adfontessoftware

Prosperon networks

AUTHORISED PARTNER

SAMPLE COMPANY
SOLARWINDS HEALTHCHECK

Prepared on Behalf of:

SAMPLE COMPANY

solarwinds

AUTHORISED PARTNER

DOCUMENT CONTROL

Documentation History			
Version	Date	Remarks	Created By
0.1		Initial draft	Raul Gonzalez
0.2		Internal Review	Mark Roberts
0.3		New features	Raul Gonzalez
0.4		Internal Review	Mark Roberts
1.0		Distributed version	Sam Leaney

Document Contributors

Name	Title	Contribution
Raul Gonzalez	Technical Engineer	Main contributor

Distribution List

Name	Title	Organisation
Bob Smith	Sample Company	IT Systems Engineer
Samantha Leaney	Prosperon Networks	Account Manager
Mark Roberts	Prosperon Networks	Technical Director
Raul Gonzalez	Prosperon Networks	Technical Engineer

Distribution Dates

Version	Date	Name	Distributed By
v1.0		SolarWinds healthcheck report	Sam Leaney

Reference Documents

Title	Description	Location
Sample Company Scope of Works	Definition of the scope of works	

Table of Contents

1 PROJECT OVERVIEW

This document details the analysis review of the health and configuration of the Sample Company Orion installation, highlighting the areas felt to be affecting performance and the efficient usage of the SolarWinds monitoring platform.

A review of the current platform is being performed in order to allow the 'As Is' state to be identified and understood, which will be used within the workshop discussions with Sample Company. The purpose of these workshops is to allow the utilisation, configuration and capabilities of the platform to be improved enhancing the benefit of the monitoring platform to the business.

2 INSTALLED SOFTWARE LICENCES

The following table provides details on the current applications installed, their versions and license sizes. A new version of each of the applications was released on 16th March and is suggested to be reviewed to determine the benefits of upgrading to these software versions.

SolarWinds Licenses	Installed Version	Current Release Version	License Size	License Used
Orion NPM	12.0.1	12.1.0	SLX	6669
Orion NTA	4.2.0	4.2.1	SLX	---
Orion NCM	7.5	7.6	DL500	290 Nodes
Orion IPAM	4.3.2	4.3.2	IP 16384	14698 IP's

Table 1 - Installed Licences

See Appendix I for more information on SolarWinds licencing.

3 SYSTEM DETAILS

3.1 Server/s Configuration

Application Server Specifications	
Hostname	Solarwinds1
Manufacturer/Model	HP Proliant
CPU	E5-2650 v3 @ 2.30GHz (2 processors)
Memory	64GB
Hard Disk	C:\ Local Disk 278GB (170GB free) D:\ Data 279GB (233GB free)
Domain	mydomain.co.uk
Operating System	Windows Server 2012 Standard
Installation Folder	D:\Program Files\SolarWinds
Installation Folder size	2.15GB
NTA Flow folder	D:\Programdata\SolarWinds\NTA\FlowStorage\Data
NTA Flow backup folder	D:\Programdata\SolarWinds\NTA\FlowStorage\Backups
Comments	Orion Permission Checker failed in two folders (C:\programdata\Solarwinds and C:\Windows\temp NTA Flow Database Server installed on main poller

Table 2 - Application Server Configuration

SQL Database Server	
Hostname	SQL01
Manufacture/Model	HP Proliant
CPU	E5640 @ 2.67GHz
Memory	16GB
Hard Disk	8 physical disks -> 4 Logical disks RAID 1 C:\Local disk 136GB D:\ SQL and SysDB 60GB G:\SQL user data 778GB J:\User logs 59GB P:\Page file 10GB S:\Backups 149GB T:\TempDB 60GB
Domain	mydomain.co.uk
Operating System	Windows Server 2012 Standard
SQL Server Version	SQL Server 2008 R2 SP3
Location of DB files	G:\
Location of Log files	J:\
Comments	High Memory utilisation RAID 1 configured throughout

Table 3 - Database Server Configuration

Key Performance Indicators		
Metric	**Value**	**Notes**
Total Orion Elements Monitored	14154	
Nodes	1542	
Interfaces	6669	
Volumes	5943	
Polling Job Weight	445%	This value indicates that you are using 445% of the available single server polling capacity*
Polling Completion	100%	Any value below 98% indicates performance issues
Database File Size	430 GB	
Data Size	370GB	
Top 3 SQL Tables by size		Traps, Trapvabinds, Interfaces
NTA Flows Per Second		Near 3000 Netflow v9 flows per second

Table 4 - Key Performance Indicators

* When Orion goes beyond 100% polling capacity, it will automatically adjust the polling frequencies of the objects to allow the polling engine to keep with it's performance capabilities. Therefore if polling is expected to be performed every 10 minutes for example at the Node level, it may well in fact have been adjusted to 12 minutes.

4 HEALTH CHECK REVIEW

4.1 Application Server

The Orion server is installed upon a physical server, and its database is installed on a separate SQL server. The operating system of the server is Windows Server 2012, with a CPU speed of 2.2 GHz (2 processors, 20 cores each processor) and 64 GB of memory. These specifications are higher than the requirements for an application server, however the NTA Flow database server application is installed on this main server. This is not a recommended configuration by SolarWinds or Prosperon and will impact on performance.

An antivirus end point application has been detected on the SolarWinds main application server (Symantec Endpoint Protection) but we didn't have access to the settings to determine if any file or folder exclusions were configured on it, as required for an installation. We recommend to apply the Anti Virus exclusions outlined on Appendix II – Anti-virus Recommendations.

SolarWinds NPM module installed is not up to date. We recommend that you review the Release Notes of the current version release in order to determine the benefits and features available that could be of benefit. Our recommendation is to upgrade the installation to the latest versions, with appropriate change management review, as these versions contain a number of performance and feature enhancements.

Please note that SolarWinds provide technical support on the last two major releases of the application.

As a guide the following are the minimum specifications for an application server, populated as the Sample Company instance is:

Application Server	
Make	Virtual or physical
CPU	Quad Core 3GHz+ (CPU less than 2.5GHz may impact on performance)
Memory	16GB
OS	Windows Server 2012 R2(with IIS in 32 bit mode)
Disk	Different RAID 10 for each drive: • C:\ Windows OS 40GB (Random I/O, 80% Read 20% Write) • D:\Page file (RAM+256MB +20% GB) (Random I/O, 50% read/write) • E:\ Programs 20GB (Random I/O, 75% read, 25% write) • F:\ Web 10GB(Random I/O, 90% read, 10% write) • G:\ Logs 50GB (Sequential I/O, 25% read 75% write)
	.Net Framework v3.5.1 & v4.0.3 or greater

Table 5 - Main Server specifications

It is recommended that the Netflow Flow Database Server is separated from the main server, with the following specifications the minimum recommended:

Flow Storage (Netflow) Database Server	
CPU	1 x Quad Core 3GHz (4 vCPUs if virtual)
Memory	16 GB RAM
OS	Windows Server 2012 (64-Bit) Windows Server 2008 R2 (64-Bit)

Server Roles & Configuration Requirements	Microsoft .Net Framework v3.5.1 Microsoft .Net Framework v4.0.3 or higher
Disk	Suggested Disk Structure • Operating System and Application (2x 146GB SAS 15K or SSD disks RAID 1 (mirroring)) • Flow Data Store (4x SAS Disks RAID 1+0 OR 2 x SSD Raid 1) Min 100GB required
Comments	The above specification is based on a total flow per second count of 3,000. If this value needs to be increased, so will the memory and potentially disk performance capabilities

Table 6 - NTA Flow Database Server Specifications

4.2 SQL Server & Database

The SQL server is configured with one CPU at 2.67GHz and 16GB RAM. The current memory utilisation is close to 95% utilised, hence we would recommend to increase the amount of memory to 32GB.

Orion NPM is a high transaction volume application and as such generates significant volumes of SQL transactions; both read and write queries. This in turn has an impact on the disk structure, which needs to be configured to cater for high I/O. RAID and other resources. SolarWinds recommends to install the SQL server upon a physical server due to performance capabilities, which is the case with your installation. The disk structure of the SQL server is configured as RAID 1.

It is highly recommended that the RAID configuration recommended is changed to RAID 1+0 with at least 6 spindles (15k spindle speed or SSD disks recommended), as there are some performance issues identified.

These are the recommended specifications of the SQL server:

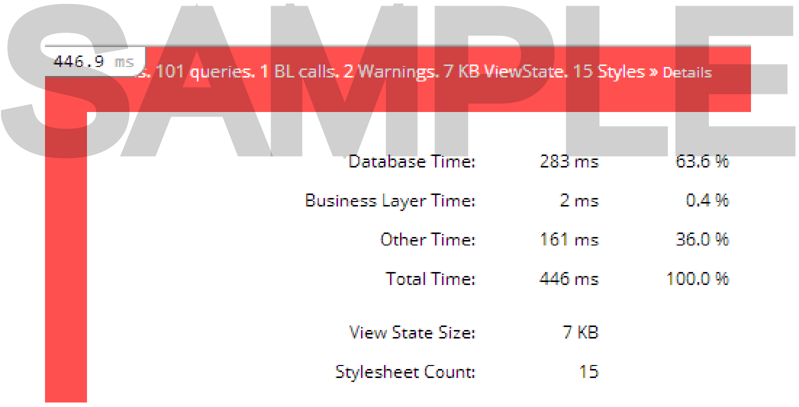
SQL Server	
Make	Physical
CPU	Quad Core Processor 3 GHz or better
Memory	32GB DDR3
OS	Windows Server 2012 R2 64 bit
SQL version	SQL Server 2014 Standard or Enterprise

Disk	Hardware RAID Controller with a battery backed-up write back cache Suggested physical structure: • Operating System and Application (2x 146GB SAS 15K or SSD disks RAID 1 (mirroring)) • SQL Data (6x SAS or 4xSSD Disks RAID 1+0) Min 500GB capacity • SQL Log(4x SAS or 2xSSD Disks RAID 1+0) Min 100GB capacity • TempDB (4x SAS or 2xSSD Disks RAID 1+0) Min 100GB capacity The following are KPI targets for the SQL Server's data store: • Data Disk latency averages 8ms and not more than 15 – 20ms • Temp DB < 8ms • 64k Block sizes • IOPS for the data drive: 1000+ For multitier SAN devices, please make sure SolarWinds database files use the top tier with best available performance.

Table 7 - SQL Server Specifications

4.3 Web Performance

The overall SolarWinds website performance is normal, however Sample Company staff mentioned that sometimes the web console can respond slowly. While it was not observed to be slow during the health check review, the SQL Server database is the primary cause of such issues. However, without analysis at the time of performance issues, it is not possible to be certain.



```
446.9 ms  s. 101 queries. 1 BL calls. 2 Warnings. 7 KB ViewState. 15 Styles » Details

          Database Time:     283 ms     63.6 %
    Business Layer Time:       2 ms      0.4 %
             Other Time:     161 ms     36.0 %
             Total Time:     446 ms    100.0 %

        View State Size:       7 KB
       Stylesheet Count:         15
```

Figure 1 - Web performance

Any database time less than 300 ms for a common SolarWinds dashboard is considered normal. However, when we run some reports, SolarWinds web console times out because of the database not being able to return all the statistics in a timely manner. The most probable reason of the slowness of the SolarWinds platform is the configuration of the SQL server, primarly:

- Low memory available
- Slow RAID configuration

4.4 Orion Configuration Settings

The frequency of data collection has been changed from the default timings, and this is impacting the performance thresholds of the Orion server itself and the quantity and volume of data stored in the database. These changes were implemented a long time ago and at a time when only network devices were being monitored in SolarWinds. The impact of the changes on the SolarWinds platform and on the polling rate, currently 445% and is highly recommended to review and adjust the polling frequencies. It has been agreed with Sample Company staff that this configuration will be internally reviewed and amended in order to reduce the polling rate. It is recommended that a global value is assigned and object (Node, Interface, Volume) level adjustments are applied.

Data Collection Frequency		
Polling Intervals	**Default Value**	**Configured Value**
Default Node Poll Interval	120 seconds	20 Seconds
Default Interface Poll Interval	120 seconds	20 Seconds
Default Volume Poll Interval	120 seconds	600 Seconds
Default Rediscovery Interval	30 minutes	1440 Minutes
Lock custom values	Yes	
Polling Statistics Intervals	**Default Value**	**Configured Value**
Default Node Topology Poll Interval	30 minutes	30 minutes
Default Node Statistics Poll Interval	10 minutes	1 minute
Default Interface Statistics Poll Interval	9 minutes	1 minute
Daily Volume Statistics Retention	15 minutes	5 minutes

Table 8 - Data Collection Frequency

However, even if reverting to the default polling intervals, at least one additional polling engine would be required to cope with the current number of elements monitored. Each polling engine can poll up to 12.000 elements when using the default polling intervals.

We suggest that we work with Sample Company in order to determine the required level of polling, from where we can make recommendations as to an appropriate architecture to support the quantity of monitored elements and frequency.

Data Retention

Orion has been configured to retain data within its database for longer periods of time than the default values. These changes impact on the performance requirements of the SolarWinds platform and result in an increase of the size of the database. We recommend to review and verify whether the current configured retention periods are truly required and if they are then it is recommended to increase the level of performance delivered by the Microsoft SQL Server.

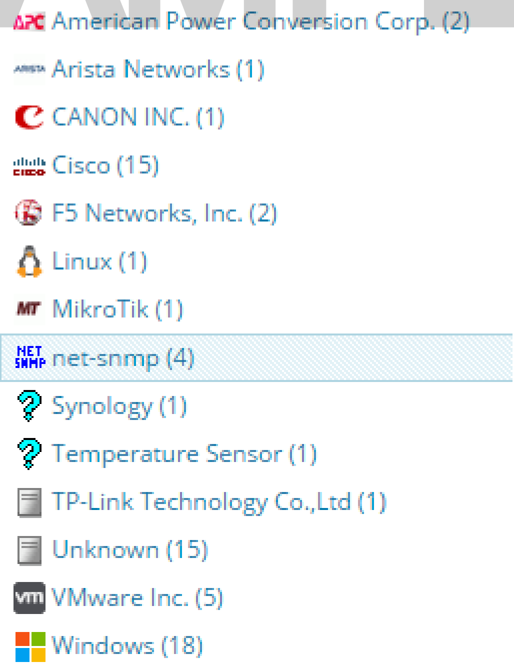
Data Retention Settings			
Data Element	**Default Value**	**Configured Value**	**Recommended Value**
Detailed Statistics Retention	7 Days	31 Days	21 Days
Hourly Statistics Retention	30 Days	90 days	65 Days

Daily Statistics Retention	365 Days	370 Days	400 Days
Detailed Interface Availability Statistics Retention	7 Days	31 Days	14 Days
Hourly Interface Availability Statistics Retention	30 Days	90 Days	65 Days
Daily Interface Availability Statistics Retention	365 Days	370 Days	400 Days
Detailed Wireless Statistics Retention	3 Days	31 Days	3 Days
Hourly Wireless Statistics Retention	14 Days	90 Days	14 Days
Daily Wireless Statistics Retention	180 Days	370 Days	180 Days
Syslog Messages Retention	7 Days	7 Days	7 Days
SNMP Traps Messages Retention	7 Days	7 Days	5 Days
Orion Events Retention	30 Days	7 Days	60 Days

Table 9 - Orion Data Retention Settings

4.5 Node population

SolarWinds supports the use of a number of different protocols in order to poll information from the devices. These protocols (ICMP, SNMP, WMI or agent based) may give you more or less detailed information, with the ICMP protocol providing the least level of information (status, latency, packet loss). In your environment you are currently polling 624 ICMP only nodes. We recommend to review whether these devices should be monitored in SolarWinds and if there is a full management protocol available to poll them.



American Power Conversion Corp. (2)
Arista Networks (1)
CANON INC. (1)
Cisco (15)
F5 Networks, Inc. (2)
Linux (1)
MikroTik (1)
net-snmp (4)
Synology (1)
Temperature Sensor (1)
TP-Link Technology Co.,Ltd (1)
Unknown (15)
VMware Inc. (5)
Windows (18)

Figure 2 - Devices populated

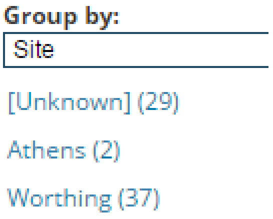
We do not recommend to monitor certain types of interfaces such as Null0 or loopback interfaces, as the metrics gathered from them will not be of any utility. At the moment there are:

- Null0: 49 interfaces
- Loopback: 334 interfaces

We recommend to delete these interfaces from the scope of SolarWinds and also perform a review to confirm he level of interface monitoring applied. A standard practice for example is to monitor only uplink interfaces on access switches.

4.6 Custom Properties

Sample Company's SolarWinds installation has 38 custom properties created for nodes and 4 custom properties for interfaces. This is quite a large number of custom properties, and the vast majority of these custom properties are empty. We would recommend to review the current custom properties and delete or consolidate them in order to reduce the current number of custom properties configured or to utilise them fully by ensuring that the fields are populated with correct data.



Group by: Site

[Unknown] (29)

Athens (2)

Worthing (37)

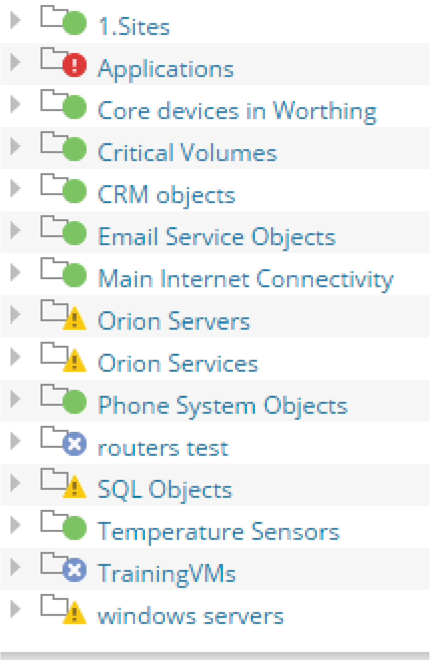
Figure 3 - Custom Properties

4.7 Groups

Orion includes the ability to create logical container groups, such as a set of nodes with similar characteristics. This feature allows creating maps and adds groups as a single identify and grouping devices for dependencies. Groups is currently used in your installation, however we feel there are a few groups missing and some others are incomplete. We recommend to create a set of groups for each location in order to create dependencies:

- Sites: a group for each location will be created. For non-data centre locations, two additional groups will be created in order to aid dependencies. Example:
  - London:
    - London WAN: group devices connected to internet (for example MPLS and ADSL devices)
    - London LAN: rest of devices (servers, switches, wireless, ESXi….)

We also recommend the use of dynamic queries to add devices into the groups, rather than manually selecting them. Dynamic queries will allow adding devices automatically into the groups once they devices have been added to Orion.



1.Sites
Applications
Core devices in Worthing
Critical Volumes
CRM objects
Email Service Objects
Main Internet Connectivity
Orion Servers
Orion Services
Phone System Objects
routers test
SQL Objects
Temperature Sensors
TrainingVMs
windows servers

Figure 4 - Groups

4.8 Dependencies

Dependencies utilise groups and allow the definition of dependency hierarchy of devices, The use of this feature within Orion prevents multiple alerts being generated where when the connectivity to a group of devices is loss based on the same root cause, such as a site route going down preventing access to the devices on the other side. We recommend to use the group structure to create dependencies between remote locations.

At the moment dependencies are not being used.

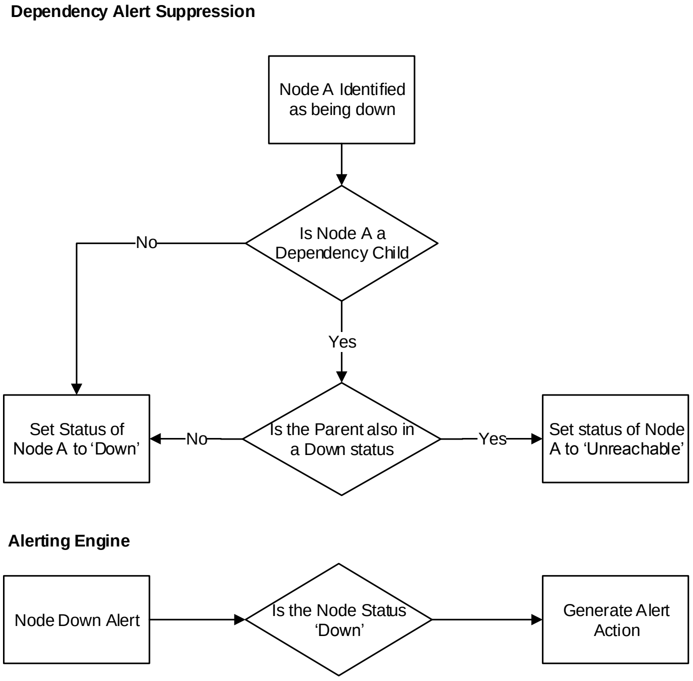
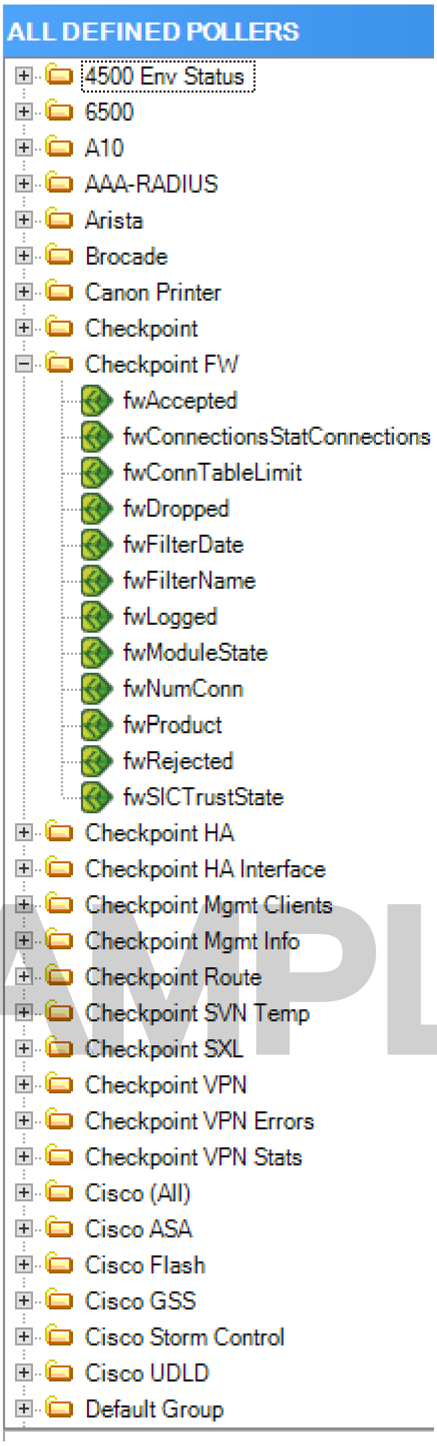

Dependency Alert Suppression
Node A Identified as being down
Is Node A a Dependency Child
No
Yes
Set Status of Node A to 'Down'
No
Is the Parent also in a Down status
Yes
Set status of Node A to 'Unreachable'
Alerting Engine
Node Down Alert
Is the Node Status 'Down'
Generate Alert Action

Figure 5 - Dependencies

4.9 Custom Pollers

SolarWinds has the ability to poll additional information using SNMP in order to capture specific functional data from devices. Some custom pollers have been created, however we recommend the following:

- Review the custom pollers availabile for some devices in order to find potential statistics that would be relevant:
  - Cisco module status
  - Juniper connections
  - Cisco ASA HA status
  - Spanning tree Topology changes
  - Netapp disk and raid information
  - APC battery remaining
  - Cisco VPN information
- Review the existing custom pollers created. Some of the information gathered is now available out of the box from SolarWinds (F5 details, topology information, OSPF data, cisco stack data…) and therefore these can now be deprecated
- CPU and memory custom pollers should be created on the new web console feature to create custom pollers for CPU and memory. This will allow SolarWinds to map that those custom pollers are CPU and memory value, and consider those metrics for alerts, reports and dashboards.
- To review the current group structure of custom pollers. The current structure is not clear and the SolarWinds users can't understand which custom pollers apply to which devices.



ALL DEFINED POLLERS

- 4500 Env Status
- 6500
- A10
- AAA-RADIUS
- Arista
- Brocade
- Canon Printer
- Checkpoint
- Checkpoint FW
  - fwAccepted
  - fwConnectionsStatConnections
  - fwConnTableLimit
  - fwDropped
  - fwFilterDate
  - fwFilterName
  - fwLogged
  - fwModuleState
  - fwNumConn
  - fwProduct
  - fwRejected
  - fwSICTrustState
- Checkpoint HA
- Checkpoint HA Interface
- Checkpoint Mgmt Clients
- Checkpoint Mgmt Info
- Checkpoint Route
- Checkpoint SVN Temp
- Checkpoint SXL
- Checkpoint VPN
- Checkpoint VPN Errors
- Checkpoint VPN Stats
- Cisco (All)
- Cisco ASA
- Cisco Flash
- Cisco GSS
- Cisco Storm Control
- Cisco UDLD
- Default Group

Figure 6 - Custom Pollers

4.10 Maps

Network Atlas mapping tool is an Orion application that has the ability to present information in a clear informative way. The use of the map feature allows for dynamic information based on the availability and threshold values of devices to be displayed in ways that make the absorption of the data easy for users of multiple skill levels.

This application feature is being used at the moment, with around 30 maps currently created. It is recommended to review the potential of this tool to take advantage of the feature to create a visual presentation of your network and application topology in a way that will aid the use of the monitoring platform, such as using interface labels to show either bandwidth utilisation (in percentage or bits per second) or link speed. A review of the maps indicate that the capabilities of the Network Atlas can be leveraged further to provide for visual presentation of data.

We also recommended reviewing whether the maps already created are used or not and if any stale maps exist that can be removed. Having lots of maps will not generated an issue to the SolarWinds platform, however it removing unnecessary maps will make on going management easier. In addition a review to determine if the quantity of sub maps is required and whether the use of the Group feature would be a more appropriate method of map topology.

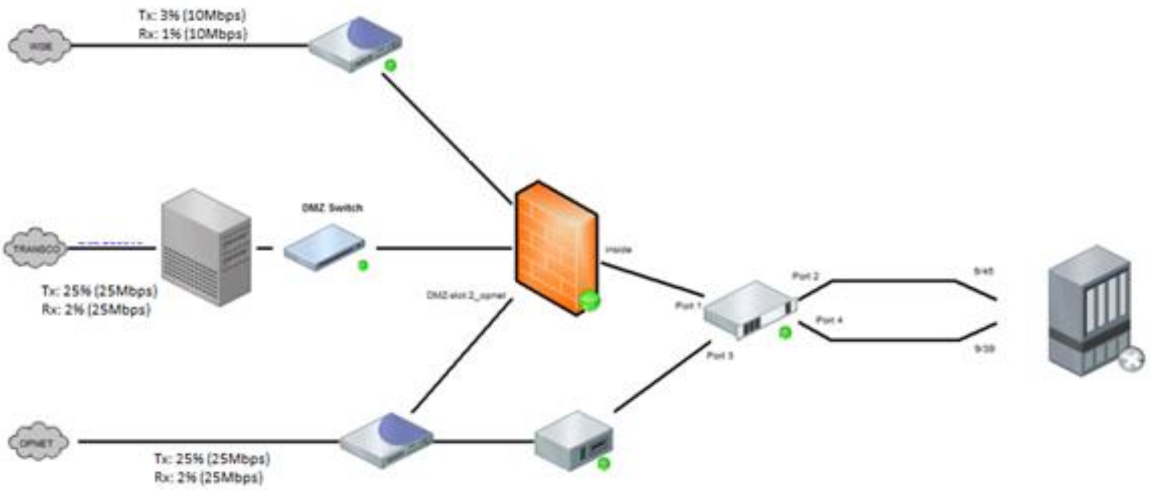


Figure 7 - Example Map with labels

Sample Company is also using the new feature available to create Wireless Heat Maps. There is one map (Wireless – CGH 2F) that is using new feature, however we would recommend to review the clients selected per access point in order to get a more accurate heat map.

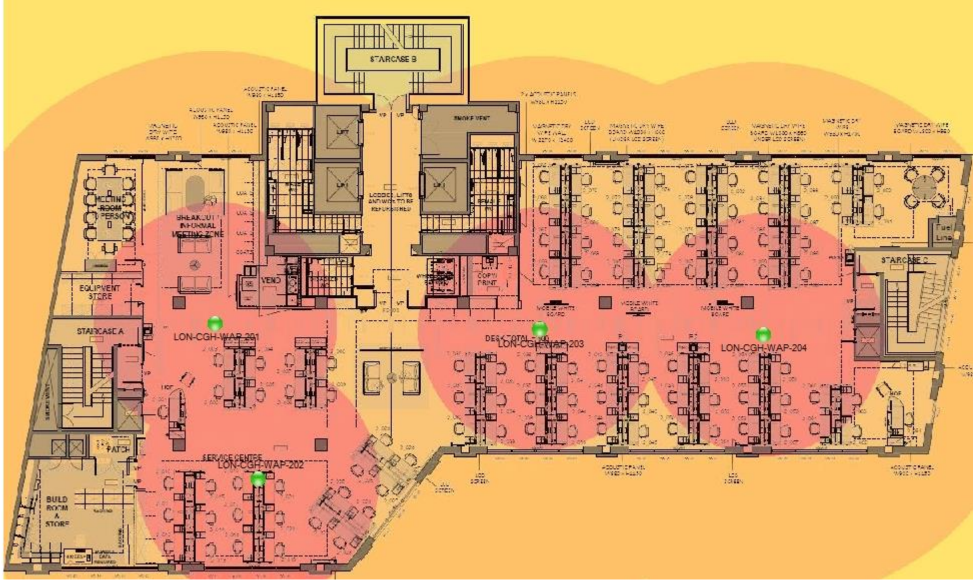


Figure 8 - Wireless Heat Map

In addition to the Network Atlas derived maps, there is a visual map feature called Worldwide Map that has the capability to display the status of nodes or an aggregated group of nodes over dynamically updated geographic display, with zoom dynamic navigation all the way down to street level display of device status. Based on the OpenStreet map online mapping service, this provides a strong method of geographic display and also in a way that can be fully automated This feature, that is not being used at the moment, is very useful for installation that includes different geographical areas.

4.11 Netpath

NetPath is a feature of Orion that allows you to discover and troubleshoot network paths hop-by-hop – not just the part of the network that you manage, but also nodes and links of the network and backbone providers.

Currently this feature is being used to monitor a couple of services, however both of them are performed from the same probe (source). We recommend to expand the use of this feature by monitoring new services and creating new probes. Common netpath services monitored:

- Connection to internet from each location
- Internal website monitoring from each location
- External website monitoring
- Internal service monitoring from each location (DNS, DHCP, Email, Voice,…)

Any windows server 2008 R2 or newer that is being monitored in SolarWinds can be used as a NetPath probe if the SolarWinds agent is installed.

4.12 Quality of Experience

The QoE feature uses deep packet inspection to provide the ability to easily determine whether a performance issue stems from application server slowness, or an issue with the underlying network. The two key metrics we surface in QoE to help determine this are: Application Response Time (ART) and Network Response Time (NRT).

At the moment there are two network sensors (Birmingham and Northampton) that are analysing and discovering automatically applications in QoE. We recommend to limit the number of applications discovered, otherwise, there are some applications discovered and monitored that don’t bring any value to this feature and can obfuscate truly useful information.

While Network sensors are the recommended method to perform the DPI analysis with this feature of Orion, it may be beneficial to utilise the deployment of server sensors. These sensors monitor the traffic generated or received on the specific server and are therefore easier to get visibility of application targeted data.

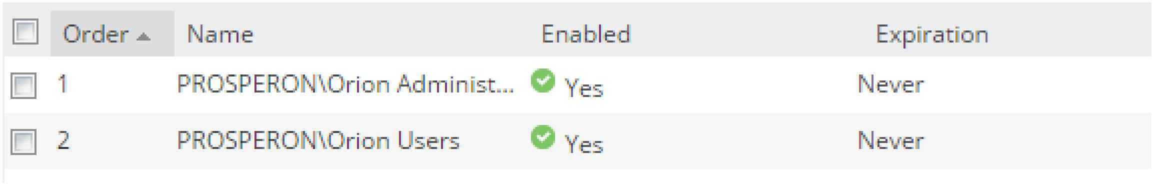
4.13 Accounts

SolarWinds supports three different types of accounts to provide controlled access to the Orion web application interface:

- Individual accounts: internal SolarWinds accounts
- Individual AD accounts: integrated AD accounts
- AD group accounts: integrate AD groups

At the moment, Sample Company has 20 Orion individual accounts and 4 AD groups. We would recommend:

- Use AD groups instead of individual as this makes it easy to map the users who need to access Orion to a group structure within your AD topology and maintain membership moving forwards.
- Review existing accounts, some of them has not been used since 2013.
- Enable automatic login on the SolarWinds Web Console. This feature will grab the AD login from the windows session and automatically log in the user on the SolarWinds web console.



□	Order ▲	Name	Enabled	Expiration
□	1	PROSPERON\Orion Administ...	✓ Yes	Never
□	2	PROSPERON\Orion Users	✓ Yes	Never

Figure 9 - Accounts

Some of the accounts configured have account limitations. Although this is an available option in SolarWinds, we normally don't recommend to create limitation on the account level unless is completely necessary. The primary requirement for using Account level limitations is for security in order to ensure that restrictions are applied to users who should not have visibility of potential secure information that they should not have access to.

We recommend to create dashboards with limitations and assign these dashboards to different users.

4.14 Syslog & SNMP Traps

SolarWinds has a built in Syslog and trap server that allows us to receive Syslog messages or SNMP traps in order to correlate this information with the data polled from the devices. However the SolarWinds server is not a full SIEM solution and has limited capability in terms of messages received and in terms of reporting functionality. At the moment the level of messages received on the SolarWinds server is exceeding the maximum rate recommended (100 messages per second):

Protocol	Average Rate	Peak Rate
Syslog	800	3000
SNMP Trap	600	3000

Table 10 - Syslog and Traps

Sample Company just purchased a license of the SolarWinds SIEM tool called Log and Event Manager (LEM). We recommend to configure all the network devices to point to the LEM server and create several rules to forward only import messages from LEM to the SolarWinds server:

- Severity: Emergency, alert, critical, error
- Technologies: routing protocols (BGP, OSPF, EIGRP), layer 2 technologies (Spanning tree),…
- Security: port security, control plane security,….

4.15 Alerting

The alerting engine is a feature of Orion that provides a proactive way to generate event log entries, but primarily a method to generate external notification output on the health and status of the network as identified by Orion. It provides a number of different ways to notify to the users when an event happens in the network, from email, SMS, event log output (Syslog, SNMP Traps etc.), running of scripts and more advanced functionality such as helpdesk ticket solution integration.

The number of active alerts is just under 2000 alerts, which is a significant number and, even though there are just 159 unacknowledged alerts, this is felt to be a detrimental number whereby alerting output from Orion is likely to be ignored and therefore genuine issues missed.

Analysis of the alerting output determined that there are some alert definitions that are triggering the majority of the alert output:

- F5 LTM pool goes down

- F5 pool has less than 30% of active servers
- IOS version change

In order to remove and avoid the volume of alerting output, whether these are false positives or unnecessary alert conditions, and to complete the current alert definitions, we would recommend to:

- Create exclusions on the alerts listed above in order not alert on those active alerts acknowledged
- Disable all alerts based on technologies that are not used
- Create alerts on those events that are the moment wouldn't be captured by the current alert definitions:
    - Capacity forecast alerts
    - CBQoS drops
    - Thin Aps alerts
    - Packet loss
    - End of support
- Use custom thresholds, individual for each node, for alerting on:
    - CPU
    - Memory
    - Packet Loss
    - Response time
    - Interface traffic
- Configure alerting analysis visibility to allow continuous monitoring of the alerting generated by the Orion platform, to ensure that alerting is always maintained at appriorate levels

4.16 Reporting

This feature provides a way to report on a wide range of the data metrics collected by Orion and stored within the Orion database. SolarWinds provide a large number of out of the box reports, which are sufficient for many SolarWinds users reporting needs, however there are likely to be more specific reporting needs. Sample Company have created some further custom reports, with these having been built within the 'Report Writer' application, which is acceptable for tabular reports, however the newer Web based reporting engine allows for visual graphs to be included within the report to enhance the interrogation of the data.

We would recommend to convert to using the new reporting engine in order to create reports (Web based reports) as it gives more filtering capabilities and visual presentation options.

We recommend to expand the usage of reporting by creating these reports, with the following common reports we deploy for customers:

Report	Definition
Nodes availability	Displays table with node availability for the last 7 days and last month
Application availability	Displays table with application availability for the last 7 days and last month
WAN interfaces traffic	Displays chart and table with the average and peak % utilisation of the WAN interfaces for the 7 days and last month, including the trend
CPU and memory	Displays chart and table with the average and peak CPU and memory utilisation for the 7 days and last month, including the trend
Alert Analysis	Report which shows the number of alerts in total each device has generated, including a link to the filter Events list which will show the name of the alerts that have been created, giving the ability to identify device over alerting and why
Last Boot report	Displays list of devices and last boot time

VMs not monitored	Displays the list of vms discovered on the VM hosts that are not monitored in Orion
WMI Report	Displays the WMI accounts used to monitor servers

Table 11 - Suggested reports

Orion allows sending reports automatically based on a schedule task. It will allow scheduling reports on defined frequencies and time and for the reports to be sent to an email or file recipient. At the moment Sample Company is not using this feature.

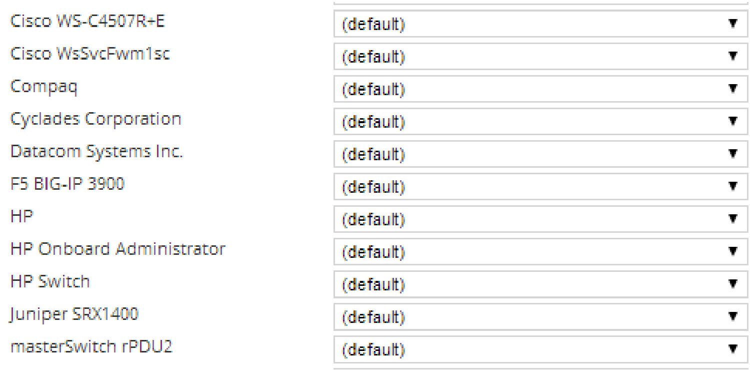
Overall it is felt that this feature is under utilised and benefits could be attained from extended use of reporting.

4.17 Web Page Presentation

The Orion web user interface is very powerful, with the ability to create bespoke views for different users and adjust detail presentations depending on the device or interface type. This provides the ability to make the interrogation of data Orion collects to be presented in a clean and efficient manner, whether it is focused to certain roles, or that pages and menus are constructed in a way to maximise the level of information available and in an easy to use manner.

These views can be grouped in menu bars that are displayed at the top of the SolarWinds webpage. The current views configured in SolarWinds are not displaying some of the major statistics that we can get from the monitored devices and therefore we feel that Sample Company are not making best of use the Orion page presentation capabilities to the point that useful information is hidden or difficult to navigate to for users. We would recommend to improve the following views:

- Node details views: there are no specific devices created for specific devices (with the exception of APC devices), and the current default view is felt to be below production level standard. Statistics such as F5 pools and vservers, cisco routing tables, hardware health information, etc are not being displayed on the node details page. This is impacting on the visibility that Sample Company staff have from the network. We would recommend to create specific views for:
    - Cisco ASA
    - F5
    - Netapp
    - ICMP only
    - VMware hosts
    - Windows



Cisco WS-C4507R+E	(default) ▼
Cisco WsSvcFwm1sc	(default) ▼
Compaq	(default) ▼
Cyclades Corporation	(default) ▼
Datacom Systems Inc.	(default) ▼
F5 BIG-IP 3900	(default) ▼
HP	(default) ▼
HP Onboard Administrator	(default) ▼
HP Switch	(default) ▼
Juniper SRX1400	(default) ▼
masterSwitch rPDU2	(default) ▼

Figure 10 - Node Details Views

- Summary views: there are a few custom summary views created, however there are mainly displaying maps, which is not a bad option, however we feel there is a lot information missing from these summary views. Potentially other summary views would improve the visibility of the network KPI's:

Summary Views	Includes	View resources
Firewalls	Statistics from firewalls	Firewalls down Firewall alerts Top 10 firewalls by CPU Top 10 firewalls by memory utilisation Top 10 firewalls by response time Top 10 firewall interfaces by bps Top 10 firewall interfaces by % Top 10 firewall interfaces by packet discards
Forecast Capacity	Forecast capacity information	Top 10 CPU capacity problems Top 10 Memory capacity problems Top 10 Disk capacity problems Top 10 interface capacity problems
Morning checklist	Current status of the network and overnight events	Down devices Current alerts Triggered alerts last 16 hours Top 10 nodes by CPU Top 10 nodes by memory utilisation Top 10 nodes by response time Top 10 nodes by packet loss Top 10 interfaces by % Top 20 volumes by percentage space used
VLANs and VRFs	VLANs and VRFs info	Vlans VRFs
SolarWinds performance	View focused on the Solarwinds server performance	Polling details QoE statistics from the SolarWinds server

Figure 11 - Recommended Summary Dashboards

4.18 Network Configuration Manager

Orion NCM is a comprehensive, configuration management solution designed to streamline and automate network configuration management. It provides a number of features around configuration management including:

- Automatic Configuration Backups
- Centralised Configuration change deployment
- Real-Time Change Detection
- Policy Reporting (Compliance and out of band configuration)
- End of Life End of Sales
- Firmware Vulnerability Assessment
- Inventory data collection and Reporting
- Firmware upgrade (available on NCM v7.6)

The current configuration of NCM doesn't includes all the devices that there should be included:

- 66 HP switches
- 25 Cisco devices
- 8 F5 devices
- 1 Juniper device

There are also a few devices in NCM that shouldn't be:

- 107 ICMP only devices
- 19 VMWare devices
- 6 net-snmp devices (oracle databases)
- 5 Windows server

We recommend to review the list of devices added in NCM in order to use this tool at full potential.

During the health check we ran the Bad logins report in order to review the number of inaccessible devices from SolarWinds using SSH or telnet. This report highlight where SolarWinds has issues to connect to some network devices. Although the vast majority of devices included in this list are devices that shouldn't be added into NCM, there were some genuine devices on the list. Please review carefully this list as all these devices are not being backed up and are not currently under active management within NCM.

System Name	IP Address	Machine Type	Login Status
Device#1	xx.xx.xx.xx	HP Switch	Connectivity issues, discarding configuration (or configuration is too short). Device IP: xx.xx.xx.xx
Device#2	xx.xx.xx.xx	Cisco WsSvcFwm1sc	Connection Refused by xx.xx.xx.xx
Device#3	xx.xx.xx.xx	Cisco WsSvcFwm1sc	Connection Refused by xx.xx.xx.xx
Device#4	xx.xx.xx.xx	Cisco WsSvcFwm1sc	Connection Refused by xx.xx.xx.xx
Device#5	xx.xx.xx.xx	Cisco WsSvcFwm1sc	Connection Refused by xx.xx.xx.xx
Device#6	xx.xx.xx.xx	Cisco PIXFirewall 525	Connection Refused by xx.xx.xx.xx
Device#7	xx.xx.xx.xx	Cisco PIXFirewall 525	Connection Refused by xx.xx.xx.xx
Device#8	xx.xx.xx.xx	Cisco MDS 9124e	Connection Refused by xx.xx.xx.xx
Device#9	xx.xx.xx.xx	Cisco MDS 9124e	Connection Refused by xx.xx.xx.xx
Device#10	xx.xx.xx.xx	Cisco IPS 4240	Connectivity issues, discarding configuration (or configuration is too short)
Device#11	xx.xx.xx.xx	Cisco CSS 11503	Connection Refused by xx.xx.xx.xx
Device#12	xx.xx.xx.xx	Cisco Catalyst 3560-8PC	
Device#13	xx.xx.xx.xx	Cisco Catalyst 3560-48TS	Connection Refused by xx.xx.xx.xx
Device#14	xx.xx.xx.xx	Cisco Catalyst 3560-48TS	Connection Refused by xx.xx.xx.xx
Device#15	xx.xx.xx.xx	Cisco ASR 1001 Router	Connection Refused by xx.xx.xx.xx
Device#16	xx.xx.xx.xx	Cisco ASR 1001 Router	Connection Refused by xx.xx.xx.xx
Device#17	xx.xx.xx.xx	Cisco ASA 5585 SSP 10SC	Connectivity issues, discarding configuration (or configuration is too short)
Device#18	xx.xx.xx.xx	Cisco ASA 5585 SSP 10SC	Connectivity issues, discarding configuration (or configuration is too short)
Device#19	xx.xx.xx.xx	Cisco ASA 5585 SSP 10SC	Connectivity issues, discarding configuration (or configuration is too

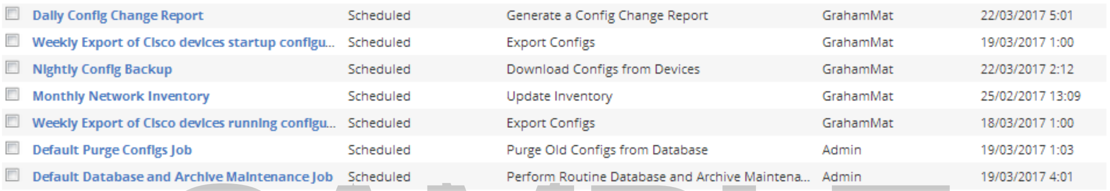
System Name	IP Address	Machine Type	Login Status
			short)
Device#20	xx.xx.xx.xx	Cisco ASA 5585 SSP 10SC	Connectivity issues, discarding configuration (or configuration is too short)
Device#21	xx.xx.xx.xx	Cisco 1941K9	Connection Refused by xx.xx.xx.xx
Device#22	xx.xx.xx.xx	Catalyst 37xx Stack	Connection Refused by xx.xx.xx.xx

Figure 12 - Login Failure Report

Jobs

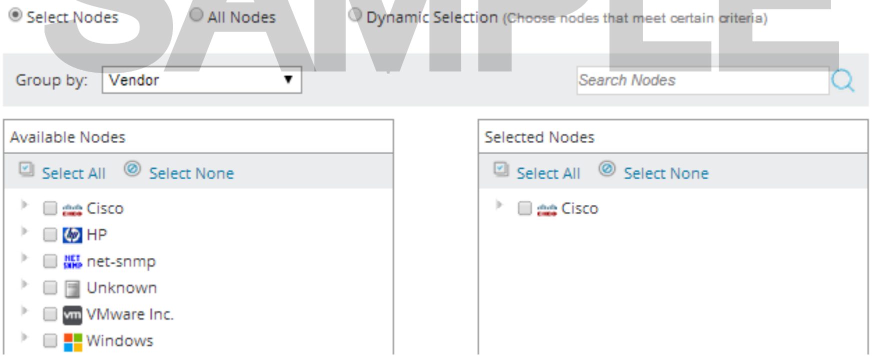
There appears to be some misconfigurations on the NCM jobs. These jobs allow SolarWinds to automate some processes such as backup jobs or scripts among others. The following issues have been found:

- Nightly config backup doesn't get backups from all devices in NCM
- Every single backup is stored on the database even if there is no change on it. This increases the size of the database unnecessarily.
- Only last 30 backups per node are available on the database. We recommend to extend the retention period of configuration backups to one year.



□	Daily Config Change Report	Scheduled	Generate a Config Change Report	GrahamMat	22/03/2017 5:01
□	Weekly Export of Cisco devices startup configu...	Scheduled	Export Configs	GrahamMat	19/03/2017 1:00
□	Nightly Config Backup	Scheduled	Download Configs from Devices	GrahamMat	22/03/2017 2:12
□	Monthly Network Inventory	Scheduled	Update Inventory	GrahamMat	25/02/2017 13:09
□	Weekly Export of Cisco devices running configu...	Scheduled	Export Configs	GrahamMat	18/03/2017 1:00
□	Default Purge Configs Job	Scheduled	Purge Old Configs from Database	Admin	19/03/2017 1:03
□	Default Database and Archive Maintenance Job	Scheduled	Perform Routine Database and Archive Maintena...	Admin	19/03/2017 4:01

Figure 13 - NCM jobs



● Select Nodes ○ All Nodes ○ Dynamic Selection (Choose nodes that meet certain criteria)

Group by: Vendor

Search Nodes

Available Nodes

Select All Select None

- □ Cisco
- □ HP
- □ net-snmp
- □ Unknown
- □ VMware Inc.
- □ Windows

Selected Nodes

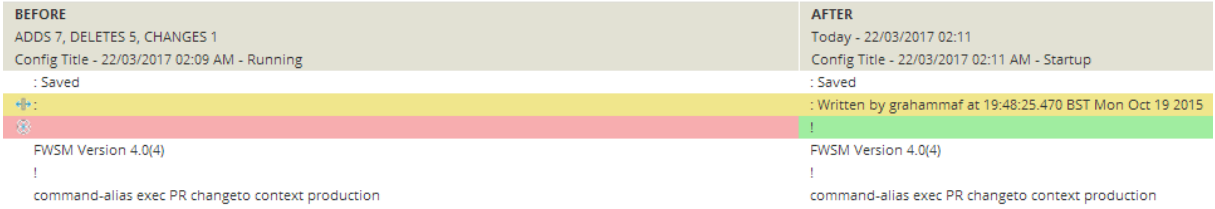
Select All Select None

- □ Cisco

Figure 14 - NCM Job misconfiguration

Comparison exclusions

Even though there are some custom comparison exclusions configured, they don't cover all the situations where configuration commands shouldn't be compared.

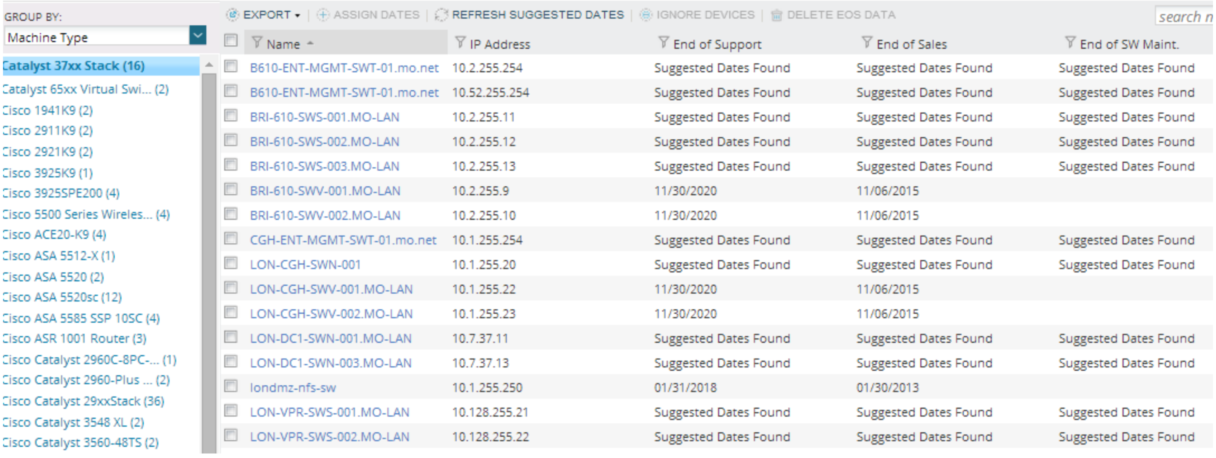


BEFORE ADDS 7, DELETES 5, CHANGES 1 Config Title - 22/03/2017 02:09 AM - Running	AFTER Today - 22/03/2017 02:11 Config Title - 22/03/2017 02:11 AM - Startup
: Saved	: Saved
:	: Written by grahammaf at 19:48:25.470 BST Mon Oct 19 2015
	!
FWSM Version 4.0(4)	FWSM Version 4.0(4)
!	!
command-alias exec PR changeto context production	command-alias exec PR changeto context production

Figure 15 - commands that should be excluded from comparison

End of Life / End of Support

End Of Life features has been configured in NCM, however not all the devices have a correct value in it. As the suggested dates by SolarWinds are not 100% accurate, as variations in models can impact the lookup results, we would recommend to complete manually the missing values.



GROUP BY: Machine Type

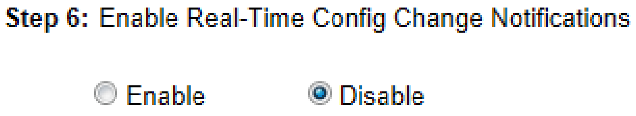
- Catalyst 37xx Stack (16)
- Catalyst 65xx Virtual Swi... (2)
- Cisco 1941K9 (2)
- Cisco 2911K9 (2)
- Cisco 2921K9 (2)
- Cisco 3925K9 (1)
- Cisco 3925SPE200 (4)
- Cisco 5500 Series Wireles... (4)
- Cisco ACE20-K9 (4)
- Cisco ASA 5512-X (1)
- Cisco ASA 5520 (2)
- Cisco ASA 5520sc (12)
- Cisco ASA 5585 SSP 10SC (4)
- Cisco ASR 1001 Router (3)
- Cisco Catalyst 2960C-8PC-... (1)
- Cisco Catalyst 2960-Plus ... (2)
- Cisco Catalyst 29xxStack (36)
- Cisco Catalyst 3548 XL (2)
- Cisco Catalyst 3560-48TS (2)

□	Name	IP Address	End of Support	End of Sales	End of SW Maint.
□	B610-ENT-MGMT-SWT-01.mo.net	10.2.255.254	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	B610-ENT-MGMT-SWT-01.mo.net	10.52.255.254	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	BRI-610-SWS-001.MO-LAN	10.2.255.11	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	BRI-610-SWS-002.MO-LAN	10.2.255.12	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	BRI-610-SWS-003.MO-LAN	10.2.255.13	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	BRI-610-SWV-001.MO-LAN	10.2.255.9	11/30/2020	11/06/2015	
□	BRI-610-SWV-002.MO-LAN	10.2.255.10	11/30/2020	11/06/2015	
□	CGH-ENT-MGMT-SWT-01.mo.net	10.1.255.254	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	LON-CGH-SWN-001	10.1.255.20	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	LON-CGH-SWV-001.MO-LAN	10.1.255.22	11/30/2020	11/06/2015	
□	LON-CGH-SWV-002.MO-LAN	10.1.255.23	11/30/2020	11/06/2015	
□	LON-DC1-SWN-001.MO-LAN	10.7.37.11	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	LON-DC1-SWN-003.MO-LAN	10.7.37.13	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	londmz-nfs-sw	10.1.255.250	01/31/2018	01/30/2013	
□	LON-VPR-SWS-001.MO-LAN	10.128.255.21	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found
□	LON-VPR-SWS-002.MO-LAN	10.128.255.22	Suggested Dates Found	Suggested Dates Found	Suggested Dates Found

Figure 16 - End Of Life

Real Time Change Detection

Real Time Change Detection (RTCD) is a NCM feature that allow us to download a fresh running configuration from the device and to get a notification when someone changes the configuration of any of our network devices. This feature is not configured at the moment, and one we recommend to utilise this feature to improve the visibility on who, when and how the network devices are being configured.



Step 6: Enable Real-Time Config Change Notifications

○ Enable ● Disable

Figure 17 - RTCD not configured

Complaince policy reports

This NCM feature allows us to detect if any configuration is in place or is missing from our network devices. Configurations such as cdp disable, enable secret, no public community string such be validated in order to avoid security issues in our environment.

This feature allows us to detect and remediate these misconfigurations throughout all the devices added into NCM. At the moment this feature is not being used.

Configuration Management Approval

NCM has a feature that allows us to control network configuration changes using SolarWinds users. This feature has been enabled however is not being actively used. We would recommend to turn off the feature, or to start using it by creating users with ‘Uploader’ role. These users will be able to execute scripts against the network devices configured in SolarWinds, but these scripts have to be accepted by a NCM admin. This feature configuration needs to be completed in order for Sample Company to take advantage.

Firmware vulnerability

This feature allows SolarWinds to check if there is any well-known vulnerability based on the firmware or IOS version of the devices. This feature is turned on, however no one is using it actively. We recommend to use this feature and start configuring the status of the found vulnerabilities to the appropriate one :

- Confirmed
- Not applicable
- Potential
- Remediated
- Remediation planned
- Waiver

4.19 IP Address Manager

This module allows us to monitor the IP usage of the Sample Company subnets and to monitor and manage the internal DHCP and DNS servers.

The current hierarchy of subnets monitored in IPAM looks adequate and simple to be maintained. However there are a few groups and supernets with no subnets within (example: Bristol 3rd Party VPN NAT). There are also 591 subnets that have been imported from the DHCP servers but have not been moved to the appropriate group and/or supernet. Please review these subnets (located under the group Imported Subnet) and review whether these subnets should be removed from the scope of IPAM or relocated to another group.

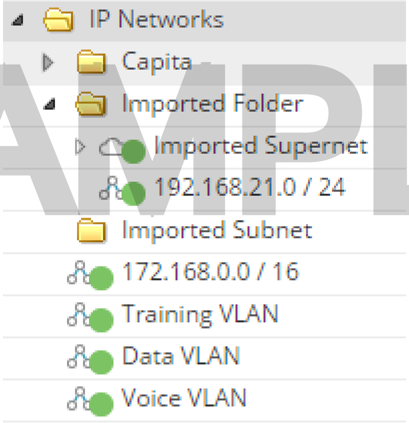
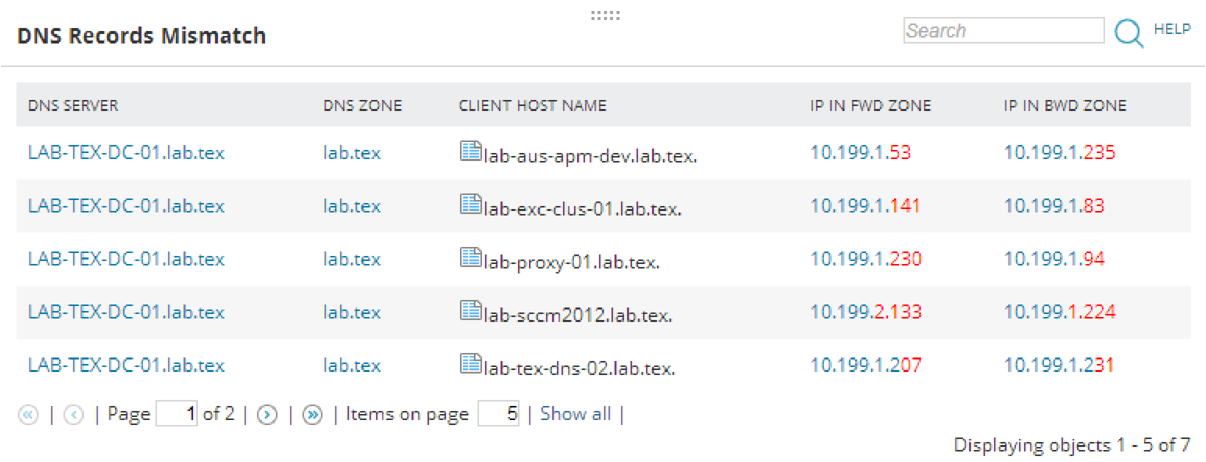


Figure 18 - IPAM subnets

There are two DHCP servers configured in IPAM, however both of them are down. Please review if these DHCP servers have been decommissioned or replaced for other DHCP servers.

At the moment there are no DNS servers added, it means there we are missing some critical information such as DNS record mismatch



DNS Records Mismatch

Search HELP

DNS SERVER	DNS ZONE	CLIENT HOST NAME	IP IN FWD ZONE	IP IN BWD ZONE
LAB-TEX-DC-01.lab.tex	lab.tex	lab-aus-apm-dev.lab.tex.	10.199.1.53	10.199.1.235
LAB-TEX-DC-01.lab.tex	lab.tex	lab-exc-clus-01.lab.tex.	10.199.1.141	10.199.1.83
LAB-TEX-DC-01.lab.tex	lab.tex	lab-proxy-01.lab.tex.	10.199.1.230	10.199.1.94
LAB-TEX-DC-01.lab.tex	lab.tex	lab-sccm2012.lab.tex.	10.199.2.133	10.199.1.224
LAB-TEX-DC-01.lab.tex	lab.tex	lab-tex-dns-02.lab.tex.	10.199.1.207	10.199.1.231

| Page 1 of 2 | | Items on page 5 | Show all |

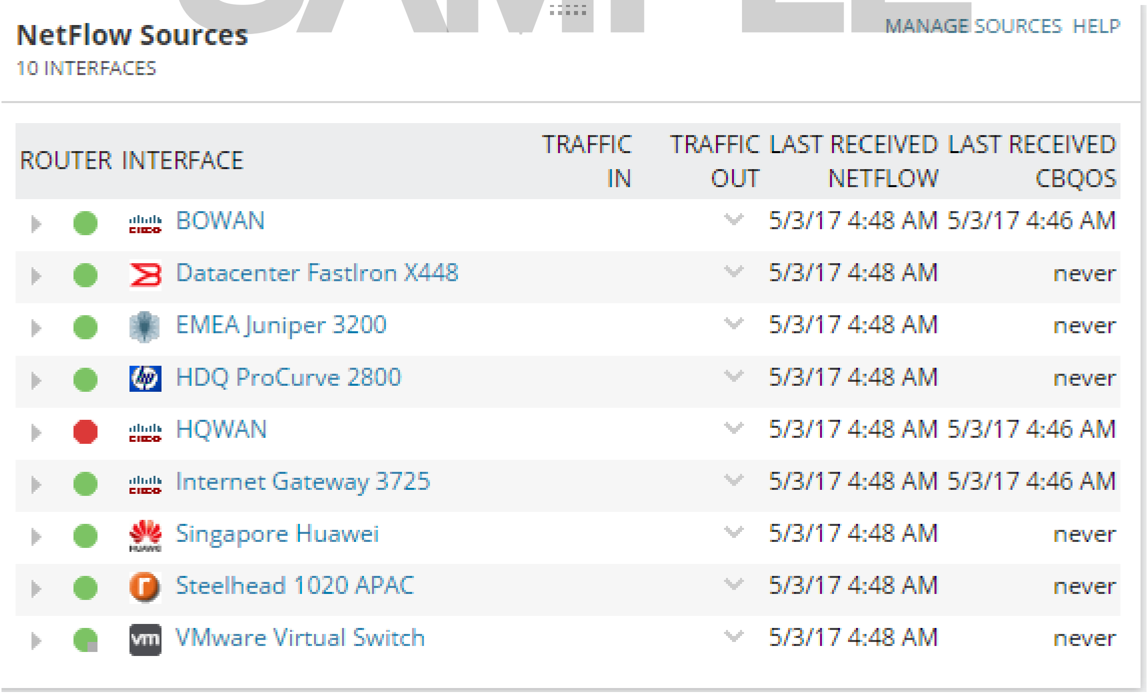
Displaying objects 1 - 5 of 7

Figure 19 - Example DNS Records Mismatch

4.20 Netflow Traffic Analyzer

Based on the number of netflow sources exporting dat to the SolarWinds server and the amount of traffic registered, it looks there is some flow information that are exported to SolarWinds more than one. We recommend to review the list of netflow exporters in order to avoid this situation. As best practices, we recommend to enable netflow on the WAN connections (MPLS, ADSL, VPN…) and, if required, on the connections to the Data Centers in order to review what type of traffic the servers are generating internally.

NOTE: SolarWinds will display netflow data received from monitored devices only. If a device that is not monitored in SolarWinds send netflow information to the SolarWinds server, this will discard that information. At the moment there are several event messages hightlighting that the SolarWinds server is receiving traffic from unmonitored devices.



NetFlow Sources

10 INTERFACES

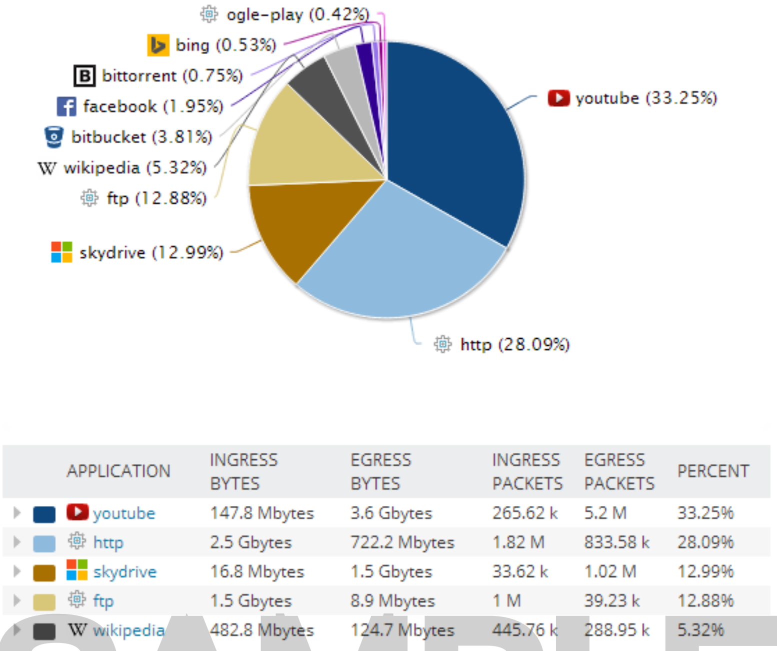
MANAGE SOURCES HELP

	ROUTER INTERFACE	TRAFFIC IN	TRAFFIC OUT	LAST RECEIVED NETFLOW	LAST RECEIVED CBQOS
🟢	BOWAN		˅	5/3/17 4:48 AM	5/3/17 4:46 AM
🟢	Datacenter FastIron X448		˅	5/3/17 4:48 AM	never
🟢	EMEA Juniper 3200		˅	5/3/17 4:48 AM	never
🟢	HDQ ProCurve 2800		˅	5/3/17 4:48 AM	never
🔴	HQWAN		˅	5/3/17 4:48 AM	5/3/17 4:46 AM
🟢	Internet Gateway 3725		˅	5/3/17 4:48 AM	5/3/17 4:46 AM
🟢	Singapore Huawei		˅	5/3/17 4:48 AM	never
🟢	Steelhead 1020 APAC		˅	5/3/17 4:48 AM	never
🟢	VMware Virtual Switch		˅	5/3/17 4:48 AM	never

Figure 20 - NTA Sources

There is a new feature available from NTA v4.2.1 that allows SolarWinds to analyse and display NBAR2 data. This cisco protocols does a deep packet inspection of each packet flowing across any monitored interface in order to determine the application. However the application is not determined only based on the destionation port, but based on the type of payload of the packet, allowing us to get a more granular information about the applications running on the network.

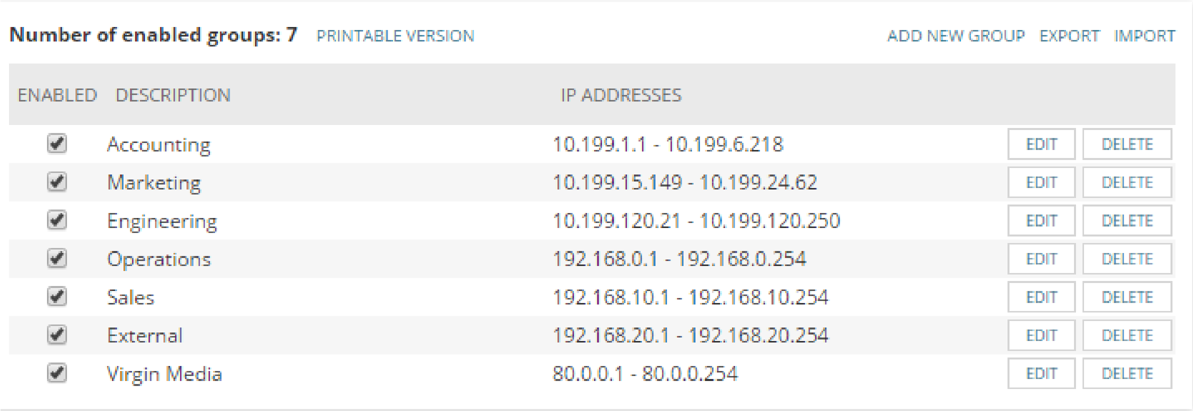
At the moment there is no device configured to export NBAR2 data, however we would recommend to review the list of devices that support this feature and determine whether or not it would be benefical to enable this feature.



	APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
■	youtube	147.8 Mbytes	3.6 Gbytes	265.62 k	5.2 M	33.25%
■	http	2.5 Gbytes	722.2 Mbytes	1.82 M	833.58 k	28.09%
■	skydrive	16.8 Mbytes	1.5 Gbytes	33.62 k	1.02 M	12.99%
■	ftp	1.5 Gbytes	8.9 Mbytes	1 M	39.23 k	12.88%
■	wikipedia	482.8 Mbytes	124.7 Mbytes	445.76 k	288.95 k	5.32%

Figure 21 - Example NBAR2 data

SolarWinds NTA has the ability to group IP address in order to create groups based on locations, departments, etc… This feature is being utilised at the moment, however the current NTA views are not displaying this data. We recommend to review the NTA dashboards in order to improve netflow information.

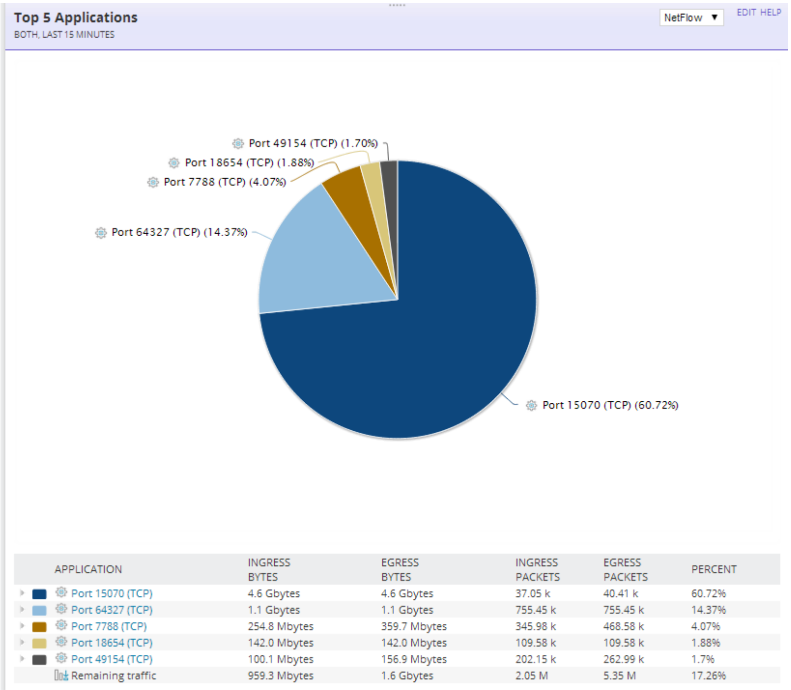


Number of enabled groups: 7

ENABLED	DESCRIPTION	IP ADDRESSES		
☑	Accounting	10.199.1.1 - 10.199.6.218	EDIT	DELETE
☑	Marketing	10.199.15.149 - 10.199.24.62	EDIT	DELETE
☑	Engineering	10.199.120.21 - 10.199.120.250	EDIT	DELETE
☑	Operations	192.168.0.1 - 192.168.0.254	EDIT	DELETE
☑	Sales	192.168.10.1 - 192.168.10.254	EDIT	DELETE
☑	External	192.168.20.1 - 192.168.20.254	EDIT	DELETE
☑	Virgin Media	80.0.0.1 - 80.0.0.254	EDIT	DELETE

Figure 22 - NTA IP Groups

By default SolarWinds NTA only displays statistics from the most common applications (around 22000 differet applications), however, as applications are based on port number, there are potentially 65535 different applications. When stastitics from an unmonitored applications are received, SolarWinds will display that traffic under the ‘unmonitored applications’ group. We recommend to review this group in order to check that no critical application is shadowed under this group.



	APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
■	Port 15070 (TCP)	4.6 Gbytes	4.6 Gbytes	37.05 k	40.41 k	60.72%
■	Port 64327 (TCP)	1.1 Gbytes	1.1 Gbytes	755.45 k	755.45 k	14.37%
■	Port 7788 (TCP)	254.8 Mbytes	359.7 Mbytes	345.98 k	468.58 k	4.07%
■	Port 18654 (TCP)	142.0 Mbytes	142.0 Mbytes	109.58 k	109.58 k	1.88%
■	Port 49154 (TCP)	100.1 Mbytes	156.9 Mbytes	202.15 k	262.99 k	1.7%
	Remaining traffic	959.3 Mbytes	1.6 Gbytes	2.05 M	5.35 M	17.26%

Figure 23 - Top Unmonitored Applications

5 CONCLUSION AND ACTION POINTS

The following table outlines the areas we feel need to be reviewed with suggested action points. The table is ordered by priority level:

- Red: immediate action
- Yellow: solve in short term
- Green: no urgent requirement

The table also includes the amount of Professional Services in hours for Prosperon to complete the recommended work.

Function	Issue	Recommended Action	PS in hours
NTA Server	It is not recommend to install NTA Flow database Server on the main poller	We recommend to install the NTA Flow Database Server in a separate server.	2
SQL Server	Performance issues	We recommend to expand the current RAM memory to 32GB and to configure RAID1+0 disks	4
Polling frequency	Polling rate is 445%	We recommend to return the polling frequencies to the default values and modify the polling frequency individually to those devices where is required.	0.5
		A minimum of one additional polling engine will be required.	1
Syslog and Traps	Too many messages per second	We recommend to use a different Syslog server (for example SolarWinds LEM) to centralise the reception of all messages, and then forward only the important messages to the SolarWinds server	-
NCM nodes	Incorrect nodes added into NCM	There are some devices that shouldn't be added into NCM, and some others that are not but should be.	4
NCM Jobs	Missing devices on jobs	We recommend to review the NCM jobs configured in order to get backups of all network devices.	1
Node population	Too many ICMP devices, and non-critical interfaces	We recommend to review the ICMP nodes monitored, and to delete the null0 and loopback interfaces.	1
Retention period	Retention periods are too long	Configure best practices on retention period.	1
Groups	Missing groups for dependencies	We recommend to follow the hierarchy proposed on to create groups for dependencies	4
Dependencies	No dependencies created	Created dependencies for each remote location	2
Alerting	Too many active alerts. Missing critical alert definitions	We recommend to review the existing alerts in order to avoid false alerts, but also get notified when any important event occurs on the network.	15

Dashboards	Poor views	We recommend to create specific node details views, and better summary views in order to improve the visibility of the statistics availabile on the SolarWinds server	15
IPAM DHCP and DNS	Not configured	We recommend to add the DHCP and DNS servers into IPAM	4
NTA sources	Too many NTA sources	We recommend to review the netflow sources configured in order to avoid duplication of data	-
NTA NBAR2	Not configured	We recommend to review the potential of this feature	-
NTA applications	Too much unmonitored traffic	We recommend to review the list of applications on the unmonitored traffic group	2
Custom pollers	Some critical information is missing, some custom pollers are polled natively from SolarWinds	We recommend to review the list of custom in order to delete those custom pollers that are now being polled natively, and created those ones suggested on.	4
Maps	Too many maps. Not displaing labels	Review maps in order to display custom labels. Too many maps impacts on the time required to maintain the existing maps.	4
Netpath	Use can be expanded	Install remote probes and create more Netpath operations	2
Quality of Experience	Too many applications, only two network sensors	We recommend to add server sensors, but limit the number of automatic applications discovered.	2
Accounts	Too many individual accounts. Some accounts have not been used in 4 years	We recommend to review the list of existing accounts in order to delete unused accounts and benefit AD accounts.	-
Reports	Missing critical reports	We recommend to create the suggested reports.	7.5
Custom properties	Lots of empty custom properties	We recommend to consolidate the existing custom properties and complete the empty ones	4
NCM End of Life	Partially configured	We recommend to configure this feature fully	4
NCM RTCD	Not Configured	We recommend to review the benefits of Real Time Change Detection	1
NCM firmware vulnerabilities	Not Used	We recommend to start using this feature	-
NCM compliance reports	Not Used	We recommend to start using this feature	2
IPAM subnets	Too many subnets	We recommend to review the existing subnets and the benefit of monitor them	4
NTA IP groups	Partially configured	We recommend to create views that can highlight this feature	2

Figure 24 - Action Points

*Should you want to trial any of these modules before purchasing the license, please install the modules in a separate server. Please do not trial modules on the production server.

6 RECOMMENDED BACKUP PROCEDURES

The SolarWinds solutions store the majority of their configuration settings and captured data within a Microsoft SQL Server Database. Therefore this is the most crucial element to ensure you have backed up. With regards to Orion NPM, the application can be rebuilt in its near entirety if you have the SQL database available.

The frequency of SQL Database backups depends on the level of acceptable data loss if you did ever need to revert to a restored database and how much space you have available to store the resultant backup file/s.

It is also recommended to backup the Program file directory/s:

e.g. C:\Program Files\SolarWinds

Reference Documents:

Orion NPM Migration Document:
http://www.solarwinds.com/support/Orion/docs/OrionServerMigration.pdf

7 SUPPORT & DOCUMENTATION

We provide direct support to the SolarWinds solutions for all licences with current maintenance purchased through Prosperon Networks. This is in addition to the support provided by the Vendor SolarWinds themselves. Active maintenance entitles you to full support on the licensed applications.

7.1 Prosperon Support Details

Telephone support available during business hours 9:00am to 5:30pm Monday to Friday

0845 833 1185

Email: support@prosperon.co.uk

7.2 SolarWinds Support Details

Administration documentation - http://www.solarwinds.com/support/documentation.aspx

Create SolarWinds Support Ticket - http://www.solarwinds.com/support/ticket/

SolarWinds Community Website – http://www.thwack.com

8 LEGAL NOTICES

8.1 Confidentiality

This document contains confidential and potential sensitive security related information. Neither Prosperon Networks nor the Customer for which this document has been created may disclose the confidential information contained herein to any third party without the written consent of Prosperon Networks, save that the Customer may disclose the contents of this document to those of its agents, principles, representatives, consultants or employees who need to know its contents for the purpose of the use of the solution.

8.2 Terms & Conditions

This document is subject to the standard Prosperon Networks Terms & Conditions which are maintained on the corporate website: http://www.prosperon.co.uk.

Prosperon Networks does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies or outdated information. This document and all information within it are provided on an "as is" basis without any warranties of any kind, express or implied.

9 APPENDIX I – SOLARWINDS LICENCING

SolarWinds Orion NPM is licensed based on the highest count from the three element types:

- Interfaces: interfaces include switch ports, physical/virtual interfaces, VLANs
- Nodes: nodes include entire devices (routers, switches, servers, APs)
- Volumes: volumes are equal to the logical disks you monitor

Examples:

SL100	Number Being Monitored
Nodes	99
Interfaces	50
Volumes	26

SL250	Number Being Monitored
Nodes	99
Interfaces	101
Volumes	99

SLX	Number Being Monitored
Nodes	1500
Interfaces	2001
Volumes	1800

10APPENDIX II – ANTI-VIRUS RECOMMENDATIONS

The following folders are recommended to be excluded from the real-time virus scans, failure to exclude these can impact performance especially on heavily used polling engines.

- %install drive%\inetpub\SolarWinds\
- %install drive%\program files(x86)\SolarWinds\
- %install drive%\program files(x86)\SolarWinds\ common files
- %install drive%\program data\SolarWinds\
- %install drive%\windows\temp\SolarWinds\
- %install drive%\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files\