DUMPSBOSS.

HCLSoftware U Certified Professional-BigFix Platform 1

HCL Software Academy HCL-BF-PRO-10

Version Demo

Total Demo Questions: 8

Total Premium Questions: 82

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An administrator is planning a BigFix deployment where 4,000 endpoints will be managed. The BigFix platform components will be installed using the default ports on the servers as follows:

• Server1 - BigFix Root Server, BigFix Client, database, Web Reports, and the WebUI

• Server2 - BigFix Client and Relay

• Server3 - BigFix Client and Relay

Which of the following ports must must be opened by the network team? (Choose two.)

A. 3443

B. 3033

C. 53211

D. 52311

E. 9031

ANSWER: D E

Explanation:

52311 is required for standard BigFix platform communication. By default, the BigFix Root Server, Relays, and Clients use this port to exchange BigFix messages, distribute content, receive reports, and relay client traffic through the deployment hierarchy. Because Server1 hosts the Root Server and Servers2 and 3 host Relays, network paths that permit the required BigFix traffic on port 52311 are fundamental to endpoint management in this topology. HCL documentation identifies 52311 as the default listening port for BigFix server, relay, and client communications; firewall and routing rules must allow the applicable TCP traffic between these components. See HCL's network configuration requirements.

9031 is the default HTTPS port used to provide browser access to the BigFix WebUI in this deployment. Since Server1 hosts the WebUI, administrators and other authorized users need network access to that service on port 9031. Opening this port allows users to reach the WebUI securely from their web browsers while preserving the default port configuration stated in the scenario. HCL's WebUI documentation describes the WebUI installation and connection requirements, including its web-service port configuration: BigFix WebUI documentation.

QUESTION NO: 2

How is the Site Administrator key generated?

A. It is generated during installation.

B. It is generated through the Bigfix License Portal.

C. It is generated by BigFix Support and attached to your license.

D. It is generated at the command line using openssl.

ANSWER: A

Explanation:

It is generated during installation. The Site Administrator key is created as part of the BigFix Server installation and initial deployment configuration. During this process, the installer requires the designated site administrator to establish protection for the private key, typically by supplying the password used to encrypt it. This key is a deployment-specific private credential rather than a key issued from an external licensing service or a generic cryptographic key created independently by an administrator.

The Site Administrator key establishes the authority needed for core site-level administration. It is used by BigFix administrative tooling and supports operations that must be digitally authorized for the deployment, including creation and maintenance of the masthead and configuration of central platform settings. Protecting the password and the resulting private-key material is therefore essential: anyone who obtains both could potentially perform sensitive administrative actions for the BigFix deployment. The installation workflow intentionally generates the key in the server environment so that the deployment begins with its own unique administrative identity and securely protected signing capability.

For the documented installation and Site Administrator procedures, see the HCL BigFix documentation on generating the Site Administrator private key and the HCL BigFix Site Administrator documentation.

QUESTION NO: 3

During a BigFix platform upgrade, which of the following version rules must be respected for the various components?

A. server version = relay version = client version

B. server version < relay version >= client version

C. server version >= relay version <= client version

D. server version >= relay version >= client version

ANSWER: D

Explanation:

The required version relationship is **server version >= relay version >= client version**. BigFix infrastructure components must be upgraded in a controlled, top-down sequence so that each downstream component is supported by the component with which it communicates. The BigFix Server is the authoritative platform component and must be at the same release level as, or a later supported release level than, its Relays. Similarly, every Relay must be at the same release level as, or a later supported release level than, the BigFix Clients that report through it. This relationship permits staged upgrades: first upgrade the server infrastructure, then relays, and finally clients. During that staged period, older clients can continue to communicate through relays that are no older than those clients, while those relays communicate with a server that is at least as current as the relays. Maintaining this ordering protects compatibility across the reporting and content-distribution path and is a core BigFix upgrade planning requirement. HCL's upgrade documentation describes the supported upgrade paths and the component upgrade sequence; administrators should confirm the target release's specific path and prerequisites before performing the upgrade. See HCL BigFix upgrade paths and upgrading BigFix on Windows systems.

QUESTION NO: 4

Which of the following statements regarding Baselines are true? (Choose two.)

A. Baseline components are pointers to their corresponding source Fixlets.

B. Baseline components can get out of synchronization with their source Fixlets.

C. Baselines can only be created by Master Operators.

D. Baselines cannot include more than 100 components.

E. Baselines can include other Baselines as components.

F. Baselines are collections of Fixlets and Tasks that can be deployed with a single action.

ANSWER: B F

Explanation:

Baseline components can get out of synchronization with their source Fixlets because a Baseline stores component content as part of the Baseline rather than maintaining a live pointer to the source content. When the source Fixlet or Task is revised, the component in an existing Baseline does not automatically inherit that revision. BigFix Console provides synchronization

capabilities so an operator can review and bring Baseline components in line with available source updates before deploying the Baseline. This makes synchronization an important part of maintaining Baselines that are reused over time.

Baselines are collections of Fixlets and Tasks that can be deployed to relevant endpoints as a single action. They enable operators to package a related set of remediations, configuration steps, or updates into one manageable deployment while retaining component-level applicability and execution settings. This is useful for repeatable operational workflows such as preparing devices for a standard configuration or applying a coordinated set of patches. HCL documentation describes Baselines as a mechanism for grouping Fixlets and Tasks, and explains how component synchronization helps maintain their content. See HCL BigFix: Baselines and HCL BigFix: Introducing Baselines.

QUESTION NO: 5

What is the purpose of the Four Eyes Approval feature?

A. It is used by the BigFix client to authenticate a BigFix operator's deployed actions.

B. It is used to enforce complex BigFix console operator passwords.

C. It is used to prevent console operators from unilaterally taking actions on the endpoints within their control.

D. It is used during the creation of BigFix operators to ensure uniformity.

ANSWER: C

Explanation:

It is used to prevent console operators from unilaterally taking actions on the endpoints within their control. Four Eyes Approval implements a separation-of-duties control for BigFix actions: an operator designated as requiring approval can prepare and request an action, but the action cannot proceed until a different authorized console operator approves it. The approver must belong to the role selected for the requesting operator, ensuring that the approval is performed by someone with the intended authority rather than by the person initiating the action. This safeguard is particularly valuable for actions with broad endpoint impact, such as deployments, configuration changes, or other operational tasks that should be reviewed before execution. It reduces the risk of accidental, inappropriate, or unauthorized endpoint changes while retaining the ability to delegate normal action creation to operational teams. In BigFix, the capability is enabled through the relevant advanced configuration setting and then applied through operator settings and approver roles. HCL documents the feature and its configuration in the BigFix Four Eyes Approval documentation and describes operator and role administration in the BigFix Console operator settings documentation.

QUESTION NO: 6

A new BigFix Client is installed using the deployment masthead. The client must be able to locate the BigFix deployment and validate the trusted content that it receives.

Which information is supplied by the masthead? (Choose two.)

A. BigFix Server communication information

B. Public-key information used to verify signed content

C. The Site Administrator private key password

D. The SQL Server database credentials

E. Private keys for signing Custom Site content

ANSWER: A B

Explanation:

The masthead contains the communication information that allows a Client to locate the BigFix deployment, including the Server URL information used to establish its initial connection. It also contains public-key information that enables the Client to validate digitally signed BigFix content.

The masthead does not contain private keys or Site Administrator passwords. Those credentials must remain protected on the server and must never be distributed to managed endpoints. A client also does not require a separate SQL Server connection because it reports through the BigFix communication hierarchy rather than connecting directly to the BigFix database.

QUESTION NO: 7

An operator is troubleshooting an Action Script that uses one of the hidden process commands.

Which of the following statements are true? (Choose two.)

A. runhidden starts a process without displaying its window and continues to the next Action Script line without waiting for completion.

B. waithidden starts a process without displaying its window and waits for the process to finish.

C. runhidden waits for the process to finish but displays its window to the logged-on user.

D. waithidden can be used only when the action is running on a Relay.

E. wait and waithidden both continue to the next line before the launched process completes.

ANSWER: A B

Explanation:

`runhidden` starts the specified process without displaying its window, but the BigFix Client continues immediately to the next Action Script line. It is appropriate only when the subsequent commands do not depend on that process having finished.

`waithidden` also starts the process without displaying its window, but it waits for the process to terminate before the action continues. This is appropriate when later commands depend on the result of the program, such as checking an exit-dependent file or deleting an installation package after installation completes.

QUESTION NO: 8

An administrator needs to reconfigure a proxy server on a Windows BigFix Root server. How does this get accomplished?

A. By updating a Client Setting named BESClient Comm Proxy.

B. By running the command BESAdmin.exe /setproxy from the BES Server folder.

C. By installing the Proxy Bypass plugin on the Root Server.

ANSWER: B

Explanation:

Running `BESAdmin.exe /setproxy` from the BES Server folder is the supported method for configuring or reconfiguring the proxy used by a Windows BigFix Root Server. BESAdmin is the administrative command-line utility installed with the BigFix server components, and its proxy configuration command records the applicable proxy connection settings for the server. This is important because the Root Server may require an outbound proxy to reach external services, such as BigFix content sites or internet-based downloads, while retaining the server's normal responsibilities for relaying content and gathering data within the deployment. The command should be run by an administrator on the Root Server, using the BES Server installation directory, so that it updates the server-level configuration in the expected context. After entering the proxy details, administrators should confirm that the configured proxy permits the required outbound destinations and

authentication method, if applicable. HCL's platform documentation identifies BESAdmin as the tool for server administration and configuration; see the Using the BESAdmin tool documentation and the BESAdmin command reference.