

Riverbed 299-01

**Riverbed Certified Solutions Professional - Network
Performance Management
Version: 5.0**

Topic 1, Volume A**QUESTION NO: 1**

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

Explanation:

QUESTION NO: 2

Link Congestion policies apply to a specific interface and can: (Select 3)

- A. Warn if either inbound or outbound traffic increases abnormally
- B. Warn if an application component of traffic increases abnormally
- C. Warn if traffic to/from specific hosts exceeds a specific utilization level
- D. Warn if the response time across a link increases abnormally

Answer: A,B,C

Explanation:

QUESTION NO: 3

If a VLAN SPAN (VLAN101) is configured and monitored by Cascade Shark, which of the following is true? (Select 2)

- A. Inter VLAN101 traffic will be monitored; Intra VLAN101 traffic will not.
- B. Intra VLAN101 traffic will be monitored; Inter VLAN101 traffic will not.
- C. Both inter and intra VLAN101 traffic will be monitored.
- D. It is a best practice to configure the Cascade Shark monitoring port (the SPAN destination) with 'deduplication' enabled.
- E. It is a best practice to configure the Cascade Shark monitoring port (the SPAN destination) without 'deduplication' enabled.

Answer: C,D

Explanation:

QUESTION NO: 4

Quality of Service information is obtained from what Cascade sources?

- A. Cascade Sensor only
- B. Cannot get QoS data on Cascade
- C. Cascade Sensor and Cascade Gateway
- D. CascadeFlow traffic only
- E. NetFlow and IPFIX traffic only

Answer: C

Explanation:

QUESTION NO: 5

Cascade Profiler provides identity information collected from Active Directory 2008 by installing and correctly configuring the 'Cascade Connector' agent software on:

- A. Every DNS server in the AD environment
- B. Any server in the MS domain
- C. Every client desktop in the AD environment
- D. Every NTP server in the MS domain
- E. The Microsoft Event Collector component in the AD environment

Answer: E

Explanation:

QUESTION NO: 6

Which of the following statements is true regarding SNMP polling and NTP syncing among Cascade components?

- A. Cascade Gateway's poll via SNMP sources of Netflow, while Cascade Profiler, Cascade Gateway and Cascade Sensor sync NTP from a common source.
- B. Cascade Profiler's poll via SNMP sources of Netflow, while Cascade Profiler, Cascade Gateway and Cascade Sensor sync NTP from a common source.

- C. Cascade Profiler, Cascade Gateway and Cascade Sensor sync NTP from different sources, while Cascade Profiler's poll via SNMP sources of Netflow.
- D. Cascade Profiler, Cascade Gateway and Cascade Sensor sync NTP from different sources, while Cascade Gateway's poll via SNMP sources of Netflow.
- E. Cascade Profiler does all SNMP polling and is also the source of all NTP.

Answer: D

Explanation:

QUESTION NO: 7

Within Cascade Pilot, to analyze the round-trip time in a trace file, you can:

- A. Ask Riverbed Support to send you the proper View to use.
- B. Open the View folders in Cascade Pilot to look for a View named "Round-trip time".
- C. Use the View search box and enter "round".
- D. Use the Help menu and search for round.

Answer: C

Explanation:

QUESTION NO: 8

For DNS reverse lookup, Cascade Profiler caches as follows:

- A. Cache the most recent 500 IPs.
- B. Obey DNS TTLs.
- C. Cascade does not cache DNS responses.
- D. For 24 hours.

Answer: C

Explanation:

QUESTION NO: 9

What are two differences between NetFlow version 5 and NetFlow version 9 (select 2)

- A. NetFlow version 5 generally support ingress flow export only; NetFlow version 9 supports both

ingress and egress export.

B. NetFlow version 5 is used for Switches, NetFlow version 9 is used for Routers.

C. NetFlow version 9 includes information about CPU, Power-status and other router performance characteristics; NetFlow version 5 does not.

D. NetFlow version 9 includes the ability to export the Time-To-Live (TTL); NetFlow version 5 does not.

E. NetFlow version 9 includes the ability to export the packet latency, NetFlow version 5 does not.

Answer: A,D

Explanation:

QUESTION NO: 10

When changing the priority for a Layer 4 mapping on Cascade Profiler best practices indicate that Application Mappings should be given higher priorities based on:

A. Longest Match

B. Shortest Match

C. IP & Port

D. IP

Answer: A

Explanation:

QUESTION NO: 11

What is the relationship between a Host Group and a Host Group Type in Cascade Profiler?

A. A Host Group Type is a container that may contain multiple Host Groups.

B. A Host Group Type defines the name of the Host Group.

C. They are the same thing.

D. Each Host Group must be defined by the Type of application it serves; this is the Host Group Type.

Answer: A

Explanation:

QUESTION NO: 12

Cascade Profiler's Switch Integration feature uses SNMP and adds the capability for Cascade to report on which of the following. (Select 2)

- A. User name
- B. Host IP address
- C. Host MAC address
- D. The physical switch port a specific host is connected to
- E. Switch port traffic levels
- F. Switch port status
- G. SNMP traps from the switch

Answer: C,D

Explanation:

QUESTION NO: 13

What are the two types of dashboards available within the Cascade Profiler GUI? (select 2)

- A. Top Hosts
- B. Top Applications
- C. Public
- D. Private
- E. Devices and Interfaces Utilization

Answer: C,D

Explanation:

QUESTION NO: 14

If unable to connect to the Cascade Shark Appliance from the Cascade Pilot console it could be because. (Select 2)

- A. The correct communication port(s) are NOT open on the firewall between Cascade Pilot and Cascade Shark.
- B. The Cascade Shark is placed in "passthru" mode so Cascade Pilot access is not available
- C. The Cascade Shark appliance has no capture jobs configured.
- D. You may be running Cascade Pilot-Personal-Edition (PE). You need the full version of Cascade Pilot to connect to Cascade Shark.
- E. Trend/Index data is disabled on the Cascade Shark Appliance.

Answer: A,D

Explanation:

QUESTION NO: 15

What is a good way to know whether all internal IP addresses seen by the Cascade Profiler have been grouped in a particular group type?

- A. Run Automatic grouping for all group types.
- B. Configure an Undefined group type with definition 0.0.0.0/0; confirm there are no entries when you 'view members' of this 'Undefined' group'.
- C. There is no way to do this and successfully capture all the IP addresses.
- D. Configure an Undefined group type with definition 0.0.0.0/32.
- E. Run a report by hosts and look for undefined groups.

Answer: B

Explanation:

QUESTION NO: 16

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

Explanation:

QUESTION NO: 17

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

Explanation:

QUESTION NO: 18

Which of the following configuration changes can be used to reduce the number of alerts generated overall for a Service?

- A. Edit each Service policy to increase the Tolerance slider for Low and High alerts.
- B. Edit each Service policy and set a noise floor to specify the minimum amount of change that the policy can treat as deviation from normal behavior.
- C. Edit the Service and select fewer metrics to monitor for each segment that comprises the Service.
- D. Modify the location host group type used for monitoring end user traffic to use fewer groups (for example, Region instead of Site).
- E. A, B, C, and D.
- F. A and B only.

Answer: E

Explanation:

QUESTION NO: 19

If a report table on Cascade Profiler includes the "Server Delay" column but shows no value for "Server Delay" in some cells, what are the possible causes? (Select 3)

- A. The time span of the report does not cover any connection set-up points
- B. Server delay is zero.
- C. The protocol used by the application is not TCP-based.
- D. Application traffic was not seen by a Cascade Sensor.
- E. The server plug-in is needed to measure "Server Delay" and not functioning correctly.

Answer: A,C,D

Explanation:

QUESTION NO: 20

Within the Cascade Pilot GUI, filtered items are often indicated:

- A. With red text.
- B. With yellow text.
- C. With a funnel icon.
- D. With a hash-mark icon.

Answer: C

Explanation:

QUESTION NO: 21

Which of the following metrics are monitored in an Application Performance Policy? (Select 4)

- A. Increase in Server Delay
- B. Decrease in Average Connection Application-level Throughput
- C. Increases in the number of TCP retransmissions
- D. Decreases in the number of new connections to the application servers
- E. Increase in the number of Active Connections

Answer: B,C,D,E

Explanation:

QUESTION NO: 22

What are the two (at a minimum) devices you need to configure in Cascade Profiler for Switch Port Discovery integration to work for a portion of the network?

- A. At least one NetFlow sources (router, switch, or steelhead).
- B. At least one lookup router and at least one access tier switch.
- C. A Vulnerability Scanner and a Netflow source (router, switch, or steelhead).
- D. A Vulnerability Scanner and an External Link.

Answer: B

Explanation:

QUESTION NO: 23

Which fields are generally available for export using NetFlow technology?

- A. IP Addresses, Port Numbers, Protocol, TCP Flags, DSCP Marking, number of bits, number of packets, retransmitted bits
- B. IP Addresses, Port Numbers, Protocol, TCP Flags, DSCP Marking, number of bits, number of packets, inbound/outbound interface ID
- C. IP Addresses, MAC Addresses, Port Numbers, Protocol, DSCP Marking, number of bits, number of packets
- D. IP Addresses, Port Numbers, Protocol, Round Trip Time, DSCP Marking, number of bits, number of packets
- E. IP Addresses, Port Numbers, Protocol, Packet Latency, DSCP Marking, number of bits, number of packets

Answer: B

Explanation:

QUESTION NO: 24

In Cascade Profiler, what is the minimum amount of historical flow data required for an Application Performance analytic to initialize?

- A. Three weeks
- B. Three days
- C. One day
- D. Configurable from one minute to three weeks

Answer: B

Explanation:

QUESTION NO: 25

In this scenario, you have created a host group called My_Computers on Cascade Profiler. In that group you have included the subnet 192.168.1.0/25.