DUMPSARENA

Riverbed Certified Solutions Associate

Riverbed 101-01

Version Demo

Total Demo Questions: 28

Total Premium Questions: 288

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Exam Pool A	90
Topic 2, Exam Pool B	84
Topic 3, Exam Pool C	94
Total	288

QUESTION NO: 1

Login to the CMC appliance can be authenticated against what type servers? (Select 3)

A. RADIUS

B. Local

C. XAUTH

D. TACACS+

E. Kerberos

ANSWER: A B D

Explanation:

The CMC supports three relevant login-authentication choices: **RADIUS**, **Local**, and **TACACS+**. Local authentication uses accounts maintained directly on the CMC appliance and provides an administrative access method that does not depend on connectivity to an external identity service. RADIUS and TACACS+ allow the appliance to delegate user authentication to centralized AAA infrastructure, which is useful when organizations need consistent access control across network devices and centralized administration of operator credentials. These services are commonly deployed for network-device administrative access, and the CMC can be configured to use them for its management login process. When an external authentication method is configured, operational planning should preserve a usable local administrative account so that management access remains possible if the external AAA server or its network path is temporarily unavailable. Riverbed product documentation and software resources are available through the Riverbed SteelHead support portal, while Riverbed's documentation catalog is available at docs.riverbed.com.

QUESTION NO: 2

To run RSP which Steelhead appliance ports must to be connected to your network? (Select 2)

A. Primary

B. LAN

C. Inpath0_0

D. Auxiliary

E. WAN

ANSWER: A D

Explanation:

RSP requires the SteelHead appliance's **Primary** and **Auxiliary** ports to have network connectivity. The Primary interface provides the appliance's essential network and management reachability, allowing the SteelHead to be administered and to communicate with the Riverbed services used to deploy and operate the RSP environment. The Auxiliary interface is required as the separate network connection made available for the virtualized service running under RSP. Connecting both interfaces supplies the host appliance and its hosted service with the required network paths while preserving the interface separation expected by the RSP architecture. This is an RSP-specific connectivity requirement: the appliance must have both its Primary management-side connection and its Auxiliary service-side connection present before the platform can run hosted services correctly. Riverbed product documentation and software resources are available through the Riverbed Documentation portal, while current product guidance, technical documentation access, and support resources are available from Riverbed Support.

QUESTION NO: 3

Which of the following Steelhead appliance models support redundant power supplies? (Select 2)

A. 250

B. 1221

C. 2012

D. 2050

E. 5050

ANSWER: D E

Explanation:

The Steelhead 2050 and Steelhead 5050 are the applicable appliance models because their hardware designs support redundant power-supply configurations. Redundant power supplies provide power resiliency: two installed power modules can be connected to separate electrical sources, allowing the appliance to continue operating if one power supply or its associated input power fails. This is especially important for Steelhead appliances deployed at data centers, hubs, or other locations where WAN optimization availability is business-critical.

For these platforms, redundancy is a hardware capability rather than a RiOS software setting. The installed redundant supplies share the appliance power load during normal operation and enable replacement or recovery from a single-supply failure without an unplanned appliance shutdown. Administrators should connect each supply to independent power circuits when possible to obtain the intended protection. Riverbed's hardware-installation documentation and support resources provide the platform-specific power, installation, and maintenance requirements for Steelhead appliances. See the Riverbed documentation portal and the Riverbed Support portal for the relevant Steelhead hardware documentation.

QUESTION NO: 4

How many in-path rules will a LAN-initiated single connection execute on a Steelhead appliance?

A. 0

B. 1

C. 2

D. 3

ANSWER: B

Explanation:

1 is correct. For a LAN-initiated connection, the SteelHead appliance evaluates its configured in-path rules in their configured order and applies the first rule that matches the connection's traffic characteristics. That matching rule determines the handling of the connection, including whether it is optimized, passed through, discarded, or processed according to the rule's specified settings. After a rule matches, SteelHead does not continue evaluating later in-path rules for that same connection. Consequently, a single LAN-initiated flow executes one in-path rule, even when the in-path rule table contains multiple entries.

This first-match behavior makes rule order significant in SteelHead deployments. Administrators normally place more specific traffic definitions ahead of broader rules so that the intended policy is selected for a new connection. The decision is made when the connection is established and is then retained for the life of that flow, rather than repeatedly applying multiple rules to its packets. Riverbed's product documentation and support resources provide configuration guidance for SteelHead in-path deployment and traffic handling: Riverbed Documentation and Riverbed Support.

QUESTION NO: 5

What basic configuration steps should be done on the SteelHead before attempting to join it to a Windows Domain? (Choose two.)

A. Configure either a Delegation or Replication user.

B. Configure DNS to include an entry for resolution of the SteelHead primary interface IP address.

C. Enable SMB signing/Encrypted MAPI support.

D. Enable NTP and ensure time is synced with domain controllers.

ANSWER: B D

Explanation:

Before a SteelHead joins an Active Directory domain, its primary interface address must be resolvable through DNS. Active Directory domain joining relies on DNS to locate domain controllers and related AD services, while the SteelHead must also be represented correctly in name resolution so that domain members and administrators can identify and communicate with it by name. Configure DNS to include an entry for resolution of the SteelHead primary interface IP address therefore provides the required forward lookup identity and supports dependable domain-related communication.

Time synchronization is also a prerequisite for successful, reliable domain membership. A SteelHead should have NTP enabled and synchronize its clock with the domain controllers, or with an authoritative time source that is itself synchronized to the domain. Kerberos, the authentication protocol used by Active Directory, validates timestamps as part of ticket processing. Keeping the appliance clock close to the domain-controller time prevents authentication failures during the join process and during later domain-authenticated operations. These settings should be verified before initiating the domain join. Microsoft documents the importance of DNS for Active Directory at Discover domain controllers in Active Directory Domain Services and Kerberos time synchronization requirements at Kerberos authentication overview.

QUESTION NO: 6

How can Steelhead Mobile client software be distributed directly from the Steelhead Mobile Controller (SMC)? (Select 2)

A. HTTPS

B. HTTP

C. FTP

D. TFTP

E. NFS

ANSWER: A B

Explanation:

Steelhead Mobile Controller supports direct distribution of the Steelhead Mobile client installer through its web-based software-distribution service. **HTTPS** is supported so that users can retrieve the client package through an encrypted, authenticated web connection. This is the preferred approach when distribution occurs across untrusted networks because the transport session is protected with TLS. **HTTP** is also supported for direct download from the controller, which can be appropriate for controlled internal networks or environments where encrypted transport is not required by policy. In practice, an administrator enables and configures the controller's software distribution capability, then provides users with the applicable controller download URL. The user obtains the installer using a web browser and installs the Steelhead Mobile client on the endpoint. These two web protocols are therefore the direct mechanisms used by the SMC for client software distribution. Riverbed documentation and software resources are available through the Riverbed Support portal; current Steelhead WAN-optimization product information is available from Riverbed Steelhead.

QUESTION NO: 7

A service provider would like to implement multi-tenanting on a SteelCentral Controller for SteelHead (SCC) such that the customers would be able to run their own reports. Which of the following are true?

A. SCC does not support multi-tenancy. A virtual or physical SCC would need to be provisioned for each customer.

B. The SSL certificate for SCC management would need to be distributed to the customers.

C. RADIUS or TACACS+ would need to be used to offload the authentication to achieve the privileges required.

D. HTTP server should be disabled for the web UI and only SSL used.

E. Each customer would have to be configured with privileges for their own SteelHeads and no others.

ANSWER: E

Explanation:

Each customer would have to be configured with privileges for their own SteelHeads and no others. SCC supports delegated access through its user, role, and appliance-access controls, which can be used to provide a practical multi-tenant administration model. A service provider can define separate customer users and assign the appropriate monitoring or reporting permissions, while limiting the appliances visible to each customer account to that customer's SteelHeads. As a result, when a customer signs in to SCC, reports and appliance information are scoped to the SteelHeads that the customer is authorized to access. This separation is important because reporting data is collected and presented in the context of managed appliances; restricting appliance access prevents one tenant from viewing another tenant's devices, statistics, or reports. The provider retains administrative control of the SCC and can maintain the user definitions, roles, and appliance assignments as customers or managed SteelHeads change. This capability lets one SCC support multiple customer environments without exposing cross-customer operational data. Riverbed documentation and product resources are available through the Riverbed Documentation portal and the Riverbed Support portal, including SCC administration guidance for user access and managed appliances.

QUESTION NO: 8

Which of the following expansion cards are available for the Steelhead appliance xx50 series? (Select 2)

A. Four-Port Copper Gigabit-Ethernet PCI-E

B. Four-Port SX Fiber Gig-E PCI-X

C. Five-Port Copper Gigabit-Ethernet PCI-E

D. Two-Port SX Fiber Gigabit-Ethernet PCI-E

E. Three-Port SX Fiber Gig-E PCI-X

ANSWER: A D

Explanation:

The available expansion-card selections for the Steelhead xx50 appliance series are **Four-Port Copper Gigabit-Ethernet PCI-E** and **Two-Port SX Fiber Gigabit-Ethernet PCI-E**. These cards provide alternative physical network connectivity for deployments in which the appliance must connect to multiple copper Ethernet segments or to multimode fiber infrastructure using SX Gigabit Ethernet optics. The xx50 platform expansion capability is based on PCI Express, so the card descriptions correctly pair the supported port configurations with the PCI-E interface. A four-port copper card is useful where multiple 10/100/1000BASE-T connections are required, while the two-port SX fiber card supports Gigabit Ethernet fiber links commonly used for switch uplinks and data-center or campus connections. Selecting the appropriate interface card is important because SteelHead deployment design must match the existing Layer-1 media and the required number of in-path or network connections. Riverbed product documentation and support resources provide the appliance hardware and interface specifications used to verify platform-specific module compatibility. See the Riverbed documentation portal and the Riverbed Support portal for SteelHead hardware documentation.

QUESTION NO: 9

Which Riverbed products can be managed by the SteelCentral Controller for SteelHead? (Choose six.)

A. SteelFusion Core

B. SteelHead

C. SteelCentral AppResponse

D. SteelFusion Edge

E. SteelHead EX

F. SteelCentral NetProfiler

G. SteelHead Mobile

H. SteelHead Interceptor

ANSWER: A B D E G H

Explanation:

SteelCentral Controller for SteelHead (SCC) centrally manages the SteelHead family and selected related Riverbed products. Its supported-device matrix for SCC 9.2 includes SteelFusion Core for monitoring, SteelHead appliances for configuration and monitoring, SteelFusion Edge for monitoring and partial configuration, and SteelHead EX for configuration and monitoring. SCC also provides centralized management visibility for SteelHead Mobile, although the documented scope for that platform is monitoring rather than full configuration. SteelHead Interceptor is likewise a supported managed platform, with SCC providing configuration and monitoring support for supported Interceptor releases. Therefore, the six applicable product families are SteelFusion Core, SteelHead, SteelFusion Edge, SteelHead EX, SteelHead Mobile, and SteelHead Interceptor. The product name “SteelCentral Controller for Mobile” has been corrected to “SteelHead Mobile,” which is the endpoint/mobile WAN-optimization product identified in the SCC support matrix. Management capability can differ by product and software version, so the presence of a platform in this answer means that it is supported by SCC in at least the documented monitoring and/or configuration capacity. See the SCC 9.2 documentation download at Riverbed Support: SteelCentral Controller for SteelHead 9.2.1 and the Riverbed Support Portal.

QUESTION NO: 10

Which Datastore Segment Replacement Policy can be selected to overwrite data that has resided in the segstore for the longest duration of time?

A. LRU (Least Recently Used)

B. FIFO (First In First Out)

C. LIFO (Last In First Out)

D. MRU (Most Recently Used)

E. ADH (Arbitrary Data Hits)

ANSWER: B

Explanation:

FIFO (First In First Out) is the appropriate datastore segment replacement policy because it selects segments according to how long they have been present in the SteelHead segment store. When space is required, the segment that entered the segstore earliest is selected for replacement. This directly implements an age-based retention approach: data that has resided in the datastore for the longest duration is overwritten first, irrespective of whether that data might have been referenced more recently. In Riverbed WAN optimization, the segstore holds data segments used by Scalable Data Referencing so that repeated content can be represented efficiently across the WAN. Selecting FIFO therefore provides a simple, deterministic policy for reclaiming segstore capacity based on insertion order and segment age. This behavior is precisely what the question describes: “first in” data is the oldest resident data and is consequently the first eligible data to be removed when the datastore needs space. Riverbed product documentation and support resources are available through the Riverbed Documentation portal and the Riverbed Support portal.

QUESTION NO: 11

The SteelHead Admission Control feature activates when: (choose two)

A. The data store has reached full capacity

B. Throughput exceeds the licensed limit of the appliance

C. Total connections exceeds the licensed limit of the appliance

D. Optimization service memory exceeds the limit of the appliance

E. Optimized connections exceed the licensed limit of the appliance

ANSWER: B E

Explanation:

SteelHead Admission Control protects the appliance's optimization service by preventing it from accepting more work than its licensed optimization capacity permits. It activates when throughput exceeds the licensed limit of the appliance and when optimized connections exceed the licensed limit of the appliance. These two thresholds represent the licensed scale of the SteelHead: bandwidth capacity limits the volume of traffic the appliance can optimize, while the optimized-connection limit constrains the number of simultaneous flows that can receive optimization treatment. When either licensed resource boundary is reached, Admission Control limits additional optimization work so that already admitted optimized traffic can continue to receive predictable service. This behavior is important in WAN optimization deployments because it keeps the appliance operating within its purchased capacity and helps avoid resource contention caused by traffic growth or an unusually high number of concurrent optimized sessions. Admission Control is therefore a capacity-protection mechanism tied to the SteelHead's licensed throughput and optimized-connection entitlements. Riverbed describes SteelHead as its WAN-optimization platform and provides product and documentation resources at Riverbed SteelHead and Riverbed Product Documentation.

QUESTION NO: 12

By default, when a SteelHead fails, either by power loss or optimization service failure, the appliance:

A. Blocks all traffic.

B. Routes all traffic.

C. Passes through all traffic.

ANSWER: C

Explanation:

"Passes through all traffic.

" is correct because SteelHead appliances deployed in-path are designed to preserve network availability if the appliance loses power or its optimization service fails. Their in-path network interfaces use a fail-to-wire (hardware bypass) mechanism. In normal operation, traffic is intercepted for WAN optimization; when the appliance cannot operate, the bypass path physically connects the LAN and WAN sides so ordinary network forwarding can continue without optimization. This behavior is commonly described as fail-open operation. It is important operationally because a SteelHead outage should remove acceleration, compression, and other optimization services, rather than create a site-wide connectivity outage. The default bypass behavior applies to supported in-path interface configurations and is a key reason organizations can deploy SteelHead transparently in the data path. Administrators should still validate cabling, interface configuration, and high-availability or redundancy design during deployment, since those factors determine whether the intended physical bypass path is available. Riverbed's product documentation and support resources describe SteelHead deployment and in-path networking behavior: Riverbed Documentation and Riverbed Support.

QUESTION NO: 13

Which of the following is a benefit of the Riverbed Services Platform (RSP) on the Steelhead appliance? (Select 2)

A. Optimizes VoIP flowing through proxy servers

B. Removes the need for specific servers in the branch offices

C. Allows for continued operations of specific functionality in the event of a WAN failure

D. Provides parallel forwarding domains for asymmetrical routing

ANSWER: B C

Explanation:

RSP enables a SteelHead appliance to host supported virtualized branch-office services directly on the appliance, rather than requiring separate dedicated hardware servers at every remote site. Therefore, *Removes the need for specific servers in the branch offices* is a key benefit: organizations can consolidate selected branch IT functions onto the SteelHead platform, reducing equipment footprint, power requirements, and remote-site administration. RSP was designed to extend the value of a SteelHead deployment beyond WAN optimization by providing a local execution environment for approved service applications.

Allows for continued operations of specific functionality in the event of a WAN failure is also correct because services hosted locally through RSP can remain available to branch users when the connection to centralized data-center resources is interrupted. This local availability supports business continuity for the particular application or service deployed at that branch; it does not imply that every centrally hosted application remains available. The combination of local service hosting and SteelHead WAN optimization helps organizations simplify branch infrastructure while preserving access to essential local functionality during WAN disruptions. See Riverbed's SteelHead product information and the Riverbed documentation portal for platform and deployment documentation.

QUESTION NO: 14

Which xx50 Steelhead appliance models provide both inpath0_0 and inpath0_1 interfaces without adding additional network cards? (Select 3)

A. Steelhead 550

B. Steelhead 6050

C. Steelhead 1050

D. Steelhead 250

E. Steelhead 2050

ANSWER: B C E

Explanation:

Steelhead 6050, Steelhead 1050, and Steelhead 2050 are the xx50 appliance models in this list that include the two-port in-path interface pair as part of their standard appliance network-interface configuration. Riverbed uses the paired interface names `inpath0_0` and `inpath0_1` for the LAN-side and WAN-side ports of an in-path connection. This pairing allows a SteelHead to be physically inserted between the LAN and WAN while maintaining the traffic path required for transparent WAN optimization. Because these models supply that initial in-path pair without requiring an optional network-interface card, they can be deployed in a basic in-path topology using their integrated interface capability. Additional supported cards can be used where further interface pairs, specific media types, or more complex deployment designs are needed, but they are not required merely to obtain this first in-path pair. Riverbed's product documentation portal provides the appliance installation and hardware documentation that identifies platform interfaces and deployment connections: Riverbed Documentation. Riverbed also maintains SteelHead platform information and WAN-optimization resources at Riverbed SteelHead.

QUESTION NO: 15

True or False? SteelHead SaaS can provide Netflow and SteelFlow to other Riverbed products to monitor and troubleshoot SaaS performance issues.

A. True

B. False

ANSWER: A

Explanation:

True is correct. SteelHead SaaS provides WAN optimization for sanctioned SaaS applications while also supplying traffic-visibility information that can be consumed by Riverbed's performance-management and troubleshooting products. NetFlow exports summarize observed traffic into flow records, including useful attributes such as endpoints, protocols, ports, volumes, and timing. SteelFlow provides Riverbed-specific flow visibility and context that enables Riverbed monitoring tools to associate traffic with applications and users more effectively. This telemetry allows operations teams to investigate SaaS experience issues using the same Riverbed visibility ecosystem used for other enterprise traffic, rather than treating optimized SaaS traffic as opaque. In practice, flow data supports analysis of who is using a SaaS service, how much traffic is involved, where performance degradation is occurring, and whether a condition is isolated or widespread. These integrations complement SteelHead SaaS optimization by making SaaS performance observable and actionable through Riverbed monitoring workflows. Riverbed describes its SteelHead platform and associated visibility capabilities at Riverbed SteelHead; product documentation and release-specific configuration guidance are available through the Riverbed Documentation Portal.

QUESTION NO: 16

An employee who has just installed Steelhead Mobile onto her workstation notices that she never gets any reduction. It always says 0%.

The status of the mobile client appears to Be:

Optimization State: Firewalled

Controller Status: Connected

The reason she is seeing 0% reduction statistics is:

A. Location Awareness is in effect

B. The physical branch Steelhead appliance in her office is behind a firewall

C. The office firewall is stripping the IP options field

D. Her workstation is blocking TCP port 7801

E. The data center is currently firewalling all optimized connections

ANSWER: D

Explanation:

Her workstation is blocking TCP port 7801. A Steelhead Mobile client can be successfully connected to its Mobile Controller while still being unable to establish the optimization connection required to a SteelHead appliance. These are separate functions: the Controller Status confirms that the client can communicate with the management/control service, whereas an Optimization State of *Firewalled* identifies that the optimization path is not reachable through the network or host firewall policy.

Steelhead Mobile requires TCP port 7801 for its optimized connection to the remote SteelHead infrastructure. If the local workstation firewall blocks outbound TCP 7801, the Mobile Controller can remain connected, but user traffic cannot enter the Steelhead optimization process. Consequently, no optimized bytes are recorded and the client reports a persistent 0%

reduction rate. Restoring outbound access to TCP 7801 from the workstation to the applicable SteelHead peer allows the client to establish its optimized session and begin reporting reduction statistics.

Riverbed product documentation and deployment guidance are available through the Riverbed Documentation portal and the Riverbed Support portal.

QUESTION NO: 17

Automatic registration of devices with the SteelCentral Controller for SteelHead (SCC) requires which one of the following?

A. RiOS 8.0 for SteelHead and 4.0 for Interceptor

B. The SCC must have joined the Windows domain

C. Pre-trusted SSL certificates on the devices and SCC

D. The serial number of the managed device to be preconfigured in the SCC

E. The name “riverbedcmc” to be an entry in DNS resolving to the SCC primary IP address

ANSWER: E

Explanation:

The name “riverbedcmc” to be an entry in DNS resolving to the SCC primary IP address is required for automatic device registration. SteelHead appliances use this well-known DNS name to discover the SteelCentral Controller for SteelHead automatically, rather than requiring an administrator to specify the controller address individually on every managed appliance. The DNS record must resolve to the primary IP address of the SCC so that devices can reliably initiate registration and establish management communication with the active controller. This approach supports scalable deployment: once the appropriate DNS entry is available to the devices, eligible SteelHead appliances can locate SCC and register without serial-number preconfiguration or a domain-membership dependency. Riverbed documentation describes SCC as the centralized management platform for SteelHead appliances and identifies DNS-based controller discovery as part of automatic registration deployment requirements. See the Riverbed documentation portal for SteelCentral Controller for SteelHead deployment guides, and the Riverbed Support Portal for the applicable SCC and RiOS product documentation.

QUESTION NO: 18

What are two methods that can be configured to provide location awareness for a Steelhead Mobile client? (Select 2)

A. Adapter based configuration

B. Fixed-target rule

C. In-path rule

D. Latency detection

ANSWER: A D

Explanation:

Steelhead Mobile location awareness allows the client to determine whether it is operating on an enterprise network or from a remote location, so that it can apply the appropriate optimization behavior and connect to the suitable SteelHead infrastructure. **Adapter based configuration** is a location-awareness method because the client can identify a location from characteristics of the active network adapter and its associated network configuration. This enables administrators to associate known adapter or network attributes with a specific location profile.

Latency detection is also a location-awareness method. The client can use measured latency to determine whether a configured target is appropriately reachable for the client’s current network location. This approach is useful when adapter characteristics alone are insufficient or when users move between networks whose adapter settings are similar but whose

path characteristics differ. Together, adapter-based identification and latency-based detection provide location awareness for mobile users whose connectivity changes frequently. Riverbed product documentation and support resources are available through the Riverbed Support Portal and the Riverbed Documentation portal.

QUESTION NO: 19

If an administrator wanted to compare the performance of Microsoft file sharing across the WAN for two clients with and without Riverbed optimization, what strategy could you use to enable this testing?

A. In-path rule on client-side Steelhead appliance to pass through port 139 and 445 for the source IP of one of the test clients

B. Disable optimization on the Steelhead appliance

C. In-path rule on server-side Steelhead appliance to pass through port 139 and 445 for the source IP one of the test clients

D. A and C

ANSWER: A

Explanation:

In-path rule on client-side Steelhead appliance to pass through port 139 and 445 for the source IP of one of the test clients is correct. Microsoft file sharing using SMB/CIFS normally uses TCP ports 139 and 445. An in-path rule can identify traffic by source IP address and destination port, then specify that matching traffic is passed through rather than intercepted and optimized. Applying this rule on the client-side SteelHead for one test client creates a controlled comparison: that client's SMB traffic traverses the WAN without SteelHead optimization, while SMB traffic from the other client continues to be intercepted and optimized normally. Because both clients can access the same remote file-sharing service across the same WAN environment, the administrator can compare transfer time, responsiveness, and observed throughput while changing only the optimization treatment. This approach is preferable for a test because it targets the intended client and application ports without disabling optimization broadly for unrelated users or traffic. Riverbed's SteelHead platform is designed to apply WAN optimization selectively according to traffic-handling policy and deployment configuration. See the Riverbed SteelHead product overview and the Riverbed Support and documentation portal for SteelHead configuration documentation.

QUESTION NO: 20

A SteelHead is joined to a Windows Active Directory domain using the administrator password. In order to optimize SMB2 traffic, which of the following is true?

A. SMB2 optimizations must be enabled on the server-side SteelHead only.

B. A delegation or replication account must be configured on both the client-side and server-side SteelHead.

C. SMB2 optimizations must be enabled on both the client-side and server side SteelHeads.

D. A delegation or replication account must be configured on the client-side SteelHead.

ANSWER: B

Explanation:

A delegation or replication account must be configured on both the client-side and server-side SteelHead. Joining a SteelHead appliance to Active Directory with an Administrator credential establishes the appliance's domain membership, but that credential is not the ongoing credential mechanism used for SMB optimization. SMB2 optimization requires the SteelHeads to interact appropriately with Active Directory and SMB authentication so that optimized connections can be established while preserving the user and server security context. A dedicated delegation or replication account provides the required AD permissions for this process. The account configuration is required at each end because the client-side and server-side SteelHeads each participate in the optimized SMB flow and must be able to perform their respective authentication-related functions. In production, Riverbed best practice is to use a dedicated, least-privilege service account rather than relying on a highly privileged domain Administrator account after the initial domain-join operation. This separates

appliance administration from the credentials and permissions needed for SMB optimization, improves auditability, and limits the impact of credential exposure. Riverbed's SteelHead documentation and support resources are available through the Riverbed Documentation portal and the Riverbed Support portal.

QUESTION NO: 21

What WAN traffic problems do Steelhead appliances overcome? (Select 3)

A. Number of connections per second

B. Data deduplication

C. Bandwidth

D. Latency

E. TCP window size

F. Optimization

ANSWER: C D E

Explanation:

SteelHead appliances address the principal conditions that make applications perform poorly across WAN links: constrained bandwidth, WAN latency, and TCP window-size limitations. Bandwidth is conserved through data reduction techniques that avoid repeatedly transmitting redundant data, allowing more useful application traffic to traverse a limited link. Latency is mitigated through transport and application-protocol optimization, reducing the impact of round trips that would otherwise delay transactions, file operations, and interactive application responses. TCP window size is relevant because the amount of unacknowledged data a sender may have in flight directly affects achievable throughput, especially on high-bandwidth, high-latency paths. SteelHead's TCP optimization improves use of the available WAN path and helps overcome throughput constraints associated with TCP behavior over long-distance links. Together, these capabilities improve application performance without requiring an equivalent increase in WAN capacity. Riverbed describes SteelHead as a WAN optimization platform that accelerates applications by addressing WAN bandwidth and latency challenges: Riverbed SteelHead. The relationship between TCP window capacity, round-trip time, and performance on high-bandwidth paths is also defined in RFC 7323: TCP Extensions for High Performance.

QUESTION NO: 22

In order to achieve SteelHead SaaS optimization two things must happen. First acquire and install a subscription license to enable the feature, and then SteelHead SaaS must be configured.

Which statement correctly describes the configuration step?

A. Every SteelHead is configured with a registration key included in a RiOS upgrade.

B. All the configuration is done from the Riverbed Cloud Portal.

C. Every SteelHead is configured with a new license in the standard form LK1-SHSaaS-XXX.

D. Every SteelHead is configured with the same registration key copied from the Riverbed Cloud Portal.

ANSWER: D

Explanation:

Every SteelHead is configured with the same registration key copied from the Riverbed Cloud Portal. After the SteelHead SaaS subscription is installed, the Riverbed Cloud Portal provides the registration key that associates an on-premises SteelHead with the organization's SaaS optimization service. This key is entered in the SteelHead SaaS configuration on each participating SteelHead. It is an organization-level registration credential, so the same key is used across the

SteelHeads that are to participate in that organization's SaaS optimization deployment; it is not a distinct key generated by a RiOS upgrade or a separate standard appliance license for each device.

The Cloud Portal remains the centralized service-management location, including SaaS application and policy-related service configuration, while the SteelHead must still be registered locally using the portal-issued key. This registration enables the appliance to communicate with and use the subscribed SteelHead SaaS service. Riverbed's SteelHead product information is available at Riverbed SteelHead, and deployment documentation and software-specific administration resources are available through the Riverbed Support Portal.

QUESTION NO: 24

Which of the following reflects the primary benefit of configuring CIFS prepopulation on a Steelhead appliance?

A. Prelearning different CIFS dialects on the network

B. Prewarming the datastore

C. CIFS management reporting

D. Management Streamlining

ANSWER: B

Explanation:

Prewarming the datastore is correct because CIFS prepopulation proactively reads selected files from a CIFS/SMB share and places the relevant data into the SteelHead appliance's RiOS datastore before users request those files across the WAN. This prepares the optimization system with the data segments it needs to recognize and reference during subsequent client file access. When a branch-office user later opens a prepopulated file, the SteelHead can use data already present in its datastore rather than having to learn that content during the user's initial transfer. The practical benefit is improved performance for the first user access to important or frequently used file sets, especially after a deployment, a datastore reset, or a period in which the appliance has not yet observed normal file-access traffic. Prepopulation is therefore a deliberate cache-warming mechanism for CIFS/SMB file data, allowing WAN optimization benefits to be available sooner for targeted content. Riverbed SteelHead is designed to optimize application and file-transfer traffic over WAN links; CIFS prepopulation supports that purpose by preparing the datastore in advance. See the Riverbed documentation portal and the Riverbed SteelHead product overview.

QUESTION NO: 25

A server side SteelHead deployment is to be out-of-path (SSOOP).

Which of the below are limitations compared to physical or virtual in-path? (Choose two.)

A. Auto discovery is not supported.

B. Port or full transparency is not supported.

C. Only one SteelHead is supported on the server side.

D. Data store synchronization is not possible.

E. Only enhanced auto discovery can be used.

ANSWER: A C

Explanation:

In a server-side out-of-path deployment, the server-side SteelHead does not sit transparently in the traffic path. Consequently, it cannot use the normal SteelHead peer-discovery behavior that an in-path appliance uses to identify and intercept optimized connections automatically. The deployment must instead rely on explicit traffic-steering and configuration

methods appropriate to the out-of-path design. Therefore, **"Auto discovery is not supported."** is a documented operational limitation of SSOOP.

Also, an SSOOP design supports only one server-side SteelHead for a given server-side deployment. Unlike physical or virtual in-path deployments, where topology and high-availability/load-sharing designs can provide more flexible server-side appliance arrangements, SSOOP does not support multiple server-side SteelHeads for this role. Thus, **"Only one SteelHead is supported on the server side."** is also a limitation. These constraints should be considered during design, particularly when selecting traffic-steering methods and planning capacity or resiliency at the data-center side. Riverbed's SteelHead product documentation and support resources provide the applicable deployment guidance: Riverbed Documentation and Riverbed Support.

QUESTION NO: 26

Assuming the Steelhead appliance has a 250 GB datastore capacity, by enabling RSP on a supported Steelhead appliance which of the following would be true:

A. The datastore capacity will shrink due to the amount of space used by RSP

B. The datastore capacity will grow due to the amount of space added by RSP

C. The datastore capacity does not change

D. The datastore capacity will have to be reformatted

ANSWER: A

Explanation:

The datastore capacity will shrink due to the amount of space used by RSP is correct. Riverbed Services Platform (RSP) enables a supported Steelhead appliance to host a service virtual machine, but it does not add physical disk capacity to the appliance. Instead, RSP reserves a portion of the appliance's existing local disk resources for its virtual-machine and service-platform requirements. Consequently, if the appliance initially has a 250 GB datastore available for Steelhead data reduction and optimization use, the usable datastore is reduced after RSP is enabled by the capacity allocated to RSP. The exact amount reserved depends on the Steelhead model, software release, and RSP configuration, but the key operational point is that the allocation comes from existing disk capacity. Administrators should therefore account for the lower remaining datastore when planning optimization performance, because the datastore holds data used by Steelhead optimization features. Riverbed identifies SteelHead as its WAN optimization platform and provides product and documentation resources through its official product and support sites: Riverbed SteelHead product information and Riverbed Support and documentation portal.

QUESTION NO: 27

When performing a logical in-path deployment, which interface needs to be physically cabled for optimization to occur?

A. LAN

B. AUX

C. WAN

D. Primary

ANSWER: D

Explanation:

Primary is correct. In a logical in-path deployment, the SteelHead is not physically inserted inline between the LAN and WAN segments. Instead, the network redirects selected traffic to the SteelHead using a routing or traffic-redirection method, such as policy-based routing or WCCP. The appliance receives and returns this traffic through its Primary interface, so that interface must have physical network connectivity for the SteelHead to participate in the optimized flow.

This deployment method is useful where inserting the appliance directly into the data path is impractical or where the network design requires traffic steering at a router or switch. Once traffic reaches the Primary interface, the SteelHead can identify eligible TCP connections, apply its WAN-optimization techniques, and send the optimized traffic back toward the redirecting network device. The logical role of the deployment is provided by the network's redirection configuration; it does not require a physical inline LAN-to-WAN connection through dedicated in-path ports.

Riverbed's official documentation portal provides SteelHead deployment and configuration documentation: Riverbed Documentation. Additional product support resources, including deployment guides, are available at Riverbed Support.

QUESTION NO: 28

What basic configuration steps should be done on the SteelHead before attempting to join it to a Windows Domain? (Choose two.)

A. Configure either a Delegation or Replication user.

B. Configure DNS to include an entry for resolution of the SteelHead primary interface IP address.

C. Enable SMB signing/Encrypted MAPI support.

D. Ensble NTP and ensure time is synced with domain controllers.

ANSWER: B D

Explanation:

Before a SteelHead can join a Windows domain, its primary interface must be resolvable through the domain DNS infrastructure. Configuring DNS to include an entry for resolution of the SteelHead primary interface IP address provides the forward hostname lookup needed for domain integration. In practice, this means creating an appropriate host (A) record for the SteelHead and configuring the appliance to use DNS servers that can resolve the domain and its domain controllers. Reliable DNS resolution lets the appliance locate the required Active Directory services using fully qualified domain names.

Enabling NTP and ensuring time is synchronized with domain controllers is also essential. Windows domain authentication relies on Kerberos, which has strict time-skew tolerances between participating systems. Synchronizing the SteelHead with the same reliable NTP time source used by the domain controllers helps ensure that authentication and domain-join operations succeed consistently. These two preparations address the core name-resolution and time-synchronization dependencies that must be in place before initiating the domain join. Riverbed's guidance for secure Windows environments describes the DNS hostname-resolution and synchronized-time prerequisites; see Riverbed: Optimization in a Secure Windows Environment. For background on Windows Time Service operation in Active Directory domains, see Microsoft Windows Time Service tools and settings.