SolarWinds Orion

NetFlow Traffic Analyzer Administrator Guide

solarwinds

ORION NETFLOW TRAFFIC ANALYZER

Copyright© 1995-2009 SolarWinds, Inc., all rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft®, Windows 2000 Server®, and Windows 2003 Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide, Version 3.5, 08.13.2009

About SolarWinds

SolarWinds, Inc develops and markets an array of network management, monitoring, and discovery tools to meet the diverse requirements of today's network management and consulting professionals. SolarWinds products continue to set benchmarks for quality and performance and have positioned the company as the leader in network management and discovery technology. The SolarWinds customer base includes over 45 percent of the Fortune 500 and customers from over 90 countries. Our global business partner distributor network exceeds 100 distributors and resellers.

Contacting SolarWinds

You can contact SolarWinds in a number of ways, including the following:

Team	Contact Information
Sales	sales@solarwinds.com www.solarwinds.com 1.866.530.8100 +353.21.5002900
Technical Support	www.solarwinds.com/support
User Forums	www.thwack.com

Conventions

The documentation uses consistent conventions to help you identify items throughout the printed and online library.

Convention	Specifying
Bold	Window items, including buttons and fields.
Italics	Book and CD titles, variable names, new terms
`Fixed font`	File and directory names, commands and code examples, text typed by you
Straight brackets, as in [*value*]	Optional command parameters
Curly braces, as in {*value*}	Required command parameters
Logical OR, as in *value1*|*value2*	Exclusive command parameters where only one of the options can be specified

Orion NetFlow Traffic Analyzer Documentation Library

The following documents are included in the Orion NetFlow Traffic Analyzer documentation library:

Document	Purpose
Administrator Guide	Provides detailed setup, configuration, and conceptual information.
Evaluation Guide	Provides an introduction to Orion NetFlow Traffic Analyzer features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the Orion NetFlow Traffic Analyzer user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

The following documents supplement the Orion NetFlow Traffic Analyzer documentation library with information about Orion Network Performance Monitor:

Document	Purpose
Orion Network Performance Monitor Administrator Guide	Provides detailed setup, configuration, and conceptual information for Orion Network Performance Monitor.
Orion Network Performance Monitor Evaluation Guide	Provides an introduction to Orion Network Performance Monitor features and instructions for installation and initial configuration.
Page Help	Provides help for every window in the Orion Network Performance Monitor user interface
Release Notes	Provides late-breaking information, known issues, and updates. The latest Release Notes can be found at www.solarwinds.com.

Contents

About SolarWinds ..... *iii*

Contacting SolarWinds ..... *iii*

Conventions ..... *iii*

Orion NetFlow Traffic Analyzer Documentation Library ..... *iv*

Chapter 1

Introduction **1**

Why Install Orion NTA *1*

How Orion NTA Works *2*

Why Use Orion NTA *3*

Chapter 2

Installing Orion NetFlow Traffic Analyzer **5**

Licensing Orion NetFlow Traffic Analyzer *5*

Requirements *5*

- *Software Requirements* *6*
- *Hardware Requirements* *7*
- *Virtual Machine Requirements* *7*

NetFlow, IPFIX J-Flow, and sFlow Requirements *8*

Installing Orion NTA *8*

Configuring Basic Failover *10*

Chapter 3

Getting Started **11**

Adding Flow-enabled Devices and Interfaces *11*

Adding Flow Sources to Orion NTA *12*

Enabling the NetFlow Traffic Analysis Summary View *13*

Configuring Orion NTA Settings *14*

- *Configuring NetFlow Data Compression* *14*
- *Configuring Orion NTA Resources* *15*
- *Enabling the Automatic Addition of Flow Sources* *17*
- *Configuring Data Retention for Flows on Unmonitored Ports* *17*

Enabling Monitoring of Flows from Unmanaged Interfaces *18*
Configuring DNS and NetBIOS Resolution *19*
Configuring Database Maintenance *21*
Configuring Charting and Graphing Settings *22*
Configuring Monitored Ports and Applications *23*
Selecting IP Address Groups for Monitoring *25*
Configuring Protocol Monitoring *26*
Configuring NetFlow Types of Services *27*
Configuring NetFlow Collector Services Ports *28*

Deleting a NetFlow Source *29*

Chapter 4

Creating NetFlow Traffic Analyzer Reports **31**

Using Report Writer with Orion NTA *31*

NetFlow-specific Predefined Reports *31*

Chapter 5

Viewing NetFlow Traffic Analyzer Data in the Orion Web Console **33**

Adding NetFlow Resources to Web Console Views *33*

Monitoring Traffic Flow Directions *34*

Creating View Limitations *35*

Customizing Charts in NetFlow Traffic Analyzer *35*

Edit Resource Page *35*
Customize Chart Page *36*

Customizing Top XX Resources *37*

Using the NetFlow Traffic View Builder *37*

Interacting with the thwack® User Community *38*

Performing an Immediate Hostname Lookup *38*

Viewing Class-based Quality of Service (CBQoS) Data *39*

Chapter 6

Working with Orion NTA **41**

Locating and Isolating an Infected Computer *41*

Locating and Blocking Unwanted Use *42*

Recognizing and Thwarting a DOS Attack *42*

Appendix A

Software License Key 45

Installing License Manager 45

Using License Manager 46

Appendix B

Device Configuration Examples 47

Cisco NetFlow Configuration 47

Extreme sFlow Configuration 48

Foundry sFlow Configuration 48

HP sFlow Configuration 49

Index

Index 51

Chapter 1

Introduction

Orion NetFlow Traffic Analyzer (Orion NTA) provides a simple-to-use, scalable network monitoring solution for IT professionals that are managing any size sFlow, J-Flow, IPFIX, or NetFlow-enabled network.

Why Install Orion NTA

As companies and their networks grow, bandwidth needs grow exponentially. All modern connected industries invest significant amounts of time and money to ensure that enough bandwidth is available for business-critical activities and applications. When bandwidth needs exceed currently available capacity or when demand seems to expand beyond the abilities of your network, understanding bandwidth use is no longer a novel interest, but it becomes critical to deciding whether it is necessary to invest in more bandwidth or if stricter usage guidelines are sufficient to regain lost bandwidth.

With the advent of streaming media, voice over IP (VoIP) technologies, online gaming, and other bandwidth-intensive applications, you, as a network engineer, must answer more than the simple question of whether the network is up or down. You must answer why the network is not performing up to expectations.

If you need to know how and by whom your bandwidth is being used, Orion NTA provides a simple, integrated answer. You can quickly trace and monitor the bandwidth usage of a particular application or type of traffic. For example, if you see excessive bandwidth use on a particular interface, you can use Orion NetFlow Traffic Analyzer to see that the company meeting, consisting of streaming video, is consuming 80% of the available bandwidth through a particular switch. Unlike many other NetFlow analysis products, the network and Flow data presented in Orion NTA solution are not purely extrapolated data, but they are based on real information collected about the network by the Orion Network Performance Monitor product that is at the heart of Orion NetFlow Traffic Analyzer.

Out of the box, Orion NetFlow Traffic Analyzer offers broad monitoring and charting capabilities, coupled with detail-driven statistics, including the following:

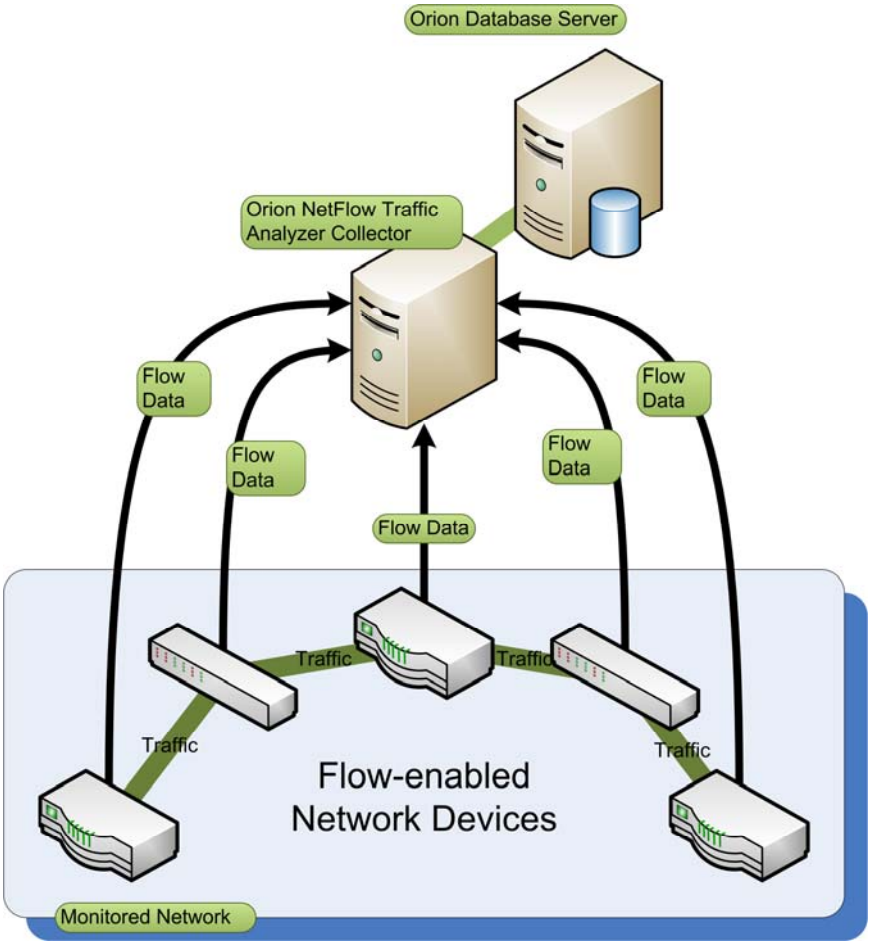
- Distribution of bandwidth across traffic types
- Usage patterns over time
- External traffic identification and tracking
- Tight integration with detailed interface performance statistics

These monitoring capabilities, along with the customizable Orion Web Console and reporting engines, make Orion NTA the easiest choice you will make involving your Flow monitoring needs.

How Orion NTA Works

Flow-enabled devices provide a wealth of IP-related traffic information. Orion NTA collects this Flow data, correlates it into a useable format, and then presents it, with detailed network performance data collected by Orion NPM, as easily read graphs and reports on bandwidth use in and to your network. These reports help you monitor bandwidth, track conversations between internal and external endpoints, analyze traffic, and plan bandwidth capacity needs.

The following diagram provides an overview of a simple Orion NTA installation to show, generally, how Orion NTA works.



Why Use Orion NTA

The following valuable features provided the impetus for the development of Orion NTA, and they are the foundation upon which Orion NTA is built:

Filtered views including both ingress and egress traffic

Orion NTA now provides the ability to select the direction of traffic over any viewed interface. On any monitored interface, you can now view traffic data for ingress traffic, egress traffic, or both.

Support for IPFIX-enabled devices

Internet Protocol Flow Information Export is a developing standard for formatting and transmitting IP-based network traffic information. As more devices features IPFIX capability, Orion NTA will immediately be able to provide IPFIX Flow monitoring.

Cisco Class-based quality of service (CBQoS) monitoring

Orion NTA provides resources giving you the ability to easiily view, chart, and report on the effects of the class-based quality of service policies you have enabled on your CBQoS-capable Cisco devices.

Improved availability and performance

With Orion NTA, you can more quickly detect, diagnose, and resolve network slowdowns and outages.

Analytical capacity planning

Orion NTA highlights trends in network traffic, enabling you to intelligently anticipate changes in bandwidth to areas that are experiencing bottlenecks.

Optimized network resource allocation

Information provided by Orion NTA enables you to identify and reassign areas with excess bandwidth capabilities to areas with limited or stressed connections.

Alignment of IT resources with enterprise business needs

Because Orion NTA is built on the proven Orion NPM infrastructure, you can assess both the needs of the enterprise network in a high-level overview and the functional details of specific interfaces and nodes.

Increased network security

Orion NTA gives you the ability to quickly and precisely pinpoint network traffic and expose curious patterns, unwanted behaviors, and anomalous usage that may indicate possible virus, bot, or spyware infection.

Support for multiple Flow ports

The number and types of available Flow-enabled devices has increased, so the number of ports over which Flow data is transmitted has also increased. Orion NTA now supports the designation of multiple ports on which Flow data may be received.

An all-in-one NetFlow, sFlow, J-Flow, and IPFIX monitoring solution

Now you can stop switching between network monitoring packages to acquire a complete picture of the usage, performance, and needs of your network, regardless of the type of Flow records provided by your various network devices.

Chapter 2

Installing Orion NetFlow Traffic Analyzer

Orion NTA provides a simple, wizard-driven installation process for collecting data from any Flow-enabled devices monitored by Orion Network Performance Monitor. For an enterprise-class product, the requirements are nominal, even though Flow data is extensive and can use a large amount of database space.

Licensing Orion NetFlow Traffic Analyzer

Licensing for NetFlow Traffic Analyzer follows the licensing levels of your underlying Orion Network Performance Monitor installation. For more information about Orion NPM licensing, see “Licensing Orion Network Performance Monitor” in the *Orion Network Performance Monitor Administrator Guide*.

The following types of NetFlow licenses are currently available.

- Orion NetFlow Traffic Analyzer for Orion SL100
- Orion NetFlow Traffic Analyzer for Orion SL250
- Orion NetFlow Traffic Analyzer for Orion SL500
- Orion NetFlow Traffic Analyzer for Orion SL2000
- Orion NetFlow Traffic Analyzer for Orion SLX

Notes:

- As your database size increases with the addition of more Flow-enabled interfaces, consider first collecting NetFlow data on one or two interfaces for a period of time to understand the memory requirements of your installation of Orion NTA. Then, add more interfaces to ensure that your database scales as needed and that your memory needs are fully understood.
- Though licensing limits the maximum number of interfaces you can monitor with Orion NTA, the effective capacity of your installation may be lower if monitored interface throughput is especially high.

Requirements

The server you use to host your NetFlow solution must support both Orion NPM and Orion NTA as Orion NTA is built on and extends Orion NPM. The following sections provide minimum configuration requirements.

Note: By default, Orion NTA listens for Flow data on port 2055 (UDP). Ensure that port 2055 is open for UDP communication on any Orion NTA collector.

Software Requirements

The following tables list software requirements for the current Orion NTA version. With the exception of the recommendation against using SQL Express for even a small network, the following software requirements are met by an installation where Orion NPM version 9.5 and SQL Server are on separate servers.

Notes:

- Orion NTA and SQL Server must be installed on separate physical servers.
- SQL Express and MSDE restrict the size of any database to 4GB and 2GB, respectively. For this reason, SolarWinds does not support the use of either SQL Express or MSDE with Orion NTA in production environments.

Orion NTA Server Software	**Requirements**
Orion NPM	Version 9.5 SP2 or higher
Operating System	Windows 2008 Server (32- or 64-bit) Windows 2003 Server R2, SP1 and higher (32- or 64-bit) IIS must be installed, running in 32-bit mode. SolarWinds recommends that Orion NPM administrators have local administrator privileges to ensure full functionality of local Orion NPM tools. Accounts limited to use of the web console do not require administrator privileges. **Note:** SolarWinds does not support production environment installations of Orion NTA on Windows XP or Vista.
Web Server	Microsoft IIS version 6.0 and later. DNS specifications require that hostnames be composed of alphanumeric characters (`A-Z`, `0-9`), the minus sign (`-`), and periods (`.`). Underscore characters (_) are not allowed. For more information, see *RFC 952*. **Note:** SolarWinds neither recommends nor supports the installation of Orion NTA on the same server or using the same database server as a Research in Motion (RIM) Blackberry server.
.NET Framework	Version 3.5 or later
SNMP Trap Services	Windows operating system management and monitoring tools component
Web Console Browser	Microsoft Internet Explorer version 6 or later with Active scripting Mozilla Firefox 3.0 or later

SQL Server Software	**Requirements**
Operating System	Windows 2008 Server (32- or 64-bit) Windows 2003 Server R2, SP1 and higher (32- or 64-bit) IIS must be installed, running in 32-bit mode. SolarWinds recommends that Orion NPM administrators have local administrator privileges to ensure full functionality of local Orion NPM tools. Accounts limited to use of the web console do not require administrator privileges.
SQL Server	SQL Server 2005 SP1 Standard or Enterprise SQL Server 2008 Standard, or Enterprise **Note:** Though SQL Express may be used, for evaluation purposes, to monitor one or two interfaces, for a very limited time, SolarWinds recommends against its use for larger networks.

Hardware Requirements

The following table lists minimum hardware requirements for monitoring a typical network with the current version of Orion NTA.

Note: Orion NTA requires that TCP port 17777 is opened both to send and to receive traffic between Orion NPM and any other Orion modules.

Warning: The only RAID configurations that should be used with Orion NTA are 0, 1, 0+1, or 1+0. Due to the high speed and large memory requirements of NetFlow data transactions, SANs or other RAID configurations should not be used, as they may result in data losses and significantly decreased performance.

Hardware	Requirements
CPU	3GHz or faster, dual processors with dual cores
RAM	2GB or more
Hard Drive Space	**Orion NTA server:** 5GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended. **SQL Server:** 5GB or more, RAID 0, 1, 01, or 10 on at least 6 spindles. Other RAID or SAN configurations are not recommended.
NetFlow devices	Cisco devices using NetFlow version 5 or 9 **Note:** Orion NTA only recognizes NetFlow version 9 templates that include all fields included in the NetFlow version 5 template.
IPFIX devices	Network devices using IPFIX
J-Flow devices	Network devices using J-Flow
sFlow devices	Network devices using sFlow version 5

For more information about Flows supported by Orion NTA, see “NetFlow, IPFIX J-Flow, and sFlow Requirements” on page 8.

Virtual Machine Requirements

Orion NTA may be installed on VMware Virtual Machines and Microsoft Virtual Servers if the following requirements are met by each virtual machine.

Virtual Machine Configuration	Requirements
CPU Speed	3.0 GHz
Allocated Hard Drive Space	**Orion NTA server:** 5GB or more, RAID 0, 1, 01, or 10. Other RAID or SAN configurations are not recommended. **SQL Server:** 5GB or more, RAID 0, 1, 01, or 10 on at least 6 spindles. Other RAID or SAN configurations are not recommended.
Memory	2GB or more
Network Interface	Each installation of Orion NPM should have its own, dedicated NIC **Note:** Since Orion NPM uses SNMP to monitor your network, if you are unable to dedicate a network interface card to your Orion NPM installation, you may experience gaps in monitoring data due to the low priority generally assigned to SNMP traffic.

For more information about Orion NPM requirements, see “Requirements” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

NetFlow, IPFIX J-Flow, and sFlow Requirements

Most Flow-enabled devices use a set of static templates to which exported flows conform. Any NetFlow, IPFIX, J-Flow, or sFlow packets that do not include the following field types and field values are ignored by Orion NTA:

Field Type	Field Type Number	Description
`IN_BYTES`	1	Ingress bytes counter
`IN_PKTS`	2	Ingress packets counter
`PROTOCOL`	4	Layer 4 protocol
`SRC_TOS`	5	Type of Service byte setting on ingress interface
`L4_SRC_PORT`	7	Source TCP/UDP port
`IPV4_SRC_ADDR`	8	Source IP address
`INPUT_SNMP`	10	SNMP ingress interface index
`L4_DST_PORT`	11	Destination TCP/UDP port
`IPV4_DST_ADDR`	12	Destination IP address
`OUTPUT_SNMP`	14	SNMP egress interface index

Notes:

- Only one interface index is absolutely required, but both interface indexes (`INPUT_SNMP` and `OUTPUT_SNMP`) should be provided to view accurate statistics for both ingress and egress flows.
- If SolarWinds states that Orion NTA supports Flow monitoring for a device, at least one of the templates the device exports satisfies these requirements.

Installing Orion NTA

Complete the following procedure to install Orion NTA. You must provide your NetFlow traffic port and confirm that it is enabled and sending Flow data in order to complete your installation.

To install Orion NetFlow Traffic Analyzer:

1. Log on to the Orion NPM server that you want to use for Flow analysis.

   Notes:

   - SolarWinds generally recommends that you backup your database before performing any upgrade.
   - Current Orion NTA versions require Orion NPM version 9.5 SP2 or later.
   - If you are upgrading from Orion NTA version 1.0, you must first uninstall Orion NTA version 1.0 before installing the current release.
   - You must upgrade to Orion NTA version 3.1 before upgrading to the current version of Orion NTA.

2. ***If you are installing Orion NTA on a terminal server,*** perform the following steps before continuing with your installation:
   a. Click **Start > Control Panel > Add or Remove Programs**.
   b. Click **Add New Programs**.
   c. Click **CD or Floppy**.
   d. Click **Next** in the Install Program From Floppy Disk or CD-ROM window.
3. ***If you downloaded the product from the SolarWinds website,*** navigate to your download location, and then launch the executable.
4. ***If you received physical media,*** navigate to the autorun, and then launch the setup program. If the autorun does not automatically start, run the `autorun.exe` in the root of the DVD.
5. ***If this installation is an upgrade of a previous version of Orion NTA,*** click **Yes** when you are asked to continue to perform an upgrade of SolarWinds Orion NetFlow Traffic Analyzer.
6. Review the Welcome text, and then click **Next**.
7. Accept the terms of the license agreement, and then click **Next**.
8. Click **Install**.
9. Provide the appropriate information on the Install Software License Key window, and then click **Continue**.

   Note: You need your customer ID and password to successfully install the key. For more information, see “Software License Key” on page 45.
10. Click **Continue** when the license is successfully installed.
11. When the InstallShield Wizard completes, click **Finish** to exit the wizard.
12. ***If you are installing NetFlow Traffic Analyzer on a terminal server,*** click **No** if the wizard asks you to reboot your server. Otherwise, click **Yes** if the wizard prompts you to reboot your server.
13. ***If the Configuration Wizard does not start automatically,*** click **Start > All Programs > SolarWinds Orion > Configuration Wizard**.
14. Review the Orion Configuration Wizard welcome text, and then click **Next**.
15. Confirm that all services that you want to install are checked in the Service Settings window, and then click **Next**.
16. Review the configuration summary, and then click **Next**.
17. Click **Finish** when the Orion Configuration Wizard completes.

18. ***If you are asked to select a polling engine to manage,*** select the Orion server you are using as your NetFlow collector, and then click **Connect to Polling Engine**.

19. Proceed to add your NetFlow devices and interfaces to Orion Network Performance Monitor. For more information about adding NetFlow devices, see “Adding Flow-enabled Devices and Interfaces” on page 11.

Configuring Basic Failover

If you have an Orion Hot Standby engine installed with Orion NetFlow Traffic Analyzer and your Flow-enabled device allows you to define two or more export targets, you can configure a basic Orion NTA failover system.

To configure basic failover for Orion NetFlow Traffic Analyzer:

1. Either use SolarWinds Orion Network Configuration Manager (Orion NCM) or connect to the console of your device to configure your Flow-enabled device to send exported Flow data to both your Orion Hot Standby server and the primary Orion server.

   Note: Not all devices support the ability to define two or more export targets. For more information, see your device documentation.

2. Configure an alert to notify you when your primary Orion server is no longer responding. For more information, see *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Chapter 3

Getting Started

To begin analyzing available Flow data produced by devices within your network, you must either add a Flow-enabled interface to your Orion database or monitor a previously added interface that is capable of generating NetFlow data. Adding your NetFlow devices and interfaces to the Orion database and adding your NetFlow devices and interfaces to Orion NTA as NetFlow sources are separate procedures, detailed in separate sections, as follows.

Note: If you already have Flow-enabled devices on your network, Orion NTA can automatically add them as NetFlow sources if you configure your Flow-enabled devices to send their Flows to your designated Orion NTA server. For more information, see “Device Configuration Examples” in the *SolarWinds Orion NetFlow Traffic Analyzer Administrator Guide*.

Adding Flow-enabled Devices and Interfaces

Before Orion NTA can analyze network traffic, the Flow-enabled network interfaces on which you want to monitor traffic must be managed by Orion NPM. An arrangement of this kind does not affect licensing requirements for either Orion NPM or Orion NTA.

Adding Flow-enabled devices and interfaces to Orion NPM and designating the same devices and interfaces as Flow sources in Orion NTA are separate actions. Flow-enabled devices must be added to the Orion database using either Network Sonar or Web Node Management in Orion NPM before they can be monitored by Orion NTA. For more information about designating Flow sources in Orion NTA, see “Adding Flow Sources to Orion NTA” on page 12.

The discovery methods in the following procedure add devices and interfaces to Orion NPM. If you have already configured device interfaces to send Flow data, Orion NTA will detect and analyze Flow data, as soon as the device is added,.

To add your devices and Flow-enabled interfaces to Orion NPM:

1. Log on to the Orion NPM server that hosts Orion NTA.

   Note: The current version of Orion NTA requires Orion NPM 9.5 SP2 or later.

2. ***If you are adding a large number of nodes,*** use Orion Network Sonar. For more information, see “Discovering and Adding Network Devices” in the *Orion Network Performance Monitor Administrator Guide*.

   Note: Confirm that you add all Flow-enabled interfaces on added devices.

3. ***If you are only adding a few nodes,*** it may be easier to use Web Node Management in the Orion Web Console. For more information, see “Adding Devices for Monitoring in the Web Console” in the *Orion Network Performance Monitor Administrator Guide*.

4. Click **NetFlow Traffic Analysis** in the Modules menu bar to confirm the addition of all Flow sources on your network. For more information, see “Adding Flow Sources to Orion NTA” on page 12.

After installing Orion NTA, the Orion NPM polling engine establishes a baseline by collecting network status and statistics immediately. Then, 30 seconds later, the Orion NPM polling engine performs another collection. You may notice an increase in your CPU usage during this time. After these initial collections, Orion NPM collects network information every 10 minutes for nodes and every 9 minutes for interfaces. Meaningful Flow analysis data should display in the web console within minutes. Before leaving Orion NTA to gather data, ensure you are collecting Flow data for the correct interface ports and applications. For more information, see “Configuring Monitored Ports and Applications” on page 23.

Adding Flow Sources to Orion NTA

After devices with Flow-enabled interfaces have been added to Orion NPM, Orion NTA must recognize the new devices for monitoring. If a Flow-enabled device is already properly configured and sending Flow data to the Orion server, Orion NTA will automatically detect the new Flow source. Depending on your Orion NTA configuration, you will be prompted to add the detected Flow-enabled device or the Flow-enabled device will be automatically added. The following procedure confirms the addition of Flow sources to Orion NTA.

Note: If you are using NetFlow version 9 you must confirm that the template you are using includes all fields included in NetFlow version 5 PDUs.

To confirm the addition of Flow sources to Orion NTA:

1. Log on to the Orion NPM server that hosts Orion NTA.

2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.

3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. ***If automatic addition of NetFlow sources is enabled,*** the new Flow source will display in the NetFlow Sources resource. For more information about the automatic addition of NetFlow Sources option, see “Enabling the Automatic Addition of Flow Sources” on page 17.

5. ***If the NetFlow Sources resource is present,*** click **Edit** in the resource header.

   Notes: The NetFlow Sources resource is included, by default, in the NetFlow Traffic Analysis Summary View. If the NetFlow Traffic Analysis Summary view, including the NetFlow Source resource, is not enabled as the default NetFlow Web Console view, see “Enabling the NetFlow Traffic Analysis Summary View” on page 13.

6. ***If the NetFlow Sources resource is not displayed,*** complete the following steps:

   a. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

   b. Click **Edit** under the NetFlow Sources heading.

7. ***If you want to select all available interfaces for monitoring,*** select **All…** from the Showing menu, check next to ROUTER and INTERFACE, and then click **Submit**.

   Note: Exporters only (last 15 minutes) is the default filter. This option shows all devices in your Orion database that have sent Flow data within the last 15 minutes. If you expect other devices to export Flow data in the future, select another option, as described in the following steps.

8. ***If you want to select specific interfaces for monitoring,*** use the following procedure:

   a. Click **+** as necessary to see all available interfaces, and then select interfaces by any of the following methods:

      - Check individual interfaces
      - Check nodes to select all interfaces on the selected node
      - Check device types to select all devices of the selected types.

   b. When you have selected all interfaces to monitor, click **Submit**.

Enabling the NetFlow Traffic Analysis Summary View

If the NetFlow Web Console does not display the NetFlow Traffic Analysis Summary view by default, use the following steps to enable it.

To enable the NetFlow Traffic Analysis Summary view:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.

3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. Click **Admin** in the Views menu bar, and then click **Account Manager** in the Accounts grouping of the Orion Website Administration page.
5. Select **Admin**, and then click **Edit**.
6. Under the Default Menu Bar and Views heading, click **+** next to **Admin's NetFlow Traffic Analysis Settings**.
7. In the NetFlow Traffic Analysis View field select **NetFlow Traffic Analysis Summary**.
8. Click **Submit** at the bottom of the page.
9. Click **NetFlow Traffic Analyis** in the Modules menu bar to display the NetFlow Traffic Analysis Summary page.

Configuring Orion NTA Settings

Each of the following sections provides instructions for configuring Orion NTA and customizing it to meet your network analysis requirements.

Note: The configuration actions in the following sections require administrative access to the Orion Web Console.

Configuring NetFlow Data Compression

Flow-enabled devices can provide a great amount of data. As a result, the Orion database may quickly become unmanageable unless received Flow statistics are compressed. Flow data compression in Orion NTA proceeds as follows:

1. By default, received Flow data is stored in an uncompressed state for 60 minutes, as designated in the **Keep uncompressed data for** field on the NetFlow Settings view.

   Note: This period of may be extended to four hours.

2. As stored Flow data ages beyond the uncompressed data retention period, it is summarized into 15-minute intervals.
3. After a full day, 15-minute intervals are summarized into one-hour intervals.
4. After one week, one-hour intervals are summarized into daily intervals and then stored for the period indicated in the **Keep compressed data for** field on the NetFlow Settings view.
5. Compressed data that is older than the period designated in the **Keep compressed data for** field is then deleted.

The following procedure configures Orion NTA data compression settings on the NetFlow Settings view.

Note: Collect data for a day before adjusting these settings. You should then have an idea of the volume of data your network produces with NetFlow enabled.

To configure data compression in Orion NTA:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar.
5. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
6. Click **Edit** under the Global Settings heading.
7. Select a number of minutes in the **Keep uncompressed data for** field.

   Note: The smallest uncompressed period that you can set is 15 minutes. This minimum ensures that at least 15 minutes of realtime data is collected and compressed before any of it is possibly deleted. NetFlow data that is older than this value is compressed and stored.
8. Type a number of days in the **Keep compressed data for** field.

   Note: NetFlow data may be stored in a compressed form for a longer period of time before it is finally deleted from your database. All data older than the value set here is deleted, but it may take up to a few days to fully remove compressed data, especially in large databases, after changing this setting.
9. Click **Submit**.

Configuring Orion NTA Resources

Orion NTA provides global options for both resource time periods and the type of percentages used in Top *XX* resources, as described in the following sections:

Configuring Top *XX* Resource Percentages

Orion NTA Top *XX* resources may be configured to show any number of items, listed in either absolute or relative terms of overall traffic percentage. Absolute percentages are calculated for each item based on all monitored items. Relative percentages for each item are calculated in terms of the total number of items displayed in the selected resource.

For example, a given node (HOME) is communicating with 4 other endpoints (1, 2, 3, and 4). The following table details the two percentage types calculated and displayed for both Top 3 Endpoints and Top 4 Endpoints resources.

Endpoint	Traffic	Percentage of Total Actual Traffic	Absolute Percentage		Relative Percentage	
			Top 4	Top 3	Top 4	Top3
1	4 MB	40 %	40 %	40 %	40 %	44.4%
2	3 MB	30 %	30 %	30 %	30 %	33.3%
3	2 MB	20 %	20 %	20 %	20 %	22.2
4	1 MB	10 %	10 %	Not Shown	10 %	Not Shown
TOTAL	10 MB	100 %	100 %	90 %	100 %	100 %

The following procedure configures Top *XX* resource percentages.

To configure the percentage type used for Top *XX* resources:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the Global Settings heading.
6. Below the available data compression options, select either **Calculate Absolute Percentages for Top XX Lists Percentages** or **Calculate Relative Percentages for Top XX Lists Percentages**, as appropriate.
7. Click **Submit**.

Configuring Resource Default Time Periods

By default, all Orion NTA resources are configured to display data for the last 15 minutes. The time period for any Orion NTA resource may be configured either by clicking **Edit** in the header of each individual Orion NTA resource, or by globally setting the default time period for all Orion NTA resources on the Edit Global Settings page, as shown in the following procedure.

To globally configure the default resource time period:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.

3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the Global Settings heading.
6. Below the data compression and Top *XX* list percentage options, provide a value and appropriate time units as the default resource time period.
7. Click **Submit**.

Enabling the Automatic Addition of Flow Sources

Orion NTA is capable of detecting and automatically adding Flow sources as soon as they are added to Orion NPM for monitoring. The following procedure enables this option in Orion NTA.

To enable the automatic addition of Flow sources:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. Click **Admin** in the Views menu bar.
5. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
6. Click **Edit** under the Global Settings heading.
7. Check **Enable automatic addition of NetFlow sources**.
8. Click **Submit**.

Configuring Data Retention for Flows on Unmonitored Ports

Orion NTA provides the option to retain data for any Flow occurring over an unmonitored port. By default, Orion NTA retains data for traffic on unmonitored ports, but some significant savings in terms of database storage space and server processing loads may be realized by disabling this option. For more information about unmonitored ports in Orion NTA, see “Configuring Monitored Ports and Applications” on page 23.

The following procedure configures the option of retaining data for traffic on unmonitored ports in Orion NTA.

Note: Enabling this option may significantly increase the processing load on both your Orion NTA server and your Orion database server.

To configure data retention for flows on unmonitored ports:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the Global Settings heading.
6. Check **Enable data retention for traffic on unmonitored ports**.
7. Click **Submit**.

Enabling Monitoring of Flows from Unmanaged Interfaces

In older versions, Orion NTA discarded any Flow record that referred to traffic involving an interface not already managed by Orion NPM. Currently, however, Orion NTA provides the option to retain data for any Flow defined by at least one managed interface. For more information about managing interfaces in Orion NPM, see “Discovering and Adding Network Devices” in the *SolarWinds Orion Network Performance Monitor Adminstrator Guide*.

The following procedure enables the option of monitoring traffic on unmanaged interfaces in Orion NTA.

Note: Disabling this option may significantly decrease the processing load on both your Orion NTA server and your Orion database server, but it will also decrease the amount of Flow data stored in your Orion database.

To enable the automatic addition of Flow sources:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the Global Settings heading.
6. Check **Allow monitoring of flows from unmanaged interfaces**.
7. Click **Submit**.

Configuring DNS and NetBIOS Resolution

To meet varied network requirements, Orion NTA provides options for both NetBIOS and DNS resolution of endpoint domain names. The following sections provide more information about each available type of domain name resolution.

Enabling NetBIOS Resolution

For networks where NetBIOS is the naming convention of preferred use, Orion NTA provides the option to resolve endpoint domain names using NetBIOS. The following procedure enables NetBIOS resolution in Orion NTA.

Note: Enabling NetBIOS resolution does not automatically disable DNS resolution of the same devices. For more information about configuring DNS resolution, see “Configuring DNS Resolution” on page 19.

To enable NetBIOS resolution:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar.
5. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
6. Click **Edit** under the Global Settings heading.
7. Check **Enable NetBIOS resolution of endpoints**.
8. Click **Submit**.

Configuring DNS Resolution

By default, Orion NTA uses persistent DNS to resolve the domain names of all endpoints referenced in monitored Flows. For most users, persistent DNS resolution optimizes overall performance. However, if you have a large number of

monitored endpoints, you may see measurable improvements in database query times by taking advantage of on-demand DNS resolution. To meet your specific network monitoring needs, Orion NTA provides the following options for configuring DNS resolution:

- **Persistent** DNS resolution is the default option, and it should be optimal for most users. For typically-sized networks, Orion NTA views will generally load more quickly as resolved domain names are retained.
- **On Demand** DNS resolution is intended to assist users with larger networks. With this option, an endpoint domain name is only resolved when information about it is actually requested from the Orion database. Database query times may be improved with this option as queries are limited, but the load time for some endpoint-related resources may increase as Orion NTA waits for domain name resolution.

  Warning: Top Domains resources and Orion reports that include DNS names require persistent domain name resolution, so they will not display DNS names if On Demand DNS resolution is enabled.
- Selecting **Disabled** turns DNS resolution off for the endpoints of flows monitored in Orion NTA. This is not generally recommended unless NetBIOS resolution already is enabled. For more information about enabling NetBIOS resolution, see “Enabling NetBIOS Resolution” on page 19.

  Warning: If DNS resolution is disabled, all DNS information will be deleted from the database to improve database performance,

Orion NTA also allows you to configure the interval between DNS lookups. Orion NTA performs regular DNS lookups on all monitored devices. By default, if the domain of a monitored device resolves successfully, Orion NTA will not attempt another DNS lookup on the same device for 7 days. If the domain name of a monitored device does not resolve successfully, by default, Orion will attempt to resolve the same device again in 2 days.

The following procedure configures all DNS resolution options in Orion NTA.

To configure DNS resolution:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

5. Click **Edit** under the Global Settings heading.
6. Select the type of **DNS Resolution** you want Orion NTA to use.
7. Provide the **Default number of days to wait until next DNS lookup**.

   Note: This value sets the interval on which endpoint domain names are refreshed in the Orion database if the persistent DNS resolution option is selected.
8. Provide the **Default number of days to wait until next DNS lookup for unresolved IP addresses**.

   Note: This value sets the interval on which Orion NTA makes an attempt to resolve domain names for unresolved endpoints in the Orion database if the persistent DNS resolution option is selected.
9. Click **Submit**.

Configuring Database Maintenance

Depending on the size, configuration, and usage levels of your network, your Flow-enabled network devices are capable of generating very large amounts of traffic data in a relatively short period of time. The volume of network data provided by your Flow-enabled devices can overwhelm even a large database very quickly if you do not enact scheduled database maintenance. With its scheduled database maintenance features, Orion NTA gives you the ability to properly manage the size of your Orion database. The following procedure configures your Orion database maintenance settings.

To configure scheduled database maintenance:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the Database Maintenance Settings heading.
6. Confirm that **Enable Database Maintenance** is checked.

   Note: Due to the high volume of data provided by Flow-enabled devices, some level of database maintenance is recommended for all monitored, Flow-enabled networks.

7. Provide an **Execution Time** at which database maintenance is to occur.

   Notes:

   - The database maintenance execution time should be well inside an established off-peak network usage window to minimize any potential disruption of required monitoring.
   - The **Execution Time** field can accept times entered in either 24-hour (`HH:MM`) or standard (`H:MM AM/PM` or `HH:MM AM/PM`) formats.

8. Select the frequency with which you want to **Delete expired flow data**.

   Note: SolarWinds recommends deletion of expired flow data **Once a day**.

9. Provide the **Custom number of expired IPs** to delete during each session of database maintenance.

   Note: Deleting a large number of expired IP addresses during any period of high network traffic may negatively affect Orion NTA performance.

10. Provide the **Custom number of minutes** to limit the amount of time spent deleting IP addresses during each session of database maintenance.

11. ***If you want to continuously delete flow records corresponding to expired IP addresses,*** select **Never stop processing expired IPs** in the Maximum minutes to process expired IPs area.

    Note: Continuously deleting expired IP addresses may negatively affect Orion NTA performance. By default, Orion NTA sets a maximum period of 15 minutes for processing expired IP addresses to ensure that excessive processing resources are not drawn away from monitoring your network.

12. Select how often you want to **Compress database and log files**.

    Note: SolarWinds recommends that you choose to compress database and log files **Once every ten days**.

13. Click **Submit**.

For more information about the Database Maintenance application packaged with Orion NPM, see “Database Maintenance” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

Configuring Charting and Graphing Settings

Due to the large amount of data that can be required to complete all charts on any web console view, the load times of some Orion NTA views can become significant. To help this condition, Orion NTA provides a progressive charting option that is enabled by default. The progressive charting option configures Orion NTA to draw charts incrementally, spreading the chart generation load over multiple database queries. For NetFlow installations monitoring and processing numerous data flows, progressive charting can minimize the amount of time you

have to wait before actually seeing charted data. The following procedure opens the Edit Charting and Graphing Settings page, where progressive charting may be enabled or disabled, as necessary.

To configure progressive charting:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the Charting and Graphing Settings heading.
6. ***If you want to disable progressive charting,*** clear **Enable Progressive Charting**.

   Note: Disabling progressive charting may significantly increase the amount of time it takes to load data into charts and graphs in web console views.
7. ***If you want to enable progressive charting,*** confirm that **Enable Progressive Charting** is checked.
8. Click **Submit**.

Configuring Monitored Ports and Applications

Orion NTA allows you to directly specify the applications and ports you want to monitor. Additionally, you can specify protocol types on a per-application basis, giving you the ability to monitor multiple applications on the same port if each application uses a different protocol. You should review this list of ports and applications and select the ports and applications you want to monitor, adding any that you do not see but need to monitor, as in the following procedure.

Note: The number of monitored applications directly affects the amount of NetFlow data stored in the database. The more applications and ports you monitor, the more data is stored. For more information about solving database size issues, see “Configuring NetFlow Data Compression” on page 14.

To configure monitored applications and ports:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.

3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.

4. Click **Admin** in the Views menu bar.

5. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.

6. Click **Edit** under Application and Service Ports.

7. Group the viewed applications and service ports by selecting the appropriate view type from the View menu on the left of the Manage Applications and Service Ports view.

   Note: By default, applications are listed by increasing associated port number, with mulit-port applications listed first.

8. ***If you do not know the port number or application name you want to monitor, but you do know a keyword in the application description,*** type the keyword in the **Search applications & ports** field, and then click **Search** to generate a list of related applications with their port numbers.

9. ***If you want to monitor all listed ports and applications,*** click **Enable All Monitoring** above the application list.

   Note: Due to the potential volume of data from Flow-enabled network devices, Monitoring all ports and applications may severely affect the performance of both the Orion database and the Orion Web Console. If you are not initially sure what ports and applications you should monitor with Orion NTA, click **Monitor Recommended Ports** to monitor the most typical, high-traffic ports and applications.

10. ***If you want to disable monitoring for all listed ports and applications,*** click **Disable All Monitoring** above the application list.

    Note: If, at first, you are not sure what ports and applications to monitor, click **Monitor Recommended Ports** to monitor the most typical, high-traffic ports.

11. ***If you do not see a port or application you want to monitor,*** complete the following steps to add a new application:

    a. Click **Add Application**.

    b. Provide the **Port(s)** and **Description** you want to add.

       Note: ***If you want to add a new multi-port application,*** enter port ranges or multiple ports, separated by commas, in the **Port(s)** field.

    c. Select the appropriate **Protocol** for the new application.

    d. Click **Add Application**.

12. ***If you want to disable monitoring for a single listed port or application,*** click **Disable** in the **Actions** field of the selected application.
13. ***If you want to delete a single listed port or application,*** click **Delete** in the **Actions** field of the selected application, and then click **Delete Application** in the Delete Application dialog.
14. ***If you want to edit the properties of a monitored port or application,*** complete the following steps:
    a. Click **Edit** in the **Actions** field of the selected application, and then edit the **Port(s)** and **Description** information for the selected application.

       Notes:

       - ***If you want to edit a multi-port application,*** enter port ranges or multiple ports, separated by commas, in the **Port(s)** field.
       - Some default multi-port applications may be configured with overlapping port assignments. Traffic will only be associated with one of the conflicting applications. To avoid this conflist, remove the port range of conflict or delete or disable a conflicting application.

    b. Select the appropriate **Protocol** for the selected application, and then click **Update Application**.

Selecting IP Address Groups for Monitoring

Orion NTA allows you to establish IP address groups for selective monitoring of custom categories or segments of your network. The following procedure sets ranges and descriptions for your network IP addresses so you can better characterize and assess the Flow data you receive.

To configure IP address group monitoring:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the IP Address Groups heading.
6. ***If any one of the pre-existing ranges contains the addresses you want Orion NTA to monitor,*** confirm that the range is checked.

7. ***If you want to edit an existing group,*** complete the following steps:
   a. Check the IP address group to edit, and then click **Edit**.
   b. Provide the starting and ending IP addresses of the range.
   c. Edit the Description, as necessary, and then click **Update**.
8. ***If you want to add a new group,*** complete the following steps:
   a. Click **Add New Group**.
   b. Provide the starting and ending IP addresses of the range.
   c. Provide a Description, and then click **Update**.
9. ***If you want to delete an existing group,*** check the group range, and then click **Delete** at the end of the IP address group row.

Configuring Protocol Monitoring

The types of transport protocols that Orion NTA monitors may be configured from the Monitored Transport Protocols page. This page allows you to specify precisely which protocols Orion NTA monitors. Selectively specifying monitored protocols can reduce the amount of Flow traffic Orion NTA has to process, improving overall performance. The following procedure enables selective transport protocol monitoring.

To specify protocols monitored by NetFlow Traffic Analyzer:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under Monitored Protocols.
6. Confirm that any and all protocols you do not want to monitor are cleared, and then confirm that all the protocols you do want to monitor are checked.

Configuring NetFlow Types of Services

Orion NTA recognizes the Differentiated Services model of packet delivery prioritization. All Flow-enabled devices may be configured to set a Type of Service byte, referred to as the Differentiated Service Code Point (DSCP), on all NetFlow packets that are sent. The DSCP prioritizes NetFlow packet delivery over the Flow-enabled devices on your network by assigning each packet both a Differentiated Service class (1, 2, 3, or 4) and a packet-dropping precedence (low, medium, or high). NetFlow packets of the same class are grouped together. Differentiated Services uses the DSCP to communicate per-hop behaviors (PHBs), including Assured Forwarding (AF) and Expedited Forwarding (EF), to the node services that a given packet encounters. PHBs are configured on individual devices when NetFlow is initially enabled. If a given node is overloaded with NetFlow traffic, node services will keep or drop NetFlow packets in accordance with the configured PHB that matches the DSCP in each NetFlow packet. For more information about Differentiated Services, see RFC 2474, RFC 2475, and RFC 3140.

PHBs, corresponding to Types of Services on Flow-enabled devices, may be configured with DSCPs within Orion NTA, as shown in the following procedure.

To configure types of services for NetFlow packets:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar, and then click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
5. Click **Edit** under the NetFlow Types of Service heading.
6. ***If you want to edit an existing type of service***, click **Edit** at the end of each Type of Service Name listing, edit the assigned name, and then click **Update** on the same line.

   Note: Individual DiffServ Code Points can not share multiple Type of Service Names, and individual Type of Service Names can not share multiple DiffServ Code Points.

Configuring NetFlow Collector Services Ports

NetFlow Collector Services provides status information about the NetFlow collector that is running Orion NTA. In case your Flow-enabled device configuration requires it, the following procedure resets or adds Flow collection ports on which your Orion NTA collector listens for Flow data. You can also delete a collector, if necessary.

Notes:

- If you are employing a firewall on your NetFlow collector, all ports on which the NetFlow collector listens for Flow data should be listed as firewall exceptions for UDP communications.
- By default, Orion NTA listens for Flow data on port 2055, but some Flow-enabled devices, including some Nortel IPFIX-enabled devices, send Flow data on port 9995. For more information about requirements for IPFIX-enabled devices, see “NetFlow, IPFIX J-Flow, and sFlow Requirements” on page 8.

To configure NetFlow collector services:

1. Log on to the Orion NPM server that hosts Orion NTA.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** in the Views menu bar.
5. Click **NTA Settings** in the Settings grouping of the Orion Website Administration page.
6. Click **Edit** under the NetFlow Collector Services heading.
7. ***If you want to add or reset a collection port,*** type the new port number in the **Collection Port** field of the collector that you want to edit.

   Notes:

   - Separate listed ports with a single comma, as in `2055,9995`.
   - The **Status Icon** displays your collector status visually, green indicating that the collector can receive Flow data and red indicating that it can not. **Server Name** provides the network identification of your collector, and **Receiver Status** is a verbal statement of collector status.

8. ***If you want to delete a collector,*** click **Delete**.

   Note: If you delete all collectors, you must either run the Configuration Wizard again to restore your initial settings or provide another collector from a different Orion poller.

9. Click **Submit** when you finish configuring your NetFlow collectors.

Deleting a NetFlow Source

To remove a NetFlow source, complete the following procedure.

To delete a NetFlow source:

1. Click **Edit** in the title bar of the NetFlow Sources resource
2. Select the type of device you want to delete from the **Showing** menu.
3. Expand the node tree to locate the source you want to delete, and then expand the source you want to delete.
4. ***If the source you want to delete is not already checked,*** check it.
5. Uncheck the source to stop monitoring it and all its interfaces.

   Note: Checking a node automatically selects all its interfaces.

Chapter 4

Creating NetFlow Traffic Analyzer Reports

Your Orion database can accumulate a great deal of Flow information that can be presented in a variety of formats using the Report Writer feature of Orion NPM. SolarWinds has developed Orion Report Writer to help you quickly and easily extract viewable data, including Flow statistics, from your Orion database.

Using Report Writer with Orion NTA

Several standard NetFlow-specific reports that you can modify are included in the Report Writer distribution, and you can create new reports as necessary. For more information, see “NetFlow-specific Predefined Reports” on page 31. In addition, as an Orion module, Orion NTA can also generate any of the predefined reports packaged with Orion NPM. For more information, see “Predefined Reports” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*. For more information about Report Writer, see “Creating Reports” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

When you have finished editing your reports, you can print them with the click of a button. You can also view most reports in the Orion Web Console by default. For more information, see “Customizing Views” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*. To schedule automatic email reports for individual users or groups of users, open the Orion Report Scheduler by clicking **Start > All Programs > SolarWinds Orion > Alerting, reporting, and Mapping > Orion Report Scheduler**.

Report Writer capabilities are enhanced when they are used in conjunction with the Custom Property Editor. Once added, properties are available for report sorting and filtering. For more information, see “Creating Custom Properties” in the *Orion Network Performance Monitor Administrator Guide*.

NetFlow-specific Predefined Reports

The following reports are immediately available with your NetFlow Traffic Analyzer installation under the heading Historical NetFlow Reports on the Network Performance Monitor Reports page, accessible by clicking **Reports** in the Views toolbar. These reports may be modified with Report Writer, as necessary, to suit your network performance reporting requirements. The following reports are predefined for your Flow-enabled network devices.

Note: All reports with domain information require persistent DNS resolution. For more information, see “Configuring DNS and NetBIOS Resolution” on page 19.

Top 100 Applications – Last 24 Hours

Displays the application name, port number used, user node, and bytes processed for the top 100 applications used by monitored devices on your network in the last 24 hours.

Top 20 Traffic Destinations by Domain – Last 24 Hours

Displays the destination domain name, source node, and bytes transferred for the top 20 destinations of traffic from monitored devices on your network in the last 24 hours.

Top 20 Traffic Sources by Domain – Last 24 Hours

Displays the source domain name, destination node, and bytes transferred for the top 20 sources of traffic to monitored devices on your network in the last 24 hours.

Top 5 Protocols – Last 24 Hours

Displays the protocol name and description, parent node, and bytes transferred for the top 5 protocols used by monitored devices on your network in the last 24 hours.

Top 5 Traffic Destinations by IP Address Group – Last 24 Hours

Displays the destination IP address group, source node, and bytes transferred for the top 5 destinations of traffic, by IP address group, from monitored devices on your network in the last 24 hours.

Top 5 Traffic Sources by IP Address Group – Last 24 Hours

Displays the source IP address group, destination node, and bytes transferred for the top 5 sources of traffic, by IP address group, to monitored devices on your network in the last 24 hours.

Top 50 Receivers – Last 24 Hours

Displays the full hostname, if available, IP address, source node, and bytes transferred for the top 50 receivers of traffic from monitored devices on your network in the last 24 hours.

Top 50 Transmitters – Last 24 Hours

Displays the full hostname, if available, IP address, destination node, and bytes transferred for the top 50 transmitters of traffic to monitored devices on your network in the last 24 hours.

Chapter 5

Viewing NetFlow Traffic Analyzer Data in the Orion Web Console

Once you have configured and enabled a NetFlow source, you can view the various types of NetFlow statistics that it records in the Orion NPM Web Console. Available NetFlow-specific resources are listed in the following table.

NetFlow-specific Resources for Web Console Views	
NetFlow Traffic Analysis Summary	NetFlow Endpoints
NetFlow Protocols	NetFlow Applications
NetFlow IP Address Group	NetFlow Conversation
NetFlow Country	NetFlow Domain
NetFlow Traffic Analysis Summary	Search
NetFlow Traffic Analysis Summary	Events
NetFlow Traffic Analysis Summary	Sources by % Utilization
NetFlow Traffic Analysis Summary	NetFlow Types of Service

The following procedure configures your Orion NPM Web Console to show NetFlow Traffic Analyzer resources.

Adding NetFlow Resources to Web Console Views

The following procedure adds a NetFlow-specific resource to any Orion NPM Web Console view.

To add a NetFlow resource to a web console view:

1. Log on to the Orion NPM server that you are using for NetFlow traffic analysis.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** on the Views menu bar, and then click **Manage Views** in the Admin menu on the left.
5. Select the view to which you want to add a NetFlow-specific resource, and then click **Edit**.

6. Click **+** next to the resource column in which you want to display the additional NetFlow resource.
7. Click **+** next to any of the NetFlow resource types listed in the previous table to expand the resource tree and display all available resources for the group.

   Note: Resources that are already listed in your view will not be checked on this page, as it is a view of all available resources. Therefore, it is possible to pick duplicates of resources that you are already displaying.
8. Check the resources that you want to add, and then click **Submit**.

   Note: You are returned to the **Customize View** page, where you may arrange the display of resources using the arrow buttons provided next to each resource column.
9. ***If you still want to change aspects of your view,*** repeat the preceding steps as needed.

   Notes:

   - For more information about using your customized view as a default view assigned to a user, see “Editing User Accounts” in the *Orion Network Performance Monitor Administrator Guide*.
   - To add your customized view to a menu bar as a custom item, see “Adding a Custom Menu Item” in the *Orion Network Performance Monitor Administrator Guide*.

Monitoring Traffic Flow Directions

Orion NTA monitors traffic flow over interfaces on your network devices. On any selected device interface, network traffic can flow both into the device (ingress) and out from the device (egress). The header of any Orion NTA view showing interface-level traffic provides a control that gives you the ability to choose the traffic direction you want to monitor. The traffic direction control gives you the following options for traffic flow monitoring:

- **Egress** displays only traffic flowing out of the selected node over the selected interface.
- **Ingress** displays only traffic flowing into the selected node over the selected interface.
- **Both** displays a summation of all traffic flowing both in and out of the selected node over the selected interface.

Creating View Limitations

NetFlow Traffic Analyzer views may also be limited to show NetFlow information from selected types of NetFlow sources. The procedure for setting view limitations is as follows.

To create view limitations in NetFlow Traffic Analyzer:

1. Log on to the Orion NPM server you are using for NetFlow traffic analysis.
2. Click **Start > All Programs > SolarWinds Orion > NetFlow Traffic Analyzer > NetFlow Web Console**.
3. Log in to the NetFlow Web Console using a **User ID** with administrative privileges.

   Note: Initially, `Admin` is the default administrator **User ID** with a blank **Password**.
4. Click **Admin** on the Views menu bar.
5. Click **Manage Views** in the Admin menu on the left.
6. Select the view that you want to limit, and then click **Edit**.
7. Click **Edit** below the View Limitation heading.
8. Select the type of limitation that you want to apply.
9. Click **Continue**.
10. Select the appropriate limitations.
11. Click **Submit**.

Customizing Charts in NetFlow Traffic Analyzer

Charts produced within the Orion Network Performance Monitor Web Console are easily customizable. Depending upon the resource, charts are customized either on an Edit *Resource* page or from a Customize Charts page. The following sections describe the available options in either case.

Edit *Resource* Page

Click **Edit** in the title bar of any chart resource to access customizable chart options, including the Maximum Number of Items to Display (for Top *XX* charts) and the Resource Style. The following Chart Styles are also available:

- 2-D or 3-D Pie Chart
- Area Chart

Customize Chart Page

The following sections describe options that are available on the Customize Chart page to modify the presentation of a selected chart.

Notes:

- Click **Refresh** at any time to review changes that you have made.
- Depending on the type of chart displayed, some resources may not provide all of the options described in the following sections.

Chart Titles

Chart Titles are displayed at the top center of a generated chart. The Chart Titles area allows you to modify the Title and Subtitles of your generated chart.

Note: Orion Network Performance Monitor may provide default chart titles and subtitles. If you edit any of the **Chart Titles** fields on the Custom Chart page, you can restore the default titles and subtitles by clearing the respective fields, and then clicking **Submit**.

Time Periods

Predefined and custom time periods are available for generated charts. You may designate the time period for your chart by either of the following methods:

- Select a predefined time period from the **Adjust Time Period for Chart** menu.
- Provide custom Beginning and Ending Dates/Times in the appropriate fields in the **Enter Date / Time Period** area.

Adjust Sample Interval

The sample interval dictates the precision of your generated chart. A single point or bar is plotted for each sample interval. If a sample interval spans multiple polls, polled data is automatically summarized and plotted as a single point or bar on the chart.

Note: Due to limits of memory allocation, some combinations of time periods and sample intervals may require too many system resources to display, due to the large number of polled data points. As a result, charts may not display if the time period is too long or if the sample interval is too small.

Chart Size

Chart Size options configure the width and height, in pixels, of the chart. You can maintain the same width/height aspect ratio, or scale the chart in size, by typing a width in the **Width** field and then typing `0` for the **Height**.

Customizing Top XX Resources

Top *XX* resources provide charts and data that characterize the types of traffic on your network. Traffic is reported both visually, with customizable charts, and numerically, in terms of percentages. The following procedure presents the available custom options for presenting data in Top *XX* resources.

To customize Top *XX* resource titles and chart types:

1. Click **Edit** in the Top *XX* resource title bar.
2. Edit the resource **Title** as appropriate.
3. Select and configure a **Named**, **Relative**, or **Absolute** time period.
4. Select from the following **Chart Style** options:
   - **2D Pie Chart** presents a “flat” view of your data
   - **3D Pie Chart**
   - **Area Chart** presents a historical view of your data as represented by areas calculated at past polling times.
5. Select either **Chart** or **No Chart** as the **Resource Style**.
6. Type the number of items that you want to display in the **Maximum Number of Items to Display** field.

Items are displayed in Top *XX* resources based on traffic percentages. Individual Top *XX* resources may be configured to show any number of items. Absolute percentages are calculated for each item based on all monitored items. Relative percentages for each item are calculated in terms of the total number of items displayed in the selected resource. For more information, see “Configuring Top *XX* Resource Percentages” on page 15.

Using the NetFlow Traffic View Builder

You can create custom traffic views directly from the NetFlow Traffic Analysis Summary view, using the Traffic View Builder resource. These custom filters allow you to view specific statistics about your entire network and its devices without having to navigate through the web console a single device view at a time. You can configure your custom traffic view to include devices, applications, time periods, and more, all from one configuration page, as shown in the following procedure.

To create a custom NetFlow traffic view with the Traffic View Builder:

1. Log in to the Orion Web Console as an administrator.
2. Click **NetFlow Traffic Analysis** in the Modules menu bar.

3. In the Traffic View Builder resource, select the type of custom, filtered view you want to create, and then click **Build**.

   Note: The Traffic View Builder resource is available on the NetFlow Traffic Analysis Summary view, but it is also available for inclusion on any other Orion Web Console view. For more information, see “Customizing Views” in the *SolarWinds Orion Network Performance Monitor Administrator Guide*.

4. Select the appropriate network characteristics and the time period for which you want to view filtered data.

5. ***If filter options are provided,*** complete the following steps to filter your custom traffic view:

   Note: Repeat the following procedure for each filter type you want to use to define your custom traffic view.

   a. Click **+** next to any filter type you want to apply.

   b. ***If you want to select items to exclude from your view,*** check **Exclude selected *items***.

   c. Select an item to define your filter appropriately, and then click **Add**.

      Note: Repeat this step until you have completely defined your filter type.

   d. ***If you want to delete a selected item***, click **X** next to the item to delete.

6. Click **Submit**.

7. ***If you want to save your custom view for future reference,*** click **Bookmark This Page** at the top of your new view.

   Note: Bookmarked views are only saved locally to the browser on the computer on which you are viewing the web console.

Interacting with the thwack® User Community

By default, Orion NTA provides the thwack Recent NetFlow Posts resource on the NetFlow Traffic Analysis Summary view. This resource shows the most recent Orion NTA-related posts that have been submitted to thwack, the online SolarWinds user community. Clicking any post title listed in the resource opens the associated post in the Orion NTA forum on thwack.

Performing an Immediate Hostname Lookup

From any NetFlow Endpoint view, you can resolve the hostname of the viewed endpoint using immediate hostname lookup. To perform a lookup, browse to an Endpoint Details resource, and then click **Lookup** in the Hostname field.

Note: The hostname is also retrieved on a scheduled basis. For more information, see “Configuring DNS and NetBIOS Resolution” on page 19.

Viewing Class-based Quality of Service (CBQoS) Data

CBQoS is a proprietary, SNMP-based, Cisco technology available on selected Cisco devices that gives you the ability to prioritize and manage traffic on your network. Using policy maps, the different types of traffic on your network are categorized and then given a priority. Based on respectively assigned priorities, only specified amounts of selected traffic types are allowed through designated, CBQoS-enabled devices. For example, you could define a policy map in which only 5 percent of the total traffic over a selected interface may be attributed to YouTube. For more information about configuring class maps for your CBQoS-enabled network devices, search `CBQoS` at www.cisco.com.

For CBQoS-enabled Cisco devices on your network, Orion NTA can provide immediate insight into the effect of your currently enacted policy maps. The following CBQoS resources are available for inclusion on NetFlow Interface Details views, Orion NPM Interface Details views, and CBQoS Details views:

Notes:

- Orion NTA does not currently provide a CBQoS configuration capability.
- All nodes managed by Orion NPM are polled for CBQoS information. If SNMP polls of the MIB for monitored devices are unsuccessful for CBQoS OIDs, CBQoS resources are automatically hidden because they are empty.

CBQoS Drops

If it is included on a NetFlow Interface Details view, the CBQoS Drops resource provides both a graph and a table reporting each of the defined classes and corresponding amounts of traffic that are filtered out or dropped as a result of policy maps currently enacted on the viewed interface.

If it is included on the CBQoS Details view, the CBQoS Drops resource provides both a graph and a table reporting the amount of traffic corresponding to the selected CBQoS policy class that is filtered out or dropped as a result of policy maps currently enacted on the viewed interface.

CBQoS Policy Details

If it is included on a NetFlow Interface Details view, the CBQoS Policy Details resource provides both a graph and a table reporting the amount of traffic corresponding to defined classes that has passed over the viewed interface in both the hour and the 24 hours prior to the currently viewed time period.

If it is included on the CBQoS Details view, the CBQoS Policy Details resource provides both a graph and a table detailing the amount of traffic corresponding to the selected CBQoS policy class that has passed over the viewed interface in both the hour and the 24 hours prior to the currently viewed time period.

CBQoS Post-Policy Class Map

If it is included on a NetFlow Interface Details view, the CBQoS Post-Policy Class Map resource provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to defined classes passing through the viewed interface resulting from the application of policy maps on the viewed interface.

If it is included on the CBQoS Details view, the CBQoS Post-Policy Class Map resource provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to the selected CBQoS policy class passing through the viewed interface resulting from the application of policy maps on the viewed interface.

CBQoS Pre-Policy Class Map

If it is included on a NetFlow Interface Details view, the CBQoS Pre-Policy Class Map resource provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to defined classes passing through the viewed interface prior to the application of any policy maps.

If it is included on the CBQoS Details view, the CBQoS Pre-Policy Class Map resource provides both a graph and a table detailing both the average and the most recently polled amount of traffic corresponding to the selected CBQoS policy class passing through the viewed interface prior to the application of any policy maps.

Chapter 6

Working with Orion NTA

While Orion NPM can tell you the bandwidth usage on a given interface, Orion NetFlow Traffic Analyzer takes this capability one step further, providing you with more information about the actual user of that bandwidth and the applications they are using.

The following scenarios illustrate the value of Orion NetFlow Traffic Analyzer and how it can immediately offer you a significant return on your investment.

Locating and Isolating an Infected Computer

You can use your currently installed Orion instance, with the addition of Orion NetFlow Traffic Analyzer, to quickly pinpoint and respond to the wide variety of self-propagating viruses that can attack your network. Consider the following scenario:

1. A local branch of your banking network that handles all of your credit card transactions complains of an extremely sluggish network, causing frequent timeouts during sensitive data transfers.
2. You open the Orion NPM Web Console to see that the link to the network is up at the branch site. You consult your Percent Utilization chart and immediately see that, though your normal utilization is 15-25%, current utilization is 98%.
3. You click the NetFlow Traffic Analyzer tab, and then click the link to the branch site.
4. Taking a quick look at the Top 5 Endpoints, you see that a single computer in the `10.10.10.0-10.10.10.255` IP range is generating 80% of the load on the branch link.
5. You know that this computer resides in a part of the branch that is accessible to customers for personal transactions using the web.
6. You quickly see that 100% of the last two hours of traffic generated by this computer has been over port 1883.
7. Knowing that you don’t have any devices using IBM MQSeries messaging in the customer accessible location, nor any other services or protocols that require 1883, you recognize that this is a virus exploit.
8. You quickly use your configuration management tool, for example Cirrus Configuration Manager, to push a new configuration to your firewall that blocks port 1883.

Locating and Blocking Unwanted Use

Within your network, you can easily chart the increasing usage of your different uplinks. With the addition of Orion NetFlow Traffic Analyzer, you are able to chart utilization as you can with a basic Orion NPM installation, and you can locate specific instances of unwanted use and take corrective action. Consider the following scenario:

1. Your uplink to the internet has been slowing progressively over the last 6 months, even though your head count, application use, and dedicated bandwidth have all been stable.
2. You open the Orion NPM Web Console to see that the link to the net is up at your site. You click your specific uplink and consult your Current Percent Utilization of each Interface chart. You can see that the current utilization of your web-facing interface is 80%.
3. You click this specific interface. Using the Percent Utilization chart and customizing the chart to show the last 6 months, you see that there has been steady growth from 15% to 80% consumption over time. There are even spikes into the high 90s.
4. You click the NetFlow Traffic Analyzer tab, and then click the uplink at that site. Taking a quick look at the top 50 Endpoints, you see that a group of computers in the `10.10.12.0-10.10.12.255` IP range is consuming most of the bandwidth.
5. These computers reside in your internal sales IP range. You begin to drill into each of the offending IP addresses.
6. Each IP you investigate shows Kazaa (port 1214) and World of Warcraft (port 3724) usage in the Top 5 applications.
7. You push a new configuration to your firewall using Cirrus Configuration Manager that blocks all traffic on these two ports.
8. Within minutes, you see the traffic on your interface drop back to 25%.

Recognizing and Thwarting a DOS Attack

Orion NetFlow Traffic Analyzer helps you easily identify both outgoing and incoming traffic. This capability becomes ever more important as corporate networks are exposed to increasingly malicious DOS attacks. Consider the following scenario:

1. You receive a page from Orion NPM. Your router is having trouble linking out to the internet and maintaining a stable connection.
2. You open the Orion NPM Web Console and begin sifting through the possible issues. Your connections are currently up; bandwidth utilization

looks good, and then you notice your CPU utilization on the firewall. It is steady between 99% and 100%.

3. You open the firewall node and begin to drill into the interfaces.
4. On the NetFlow Traffic Analyzer tab, you take a quick look at the top 50 Endpoints.
5. The top six computers attempting to access your network are from overseas.
6. You realize that you are being port scanned and that your firewall is interactively blocking these attacks.
7. You push a new configuration to your firewall using Cirrus Configuration Manager that blocks all traffic over the IP range that is attempting to access your network.
8. In minutes, your CPU drops back to normal.

Appendix A

Software License Key

During installation, you may be prompted with the Install Software License Key window requesting that you supply your name, e-mail address, phone number, customer ID, and password. If this is the case, follow the instructions below to enable a software license key.

To enable a software license key:

1. ***If the computer on which you are installing Orion NetFlow Traffic Analyzer is connected to the Internet,*** type the requested information on the Install Software License Key window, and then click **Continue**.

   Note: The SolarWinds license registration server will immediately issue a license key that will allow NetFlow Traffic Analyzer to operate.

2. ***If the computer on which you are installing Orion NetFlow Traffic Analyzer is not connected to the Internet,*** your server cannot authenticate to the SolarWinds license registration server, so you must complete the following procedure.

   a. Click **Skip This and Enter Software License Key Now** on the Install Software License Key window.

   b. Using another computer that is connected to the Internet, log in to the customer area of the SolarWinds website at `www.solarwinds.com/keys`.

   c. Click **Software Keys** from the Customer Area menu.

   d. Select the product for which you need a key, and follow the instructions on the page to obtain a key.

   e. Type the key in the **Enter Software License Key** text box.

3. Click **Continue** to complete your Software License Key installation.

Installing License Manager

If you need to move your installation from one computer to another, install License Manager on the computer from which you are uninstalling currently licensed products.

To install License Manager:

1. Navigate to http://support.solarwinds.com/support/default.cfm.
2. Provide your SolarWinds Customer ID and password, and then click **Login**.

3. Click **Downloads & Updates** in the left navigation pane.
4. Locate the Download Licensed Software section of the page, and click **SolarWinds License Manager**.
5. Unzip the downloaded file, and then run `LicenseManager.exe`.

Using License Manager

License Manager must be run on the computer where the currently licensed SolarWinds product is installed.

To deactivate currently installed licenses:

1. Start the License Manager from the SolarWinds Program group.
2. Check the products you want to deactivate on this computer.
3. Click **Deactivate**.
4. Specify your SolarWinds Customer ID and password when prompted, and then click **Deactivate**.

   Note: Deactivated licenses are now available for activation on a new computer.

When you have successfully deactivated your products, log on to the computer on which you want to install your products and begin the installation procedure. When asked to specify your licenses, provide the appropriate information. The license you deactivated earlier is assigned to the new installation.

Appendix B

Device Configuration Examples

The following examples of device configurations can be used to help configure your devices to send flow data to Orion NetFlow Traffic Analyzer.

Cisco NetFlow Configuration

The port used for NetFlow traffic is specified in the configuration of your Flow-enabled Cisco appliance. The following excerpts from a Cisco router configuration file offer an example of where to look to enable NetFlow traffic on a Cisco router:

```
!

interface GigabitEthernet0/1

description link to PIX

ip address 10.3.1.2 255.255.255.252

ip route-cache flow

!

ip flow-export source GigabitEthernet0/1

ip flow-export version 5

ip flow-export destination 1.2.0.12 2055

!
```

The `ip flow-export destination` value must reflect the IP address of your Orion NPM server. This value also contains the port number (`2055`) that is required in this step. The `ip route-cache flow, ip flow export source`, and `ip flow-export version` values are required to enable NetFlow traffic. Orion NetFlow Traffic Analyzer supports NetFlow version 5 and version 9. For more information about NetFlow version 5 or 9, see your Cisco router documentation or the Cisco website at `www.cisco.com`. For more information on enabling NetFlow traffic on Cisco switches, see the “Enabling NetFlow and NetFlow Data Export on Cisco Catalyst Switches” technical reference on the SolarWinds website or your Cisco documentation.

Extreme sFlow Configuration

To support Extreme devices, you must configure the device using the following configuration template.

```
enable sflow

configure sflow config agent 10.199.5.10

configure sflow collector 192.168.72.67 port 2055

configure sflow sample-rate 128

configure sflow poll-interval 30

configure sflow backoff-threshold 50

enable sflow backoff-threshold

enable sflow ports all
```

The `sFlow collector` value must reflect the IP address of your Orion NPM server. This value also contains the port number (`2055`) that is required in this step.

Foundry sFlow Configuration

To support Foundry devices, you must configure the device using the following configuration template.

Note: Ensure your Foundry device supports sFlow version 5.

```
config> int e 1/1 to 4/48

interface> sflow forwarding

config> sflow destination 10.199.1.199 2055

config> sflow sample 128

config> sflow polling-interval 30

config> sflow enable
```

The `sFlow destination` value must reflect the IP address of your Orion NPM server. This value also contains the port number (`2055`) that is required in this step.

HP sFlow Configuration

To support HP devices, you must configure the device using the following configuration template.

Note: This will not show up in the command line interface. Because of this it will not return if the switch is reset.

```
setmib sFlowRcvrAddress.1 -o 0AC70199

setmib sFlowRcvrPort.1 -i 6343

setmib sFlowRcvrOwner.1 -D net sFlowRcvrTimeout.1 -i 100000000

setmib 1.3.6.1.4.1.14706.1.1.5.1.4.11.1.3.6.1.2.1.2.2.1.1.1.1 -i
37

setmib 1.3.6.1.4.1.14706.1.1.5.1.3.11.1.3.6.1.2.1.2.2.1.1.1.1 -i 1

setmib 1.3.6.1.4.1.14706.1.1.6.1.4.11.1.3.6.1.2.1.2.2.1.1.53.1 -i
8

setmib 1.3.6.1.4.1.14706.1.1.6.1.3.11.1.3.6.1.2.1.2.2.1.1.53.1 -i
1
```

Where `0AC70199` is the IP address of your Orion NPM server in hex format. Line 4 sets the sample rate. Line 5 enables sFlow. Line 6 sets the polling interval, and line 7 enables polling.

Index

A
absolute percentages 37
applications
configuration 23
automatic source addition 17
C
CBQoS 39
Drops 39
Policy Details 39
Post-Policy Class Map 40
Pre-Policy Class Map 40
resources 39
charts
configuration 22
customizing 36
editing 35
sample intervals 36
size 36
time periods 36
titles 36
collection ports 28
collector services
configuration 28
configuration
device examples 47
Custom Property Editor 31
custom views 37
D
data collection
intervals 12
data compression
configuration 14
database maintenance
configuration 21
deleting
Flow source 29
devices
adding to NetFlow Traffic Analyzer 12
adding to Orion 11
configuration examples 47
data collection intervals 12
differentiated service code point
configuration 27
DNS resolution
configuration 19
on demand 19
persistent 19
documentation iv
DSCP *See* differentiated service code point
E
egress 34
examples 41
F
failover
configuration 10
features 3
Flow sources
automatic addition 17
Flows
from unmanaged interfaces 18
unmonitored ports 17
G
graphs
configuration 22
H
hostname lookup 38
I
ingress 34
installing 5
procedure 8
requirements 5
interfaces
adding to NetFlow Traffic Analyzer 12
adding to Orion 11
data collection intervals 12
unmanaged 18

IP address groups
  selection 25
IPFIX
  requirements 8
J
J-Flow
  requirements 8
L
License Manager
  installing 45
  using 46
licensing 5
  software license key 45
lookup 38
M
monitored ports
  configuration 23
monitoring
  IP address groups 25
  protocols 26
N
NetBIOS resolution
  configuration 19
NetFlow
  requirements 8
NetFlow Collector Services *See*
  collector services
NetFlow source
  deleting 29
nodes *See* devices
O
Orion
  Custom Property Editor *See*
    Custom Property Editor
  documentation iv
  Report Writer *See* Report Writer
Orion NTA
  features 3
  functional overview 2
  introduction 1
  why install? 1
P
per hop behavior
  configuration 27
percentages
  absolute 37
  relative 37
  Top XX resources 37
PHB *See* per hop behavior
policy maps 39
polling engine
  baseline 12
port
  -1 23
  unmonitored traffic 23
ports
  collection 28
  unmonitored 17
ports, monitored
  configuration 23
ports, NetFlow traffic
  Cisco configuration 47
ports, sFlow traffic
  Extreme configuration 48
  Foundry configuration 48
  HP configuration 49
progressive charting 22
protocols
  configuration 23
  monitoring 26
Q
QoS
  class-based 39
R
relative percentages 37
Report Scheduler 31
Report Writer
  creating reports 31
  using custom properties 31
reports *See also* Report Writer
  creating 31
  Flow 31
  using custom properties 31
requirements 5
  Flow sources 8
  hardware 7
  software 6
  virtual machine 7
resources
  configuration 15
  percentage calculation 15

time period 15
Top XX 37

S

sFlow
requirements 8
software license key
enabling 45
SolarWinds
contacting iii
sources
automatic addition 17

T

thwack 38
time period
resource default 15
top XX lists
percentage calculation 15
traffic
unmonitored port 23
Traffic View Builder 37
types of service
configuration 27

U

unmonitored traffic 23
use cases 41

V

views
adding resources 33
available resources 33
creating limitations 35
custom 37
customizing 33
NetFlow Traffic Analysis
Summary 13
setting default 13
traffic flow directions 34
volumes
data collection intervals 12