PassQueen
a.k.a dumpsqueen.com

RCPE Certified Professional Network & Infrastructure Visibility

Riverbed 810-01

Version Demo

Total Demo Questions: 8

Total Premium Questions: 81

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which AppResponse applications can be managed by NetProfiler?

A. General and URL

B. General

C. General, URL, Advanced Web and Auto-recognized

D. General, URL and Advanced Web

ANSWER: D

Explanation:

General, URL and Advanced Web is correct because NetProfiler can centrally create, edit, distribute, and maintain these defined application types on managed AppResponse appliances. General applications provide classification based on traffic characteristics such as ports, protocols, hosts, and subnets. URL applications extend application definition to web traffic identified through URL matching, while Advanced Web applications support more detailed web-application recognition and analysis. Managing these definitions from NetProfiler provides a consistent application taxonomy across the AppResponse environment, which in turn makes reporting, drill-down analysis, and traffic attribution comparable between appliances.

These application definitions are part of the NetProfiler-to-AppResponse integration workflow: NetProfiler acts as the central management point for supported application definitions, and AppResponse applies the resulting definitions while observing and analyzing traffic. Riverbed's AppResponse and NetProfiler software resources provide the relevant product documentation, release information, and supported integration material: Riverbed AppResponse support resources and Riverbed NetProfiler support resources.

QUESTION NO: 2

Which functions can a Packet Broker perform when distributing monitored traffic to visibility tools? (Choose all that apply.)

A. Filter traffic before delivery

B. Replicate traffic to multiple tools

C. Load balance traffic across tool ports

D. Route production user traffic

E. Assign IP addresses to monitored hosts

ANSWER: A B C

Explanation:

Packet Brokers can **filter traffic**, **replicate traffic to multiple tools**, and **load balance traffic across tool ports**. Filtering removes traffic that is not needed by a connected monitoring or security tool. Replication enables multiple tools to receive the same relevant traffic, while load balancing distributes traffic across a group of analysis tools to support higher monitoring capacity.

A Packet Broker operates on copies of production traffic obtained from TAPs, SPAN ports, or similar sources. It does not route production application traffic or replace the forwarding functions of a network switch or router. Riverbed product and documentation resources are available through the Riverbed Documentation portal.

QUESTION NO: 3

Which SteelCentral solutions are used to provide the initial data to build an application model framework in Portal? (Choose all that apply.)

A. AppInternals

B. NetProfiler

C. NetIM

D. AppResponse

E. Aternity

ANSWER: B D

Explanation:

NetProfiler and AppResponse provide the initial information used by SteelCentral Portal to establish an application-model framework. NetProfiler supplies network-derived application intelligence, including traffic and dependency context that helps identify the network services and communications associated with an application. AppResponse contributes packet- and flow-based visibility into application transactions, servers, and infrastructure interactions. Portal uses these complementary data sources to correlate monitored entities and present a unified application-centric operational view.

This initial model is important because Portal is intended to reduce the separation between network-performance data and application-performance evidence. By starting with the network and transaction context discovered by NetProfiler and AppResponse, users can organize subsequent investigation around an application and its supporting components rather than beginning with isolated device or interface metrics. The resulting framework supports cross-domain troubleshooting and navigation from an application symptom toward relevant network and transaction details. Riverbed describes its visibility portfolio and application-performance capabilities in its product portfolio and provides product documentation resources through the Riverbed Support portal.

QUESTION NO: 4

Assume you want to identify which modules and cards belong to each chassis in your environment.

Which NetIM function can provide this information?

A. Device and Platform Info

B. Link and Connection Inference

C. Auto-discovery

D. Auto-grouping

ANSWER: A

Explanation:

Device and Platform Info is the NetIM function that supplies chassis inventory and hardware-platform details. NetIM discovers and models a managed device's physical composition, including the chassis and the modular components installed within it, such as cards, modules, slots, and associated hardware attributes. This lets an administrator determine which physical components belong to a particular chassis rather than only seeing the device as a single logical network node.

This capability is especially useful for operations teams maintaining an accurate inventory of modular switches, routers, and other chassis-based equipment. The collected platform information supports hardware identification, asset awareness, and troubleshooting by presenting the device's underlying physical hierarchy. It therefore directly answers a request to identify the modules and cards associated with each chassis in the monitored environment.

Riverbed documents its network-visibility products and their discovery and inventory capabilities through the Riverbed NetIM product page and the Riverbed Support Portal, where product documentation describes the device and platform information gathered by NetIM.

QUESTION NO: 5

Which data source is required before Portal can generate the AppNetwork Path between an IP address pair?

A. AppInternals

B. NetProfiler

C. NetIM

D. AppResponse

ANSWER: C

Explanation:

NetIM is required because AppNetwork Path depends on network-discovery and topology information to calculate and display the route between the selected source and destination IP addresses. NetIM discovers network devices, interfaces, Layer 2 and Layer 3 connectivity, and routing-related relationships. Portal uses this modeled infrastructure data to determine the intermediate hops and present the end-to-end application-network path in context.

The path is therefore not merely a traffic conversation or a packet capture; it is a topology-aware representation of how the communicating endpoints are connected across the monitored network. Before Portal can render that view, it must have access to a configured, populated NetIM data source containing the relevant discovered devices and endpoint connectivity. Keeping NetIM discovery current is important so that Portal can represent the active network structure accurately when an IP-address pair is selected.

Riverbed product documentation and support resources describe NetIM as the infrastructure monitoring and topology-discovery component used alongside other Riverbed observability products: Riverbed Documentation and Riverbed Support.

QUESTION NO: 6

Which component of the SteelCentral NPM architecture uses SNMP polling to retrieve Hostnames and interface information from flow reporting devices?

A. AppResponse

B. Flow Gateway

C. Packet Analyzer

D. NetProfiler

ANSWER: B

Explanation:

Flow Gateway is correct because it performs the device-enrichment role for flow sources in a SteelCentral Network Performance Management deployment. Flow-reporting devices export flow records containing traffic and interface identifiers, but useful reporting also requires associated device metadata, such as the reporting device's hostname and interface details. Flow Gateway obtains that metadata by polling the flow-reporting devices through SNMP, then makes the enriched information available for use in the flow-monitoring environment. This process enables flow data to be identified and presented using meaningful device and interface context rather than only raw numeric identifiers.

In practical deployment terms, SNMP reachability and appropriate SNMP credentials must be configured so Flow Gateway can successfully query the relevant exporters. The SteelCentral NPM Deployment Guide describes Flow Gateway's use of SNMP to retrieve hostname and interface information from flow-reporting devices as part of its integration responsibilities. See the SteelCentral NPM Deployment Guide and Riverbed's Network Performance Management product information.

QUESTION NO: 7

Which actions help ensure that a packet-capture deployment can support investigation of intermittent application-performance problems? (Choose all that apply.)

A. Use continuous capture with retention appropriate to the incident window

B. Capture both directions of relevant conversations

C. Validate that the capture path can sustain expected traffic rates

D. Apply focused capture filters where appropriate

E. Start packet capture only after every incident has ended

ANSWER: A B C D

Explanation:

Use continuous capture with retention appropriate to the incident window preserves packet evidence before an issue is reported. **Capture both directions of relevant conversations** enables complete transaction and TCP analysis. **Validate that the capture path can sustain expected traffic rates** reduces the risk of dropped packets during busy periods. **Apply focused capture filters where appropriate** can conserve storage and analysis capacity while retaining traffic relevant to the investigation.

Packet capture should be designed around the required pre-event history, link utilization, expected traffic volume, and investigative objectives. Beginning a capture only after an unpredictable incident is reported may miss the evidence needed to diagnose it. See the Riverbed Packet Analyzer Plus product page and the Riverbed Documentation portal.

QUESTION NO: 8

What types of metric data are used to populate Application/Server Performance Panels in Portal Application Dashboards? (Choose all that apply.)

A. Per Instance metrics based on AppInternals

B. Per System metrics based on NetIM Data

C. Flow collection Metrics from NetProfiler

D. Packet Inspection Metrics from AppResponse

E. End User Device Data from Aternity

ANSWER: A C

Explanation:

Portal Application Dashboards use both application-instance telemetry and network-flow telemetry to provide a useful application/server performance view. **Per Instance metrics based on AppInternals** is correct because AppInternals supplies application-centric performance information at the monitored application-instance level. This enables Portal to present performance data associated with the application and server context rather than only an aggregated network perspective. Riverbed describes AppInternals as an application performance monitoring solution that provides visibility into application behavior and transaction performance.

Flow collection Metrics from NetProfiler is also correct because NetProfiler contributes flow-derived network and application traffic information. Flow data provides the network context needed by an application dashboard, including communication and traffic behavior associated with applications and servers. Combining these sources lets Portal correlate application-instance performance with observed flow activity, which supports investigation across application and network domains from a consolidated dashboard. See Riverbed's AppInternals product information and NetProfiler product information for the respective application-performance and flow-visibility capabilities.