved for Observer.

Table 3. Reserved memory requirements

Operating System	RAM required for the operating system
64-bit with less than 4 GB RAM	800 MB
64-bit with 4 GB RAM	4 GB [1]
64-bit with 6+ GB RAM	4 GB
32-bit[2]	256 MB (although 400+ MB is recommended)

1. Because of how 64-bit Windows loads its drivers when 4 GB of RAM is installed all 4 GB is used by Windows. This is sometimes referred to as the BIOS memory hole and means you cannot reserve any memory for Observer. To capture packets on 64-bit Windows install either more than or less than 4 GB of RAM.

2. 32-bit operating systems do not support more than 4 GB of RAM. Observer cannot use any RAM above 4 GB.

1. To see how much protected memory the probe has, click the **Memory Management tab**.

2. Click the **Configure Memory** button at the top of the window to view and modify how Observer uses the protected memory for this probe instance. The Edit Probe Instance window opens.

   On the Edit Probe Instance window, you can see how memory is allocated for:

   - Packet capture
   - Statistics queue buffer

   You can also see how much protected memory is still available in the Windows memory pool.

3. Use the arrows to the right of the Packet capture and Statistics queue buffer to increase or decrease the amount of RAM you want dedicated to each. See How to allocate the reserved RAM (page 11) to help determine how to divide the memory.
4. After reserving memory for Observer you must restart the system for the changes to take affect. After you restart the system you can allocate the memory to the different probe instances.

How to allocate the reserved RAM

After you have the RAM reserved for Observer, you must allocate it for the probe instances. Here are our basic recommendations for allocating the memory. These are just recommendations and may be changed or modified for your circumstances.

How many probe instances will you have on this system? How are you using the probe instance(s)? Are you using it to capture packets or to analyze statistics? After you know how you want to use the probe instance, you can decide how to properly divide the memory amongst the probe instances, and further how you will allocate the memory between the packet capture and statistics queue buffers.

You want to create and use as few probe instances as absolutely necessary. Each probe instance you create divides the memory pool into smaller chunks. The more probe instances you have, the more processing the system must do.

> **Note:** If you have a lot of network traffic, then you may need to allocate at least one gigabyte of RAM to the packet capture buffer, the statistics queue buffer, or both.

For each probe instance determine:

- If you want to mostly capture packets, then allocate 90% of the reserved RAM to packet capture and 10% to the statistics queue buffer. At a minimum, you should allocate 12 MB to collect statistics. If you are using a GigaStor, you should allocate the vast majority of the reserved RAM for the *active probe instance* to packet capture.
- If you want to collect statistics or trending data, or use analysis, then allocate 90% (or even 100%) of the reserved RAM to the statistics queue buffer.
- If you want to do both, determine which you want to do more of and allocate the memory accordingly.

How to configure the capture buffer settings

Observer can perform packet captures without additional setup. However, to maximize Observer performance, you should consider configuring your capture settings manually.

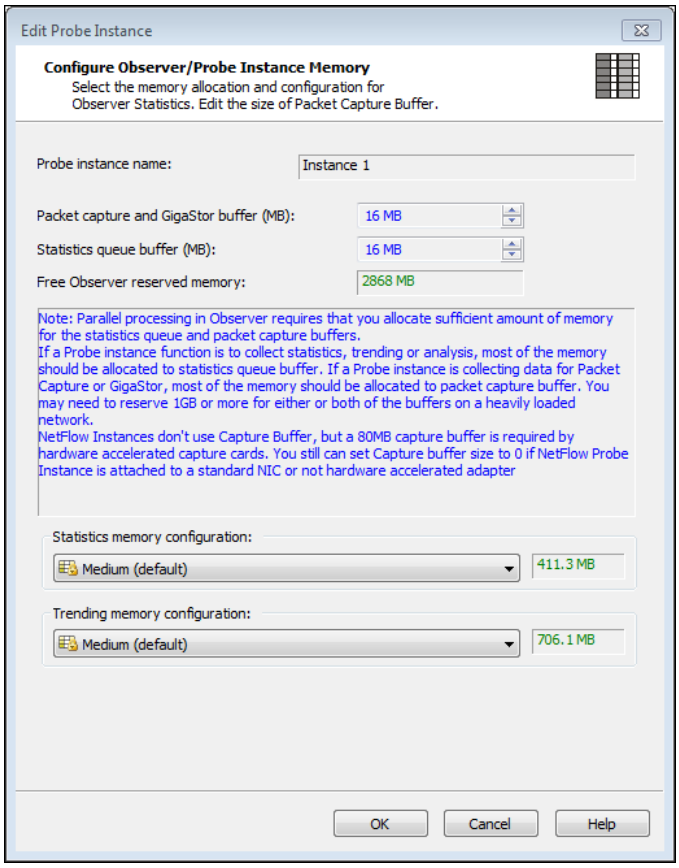
During the creation of your probe instance(s), you set the size of your buffers. The capture buffer is used to store raw data captured from the network before it is written to disk, and the statistical buffer stores statistical data entries (example buffer change shown in Figure 1 (page 12)).

Note: All packets seen by the capture card interface are time-stamped immediately, then are passed to the capture buffer. This ensures the most accurate time stamp.

Experimenting with buffer sizes is encouraged; it may take some time to find a balance between how large or small your buffer sizes should be for a probe instance, and it depends greatly on how the probe instance is used. Try finding the best balance between what the probe instance needs to operate efficiently and how much RAM a fully-maxed buffer would leave for other services to use.

The default settings for the statistical buffer work perfectly well for most installations—change them if they do not. The packet capture buffer, however, typically needs increasing or decreasing to best reflect your system.

Figure 1: Changing your buffer sizes



To change the buffer sizes of probe instances, complete the following:

1. On the Home tab, in the Probe group, click **Setup** > **Memory and Security Administration**.
2. Double-click the probe instance you want to configure.
3. Change the buffer sizes to better match the needs of your chosen probe instance.
4. (Optional) Select a statistics memory configuration from the list.

   (Optional) These choices affect the maximum number of entries per statistic tracked in real-time statistic modes. A larger choice allows more statistical entries to be held in non-reserved system memory (RAM available to Windows) than its preceding, smaller choice. The size shown is the maximum memory allowed to be used for this purpose—the memory footprint can grow up to this size but never greater. The memory used here follows FIFO rules (first-in, first-out), meaning if the limit is reached, the oldest data is discarded as the newest data arrives. Remember, this setting only affects real-time statistics modes only, and any statistics modes running will continue to fill up to your chosen limit for however long your real-time

statistics tools are running. This is because the memory is not flushed until all statistical mode windows are closed.

5. (Optional) Select a trending memory configuration from the list.

   (Optional) These choices affect the maximum number of entries per statistic tracked in network trending during a 1-minute collection interval. One IP pair would be an example of one entry. The size shown is the maximum memory allowed to be used for this purpose—the memory footprint can grow up to this size but never greater. The memory used here follows FIFO rules (first-in, first-out), meaning if the limit is reached, the oldest data is discarded as the newest data arrives.

6. Click **OK** twice to confirm and save your changes.

You successfully changed the buffer sizes of a chosen probe instance. In the future, you may need to re-evaluate your buffer sizes using the same process; this is especially true after adding or removing memory from your system or after adding new probe instances.

How to install a version of GigaStor

Installing a software upgrade downloads the self-extracting setup executable and immediately installs the upgrade.

To install a software upgrade:

1. Click the File tab, and click **Info** > **Update Observer**.
2. Select an item by clicking it.
3. Click the install icon .

   The download begins, and you can view its transfer progress.

   After the download completes, the software upgrade begins installing.

You successfully installed the selected software upgrade. A notification appears if any errors occur during the upgrade.

How to change the GigaStor storage directory or drive

You can change the directory where packets collected by your GigaStor are stored. However, if you are using a GigaStor hardware appliance, this should always remain set to `D:\DATA`.

This can also be performed on any Observer and is not limited to the GigaStor.

Some reasons for changing the GigaStor storage directory include:

- You are using the GigaStor Software Edition and need to store packets somewhere else than the C:\ drive.
- You regularly schedule packet captures, so you want those captures to be saved in a specific location.
- You need to store packet captures on a higher capacity hard disk.

To change the directory where collected packets are stored:

1. Click the File tab, and click **Options** > **General Options**.
2. Click the **Folders** tab.
3. Change the directory used for packet captures.

How to change the monitored network adapter

If your probe has multiple network cards in it, you can choose which card you want to monitor.

This section applies to all probes and all versions of them, including Single Probe, Multi Probe, and Expert Probe on VIAVI or third party hardware.

> **Tip!** If you are seeing only broadcast traffic, you do not have the correct network card selected or you do not have your switch port configured correctly as a SPAN/mirror port. Change the network adapter you are monitoring or configure the SPAN/mirror port.

- When choosing the monitored adapter from within Observer for all probe versions:

1. In the probes list, select the probe instance.
2. Choose **Setup** > **Select NIC**.

   The **Select Network Adapter** window appears.
3. Select the network adapter you want to monitor, and click **Select**.

The probe instance is now using the newly selected adapter.

Understanding GigaStor protocol and port settings

Allow the GigaStor to get smarter by collecting more information. Over time as the GigaStor sees more of your network's traffic, it gets smarter about the traffic on your network.

Unless you have a specific reason to do so, we recommend that you leave these options selected:

Enable intelligent TCP protocol determination—when checked, all new data collected is indexed by protocol, only if SYN-SYNACK-ACK packets are observed at the start of the conversation. If this combination is found, reports show this conversation by protocol name (or custom name), IANA name, or port number (based on statistics lists setting). Otherwise the conversation is not listed. If you try to analyze data prior to the time that this option was enabled, you will not see this data. Data must be collected with this option enabled for GigaStor reports to present the data correctly using the **Update Reports** button. By clearing this option, you ensure you get all protocol information regardless of SYN-SYNACK-ACK packets.

Limit to ports defined in "Protocol Definitions"—limits the displayed data to the ports specifically defined in the **Options** > **Protocol Definitions** dialog. Again, this is written to the internal GigaStor index. This option only shows custom protocols defined on new data collected after a protocol port has been defined. You must also choose **Apply Protocol to all Instances** to ensure this data is shown on all instances used for analysis. By clearing this setting, all ports are used.

Setting a schedule for when data captures should occur

One way to ensure you always have timely packet captures is to schedule them. For example, you may want to automatically start a packet capture at the beginning of business hours each day; you can accomplish this by scheduling your packet captures accordingly.

To schedule packet captures to begin at preset times, complete the following steps:

1. On the Home tab, in the Capture group, click **GigaStor**.
2. Click the **Settings** button.

   The **GigaStor Settings** window appears.
3. Click the **Schedule tab**.
4. Select one of the following scheduling types. For the GigaStor active instance you should choose **Always** unless you have a specific reason to choose a different option.

   - No scheduling—captures are never scheduled

- Always—capture runs at all times
- Daily at specified times—capture runs at same time each day

  You must specify a capture begin and end time by clicking the Add button for each day you select. Multiple time intervals are configurable, per day, if the times do not conflict.

5. In the **Reserve scheduling for** section, select GigaStor and click **OK**.

   You may receive a notice about scheduling reservation. If you do, click **Yes** to change the scheduling.

6. Click **OK** to confirm and save your changes

Scheduling your network trending data collection

You can configure Observer to run network trending data collection continuously or at certain days and times.

To do this, complete the following steps:

1. On the Home tab, in the Capture group, click **Network Trending** > **Network Trending**.
2. Click the **Settings** button. The **Network Trending Settings** window appears.
3. Ensure the General group tab is selected, and click the Schedule tab.
4. Select a scheduling type for network trending data collection.
5. Click **OK** to save your changes.

The trending types you enable continue to be collected according to schedule.

Index

Numerics

10 Gb Probe 9
32-bit 10
64-bit 10
64-bit, RAM 10

A

allocating 11

B

BIOS memory hole 10
broadcast traffic 13
buffers 10
  configuring 11

C

capacity 8
configuration 4
configure 4
configuring 11

D

data rate 9
data storage 13
data, collecting 15
defining its purpose 11
directory 13

E

Expert Probe
  changing NIC 13

G

Gigabit Probe 9
GigaStor 11
  RAM 11
  reserved memory 11
GigaStor Control Panel
  packet capture 14, 14
  scheduled capture 14
GigaStor Software Edition 6
GSE 4, 6, 8

H

hardware 6

I

installation 4
installing 4

L

license 8

M

minimum specifications 6
minimum specs 6
missing from Observer 13
Multi Probe
  changing NIC 13

N

network adapter, see also NIC 13
network trending
  data, collecting 15
  scheduling 15
network trending disk space requirements 9
network trending hard drive space 9
Network Trending Schedule 15
network trending space required 9
NIC
  broadcast traffic 13
  changing 13
  missing 13
  missing from Observer 13
no network card 13

O

Observer
  no network card 13
Observer Analyzer 9
Observer GigaStor 9
operating system 8

P

packet capture 14, 14
packet capture directory 13
packet captures
  configuring 11
ports 14
probe instance
  defining its purpose 11
protected memory 10
protocols 14

R

RAM 6, 11
allocating 11
GigaStor 11
recommendations 10
RAM needed for busy networks 11
recommendations 10
recommended specifications 6
recommended specs 6
reserved memory 10, 11

S

scheduled capture 14
scheduling 15
set up 4
Single Probe
changing NIC 13
software edition 4
SPAN ports
broadcast traffic 13
specifications 6
specs 6
statistics
RAM needed for busy networks 11
statistics queue buffer 10, 11
storage 6
storage size 8
system specification 6

T

third-party hardware 6

V

virtual machine 6
VM specs 6
VMware 6
vSphere 6

W

Windows
32-bit 10
64-bit 10
Windows 10 8
Windows 2003 8
Windows 2008 8
Windows 2012 8
Windows 2016 8
Windows 7 8
Windows 8 8
Windows Vista 8