DUMPSARENA

SolarWinds Certified Professional

SolarWinds SCP-500

Version Demo

Total Demo Questions: 16

Total Premium Questions: 165

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Company A and company B have merged and are currently planning to combine their network backbones. All 18 of company A's routers run OSPF, but company B's hardware only supports RIPv2. You need to monitor both networks from a single NMS. Which solution in volves the fewest configuration steps to meet these monitoring requirements?

A. move to static routing for all routers

B. change the routing protocol on company A's routers to RIP

C. use router redistribution

D. configure company A's routers to run RIP along with OSPF

ANSWER: C

Explanation:

use router redistribution is the appropriate solution because it permits routes learned through OSPF to be advertised into RIPv2 and routes learned through RIPv2 to be advertised into OSPF at the boundary between the two networks. This preserves each company's existing routing design while establishing the Layer 3 reachability needed for a centrally located network management system to communicate with and monitor devices in both routing domains. Rather than modifying every router, redistribution is normally configured only on the router or routers that connect the OSPF and RIP portions of the merged backbone. That makes it the lowest-impact approach when the existing hardware and protocol constraints must remain in place. Careful route filtering, route tags, and metric assignment should be used during implementation so that redistributed routes are controlled and do not create routing feedback loops. SolarWinds Network Performance Monitor collects device and interface status using management protocols such as SNMP once the NMS has IP connectivity to the monitored nodes; maintaining reachability across the combined network is therefore essential. Cisco's routing documentation describes redistribution as the exchange of routing information between different routing protocols: Cisco: Redistributing Routing Protocols. For SolarWinds monitoring requirements and polling fundamentals, see SolarWinds Platform SNMP credentials documentation.

QUESTION NO: 2

A network device is added to SolarWinds using SNMPv3 with authentication and privacy enabled. The device responds to ICMP, but SNMP polling fails. Which configuration mismatch is most likely to cause this issue?

A. the SNMPv3 privacy password or privacy protocol does not match the device configuration

B. the device does not have a default gateway

C. the node has an incorrect ICMP polling interval

D. the SolarWinds web console uses HTTPS

ANSWER: A

Explanation:

the SNMPv3 privacy password or privacy protocol does not match the device configuration is correct because SNMPv3 authentication and privacy settings must match exactly between the SolarWinds credential and the device SNMP agent. When privacy is enabled, the selected privacy protocol and password are used to encrypt and decrypt the SNMP message payload. A mismatch prevents the device from accepting the polling request or the polling engine from processing a valid response.

ICMP reachability establishes only that an IP path exists. It does not validate the SNMPv3 user name, authentication method, authentication password, privacy method, or privacy password. SolarWinds documents the required SNMPv3 credential settings in its SNMPv3 credentials documentation.

QUESTION NO: 3

You are monitoring your Internet connection, and your ISP has guaranteed512 Kbps.

Historical data shows that your connection speed holds at 256 Kbps for long periods of time, but never exceeds this speed. What does this indicate?

A. the ISP has misconfigured the link.

B. the WAN router is misconfigured.

C. the NAT table is overloaded.

D. QoS is dropping low priority traffic.

ANSWER: A

Explanation:

the ISP has misconfigured the link. is correct because a sustained, repeatable ceiling at exactly 256 Kbps, despite a contracted or guaranteed 512-Kbps service, strongly indicates that an upstream rate limit has been applied at the wrong value. This is characteristic of an ISP-side provisioning, traffic-shaping, or policing configuration that has set the circuit profile to 256 Kbps rather than the purchased 512 Kbps. Historical monitoring is important here: a temporary reduction could result from congestion, but a long-term maximum that never rises above a fixed threshold points to a configured cap rather than ordinary fluctuations in available bandwidth.

SolarWinds performance monitoring uses historical interface and bandwidth-utilization data to establish expected behavior and identify persistent capacity or configuration issues. In this scenario, the monitored throughput provides evidence to open a service case with the provider and request verification of the circuit's provisioning and applied bandwidth policy. SolarWinds documents the use of historical performance data and baselines for identifying abnormal network behavior in its Network Performance Monitor baseline documentation. For the general distinction between an ISP's committed service level and a configured traffic policer, see the Cisco documentation on policing and shaping.

QUESTION NO: 4

Which two conditions can cause a SolarWinds node to show an Unknown status? (Choose two.)

A. the polling engine cannot determine the node status

B. the node is unmanaged

C. the node has exceeded its CPU threshold

D. the node has received an SNMP trap

E. the node has an assigned custom property

ANSWER: A B

Explanation:

The polling engine cannot determine the node status and **the node is unmanaged** are correct. Unknown indicates that the platform does not currently have a usable status determination for the monitored object. This can occur when the polling engine cannot obtain the required response because of a communication, credential, or polling problem.

An unmanaged object is also not actively polled during its unmanaged period. As a result, it does not receive a current monitored status until monitoring resumes and the polling engine successfully evaluates it. Administrators should review the node status, polling method, event history, and any active unmanaged schedules when investigating an Unknown node. See the SolarWinds Platform node status documentation and unmanage objects documentation.

QUESTION NO: 5

Which two actions can help prevent alert storms when a core router failure causes many dependent network objects to become unreachable? (Choose two.)

A. create dependency relationships between the core router and affected objects

B. configure alerts to suppress actions when the related node is unmanaged

C. increase all interface polling intervals to 60 minutes

D. disable status monitoring for all downstream nodes

E. configure each downstream node as a parent of the core router

ANSWER: A B

Explanation:

create dependency relationships between the core router and affected objects is correct because dependencies identify the upstream object whose failure explains the status of other monitored objects. When the parent router is unavailable, SolarWinds can suppress the dependent status conditions and associated alerts for the downstream objects.

configure alerts to suppress actions when the related node is unmanaged is also correct. During planned maintenance, placing an object into an unmanaged state prevents expected maintenance-related conditions from producing notifications. Dependencies address operational root-cause failures, while unmanaged scheduling addresses expected administrative work. SolarWinds describes these controls in its dependencies documentation and manage and unmanage nodes documentation.

QUESTION NO: 6

You want to create an Orion NPM Advanced Alert that will send an email when a node goes down. You need to know:

when the node went down the node vendor

the type of device

the last known statistics for the device

How should you ensure that the alert email contains this information?

A. include a URL pointing to the appropriate Orion Node Details view

B. use Orion alert variables to embed the information

C. embed resources from the Orion Node Details view

D. use Orion SQL queries to include the relevant information

ANSWER: B

Explanation:

Use Orion alert variables to embed the information. SolarWinds alert actions, including email actions, support variables that are resolved when the alert is triggered. This lets the message dynamically include alert-specific details such as the time the alert was triggered, the affected node's vendor and machine type, and applicable node or interface status and statistic values. For a node-down alert, variables in the alert context provide the relevant object and alert properties without requiring a recipient to open a separate web page or requiring a custom query simply to populate standard notification details.

Variables can be inserted into the email subject and body through the alert action editor. SolarWinds provides the variable picker so administrators can select supported alert, node, and related-object properties, rather than having to memorize variable syntax. The available values depend on the alert's trigger object and configured alert scope, so the alert should be tested after configuring its message. This approach produces an actionable notification containing the requested information at the time the email is sent. See SolarWinds' Alert variables documentation and email alert action documentation.

QUESTION NO: 7

What are two possible cause sofa Universal Device Poller (UnDP) OID test failure in Orion NPM? (Choose two.)

A. The OID is not in the Orion MIB database.

B. The device is not reachable.

C. The OID is stored in a table.

D. SNMPv3 is required.

E. The OID is unsupported.

ANSWER: B E

Explanation:

“The device is not reachable.” is a valid cause because the Universal Device Poller test must be able to contact the target node through the configured management address and SNMP settings. If the node cannot be reached because of a network-path issue, an unavailable device, blocked SNMP traffic, or an address/credential configuration problem, Orion cannot send the SNMP request and receive a response for the OID test.

“The OID is unsupported.” is also correct because an OID must be implemented by the target device’s SNMP agent and available in the applicable device context. A numeric OID can be syntactically valid yet still return no usable value when that particular model, operating-system version, feature set, or agent does not expose it. The UnDP test is intended to verify that the selected device can successfully return a value for the requested OID before a custom poller is created and assigned. SolarWinds describes UnDP as a mechanism for polling custom SNMP OIDs on monitored devices, so both successful device communication and support for the requested OID are necessary prerequisites. See the SolarWinds Universal Device Poller documentation and the SolarWinds SNMP credentials documentation.

QUESTION NO: 8

A network engineer has created a custom report in Orion NPM with the following parameters:

1. Fields are set to "Node ID, Node Name, Average Response Time."

2. Timeframe is set to "Last30 days."

3. Summarization is set to "Month."

What is an accurate representation of what this report will display?

A. average response time for the last month on all devices and interfaces

B. average response time for the last month on all devices

C. average response time per day of the last month on all devices and interfaces

D. average response time per day of the last month on all devices

ANSWER: B

Explanation:

average response time for the last month on all devices is the accurate representation. The selected fields are node-level fields: Node ID and Node Name identify monitored nodes, while Average Response Time is a node availability/performance statistic collected for those nodes. Consequently, the report scope is devices (nodes), not interfaces. The Last 30 days timeframe limits the source data to the preceding 30-day reporting period. Selecting Month as the summarization interval aggregates the response-time data at the monthly level instead of producing a separate daily value. In practical terms, the result presents each included node and its average response-time value for the selected monthly reporting period. SolarWinds reporting uses the report’s selected objects, fields, time period, and grouping/summarization settings to determine the displayed result. Node response time is a standard NPM node statistic, and reports can use

historical data across a selected time range. See the SolarWinds Platform reports documentation and the NPM ICMP monitoring documentation for details on reporting and node response-time monitoring.

QUESTION NO: 9

A firewall separates Orion NPM and the network devices it is monitoring. Only encrypted communication will be allowed from the server for polling and configuration management. Which two ports will need to be allowed through the firewall? (Choose two.)

A. 22

B. 23

C. 69

D. 80

E. 161

F. 2055

ANSWER: A E

Explanation:

22 and **161** are required when the environment permits only encrypted polling and configuration-management traffic. Orion Network Performance Monitor uses Secure Shell on TCP port 22 for secure command-line access to managed devices. This provides encrypted remote access for activities that require device CLI communication, including configuration-related operations when SolarWinds Network Configuration Manager capabilities are involved.

For monitoring, Orion polls devices with SNMP. UDP port 161 is the standard destination port for SNMP queries. To meet the encryption requirement, the monitored devices must be configured for SNMPv3 with privacy enabled, rather than community-string-based SNMP versions. SNMPv3 supports authentication and encryption of management messages while continuing to use UDP 161 for polling requests. Therefore, firewall rules should allow the Orion polling engine to initiate TCP 22 and UDP 161 traffic to the managed network devices, with return traffic permitted according to the firewall's stateful-policy design.

SolarWinds documents the polling-engine-to-node SNMP port requirement in its Orion Platform network ports reference. The IETF's SNMPv3 User-based Security Model specification describes the authentication and privacy mechanisms that enable protected SNMP management communication.

QUESTION NO: 10

When using a network management system (NMS) to monitor network interfaces on a router, you notice that statistics are wrong after an interface card is physically removed from the device. What has most likely caused this problem?

A. interface re-indexing

B. device configuration

C. counter rollovers

D. access lists

ANSWER: A

Explanation:

interface re-indexing is the most likely cause. Network management systems commonly poll router interfaces through SNMP and associate collected statistics with entries in the device's interface table. Each interface is represented by an `ifIndex` value. When hardware such as an interface card is removed, the device may rebuild or renumber its interface

table, causing the remaining interfaces to receive different index values. If the NMS continues to associate its existing monitored objects with the prior indexes, it can display traffic, error, or utilization statistics from a different physical or logical interface than the one named in the monitoring view.

This behavior is especially relevant after hardware inventory changes, reboots, or configuration events that alter the interface set. To preserve reliable historical monitoring, administrators should use stable interface identification where the platform and NMS support it, validate interface mappings after hardware changes, and rediscover or remap interfaces as needed. The standard SNMP interface table and its index are defined in RFC 2863, The Interfaces Group MIB. SolarWinds also documents how its platform uses interface indexing and supports methods for managing interface index changes in its interface indexing documentation.

QUESTION NO: 11

When planning the deployment of the database server for Orion NPM, what are two primary considerations? (Choose two.)

A. database clustering

B. RAID configurations

C. CPU and memory size

D. type of NIC card used

E. type of RAM

ANSWER: B C

Explanation:

RAID configurations and **CPU and memory size** are primary database-server planning considerations for an Orion Network Performance Monitor deployment. The Orion SQL database handles continuous writes from polling, event, and historical data collection, along with read-intensive reporting and web-console queries. Storage therefore needs both adequate capacity and reliable, high-performance input/output behavior. A suitable RAID design helps provide the disk throughput and resiliency needed for the SQL data and transaction-log workloads, especially as the number of monitored elements, polling frequency, retention period, and report usage increase.

CPU and memory must also be sized for the anticipated database load. SQL Server uses processor resources to execute queries, aggregate and maintain monitored-data records, and support concurrent Orion services and user requests. Sufficient memory allows SQL Server to cache frequently used data pages and reduce unnecessary disk access, which directly supports responsive polling, views, alerts, and reports. SolarWinds publishes deployment requirements and scaling guidance so that the SQL Server resources can be matched to the Orion environment's monitored-object count and workload. Review the SolarWinds Orion Platform server software requirements and the SolarWinds SQL Server requirements when designing the deployment.

QUESTION NO: 12

Which two actions are required to integrate Engineer's Toolset with the Orion Web Console? (Choose two.)

A. install Toolset on the user's machine

B. install Orion Web Console on the user's machine

C. enable Allow Administrator Rights on the user's account

D. enable Allow Browser Integration on the user's account

E. enable Advanced Customization on the user's account

ANSWER: A D

Explanation:

Integration requires installation of Engineer's Toolset on the user's machine because the integrated tools are desktop applications that run locally, rather than applications hosted by the Orion Web Console. When a permitted user selects an Engineer's Toolset action from the web console, browser integration hands the relevant monitored-node information to the locally installed Toolset application, allowing that application to open with the appropriate target context. SolarWinds describes Engineer's Toolset as a collection of desktop network-management tools, so each user who needs to launch those tools through the console needs a local installation. See the SolarWinds Engineer's Toolset product page.

The user account must also have Allow Browser Integration enabled. This account-level authorization permits the Orion Web Console to expose and initiate the browser-integration workflow for that user. It is therefore the required web-console permission that connects the user's authenticated Orion session to the locally installed Toolset. The integration depends on both pieces being present: a local Toolset installation capable of launching the tools and browser-integration permission for the user who is launching them. SolarWinds Orion administrative documentation is available through the Orion Platform Administrator Guide.

QUESTION NO: 13

A network engineer wants an alert to notify the on-call team only after a router has remained down for 10 minutes. Which alert setting should be configured?

A. trigger condition must exist for more than 10 minutes

B. alert evaluation frequency must be 10 minutes

C. reset condition must exist for more than 10 minutes

D. alert suppression interval must be 10 minutes

ANSWER: A

Explanation:

trigger condition must exist for more than 10 minutes is correct because it prevents the alert from triggering immediately when the router first enters a Down state. The SolarWinds Platform continuously evaluates the trigger condition, and the condition must remain true for the configured period before the alert is activated. This helps avoid notifications caused by brief connectivity interruptions or transient device reboots.

The polling interval must also be appropriate for the required detection time. For example, a status polling interval longer than 10 minutes would not reliably support this requirement. SolarWinds documents alert trigger conditions and timing behavior in its alert trigger conditions documentation.

QUESTION NO: 14

The NOC team wants to add a simple map within Orion NPM that shows the United States and the edge router status for each of the company sites.

Which two operations are required to set up this map? (Choose two.)

A. modify back ground image

B. drag and drop hyperlinks onto map

C. drag and drop status icons onto map

D. associate network interfaces with map lines

E. drag and drop interfaces onto map

ANSWER: A C

Explanation:

To create this type of Orion NPM map, the map needs a geographic visual foundation and map objects that dynamically represent the monitored routers. “modify back ground image” supplies that foundation: the administrator can use a United States image as the map background, then position site-related objects over the appropriate locations. A background image is particularly useful when the map is intended to communicate geographic context quickly to NOC personnel rather than merely show a logical topology.

“drag and drop status icons onto map” is also required because status icons are the map objects that can be associated with monitored Orion entities, such as each site’s edge router. Their displayed state changes with the monitored object’s status, allowing the map to provide the requested at-a-glance operational view. After placing and associating those icons with the relevant router nodes, the NOC can see router health directly on the United States map.

SolarWinds describes creating and editing maps, including adding objects and configuring map presentation, in its Orion Maps documentation. For the legacy Network Atlas-based map workflow used by earlier Orion NPM versions, see the Network Atlas documentation.

QUESTION NO: 15

A network engineer is enabling SNMP on their network devices and needs to ensure it will use message integrity. Which version of SNMP should they use?

A. SNMPv1

B. SNMPv2c

C. SNMPv3

D. SNMPv4

ANSWER: C

Explanation:

SNMPv3 is the appropriate version because it adds the User-based Security Model (USM), which supports authentication and message-integrity protection. With SNMPv3 authentication enabled, messages include authentication parameters calculated with a supported hashing algorithm, such as HMAC-SHA, allowing the receiving device to verify that the message came from an authorized user and was not altered while in transit. SNMPv3 also supports optional privacy (encryption), but encryption is separate from the requirement for message integrity; an authentication-enabled SNMPv3 security level provides integrity protection even when privacy is not configured.

For SolarWinds monitoring, configure the SNMPv3 credentials assigned to a node with an authentication method and password that match the device configuration. SolarWinds documentation describes SNMPv3 as supporting authentication and privacy settings when polling monitored devices. The underlying SNMPv3 USM specification defines authentication as protection against message modification and unauthorized message generation. See SolarWinds SNMPv3 credential documentation and RFC 3414: User-based Security Model for SNMPv3.

QUESTION NO: 16

Which two performance metrics can be affected by proper QoS implementation? (Choose two.)

A. jitter

B. shaping

C. marking

D. queuing

E. latency

ANSWER: A E

Explanation:

Proper Quality of Service implementation can directly improve both **jitter** and **latency**, particularly for delay-sensitive traffic such as voice and video. Latency is the time required for traffic to travel from its source to its destination. QoS policies can reduce latency by classifying important traffic, placing it into an appropriate priority queue, and helping that traffic receive timely forwarding during periods of network congestion. Lower and more predictable latency supports responsive real-time communication and application performance.

Jitter is the variation in packet-delay timing. Even when average latency is acceptable, inconsistent arrival times can cause voice or video playback to sound distorted, break up, or require buffering. QoS supports lower jitter by giving real-time traffic consistent scheduling treatment and reducing the likelihood that packets experience widely varying queue delays. SolarWinds network-performance monitoring tools can measure and visualize latency and jitter for monitored paths, helping administrators validate whether QoS policies are achieving the intended service quality. See SolarWinds' QoS monitoring documentation and the Network QoS monitoring overview.