

# DUMPSQUEEN

## Riverbed Certified Solutions Professional - Network Performance Management

Riverbed 299-01

Version Demo

Total Demo Questions: 15

Total Premium Questions: 245

Buy Premium PDF

<https://dumpsqueen.com>

[support@dumpsqueen.com](mailto:support@dumpsqueen.com)

dumpsqueen.com

## Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	99
Topic 2, Volume B	146
<b>Total</b>	<b>245</b>

## QUESTION NO: 1

Before running your first report on Cascade Profiler after installation, where is the best place to go to verify traffic flows are currently being received?

- A. System Information > Devices/Interfaces
- B. System Information > Profiler
- C. Dashboard
- D. Log in to the shell and view the /usr/mazu/var/log/Sensor.log
- E. Ping devices on UDP port 2055 to see if they are up and running

**ANSWER: A**

## QUESTION NO: 2

Which filter should be used to analyze a capture job within Cascade Pilot?

Use a BPF filter to speed up the View.

Apply a generic View and then define a filter by drilling-down through a more specific View.

- C. Use a Cascade Pilot filter first and then a BPF filter.
- D. Create a time filter and then apply a View with a Cascade Pilot filter.

**Answer: D**

- A. Use a Cascade Pilot filter first and then a BPF filter.
- B. Create a time filter and then apply a View with a Cascade Pilot filter.

**ANSWER: B**

## QUESTION NO: 3

When sending data from a Gateway or Sensor to a Profiler which ports must be opened between the devices? (Select 3)

- A. tcp/8443
- B. udp/123
- C. tcp/41017

D. tcp/42999

E. tcp/123

**ANSWER: A B C**

## QUESTION NO: 4

When analyzing a large (100GB, for example) trace file within Cascade Pilot, you should:

- A. Copy the file onto a Cascade Shark to ensure better performance.
- B. Create an index so that processing of the View analytics will be faster.
- C. Apply a View with a specific filter.
- D. Use Wireshark tools to split the trace file in multiple and smaller trace files.

**ANSWER: B**

## QUESTION NO: 5

Which of the following statements are true (select 2)

- A. SNMP based technology can query a network device for statistics such as number of packets and bytes sent out an interface but typically doesn't have conversation-level details (such as which IP Addresses were talking at a given time)
- B. NetFlow based technology can query a network device for statistics such as number of packets and bytes sent out an interface but typically doesn't have conversation-level details (such as which IP Addresses were talking at a given time)
- C. NetFlow based technology does NOT typically include response time information, packet inspection is necessary to measure response times
- D. It is NOT possible to understand which conversations traversed a link without full packet capture
- E. SNMP based technology querying routers in the network can be used to view end to end conversations across a network to determine top talkers

**ANSWER: A C**

## QUESTION NO: 6

Filtering in Cascade Pilot: (Select 2)

- A. Is either a BPF or Wireshark Display filter only.
- B. Can be created from a chart.

- C. Can be changed after applying a View.
- D. Is the equivalent of the Wireshark "display filter input".

**ANSWER: B C**

## QUESTION NO: 7

What can be configured on the Cascade Profiler to detect utilization for an interface?

(Select 2)

- A. Manually configure the interface speeds on the Devices/Interfaces page.
- B. Configure and enable SNMP access to the reporting devices on the Devices/Interfaces page.
- C. Enable NBAR on the routers.
- D. Check the "Interface Utilization" box under the Devices/Interfaces page for each router and/or Steelhead desired.
- E. Configure the appropriate Device Interface Analytic.

**ANSWER: A B**

## QUESTION NO: 8

When editing a previously configured service policy, what options become available if you click the 'show advanced settings' checkbox? (Select 3)

- A. Allows enabling/disabling the detection of dips in the metric.
- B. Allows tuning of the tolerance range of the metric.
- C. Allows setting of a noise floor for the metric.
- D. Allows adjusting the notifications for the metric.
- E. Allows enabling/disabling the detection of spikes in the metric.

**ANSWER: A C E**

## QUESTION NO: 9

Within Cascade Profiler the Event Policy categories for which you can receive alerts include. (Select 4)

- A. Performance and Availability
- B. TCP Health

- C. VoIP
- D. Security
- E. Health
- F. User-defined Policy

**ANSWER: A D E F**

## QUESTION NO: 10

Cascade provides a means for contacting other network devices for additional information about a host or user of interest. Right-clicking a host name, IP address, MAC address or port number and choosing \_\_\_\_\_ from the shortcut menu sends a query to the other network device.

- A. View Packets
- B. Error Report
- C. Restart Service
- D. View Switch Port
- E. External Link

**ANSWER: E**

## QUESTION NO: 11

Within Cascade Pilot, when packet capture (pcap) files have associated trending/indexing data the following are true (select 2)

- A. They appear in the my-views main directory.
- B. Views that take advantage of the trending/indexing data load faster.
- C. The file icon includes a colored-lightning bolt.
- D. The file loads faster into Wireshark.
- E. Additional pre-defined filters and watches are available.

**ANSWER: B C**

## QUESTION NO: 12

When creating an analytic service, the discovery process requires a minimum of:

- A. At least three days of data available.
- B. At least three weeks of data available.
- C. The application specialist available.
- D. Some historical data and some starting point (a server, port, application).
- E. A customer network diagram available.

**ANSWER: D**

## QUESTION NO: 13

The "Policies Usage" that is reported under System – Information pertains to which of the following:

- A. All Service-based application performance policies
- B. All Service-based policies plus all Performance and Availability analytic policies
- C. All Service-based policies plus all Performance and Availability analytic policies plus all User-Defined Policies
- D. All Service-based policies plus all Performance and Availability analytic policies plus all User-Defined Policies plus all Security policies
- E. None of the above

**ANSWER: B**

## QUESTION NO: 14

What defines a "Recipient" for Cascade Profiler Notifications?

- A. An Email Address only
- B. An SNMP receiver only
- C. An SNMP receiver only tied to a set of Host Groups
- D. An Email Address and/or one or two SNMP receivers optionally tied to a set of Host Groups
- E. An Email Address and/or one or two SNMP receivers optionally tied to a set of User Accounts
- F. A User Account

**ANSWER: D**

## QUESTION NO: 15

How do Cascade Performance Analytics assist with Performance Monitoring?

- A.** By setting intelligent static thresholds for Application metrics and Interface metrics, tolerance can be determined. Cascade will use these thresholds and tolerances to report on deviations indicative of performance problems.
- B.** The Customer only needs to identify their critical hosts, interfaces and/or applications, and Cascade will automatically baseline their behavior and report on deviations indicative of performance problems.
- C.** The Performance Analytics use knowledge of hosts, interfaces, and/or applications are able to detect security threats such as host scans and worms.
- D.** After baselining is completed, Cascade can re-route congested traffic to avoid congested application delivery paths.

**ANSWER: B**