SCP Study Aid

Network Performance Monitor (NPM)

Table of Contents

How to use this study aid

This study aid includes topics that you will find on the SCP NPM exam. Use the available SolarWinds documentation to search and learn more about each category.

NPM Installation
NPM Getting Started Guide
NPM Administrator Guide

The intention of the topics in this aid are to supplement your years of experience and hands-on training with SolarWinds' products.

This aid is **not** all-inclusive and should only be used as a starting place for your SCP studies.

If you have a SolarWinds product under active maintenance, you have access to virtual and on-demand training.

To access SolarWinds Academy classes:

1. Log on to your Customer Portal account at https://customerportal.solarwinds.com
2. Click Education & Training > Virtual Classrooms
3. Browse the available classes and select an option:
    - Click Register Now for a live class
    - Click the On-Demand link to access a recorded course video

The SolarWinds Academy adds available classes to the Virtual Classroom calendar every month.

Note – The SolarWinds Academy classes are additional study resources and are not explicitly designed for the SCP exam.

For additional study resources, visit THWACK.

1.0 Orion

1.1 Know about NPM licensing as standalone, with other Orion Platform products, and how to verify the current number of monitored nodes, volumes and interfaces and the number of the total number of elements allowed by your license.

- NPM License Summary
- Web-based license manager

- Monitored network elements:
  - Nodes
  - Interfaces
  - Volumes

- License:
  - Product license
  - Expired license
  - License key
  - Activate license
  - Activate license offline
- License upgrades

- Domain
- Registry key
- Deactivate
- Database size
- SQL Management Studio Express
- Virtual Machines

1.2 Know product requirements, when and how to migrate products and databases, upgrade new products and existing Orion deployments.

- How to install or upgrade:
  - New environment
  - Existing Orion deployment
  - Centralized upgrade

- Installation and upgrade checklist
- System Check
- Multi-module environments guidelines
- Destination folder
- Orion permission checker

- Credentials:
  - Account
  - Database
  - Local admin server

- Back up:
  - Database
  - Custom code

- Snapshot VMs
- Configure ports
- Windows Updates
- Anti-virus scan
- Authentication

- Database account:
  - Windows
  - SQL Server

- Servers:
  - Orion
  - Orion database
  - Additional databases

- Website settings:
  - Port 443
  - Port 80
  - Website Root Directory
  - SSL certificate
  - Self-Signed Certificate
  - Website binding
  - Orion Web Console

Sample questions

1. Your weekly scheduled discoveries consistently detect 5 Windows 10 workstations. What can you do to remove those devices from being discovered in the future?
    A. Add to Ignore List
    B. Add to Watch List
    C. Add to Black List
    D. Add to White List

2. How can you encrypt the username, password, and data between your NPM server and the Orion database?
    A. Use Windows authentication to encrypt the username, password, and data
    B. Use SSL to encrypt the username, password, and data
    C. Use Windows authentication to encrypt data and SSL to encrypt the username and password
    D. Use Windows authentication to encrypt the user name and password and SSL to encrypt the data

2.0 Cloud Services

2.1 Know about deploying the Orion Platform on cloud services Amazon Web Services (AWS) and Azure. Understand how a cloud installation is the same and different from other installations.

- Availability zone
- Computer capacity
- Host location for:
  - Main Orion server
  - Orion database server
- Enabling High Availability
- Deploying agents
- Port requirements
- Security group and server instance relationship
- Cloud network:
  - Public DNS hostname
  - Public IPv4 address
- LDAP servers used for user authentication
- Windows authentication
- Instance types for deployment
- Deployment types:
  - Cloud
  - Hybrid
- Cloud:
  - Main Orion server and database in the cloud
- Hybrid:
  - Main Orion server and database in the cloud
  - Additional Polling Engine on-premise
- Hybrid:
  - Additional Polling Engines in the cloud
  - Main Orion server and database on-premise
- Manual deployment:
  - Command prompt
  - Interactive wizard

AWS only:

- Virtual private cloud (VPC)
- Amazon EC2 instance
- Amazon EC2 instance with SQL
- Amazon EC2 console

Azure only:

- Azure Virtual Network (VNet)
- Product migrations
- High Availability backups
- Azure SQL DB
- Azure Marketplace
- Azure Active Directory
- Application Secret Key
- Azure IAM Permissions
- Role-based Access Control (RBAC)
- Unique machine name

---

1. Where can you find information on instances/VMs by cloud account and region?
   A. Cloud Asset Summary
   B. Cloud Server Infrastructure
   C. Cloud Instances Status Summary
   Active Cloud Alerts

2. You can only monitor Virtual Network Gateways with NPM.
   A. True
   B. False

3.0 Interfaces

Know how to manage an environment up to the interfaces level. Know where to locate information, how to customize interfaces to suit your needs, and how to understand information provided.

- Interface
  - Status
  - Health
  - Details views
  - Sub view
  - Status Polling

- Interface history
  - Downtime
  - Status

- Node Details - Interfaces subview
  - Downtime data
  - Blocks
  - Downtime History Retention
  - Interface downtime monitoring

- Transmit and Receive Bandwidth
- Custom Bandwidth

- Maintenance mode options
  - Mute alerts
  - Stop collecting data
  - Schedule a maintenance period

- ICMP
  - Poll status
  - Poll response time

- Real Time Charts
  - CPU Load & Memory Usage Chart
  - Percent Utilization Chart
  - Current data kept in 10 minute time frames

- In or Out Utilization
- Physical layout
- Duplex Mismatch alert

- Transmit and receive:
  - Bandwidth
  - Errors

- Unmonitored interface
- Monitoring Unknown Interface
- Ports
- Half-duplex
- Full-duplex

- Duplex mode issues
  - Mismatch
  - Unknown

- Default transmit and receive bandwidths are 1000 Mb/s
- Custom Bandwidth
- values for Transmit and Receive Bandwidth, in Mb/s
- Collect Statistics
- Unpluggable
- Unknown status

- Node Management utility
  - shut down interfaces
  - enable interfaces
  - remotely override

- Manage interfaces remotely
- EnergyWise power settings
- Remote override

- Widgets
  - Interface Downtime
  - Health Summary
  - Possible Duplex Mismatches

- Rack-mountable devices
  - Cisco 2960 switches
  - EX 2200 Juniper switches
  - EX 3300 Juniper switches

- Interface:
  - Unplugged
  - Down

- Switch port reports
- Duplex mode configuration
- Customize thresholds
- Change Real Time Charts data refresh time

- Change alerting thresholds
  - Received /Transmit Interface Errors and Discards
  - Receive/Transmit Interface Utilization

- Real-time polling
  - Chart open: polls automatically every 2 seconds
  - Chart closed: polling stops after 120 seconds

Sample questions

1. What is the difference between an Operationally Up interface, and an Operationally Down interface?
   A. Operationally Up, is an interface that is up and running, Operationally Down is an interface that has gone down
   B. Operationally Up is an interface that is available to use but is not being used, Operationally Down is an interface that is not available to use
   C. Operationally Up is an interface that is up and running and being used, Operationally Down is an interface that is available to use but not being used
   D. Operationally Up is an interface that is up and running and being used, Operationally Down is an interface that is disabled in the device configuration file

2. You can only poll status and response time using only ICMP when SNMP is disabled and ICMP is enabled on the device.
   A. True
   B. False

4.0 NetPath

4.1 NetPath displays the performance details of devices inside and outside of your network. Know how to discover your network with NetPath and view applications in your network.

- Requirements:
  - Orion Integration
  - Ports and firewall settings
  - Database storage
  - Scalability
- Network path:
  - Nodes
  - Connections
  - Interfaces
- Create a:
  - Service
  - Probe
- Node connection:
  - Latency
  - Packet loss
- Reporting the issue:
  - IP addresses of the nodes in question (54.239.111.33 and 205.251.244.209 in this case)
  - Date, time, and duration of the performance issue
  - Latency and packet loss information
- NetPath Services list
- Broken/slow connections
- Probe status
- Path history
- Inspector panel
- Default NPM feature
- TCP-based network service
- Probing interval
- Assign additional probes
- Primary polling IP address

Sample questions

1. Which agent is required to run NetPath services?
   A. AIX agent
   B. Linux Agent
   C. Windows Agent
   D. Any agent

2. NetPath™ services are monitored by ____.
   A. Network Traffic Analysis
   B. Probes
   C. Wireshark
   D. Agents

5.0 Orion Maps

5.1 Know the different Orion map types and how to view details for entities on mapped entities, view connections between displayed entities, create a custom Orion Map, customize the auto-generated maps.

- Wireless:
  - Controller
  - Clients
  - Signal coverage
  - Controller node
  - Network module
  - Meraki infrastructure
  - Migration
- Autonomous access point (AP):
  - Thin
  - Rogue
- 802.11 IEEE-compliant
- cloud system
- cloud/on premise
- Cisco Meraki Dashboard API
- API key
- Monitored access points
- Clients
- Unsupported metrics:
  - SSID information
  - Response time and packet loss
  - Status of access points
- Graphic formats:
  - .gif
  - .tiff
  - .jpg
  - .bmp
  - .png
- Global HTTP proxy
- Map scale
- Online maps
- Client devices
- Signal Sample wizard
- Signal samples
  - Simple
  - Multiple
- Access point details:
  - AP name
  - IP address
  - device type
  - SSID
  - channels used
  - number of clients connected
- Client details:
  - client name
  - SSID
  - IP Address
  - MAC Address
  - Received Signal Strength Indication (RSSI)
  - time connected
  - data rate
  - bytes received
- bytes transmitted

Sample questions

1. You can use Orion Groups in Maps.
   A. True
   B. False

2. How do you configure Automatic Geolocation in the Worldwide Map?
   A. Configure Latitude and Longitude custom properties and enable Automatic Geolocation
   B. Enable Automatic Geolocation on the Worldwide Map
   C. Configure custom dependencies and turn on Automatic Geolocation
   D. Configure automatic dependencies and turn on Automatic Geolocation

6.0 Capacity Planning

6.1 Know about setup and configurations, charts and widgets, and global and individual reports. Know how to monitor capacity usage trends on the network and forecast capacity issues in NPM.

- Track capacity metrics (must be monitored in NPM):
  - Nodes
  - Volumes
  - Interfaces

- Track usage:
  - Historical data
  - Trends
  - Up to 180 days

- Calculations:
  - Peak – Daily Maximum Values
  - Average – Average Daily Values

View and Monitor in the Web Console

- Customize Views with Capacity Planning Widget
- Globally (include/exclude metrics):
  - CPU Capacity Forecast Chart
  - Memory Capacity Forecast Chart
  - Storage Capacity Forecast Chart
  - Interface Utilization Receive Forecast Chart
  - Interface Utilization Transmit Forecast Chart

- Individual Element:
  - Per element
  - Divided metrics
  - Individual widgets
  - Track individual nodes, volumes or interfaces

- Configure calculations and thresholds:
  - Calculate Warning and Critical Thresholds
  - Calculate Forecast Calculation Method by monitored element

- Out of the Box Reports:
  - Disks Approaching 100% Capacity
  - Node Capacity Forecasts

Forecast Calculations

- Peak Calculation:
  - Forecast trends using daily maximum values
  - Suitable for important/critical devices to prevent reaching certain functionality thresholds

- Average Calculation:
  - Forecast trends based on average daily values
  - Suitable for non-critical devices where short periods of exceeding thresholds are acceptable

Set Thresholds and Calculation Methods

- Global Calculation methods (recommended):
  - Set Global value to Average
  - Customize critical devices to Peak

- Individual/Group of nodes:
  - Interfaces or Volumes Settings
  - Change calculation methods Override global setting

- Capacity Planning:
  - Average CPU
  - Disk Usage
  - Percent Memory

Sample questions

1. By default, what is the longest time period taken into account for calculating the capacity forecast?
   A. 24 hours
   B. 30 days
   C. 180 days
   D. 365 days

2. You can view interface, node, and volume information in one capacity forecasting widget.
   A. True
   B. False

7.0 Custom SNMP Polling

7.1 Know which polling method to use to monitor nodes in the way that best suits different environments.

- The Device Studio can:
  - Poll multiple OIDs for a technology
  - Poll single CPU and RAM
  - Poll multiple CPUs and RAM
  - Poll for additional Node Details
  - Perform logical operations for custom polling
  - Display custom polled values in existing resources (e.g., Current CPU and Memory Utilization or Node Details)

- Polling methods
  - External Node: No Status – No data is collected
  - Status Only: ICMP – Ping, collects only status, response time, and packet loss
  - Most Devices: SNMP and ICMP – Ping and SNMP
  - Windows Servers: WMI and ICMP – Recommended for Windows servers
  - Windows & Linux Servers: Agent – Installs an agent on Windows and Linux devices
  - Meraki Wireless – API-based polling for Meraki Wireless Gear

- SNMP Agent
- SNMP Walk
- SNMP trapping
- SNMP Version

- SolarWinds® Management Information Base (MIB) database
  - MIB walk
  - MIB tree
  - MIB browser
  - MIB database

- OOTB pollers:
  - Native Pollers
  - SolarWinds pollers

- SysObject ID
- OID values
- Map Values

- Managed devices
  - IP network
  - Device IP

- MIB update ZIP file
- MIBs.cfg file
- Service Manager
- Unique devices
- MIB walk utility

- Assign pollers
- Vital Stats
- Data Source Calculations
- Automatically Poll Nodes
- Assign nodes
- Universal Device Poller (UNDP)

- Transform results
  - Data transformations
  - Data mapping

- UnDP to poll any supported SMNP technology
- OIDs in the MIB database

Sample questions

1 What can you use custom pollers for? Select all that apply.

A. Monitor a specific metric which is not monitored out-of-the box
B. Monitor special equipment
C. Monitor objects although the number of monitored objects exceeds a poller's capacity limitation
D. Monitor capacity usage trends on the network

2 Which data source can you not use for polling devices?

A. A polled value or values reported by a device on an OID
B. A calculated value that results from the transformation of polled values
C. A fixed value in the form of a constant number or text
D. A custom property value through on the Orion Web Console

8.0 Hardware Health Monitoring

8.1 Hardware Health monitoring

Understand the different ways that Hardware Health is enabled. Know how to view statistics and how to adjust sensors, thresholds, and alerts.

- Network Devices Router switches
- Network Sonar Discovery
- Enable/disable hardware health monitoring
- Collect hardware health statistics
- Hardware Health Sensors

- Hardware health:
  - Statistics
  - Sensors
  - Polling
  - Temperature units

- Monitor hardware health devices:
  - Cisco®
  - Dell®
  - F5®
  - HP®
  - Arista®
  - Juniper®

- Thresholds
  - Default
  - Custom
  - Force to Up

- Cisco device MIBs
  - CISCO-ENTITY-SENSOR-MIB (default MIB)
  - CISCO-ENVMON-MIB

- Hardware Health device statuses:
  - Up
  - Warning
  - Critical
  - Unknown

- Hardware Details
- Hardware Health resource
- Enable and disable Hardware Health poller
- Poll data for a sensor

Sample questions

1. By default, all sensors available in the selected MIB are monitored on devices with enabled hardware health monitoring.
   A. True
   B. False

2. Hardware health information is collected only for _____ where the hardware sensors are enabled.
   A. Indexes
   B. Volumes
   C. Nodes
   D. Interfaces

9.0 Network Insight

9.1 Know which Network Insight options are supported and how to implement the best options for different environments.

- Supported:
  - F5 load balancers (Network Insight for F5)
  - Cisco ASA firewalls (Network Insight for ASA)
  - Cisco Nexus switches (Network Insight for Nexus)
  - Palo Alto firewalls (Network Insight for Palo Alto)

- Network Insight for Nexus:
  - Requirements
  - SNMP/CLI polling
  - Monitor redundancy and uptime for data center connections
  - View virtual port channel (vPCs) information
  - CLI to poll data
  - vPC details
  - Custom alerts
  - vPC connection to end hosts

- Network Insight for F5:
  - Monitors all elements of the load-balancing environment (virtual servers, pools, pool members, and applications)
  - Graphically display the relationships and component statuses
  - View individual component details for troubleshooting
  - Concurrent Connections by Virtual Server
  - Performance statistics
  - Out-of-box reports/alerts
  - F5 pool member rotation
  - Virtual servers
  - Traffic groups
  - High Availability clusters

- Network Insight for Palo Alto:
  - Site-to-Site/ GlobalProtect VPNs
  - Remote Access connections
  - Custom notifications/reports
  - GlobalProtect™ information and connection details
  - Integration points: NCM, NTA, UDT
  - Perfstack
  - Site-to-Site entities
  - REST API key / session key

- Network Insight for ASA:
  - Requirements
  - ASA firewalls
  - Integration points: NPM, NCM, and UDT
  - Health, interface, user, and connection information views
  - Site to Site VPN tunnels
  - Site to Site VPN health overview/connections
  - VPN: context, load, HA, bandwidth
  - Remote Access VPN
  - SNMP/CLI polling
  - ASA high availability statuses
  - Out-of-box reports/alerts
  - Monitor contexts
  - Access lists
  - Performance Analysis dashboard

9.2 Monitoring with Cisco SwitchStack

- SwitchStack®:
  - Members
  - Rings
  - Events
  - Object
  - Node
- Master switch
- Crown icon
- Hardware Health
- Sensor status
- Member-specific monitoring
- Out-of-the-box SwitchStack alerts:
  - SwitchStack Master Changed
  - SwitchStack Data Ring Broken
  - SwitchStack Member Number Changed
  - SwitchStack Power Redundancy Lost
- Serial number
- Individual switches
- Topology maps
- Data ports
- Power ports
- SwitchStack messages:
  - Stack ring redundancy loss
  - Stack ring failure
  - Members being added or removed
  - Member number changes
  - Master switch changes
  - Power redundancy loss
  - Power capacity change

9.3 Monitoring with Cisco ACI

- Monitor Cisco ACI devices in NPM requirements:
  - ACI credentials
- Enable API polling on ACI devices to monitor these components of your SDN environment:
  - Tenants
  - Application profiles
  - Endpoint groups
  - Spine and leaf switches
- To monitor ACI-specific information:
  - Add an APIC node to NPM and edit node to turn on ACI and add credentials
  - View members and their health scores on the device.
  - View health score history in PerfStack
  - View ACI environment on Orion Maps
- ACI
  - Objects
  - Devices
  - Polling
  - Events
  - Alerts
  - Reports
  - Tenant
- APIC nodes
- Orion Maps
- SDN infrastructure
- Inspector panel
- custom notifications
- Trigger action
- Cisco OIDs
- Health scores values

Sample questions

1. How do you verify you have vPCs configured for Nexus devices?
   A. Enable CLI polling and review the node details view
   B. Run 'show vpc brief' command on the device
   C. Enable Nexus VPC in Status & Response Time
   D. Check the Interfaces subview

2. How do you enable the Network Insight for Palo Alto Site-to-Site VPNs and GlobalProtect VPN sub views?
   A. Enable Palo Alto sub views in the Additional Monitoring options
   B. Enable polling of Palo Alto devices monitored in NPM via the Palo Alto REST API
   C. Access the Orion Web Console using an administrative account with permissions set for the XML API
   D. Add the sub view by configuring the Left Navigation pane

10.0 SNMP Trapping and Syslog Management

10.1 Know how to manage SNMP Traps and Syslog with NPM.

- SNMP trap messages
- Syslog messages
- SNMP v1
- SNMP v2c
- SNMP v3

- Syslog and trap default ports:
  - Port 514 for Syslog UDP
  - Port 162 for Traps UDP

- Syslog and trap message retention

- SNMP:
  - Packets
  - Trap Service

- Get type:
  - GET
  - GET NEXT
  - GET TABLE

- Message parsing:
  - Makes the messages shorter
  - Removes DNS name from lookups

- SNMP Trap action
- SNMP Trap Editor
- SNMP authentication requests
- SNMP authentication traps
- SNMP discovery

- Orion Log Viewer (OLV):
  - Replacing Syslog and Trap viewers
  - Requires SQL 2016 SP or later database
  - View and filter multiple parameters of logs
  - Create rules for Syslogs and Traps by default

- SNMP Walk tool
- Net-SNMP
- Memory Utilization
- SNMP Trap email message
- SolarWinds Real-Time Bandwidth Monitor Tool
- SNMP community strings
- SNMP Service on F5 device
- SNMP to status mapping information

Sample questions

1. Why might you receive unreadable trap messages from NPM? Select all that apply.
   A. A firewall between the device and the NPM server is blocking SNMP
   B. The device MIBs are not in your MIB database
   C. The device does not support SNMP
   D. The device uses SNMPv3 and has not been added as a monitored node for authentication

2. What is the default retention for Syslog Messages before messages are deleted from the database?
   A. 7 days
   B. 30 days
   C. 180 days
   D. 365 days

Sample Question Answer Key

Orion	1. A 2. D
Cloud Services	1. B 2. A
Interfaces	1. C 2. A
NetPath	1. C 2. B
Orion Maps	1. A 2. A
Capacity Planning	1. C 2. B
Custom SNMP Polling	1. A, B, C 2. D
Hardware Health Monitoring	1. A 2. C
Network Insight	1. B 2. B
SNMP Trapping and Syslog Management	1. B, D 2. A