DUMPSARENA

SolarWinds Network Performance Monitor (NPM) Exam

SolarWinds SCP-NPM

Version Demo

Total Demo Questions: 9

Total Premium Questions: 96

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Network performance over an inter-campus Ethernet link is slow. One side of the connection is experiencing a high number of packet drops. What information in NPM can you review to help discover the cause of the issue?

A. Packet loss on the nodes on either side of the connection

B. MTU of each side of the link

C. Possible Duplex Mismatches

D. Routing tables on each side of the link

ANSWER: C

Explanation:

Possible Duplex Mismatches is the most useful information to review because a speed or duplex negotiation inconsistency is a common Ethernet-layer cause of severe performance degradation and one-sided packet loss. For example, when one endpoint operates in full duplex while the peer operates in half duplex, the half-duplex endpoint can register collisions or late collisions, while the full-duplex endpoint may record frame check sequence errors or discards. The resulting retransmissions and dropped frames can make an otherwise healthy inter-campus link appear slow.

NPM polls monitored interface properties and operational counters through SNMP. On the relevant Interface Details view, review the reported interface speed and duplex values together with error, discard, collision, and utilization statistics. Comparing the two connected interfaces over the same time range helps establish whether the observed drops align with a suspected negotiation mismatch. This gives an administrator actionable evidence to verify the physical-port configuration and ensure both endpoints use compatible, intentionally configured speed and duplex settings. SolarWinds documents the interface-level statistics and details available through NPM in its Interface Details documentation and provides broader interface-monitoring guidance in the NPM interface monitoring documentation.

QUESTION NO: 2

A router is monitored with the Status Only: ICMP polling method. Which three metrics can NPM collect for this node without successful SNMP polling? (Choose three.)

A. Status

B. Average response time

C. CPU utilization

D. Packet loss

E. Interface bandwidth utilization

ANSWER: A B D

Explanation:

Status, **average response time**, and **packet loss** are available through ICMP-based status polling. ICMP echo requests let NPM determine whether the router responds, calculate response time, and identify missed responses as packet loss.

CPU utilization and interface bandwidth utilization require SNMP-accessible counters and device data. Changing the polling method to SNMP and ICMP, with valid SNMP credentials and connectivity, is required to collect those metrics.

QUESTION NO: 3

You are investigating an intermittent slowdown that may involve a router, a WAN interface, and a cloud service. Which two PerfStack capabilities help you investigate the issue? (Choose two.)

A. Add time-series metrics from multiple monitored entities to one analysis

B. Automatically discover physical topology links between the selected entities

C. Save the analysis project and share its URL with authorized users

D. Bypass account limitations for users who open the shared project

ANSWER: A C

Explanation:

Add time-series metrics from multiple monitored entities to one analysis and **save the analysis project and share its URL with authorized users** are correct. PerfStack is designed to correlate performance data from multiple entities on a common timeline, which helps determine whether interface utilization, response time, and other metrics changed together. Saved projects can be shared with other authorized users for collaboration or incident handoff.

PerfStack does not automatically discover physical topology links; that is provided through topology discovery and maps. Sharing a project URL does not bypass account limitations or grant access to objects that the recipient is not authorized to view.

QUESTION NO: 4

Retention policies require you to keep Syslog messages in the database for 9 days before you can discard them. Syslog messages from 8 days ago are missing.

What is likely the issue?

A. Database compaction runs weekly

B. Default Syslog retention period is seven days

C. Default Syslog web filter is seven days

D. Detailed records are summarized after seven days

ANSWER: B

Explanation:

Default Syslog retention period is seven days is correct because the Orion Platform maintenance process removes Syslog records after the configured retention interval. In a standard configuration, Syslog messages are retained for seven days; therefore, messages that are eight days old may already have been deleted during database maintenance and will no longer be available for searches or display in the SolarWinds web console. This is a database-retention setting, not merely a console-display preference, so records removed by retention cannot be recovered through a broader search filter. To meet a policy requiring nine days of retention, an administrator should review and increase the Syslog retention setting in the Orion database-maintenance or polling/database settings, then ensure that the setting is applied before future records reach the existing deletion threshold. SolarWinds documents that the platform uses configurable database-retention periods to manage event and Syslog data growth; retention should be aligned with organizational compliance requirements and available database capacity. See the SolarWinds Orion Platform database maintenance documentation and the SolarWinds Syslog messages documentation.

QUESTION NO: 5

You want NPM to receive SNMP traps directly from a newly deployed switch. Which two conditions must be met for the switch traps to reach the SolarWinds Platform? (Choose two.)

A. Configure the switch to send traps to the SolarWinds Platform server or designated trap receiver

B. Allow SNMP trap traffic through the network path to the trap receiver

C. Create a Universal Device Poller for the trap OID

D. Change the switch to the Status Only: ICMP polling method

ANSWER: A B

Explanation:

Configure the switch to send traps to the SolarWinds Platform server or designated trap receiver is required because traps are unsolicited notifications sent by the device to its configured destination. NPM does not retrieve traps through normal SNMP polling.

Allow SNMP trap traffic through the network path to the trap receiver is also required. Firewalls or access-control lists between the switch and receiver must permit the trap traffic so the notifications can arrive for processing.

Adding a custom poller collects SNMP values through polling and is unrelated to receiving traps. Changing the device to ICMP-only monitoring does not configure or transport SNMP trap messages.

QUESTION NO: 6

You need to create a NetPath service for a business application hosted outside your network. Which two items define the service-monitoring path? (Choose two.)

A. A source probe

B. SNMP credentials for every Internet provider hop

C. A destination service

D. A Universal Device Poller assigned to the source node

ANSWER: A C

Explanation:

A source probe and **a destination service** are correct. NetPath analyzes the route from a configured probe, such as a SolarWinds Platform server or supported agent, to a destination service identified by its address and service port. The selected probe represents the location from which users or systems access the service.

SNMP credentials can be needed to monitor managed network devices, but they do not define a NetPath service. A custom poller collects a custom device statistic and is unrelated to path analysis.

QUESTION NO: 7

How do you assign users access to select reports?

A. Create the reports while logged in as each user and set permissions

B. Use custom properties and account limitations to control report access

C. Configure the report and add a Report Limitation. Assign the limitation to users who need access to the report

D. Save the reports in different sub-directories and set the permissions for each user

ANSWER: B

Explanation:

Use custom properties and account limitations to control report access. In the SolarWinds Platform, reports honor the permissions and account limitations of the user who runs or views them. Custom properties provide meaningful attributes

that can be assigned to monitored entities, such as a department, site, business unit, or customer. An administrator can then create an account limitation that filters accessible objects according to one or more of those property values and assign that limitation to the relevant account or role. For example, a Department custom property can identify the nodes owned by each department; users limited to their department will see report results only for the nodes within that authorized scope. This approach provides scalable, data-driven access control without requiring separate copies of every report. It also ensures that dashboards, views, alerts, and reports consistently respect the user's permitted monitoring data. SolarWinds documents that account limitations define the objects and data a user can access, and custom properties can be used as filtering criteria when establishing those limitations. See SolarWinds Platform account limitations and SolarWinds Platform custom properties.

QUESTION NO: 8

You want to limit a user to only monitor Windows servers and not be able to view other devices that NPM monitors. How can you do this?

A. Account limitations

B. View permissions

C. Account views

D. Alert limitations

ANSWER: A

Explanation:

Account limitations are the appropriate SolarWinds Platform mechanism for restricting what monitored objects an individual account or group can see and manage. An administrator can create a custom account limitation using a node property, such as the operating-system field, and configure its criterion to include Windows servers. When that limitation is assigned to the relevant user account or user group, the platform filters nodes and related monitored objects so the user's access is constrained to the permitted Windows systems rather than the full set of devices monitored by NPM.

This supports delegated monitoring: server administrators can work with the infrastructure for which they are responsible without gaining visibility into unrelated network equipment. Limitations can be based on built-in object properties and can also be organized through custom properties, which is useful when operating-system detection alone does not match an organization's administrative boundaries. The restriction is applied at the account level and is honored throughout applicable views, reports, and other SolarWinds Platform functions, helping ensure that authorization is consistent rather than merely changing a page's presentation.

For configuration guidance, see SolarWinds documentation on limiting user access to network areas with account limitations and creating custom account limitations.

QUESTION NO: 9

You're troubleshooting a complex network issue and need to build a comparison of several metrics across multiple devices and SolarWinds products to identify the problem. What feature can you use?

A. PerfStack

B. Network Insight

C. NetPath

D. AppStack

ANSWER: A

Explanation:

PerfStack is the appropriate feature because it provides a customizable analysis workspace for comparing and correlating time-series performance data across monitored entities and SolarWinds products. During a complex investigation, an administrator can add multiple metrics to the same project, align them on a shared timeline, and look for relationships between changes in network health, interface utilization, response time, application performance, traffic, and related monitored data. This cross-product visibility is especially useful when the underlying cause is not isolated to one node or one metric. PerfStack supports drag-and-drop chart creation and enables the analyst to save a project for continued investigation or collaboration. Its time-range controls and visual correlation capabilities help identify whether events and performance changes occurred together, which is central to efficiently narrowing down a network issue. SolarWinds documents PerfStack as a tool for comparing metrics from multiple entities and products in a single view to assist troubleshooting. See the SolarWinds PerfStack documentation and the NPM guidance for troubleshooting with PerfStack.