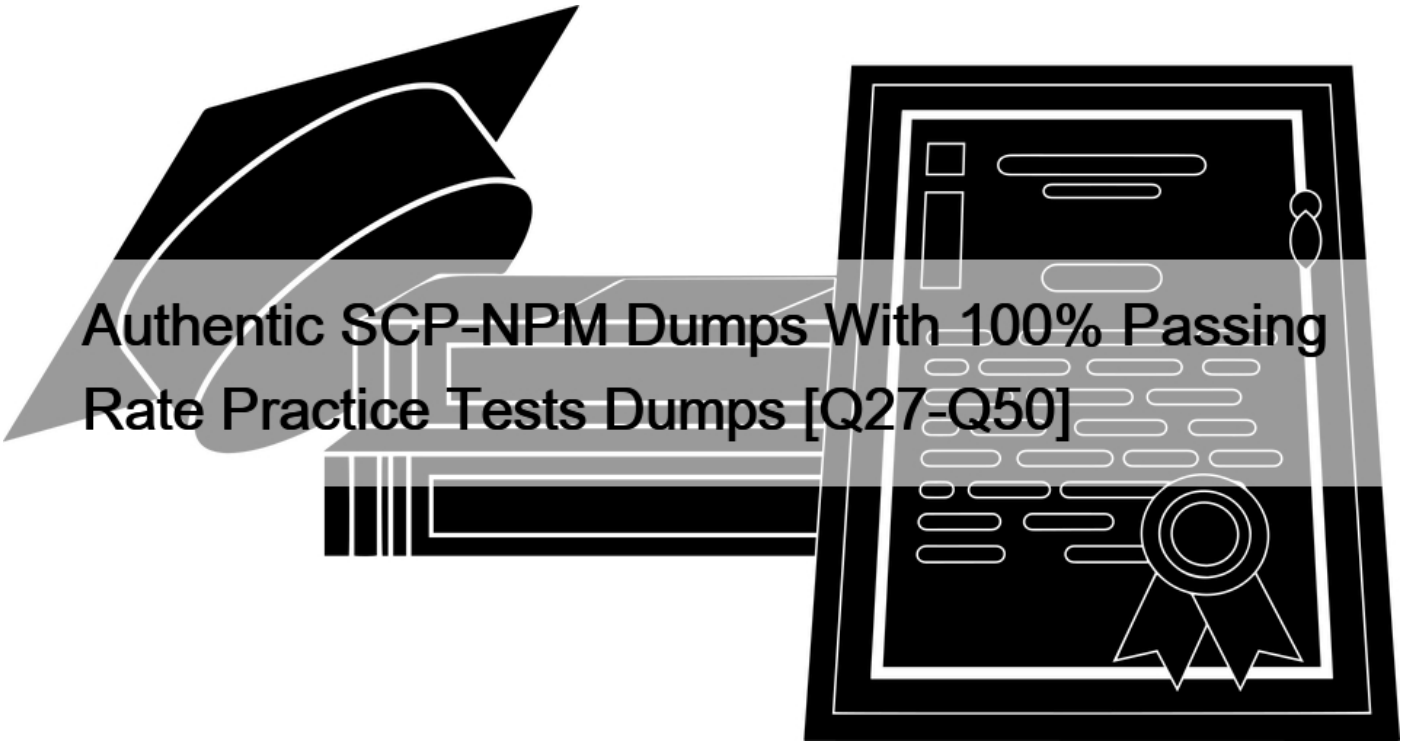
Authentic SCP-NPM Dumps With 100% Passing Rate Practice Tests Dumps [Q27-Q50



Authentic SCP-NPM Dumps With 100% Passing Rate Practice Tests Dumps
SolarWinds SCP-NPM Real Exam Questions Guaranteed Updated Dump from DumpsMaterials

The SCP-NPM certification exam is an essential credential for network professionals who use SolarWinds Network Performance Monitor. It validates the practical skills and knowledge of network administrators in using the software to monitor, troubleshoot, and optimize network performance. SolarWinds Network Performance Monitor (NPM) Exam certification is widely recognized in the industry and can help professionals advance their careers by demonstrating their proficiency in using the SolarWinds NPM software.

Q27. You can import device-specific MIBs into the SolarWinds MIB Database, but you cannot import UnDP pollers based on OIDs from device-specific MIBs.
* True
* False

Q28. You add several nodes for monitoring and can see detailed information on those nodes in the Orion Web Console. However, when you look at the nodes in Orion Maps, the connections between the nodes are not showing. What is a likely reason?
* A firewall is blocking polling between the nodes and the Orion server
* You did not enable Layer 2 and Layer 3 topology polling on those nodes
* You did not add the node topology OIDs to the MIB database
* You did not enable SNMP polling

Orion Maps show you how entities are connected based on the data collected by the Orion Platform products.

To display the connections between the nodes in Orion Maps, you need to enable Layer 2 and Layer 3 topology polling on those nodes. This will allow the Orion Platform to discover the network topology using protocols such as CDP, LLDP, or ARP. You can enable topology polling on individual nodes or in bulk using the Manage Nodes feature in the web console. You can also customize the topology polling settings and frequency on the Orion Polling Settings page. References: Intelligent Maps for SolarWinds Platform products; Understand connections on Intelligent Maps in the SolarWinds Platform; Network Mapping Tool – Automated Network Mapping | SolarWinds

Q29. How can you quickly generate a report in NPM to show the top 50 interfaces by percent utilization?
* Create a web-based report and filter the data to restrict to the top 50 interfaces
* Copy a similar default report and edit it for different time-frames
* Copy a similar default report and edit it for the top 50 interfaces
* Create an advanced SQL query report

NPM provides several default reports that can be used as templates for creating custom reports. One of them is the Top 100 Interfaces by Percent Utilization report, which shows the average and peak utilization of the most used interfaces in the network. To create a report that shows only the top 50 interfaces, you can copy this report and edit it to change the number of rows displayed. You can also modify other parameters such as the time period, the grouping, the sorting, and the filtering criteria. To copy and edit a default report, follow these steps1:

Click Reports > All Reports > Manage Reports.

Find the Top 100 Interfaces by Percent Utilization report and click Duplicate & Edit.

On the Layout Builder panel, click Edit Table.

On the Edit Resource panel, change the Maximum Number of Rows to 50.

Optionally, change other settings such as the Time Period, the Group By, the Sort By, and the Filter Results.

Click Submit.

Optionally, change the Report Name, the Report Description, and the Report Category.

Click Next and then Save.

You can now run or schedule the report to show the top 50 interfaces by percent utilization. References: 1:

Create a custom report for NPM showing availability of devices in the last 30 days

Q30. Your network has critical devices on the opposite side of a WAN link from you SolarWinds server. You do not want alerts about the devices if the router (name = “target”) that connects your SolarWinds server to the remote site is down. How do you configure Alert Suppression?
* Suppress alert when all of the following apply: Node Name is equal to “target” / Interface Status is equal to “Warning”
* Suppress alert when any of the following apply: Node Name is equal to “target” / Node Status is equal to “Warning”
* Suppress alert when any of the following apply: Node Name is equal to “target” / Interface Status is equal to “Down”
* Suppress alert when all of the following apply: Node Name is equal to “target” / Node Status is equal ta “Down”

Q31. You can display Palo Alto firewalls on Orion Maps.
* False
* True
Orion Maps 2.0 supports displaying Palo Alto firewalls as network devices, along with their interfaces, zones, policies, and traffic data. You can also view the firewall status, alerts, and events on the map. To add a Palo Alto firewall to an Orion Map, you need to have Network Insight for Palo Alto enabled in NPM, and discover the firewall using SNMP and API polling. References: Orion Maps 2.0, New Alerting, and Palo Alto Networks Monitoring – SolarWinds Lab Episode #77, SolarWinds Lab Episode 77: Orion Maps 2.0, New Alerting, and Palo Alto Networks Monitoring – Orange Matter, Network Insight for Palo Alto Networks in NPM

Q32. How do you assign users access to select reports?
* Create the reports while logged in as each user and set permissions
* Use custom properties and account limitations to control report access
* Configure the report and add a Report Limitation. Assign the limitation to users who need access to the report
* Save the reports in different sub-directories and set the permissions for each user

Q33. You deploy a new router on your network. What should you do to ensure NPM correctly interprets SNMP traps from the device?
* Verify that NPM is using the correct SNMP community strings
* Contact the router vendor fora firmware update
* Update the MIB database
* Review your firewall rules to ensure the traps are not blocked
SNMP traps are unsolicited messages sent by SNMP-enabled devices to notify the NPM server of important events or problems, such as device failures, configuration changes, or performance issues. SNMP traps contain information about the device and the event, such as the device name, IP address, timestamp, and OID (Object Identifier). An OID is a unique identifier for a specific variable in a MIB (Management Information Base), which is a hierarchical database of device information that can be accessed by SNMP. However, not all OIDs are recognized by NPM by default, as different devices may use different or custom MIBs and OIDs.

Therefore, to ensure NPM correctly interprets SNMP trapsfrom a new router on your network, you need to update the MIB database with the latest MIBs from the router vendor or from the SolarWinds website. This will allow NPM to translate the OIDs in the SNMP traps into meaningful names and values, and display them in the Trap Viewer or use them in alerts12.

To update the MIB database, follow these steps3:

Download the MIB files from the router vendor’s website or from the SolarWinds MIB Database.

Copy the MIB files to the SolarWindsOrionMibs folder on the NPM server.

Click Settings > All Settings > Manage MIBs.

Click Add New MIB and browse to the MIB file that you want to add.

Click Submit.

Repeat steps 4 and 5 for each MIB file that you want to add.

Click Compile to compile the MIBs and update the MIB database.

You can now view the SNMP traps from the new router in the Trap Viewer or use them in alerts. References:

1: SNMP Traps Explained: How to View SNMP Traps, 2: SNMP Traps in NPM, 3: Update the SolarWinds MIB Database for the SolarWinds Platform, : SolarWinds MIB Database, : 2, : 1, : 3, : 4

Q34. Your network includes the headquarters and three remote sites. Users from remote site A complain they do not have access to the company’s accounting server. Users from remote site B and C have access to the accounting server. How can you find the source of the issue?
* Use NetPath to see if there are problem areas between remote site A and the headquarters
* Verify that the accounting servers’ CPU utilization are not abnormally high
* Use NetPath to see if there are problem areas between remote site A and remote sites B and C
* Verify that the accounting servers are up

Q35. You receive an alert that one of your routers is experiencing critical level CPU utilization. The router details in the web console show as critical utilization, but you do not consider the utilization on that router to be at a critical level.

What change can you make in NPM to reflect a CPU utilization level you consider to be critical for the device?
* Copy the alert, change the trigger threshold, and limit the scope on that device
* Change the global critical CPU threshold for node statuses
* Change the critical CPU threshold on the node
* Change the trigger threshold on the alert

By default, NPM uses the global critical CPU threshold for node statuses, which is 90%. However, you can override this threshold for individual nodes by editing their properties and specifying a custom value for the critical CPU threshold. This way, you can adjust the threshold according to the specific characteristics and performance of each node. Changing the critical CPU threshold on the node will affect how the node status is calculated and displayed in the web console, as well as how the alerts are triggered based on the CPU utilization. References: Thresholds in the SolarWinds Platform; CPU Critical Threshold – Forum – Network Performance Monitor (NPM) – THWACK

Q36. The Orion platform supports agent-based monitoring for which OS types? (Choose all that apply.)
* Sun Solaris
* IBM
* AIX Unix Agents
* Windows
* Linux

Q37. You run ten reports on three assorted weekly schedules and send the results to the network operations distribution list. The email address for the distribution list changed, and you must update the new email address to send the reports. How do you implement this update?
* Use the Schedule Manager to edit each action on each report schedule, and change the email address
* Use the Action Manager to edit each action on each report schedule, and change the email address
* Make a copy of each report, edit the action to change the email address
* Edit each action on each report schedule, and change the email address

Q38. You can make bulk changes, such as changing the polling method, to nodes.
* TRUE
* FALSE

You can make bulk changes to nodes in NPM using the Manage Nodes feature. This allows you to select multiple nodes and edit their properties, such as the polling method, the polling frequency, the SNMP credentials, the custom properties, and more. You can also use the Edit Nodes feature to assign or unassign pollers to nodes, such as the Universal Device Poller (UnDP), the Hardware Health Poller, the Wireless Poller, and more12. References: 1: Change the polling method for a node3, 2: Manage pollers using Device Studio4

Q39. You can use Device Studio to create pollers for CPU and memory?
* TRUE
* FALSE

Device Studio is a feature in the SolarWinds Platform Web Console that allows you to create custom pollers for devices or technologies that are not supported by default in NPM. You can use Device Studio to create pollers for CPU and memory, as well as other metrics, by defining the object identifiers (OIDs) and formulas that you want to poll. Device Studio currently supports SNMP and WMI polling technologies, and you can test, assign, and edit your custom pollers from the Manage Pollers page. References: Create pollers in Device Studio for NPM, Device Studio, Device Studio Poller.

Q40. You have two groups of users – one in Sydney and one in Perth. How do you limit the users within the Orion Platform so they only have access to the devices in their location?
* Group devices into geographical Orion groups and use single group Account limitations to limit user access
* Configure Network Atlas to show only devices in their geographical location
* Use the Orion Service Manager to limit user access to nodes only in their location
* Configure the Orion Web Console settings to show only devices in the user’s geographical location

Q41. You inherit an environment with NPM and begin to receive High Traffic Utilization alerts from interfaces. When you view the alert, the issue is resolved. How do you modify NPM to receive fewer false alerts?
* Configure the alert so that it triggers only when traffic utilization remains high for a sustained period
* Configure the alert so that it resets only when traffic utilization remains high for a sustained period
* Increase the status polling frequency on the problematic interfaces
* Increase the statistics polling frequency on the problematic interfaces

Q42. You need to add a new subnet of 500 devices for monitoring. What is the first step to incorporate these devices into NPM?
* Collect NetFlow from a core router
* Perform a Network Discovery
* Measure network-wide bandwidth consumption
* Add the nodes using the Add Node feature in Manage Nodes

Q43. You deploy a new router on your network. What should you do to ensure NPM correctly interprets SNMP traps from the device?
* Verify that NPM is using the correct SNMP community strings
* Contact the router vendor fora firmware update
* Update the MIB database
* Review your firewall rules to ensure the traps are not blocked

Q44. Which is the best way to monitor an SNMP metric that NPM is not monitoring out-of-the-box?
* Create a custom poller
* Node Management utility
* Update the SolarWinds MIB database
* Enable CLI polling

Q45. Which metrics can NPM monitor on an Ethernet switch? (Choose all that apply.)
* Configuration changes
* Buffer misses
* Duplex mismatches
* CPU utilization

Q46. You configured devices to send SNMP traps to NPM, but do not see the messages in the Orion Web Console.

You verified that the firewall ports are open and the devices are correctly configured.

What can you verify to troubleshoot the cause?
* Verify you configured the SNMP Traps view in the Orion Web Console
* Verify that you have the SNMP Trap module installed for NPM
* Verify the SNMP trap service is running
* Verify you use Log Analyzer to view traps

The SNMP trap service is responsible for receiving, decoding, displaying, and storing the SNMP trap messages in the Log Analyzer database. If the service is not running, you will not see the messages in the Orion Web Console. You can verify the status of the service by using the Orion Service Manager or the Windows Services console. You can also restart the service if needed. The other options are not relevant for troubleshooting the cause of missing SNMP trap messages. References:

Monitor SNMP traps

Troubleshoot SNMP traps

Orion Service Manager

Q47. What is required to monitor tenants in your SDN environment with NPM Cisco ACI monitoring? (Choose all that apply.)
* View your SDN environment in Orion Maps
* Add an APIC node to NPM
* Enable API polling on the APIC node
* Enable API polling on all ACI devices

Q48. You use NPM to monitor a set of physical servers. The server team decides to virtualize these servers using VMware. Which part of your virtual infrastructure will NPM no longer be able to monitor?
* Virtualization host hardware health
* VM sprawl monitoring
* Virtualization host and VM performance metrics
* Virtualization environment tree

NPM can monitor the virtualization host hardware health, VM sprawl, and virtualization host and VM performance metrics using the Virtualization Manager Integration feature1. However,NPM cannot display the virtualization environment tree, which shows the hierarchical relationship between the virtualization hosts, clusters, datastores, and VMs. This feature is only available in Virtualization Manager2, a separate product that can be integrated with NPM. References: 1: Network Performance Monitor Administrator Guide – Monitor virtual infrastructure 2: Virtualization Manager Getting Started Guide – View the virtualization environment tree

Q49. What can you use to retrieve a single value in SNMP? (Choose all that apply.)
* GET VALUE
* GET NEXT
* GET TABLE
* GET

SNMP (Simple Network Management Protocol) is a protocol that allows network managers to monitor and control network devices using a set of standardized messages and data structures. SNMP uses a client-server model, where the network manager (client) sends requests to the network device (server) and receives responses. The network device has an SNMP agent that collects and reports the data using a MIB (Management Information Base), which is a hierarchical database of variables that describe the device’s status and configuration. Each variable in the MIB has a unique identifier called an OID (Object Identifier), which is a dot-separated sequence of numbers that follows a tree structure12.

To retrieve a single value in SNMP, you can use two types of requests: GET and GET NEXT. A GET request asks for the value of a specific OID, and the SNMP agent responds with the value if it exists, or an error if it does not. A GET NEXT request asks for the value of the next OID in the MIB tree, and the SNMP agent responds with the value and the OID of the next variable, or an error if there is no next variable. A GET NEXT request can be useful for discovering the OIDs and values of a device, or for iterating over a table of values34.

A GET VALUE request is not a valid SNMP request, and a GET TABLE request is not a single request, but a series of GET NEXT requests that retrieve all the values in a table . References: 1: SNMP Basics, 2: SNMP Tutorial Part 1 – Understanding MIBs and OIDs, 3: SNMP Tutorial Part 2 – SNMP Get, GetNext, GetBulk, 4:

SNMP Commands, : SNMP Table Operations, : SNMP Table Retrieval

Q50. While building an Orion map in the NPM web console you notice that two of your devices do not show a connection between them. You verify the two devices are connected. How can you resolve this issue? (Choose all that apply.)
* Build a new Orion map and add the related entities instead of the nodes
* Verify you are monitoring Layer 2 and 3 topologies
* Change the monitoring method from SNMP to CLI
* Build a custom connection between the devices