PassQueen
a.k.a dumpsqueen.com

Hybrid Cloud Observability Network Monitoring Exam

SolarWinds Hybrid-Cloud-Observability-Network-Monitoring

Version Demo

Total Demo Questions: 18

Total Premium Questions: 187

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Network Performance Monitoring	122
Topic 2, Network Traffic Analysis	52
Topic 3, Network Configuration Management	1
Topic 4, IP Address Management	1
Topic 5, VoIP and Network Quality Monitoring	1
Topic 6, Mix Questions	10
Total	187

QUESTION NO: 1

Which two of the following components are required to successfully create a NetPath probe? (Choose two.)

A. connection port

B. Linux agent

C. source IP address

D. Windows agent

ANSWER: A D

Explanation:

connection port and **Windows agent** are required because a NetPath service probe must have both a supported Windows-based source and a target service definition. NetPath initiates synthetic TCP-path analysis from the selected source toward a destination, and the connection port identifies the TCP service that NetPath should test, such as HTTPS on port 443 or a custom application port. The port is therefore part of the probe's required destination configuration and enables NetPath to trace the network path actually used for that service connection.

The source must be a Windows system supported by NetPath. In practice, this can be a Windows node that has the SolarWinds agent installed or an appropriate Windows agent source selected during probe creation. The agent provides the local execution point from which NetPath gathers hop, latency, and path information. SolarWinds documents that NetPath probes require a Windows node or agent as their source and do not support Linux agents as probe sources. Together, the Windows agent source and connection port provide the supported origin and the service endpoint details needed to deploy and run the probe. See the official SolarWinds NetPath Services documentation and SolarWinds NetPath overview.

QUESTION NO: 2

Which two of the following locations can be checked for network hardware health functionality? (Choose two.)

A. device view

B. node properties

C. list resources

D. manage sensors

ANSWER: C D

Explanation:

list resources and **manage sensors** are the appropriate locations for checking and configuring network hardware health monitoring in SolarWinds Network Performance Monitor. The List Resources workflow is used for a monitored node to discover the resources exposed through the device's polling method, including hardware-health entities where they are supported. It provides a practical place to verify that relevant hardware components are available for monitoring and selected for collection.

The Manage Sensors area is the dedicated hardware-health management interface. It lets an administrator review the sensors SolarWinds has discovered for monitored devices and manage monitoring for sensor categories and individual components, such as temperature, fan, voltage, power-supply, and memory sensors. This is the key location for confirming that sensor monitoring is enabled and that the resulting hardware status can be collected and surfaced in the platform.

Hardware-health availability depends on the device, its supported management interface, and the sensor data the device exposes. SolarWinds documents the discovery and management of these hardware-health sensors in its Hardware Health Monitoring documentation and its hardware health sensor management guidance.

QUESTION NO: 3

In which scenario would the device studio poller tool be considered the best tool for building a required poller?

A. Building a poller for ARP tables to display in the web console.

B. Building a poller to add missing information to node details.

C. Building a poller to monitor VPN tunnel status.

D. Building a poller to show CPU and memory status.

ANSWER: B

Explanation:

Building a poller to add missing information to node details. is correct because Device Studio is intended for extending SolarWinds monitoring support when a device exposes useful SNMP data that is not covered by the product's out-of-the-box pollers. It provides a guided workflow to identify a device, browse and test its supported OIDs, create custom polling definitions, and associate the resulting metrics with the appropriate device type. This makes it particularly suitable when the required value should become part of the monitored node's data and be available in the node details experience, alerts, reports, and custom views.

In practice, an administrator would use Device Studio when a vendor-specific platform or a newly introduced device model has operational attributes that SolarWinds does not collect by default. After validating the OID and defining how its returned value should be interpreted, the custom poller can be assigned to applicable nodes so the missing operational information is collected consistently. This approach helps retain standard SolarWinds monitoring workflows while enriching device visibility with model- or vendor-specific metrics. SolarWinds documents Device Studio as the tool for creating custom device pollers and extending monitoring coverage; see the SolarWinds Device Studio documentation and the custom poller documentation.

QUESTION NO: 4

An existing NetPath probe is examined, and it is noted that the thickness of connection lines is different on various routes between devices. What does this indicate?

A. The probing interval for the probe is shorter on one path than on the other.

B. The thicker line indicates the more likely path of traffic from source to destination.

C. The thicker line is monitored in hybrid cloud observability (HCO) and contains other metrics.

D. Two probes with different probing intervals are monitoring the same path

ANSWER: B

Explanation:

The thicker line indicates the more likely path of traffic from source to destination. NetPath does not present a single fixed route as though every probe packet must traverse identical hops. Instead, it collects path-probing results over time and visualizes the observed network paths between the probe and the monitored service. When multiple routes or connections appear in the NetPath view, line thickness represents the relative frequency with which NetPath observed traffic following that connection. A thicker connection therefore indicates a path that is more commonly observed and is consequently more likely to be used by traffic traveling from the selected source toward the destination at that time. This visualization is particularly useful when equal-cost multipath routing, load balancing, dynamic routing changes, or cloud-provider network behavior causes traffic to take more than one route. Administrators can use the relative line widths to identify the dominant path and investigate performance data in the relevant hops or networks. SolarWinds describes NetPath as a service-delivery path analysis tool that discovers and visualizes paths to on-premises and cloud services; its path display uses line weight to communicate the likelihood of a route. See the SolarWinds NetPath documentation and the SolarWinds NetPath overview.

QUESTION NO: 5

Event logs are to be collected from Windows servers in order to be analyzed in hybrid cloud observability.

Which two of the following actions must be taken in order to accomplish this task? (Choose two.)

A. configure a rule on hybrid cloud observability to poll the server and collect logs

B. configure a rule on hybrid cloud observability to read event log folder locations

C. configure server to send logs to another server running the platform

D. deploy and configure the platform agent to collect the logs

ANSWER: C D

Explanation:

Windows event-log collection requires both a method for delivering the event data to the SolarWinds Platform environment and an agent-based collection component configured to read the applicable Windows Event Log channels. Configuring the server to send logs to another server running the platform establishes the required forwarding or delivery path. This is particularly relevant when Windows Event Forwarding is used: events can be forwarded to a collector, where they are available through the Forwarded Events log for monitoring and analysis. Deploying and configuring the platform agent to collect the logs provides the local SolarWinds collection mechanism. The agent runs on the monitored or collector system, accesses the Windows event logs using the appropriate Windows permissions, and communicates collected data to the SolarWinds Platform for Log Analyzer processing, alerting, searching, and retention. In practice, administrators must ensure the agent is deployed, connected, and configured for the intended event-log sources, while also ensuring that any forwarded events arrive at the designated collector. These two steps establish both the event-data source path and the platform's means of ingesting it. SolarWinds documentation for the product is available through the Log Analyzer Success Center and the SolarWinds Platform agent deployment documentation.

QUESTION NO: 6

What is the maximum number of resources that can be displayed in flow charts created by SolarWinds' platform views?

A. 25

B. 50

C. 75

D. 100

ANSWER: B

Explanation:

50 is the maximum number of resources that SolarWinds Platform views can display in a flow chart. This limit applies to the rendered flow-chart visualization rather than to the total number of monitored objects that may exist in the environment. When configuring a view or selecting resources for a flow chart, administrators should therefore scope the chart to the most relevant nodes, interfaces, applications, or other resources so that the visualization remains within the supported display limit. Keeping the chart at or below 50 resources helps ensure that the view is rendered predictably and remains useful for quickly understanding resource relationships and status. This is particularly important in large deployments, where a narrowly focused chart provides a more usable operational view than attempting to include every related object. SolarWinds documents Platform view configuration and visualization behavior in its Orion Platform documentation; consult the SolarWinds Platform documentation for customizing views and the SolarWinds Documentation portal for the version-specific guidance applicable to the deployed platform release.

QUESTION NO: 7

Which tool can be used to display the physical layout of interfaces on graphical stencils?

A. device studio

B. device view

C. NetPath

D. network insight

ANSWER: B

Explanation:

Device View is the SolarWinds Network Performance Monitor feature designed to present a supported network device as a graphical hardware stencil. Rather than showing interfaces only as rows in a table, it maps them to their physical positions on the device faceplate, such as switch ports or chassis components. This gives administrators a quick visual way to correlate monitored interfaces with their real-world locations and assess their status directly from the device representation. Device View relies on device-specific stencils and the information SolarWinds discovers for the node, so the available layout and level of detail depend on whether the monitored hardware is supported. In the Orion Platform web console, the feature is accessed from a device's details page, where the graphical view complements conventional interface monitoring data. SolarWinds documents that Device View displays the physical layout of device interfaces using graphical stencils for supported devices. See the SolarWinds Device View documentation and the NPM views documentation for implementation and navigation details.

QUESTION NO: 8

NetPath can be used to diagnose a slow connection caused by an internal network. Details shown on the dashboard will be needed to help diagnose the problem. Which three of the following data points should be considered as possible causes? (Choose three.)

A. Date, time, and duration of performance issue.

B. Detailed alert description shown on NetPath.

C. IP addresses of the nodes in question.

D. Latency and packet loss information.

ANSWER: A C D

Explanation:

Date, time, and duration of performance issue, IP addresses of the nodes in question, and latency and packet loss information are the relevant information to collect when investigating an internally caused slow connection with NetPath. Establishing the time window and duration lets an administrator use NetPath's historical views to compare the affected period with normal behavior and correlate the degradation with a known network event or change. Identifying the affected nodes by IP address establishes the source or destination context and helps the administrator determine which monitored endpoint and path require analysis. NetPath presents the service-delivery path as a sequence of hops, allowing the investigation to focus on the portion of the internal route associated with the affected node. Latency and packet-loss measurements provide the actual performance evidence needed to identify where responsiveness declines or traffic is being dropped. Together, the timing context, endpoint identity, and hop-level performance data support isolating the internal segment contributing to the slow connection. SolarWinds describes NetPath as a tool for visualizing service-delivery paths and identifying performance issues along those paths; see the SolarWinds NetPath documentation and the service delivery paths documentation.

QUESTION NO: 9

Which three of the following actions are native log entry actions in SolarWinds Log Analyzer? (Choose three.)

A. Add a tag to the log entry

B. Continue rule processing but do not save

C. Halt further rule processing for the log entry

D. Send an email notification

ANSWER: A B C

Explanation:

SolarWinds Log Analyzer log-processing rules evaluate incoming log entries against configured conditions and can then apply built-in actions to the entry. **Add a tag to the log entry** is a native action that enriches matching entries with a tag, making those logs easier to identify, filter, and search in Log Analyzer. **Continue rule processing but do not save** is also a native processing action: it prevents the matching entry from being retained while allowing it to proceed through subsequent applicable log-processing rules. This supports selective handling where later rules may still apply additional processing. **Halt further rule processing for the log entry** is the native control-flow action used when a matching entry should not be evaluated by any additional rules. Together, these actions provide tagging, storage control, and rule-processing control directly within Log Analyzer's custom log-processing-rule workflow. SolarWinds documents log-processing rules and their available actions in its Log Analyzer documentation; see the SolarWinds Log Analyzer documentation and the Log Analyzer product and use-case overview.

QUESTION NO: 10

If an SNMP community string is changed on a device, which two of the following steps are required to re-establish successful polling on the node? (Choose two.)

A. Delete and add the node back into the platform.

B. Edit the node properties and save the changes.

C. Restart the SNMP service on the source device.

D. Update the community string in node properties.

ANSWER: B D

Explanation:

"Update the community string in node properties." is required because SolarWinds uses the credentials stored for that managed node when it sends SNMP polling requests. After the device-side community value changes, the value in the node's SNMP settings must match it exactly. Updating the stored community string restores the authentication information that SolarWinds presents to the device for SNMP v1 or v2c requests.

"Edit the node properties and save the changes." is also required because the updated credential must be committed to the node configuration. In the SolarWinds Platform web console, editing the node exposes the polling and SNMP credential settings; saving applies the new value to the monitored object so subsequent polling jobs use it. Once the device configuration and saved node properties agree, the existing node can resume normal SNMP status, availability, interface, and performance polling without changing the node's identity or historical data.

SolarWinds documents node management and editing through the web console in its Editing Nodes documentation. For broader guidance on node polling configuration and credentials, see the Add Nodes documentation.

QUESTION NO: 11

Which Cisco IOS feature is enabled to pinpoint an application causing slow network performance?

A. IPSLA

B. NetFlow

C. SNMP

D. SPAN

ANSWER: B

Explanation:

NetFlow is the correct Cisco IOS feature because it collects traffic-flow records that identify the conversations traversing a network device. Flow data includes key fields such as source and destination IP addresses, source and destination ports, IP protocol, interfaces, timestamps, and byte or packet counts. Network monitoring platforms can use these fields to associate traffic with an application or service and determine which application is consuming significant bandwidth or contributing to poor performance. For example, unusually high-volume traffic on application-specific ports can be identified and ranked, allowing an administrator to investigate the responsible hosts and traffic pattern. In SolarWinds Hybrid Cloud Observability, NetFlow Traffic Analyzer receives NetFlow and related flow telemetry and presents application, endpoint, protocol, and bandwidth-utilization views to support this type of troubleshooting. Cisco documents NetFlow as a mechanism for collecting IP flow information from network devices, while SolarWinds documents its use for identifying bandwidth consumers and analyzing application traffic. See Cisco NetFlow documentation and SolarWinds NetFlow Traffic Analyzer use cases.

QUESTION NO: 12

Which three of the following devices are supported on SolarWindsâ€™ hybrid cloud observability IP flow monitor? (Choose three.)

A. IPF1X

B. J-Flow

C. nFlow

D. sFlow

E. J-Flow, NetFlow, and sFlow

ANSWER: E

Explanation:

J-Flow, NetFlow, and sFlow are the three supported flow technologies identified by the question. SolarWinds Hybrid Cloud Observability Advanced, through its Network Traffic Analysis capabilities, collects and analyzes exported flow records to show who and what is consuming network bandwidth. NetFlow is Cisco’s flow-export technology and is also implemented in compatible forms by many other network platforms. J-Flow is Juniper Networks’ flow-export format. sFlow is a sampling-based flow technology supported by a broad range of network-device vendors. Each technology exports traffic metadata—such as source and destination addresses, ports, protocols, interfaces, and traffic volumes—to the SolarWinds collector for analysis, reporting, and alerting. Selecting the combined set is necessary because the prompt asks for three supported technologies, while a single-choice item must have one complete answer. SolarWinds documentation describes support for NetFlow, J-Flow, sFlow, and IPFIX as traffic-flow sources. See the SolarWinds Network Traffic Analyzer supported flow technologies documentation and the SolarWinds Hybrid Cloud Observability network traffic monitoring overview.

QUESTION NO: 13

The unclassified traffic in the web console has been identified as MSSQL traffic. It is known as an application mapping that hybrid cloud observability maps by default. Which two of the following reasons explain why the traffic is showing as unclassified? (Choose two.)

A. A different port is being used.

B. A firewall is blocking the traffic.

C. The source or the destination port field is not present.

D. The version of MSSQL being used is not supported.

ANSWER: A C

Explanation:

“A different port is being used.” is correct because Hybrid Cloud Observability Network Monitoring classifies flow traffic through application mappings that associate applications with their known TCP or UDP ports. Microsoft SQL Server is included in the default mappings, but its conventional listener port is TCP 1433. If a SQL Server instance listens on a different port, the flow remains unclassified unless the administrator creates or modifies an application mapping that includes the port actually reported in the flow records. This lets the product group the traffic under the intended application rather than leaving it in the unclassified category.

“The source or the destination port field is not present.” is also correct because port-based mapping requires usable source and destination port values in the received flow data. NetFlow, IPFIX, sFlow, and similar exported flow records provide the fields used to match traffic to an application mapping. When a required port value is absent, the platform cannot evaluate the flow against the MSSQL port mapping, even where the traffic is known to be SQL Server traffic. SolarWinds documents application mapping and the ability to use application and service port definitions for flow-traffic classification in its application mapping documentation and application and service ports documentation.

QUESTION NO: 14

Which status rollup mode displays groups defined as collections of redundant or backup devices?

A. show best

B. show mixed

C. show worst

D. show zero

ANSWER: A

Explanation:

The correct status rollup mode is **show best**. In SolarWinds Network Performance Monitor group status calculations, this rollup mode uses the best status among the group members. This behavior is designed for a group representing redundant, failover, or backup infrastructure: if at least one device is operating normally, the group can reflect the available service path rather than the status of a failed standby or peer device. For example, where two routers provide redundant connectivity, an issue with one router does not necessarily mean the service represented by the group is unavailable while the other router remains healthy. Selecting **show best** therefore aligns the group’s displayed status with the availability model of redundant components and avoids treating an individual backup-device failure as an overall service failure. SolarWinds documents group status rollup modes and identifies “Show Best” as the appropriate selection for groups that contain redundant devices. See the SolarWinds Network Performance Monitor groups documentation and the SolarWinds status rollup documentation.

QUESTION NO: 15

Which statement related to flow alerts is true?

A. based on custom SQL query

B. can be triggered even when NetFlow service is down

C. have no trigger actions

D. object of the alert selected from create a flow alert panel

ANSWER: D

Explanation:

The statement *object of the alert selected from create a flow alert panel* is true. SolarWinds NetFlow Traffic Analyzer (NTA) supports creating a flow alert directly from flow-focused views, allowing the administrator to begin with the traffic entity that requires monitoring. The Create a Flow Alert workflow carries the selected flow context into the alert definition, such as the

relevant endpoint, application, conversation, interface, or other flow-related object represented by the view. This approach makes alert configuration more targeted: rather than starting with a broad, generic alert condition, the administrator selects the traffic object of interest and then configures the alert's threshold, evaluation conditions, reset behavior, schedule, and notification or remediation actions. Flow alerts are therefore useful for operational cases such as identifying unusually high bandwidth use by a particular application or traffic endpoint. The alert is managed through the SolarWinds Platform alerting framework after creation, while NTA supplies the flow and traffic data used by the alert condition. SolarWinds documents the NTA alerting workflow and flow-based monitoring capabilities in its NetFlow Traffic Analyzer alerts documentation and provides related configuration guidance in the NTA Getting Started Guide.

QUESTION NO: 16

Which two of the following tools are available for troubleshooting network node connectivity issues? (Choose two.)

A. asset inventory

B. MIB browser

C. NetPath

D. network insight

ANSWER: C D

Explanation:

NetPath is designed specifically for investigating connectivity and service-delivery problems. It visualizes the path from a SolarWinds polling location to a monitored service, showing hops, latency, packet loss, and the health of infrastructure along the route. This lets an administrator isolate whether a connectivity issue is occurring in the local network, at a provider boundary, or farther along the delivery path. NetPath also provides historical path and performance context, which is useful when a reported issue is intermittent rather than continuously present.

network insight is also appropriate because SolarWinds Network Insight features provide vendor- and technology-aware visibility for supported network infrastructure. These views expose operational status, relevant configuration and health information, topology or dependency context, and detailed metrics for technologies such as Cisco ASA, F5, and others. That focused visibility helps administrators investigate node and service connectivity symptoms in the context of the devices that process or control the traffic. SolarWinds describes NetPath capabilities at SolarWinds NetPath and documents Network Insight functionality at SolarWinds Network Insight documentation.

QUESTION NO: 17

A â€œno dataâ€ message is displayed in NetFlow charts. How can this be resolved?

A. Confirm account has viewing permissions.

B. Refresh the current window.

C. Restart collector service.

D. Shorten the time for view and resource.

ANSWER: C

Explanation:

Restart collector service. is the appropriate resolution because NetFlow Traffic Analyzer depends on its collector service to receive, decode, process, and store flow records exported by monitored devices. When the collector is stopped, stalled, or otherwise unable to process incoming records, charts can show a “no data” condition even though the network devices may still be exporting flows. Restarting the service restores the flow-processing component and commonly clears temporary service or processing-state issues, allowing newly received flow information to populate the charts again.

After restarting the collector, allow sufficient time for devices to export new records and for the collector to process them before checking the chart. The relevant service is normally managed from the SolarWinds Platform service-management tools, and its operational status should be confirmed as running. SolarWinds' NetFlow Traffic Analyzer documentation describes the collector's role in receiving and processing flow data, while the product troubleshooting resources provide guidance for investigating missing NetFlow information. See the SolarWinds NetFlow Traffic Analyzer Administrator Guide and SolarWinds NetFlow Traffic Analyzer support resources.

QUESTION NO: 18

Which three of the following data points directly affect the precision of capacity forecasting? (Choose three.)

A. amount of historical data used

B. exhaustion calculation method

C. polling interval

D. warning thresholds

ANSWER: A B C

Explanation:

Capacity forecasting is derived from collected performance history and from the settings used to model that history. The **amount of historical data used** directly affects forecast precision because a longer, representative history gives the forecasting engine more observations from which to identify utilization patterns, trends, and sustained growth. The **exhaustion calculation method** is also a direct input: selecting a calculation approach determines how SolarWinds projects future consumption and estimates the time at which available capacity may be depleted. Finally, the **polling interval** affects the granularity of the source measurements. More frequent polling supplies a denser time series and can better capture meaningful changes in resource utilization, supporting a more precise trend calculation. Together, these settings govern the quality and treatment of the utilization data on which a capacity forecast is based. SolarWinds capacity-planning features use historical monitored statistics to calculate trends and projected exhaustion dates; administrators should therefore ensure that monitored objects have sufficient, consistently collected historical data before relying on forecasts. See the SolarWinds Platform Capacity Planning documentation and the SolarWinds Platform historical data documentation.