Course Outline

ProTech Professional Technical Services, Inc.

HCL BigFix Operator Fundamentals + Compliance

Course Summary

Description

BigFix combines endpoint and security management into a single solution that enables users to see and manage fixed, mobile, physical and virtual endpoints on more than 90 different operating system versions. In addition to ensuring that all of a company's systems are patched and secure, BigFix automates time-intensive tasks across complex networks, queries endpoints in real-time for the presence of malicious files, allows for quick software installations, performs advanced automation, and allows for simple remote control with just a few clicks. This course will present knowledge to help BigFix administrators and operators develop the foundation knowledge they need to successfully leverage BigFix in their managed environments.

BigFix Compliance enforces continuous compliance with security policies throughout an organization for every endpoint both on and off the corporate network. It includes out-of- the-box support for most popular security benchmarks published by CIS, DISA STIG, USGCB and PCI-DSS. An intelligent agent on every endpoint monitors, enforces and reports on the security configuration status of the endpoints in real-time regardless of OS type or location. In this course, students will learn to interact and operate the BigFix Compliance solution. They will gain a solid understanding of the various components of the solution and will be able to configure, operate, develop reports, perform maintenance tasks, and troubleshoot BigFix Compliance.

Objectives

After taking this course, students will be able to:

- Gain a basic understanding of the BigFix portfolio and architecture
- Learn to use and configure the operator Console
- Explore and learn to use the BigFix Web User Interface
- Learn about Fixlets, Tasks, and Baselines and when to use them
- Learn about Roles and Users
- Explore Patch Content
- Create and deploy patches manually and through automation by using policies
- Explore and create Web Reports
- Understand Key BigFix Compliance Concepts
- Understand the Features and Functions of BigFix Compliance
- Learn to Configure and Operate BigFix Compliance
- Create custom reports including creating groups; checklist targeting and exception
- Understand how to maintain BigFix Compliance
- Be able to perform basic troubleshooting techniques

Topics

- Discuss architecture and component configuration
- Perform daily operations to support managed environment
- Find and Deploy Patches for managed endpoints
- Report on managed environment
- Perform basic troubleshooting
- Overview including key concepts, features and functions of BigFix Compliance
- Design and install BigFix Compliance (architecture, infrastructure, and implementation)
- Configure and Operate BigFix Compliance including Navigation and Checklists
- Create a wide variety of reports for different stakeholders in the organization
- Deployment tasks and technologies
- Maintain BigFix Compliance
- Troubleshoot BigFix Compliance including Disaster Recovery planning

HCL BigFix Operator Fundamentals + Compliance

Course Summary (cont'd)

Audience

This course is designed for BigFix administrators and operators.

Prerequisites

Before taking this course, students should have basic Microsoft Windows experience.

Duration

Four days

Course Outline

HCL BigFix Operator Fundamentals + Compliance

Course Outline

I. Introduction
- A. Welcome to the BigFix Family!
- B. What can BigFix do for you?
- C. Identifying the BigFix suite components.
- D. A modular approach to meeting your operational requirements.
- E. Let's take a look at the latest and greatest features of BigFix.

II. Architecture
- A. How BigFix works under the covers.
- B. Message flow - Discovering the flow of how action directives make it to endpoints and back to the BigFix server.

III. Console Operation
- A. Let's discover the console!
- B. Workflow – Get your work done with the BigFix Console
- C. Optimizing your BigFix Console experience

IV. Web User Interface
- A. What is the Web UI?
- B. Navigating the Web UI
- C. Discovering the Apps menu
- D. How do I find patches in the Web UI?
- E. Let's deploy some patches!
- F. Looking for something? Let's learn about Query
- G. Headaches keeping up with patches? Let's automate with policies!

V. Content and Sites
- A. What is content?
- B. What are Fixlets, Tasks and Baselines and when should I use them?
- C. Take Action!
- D. Discovering Analyses and Properties
- E. How to use custom computer properties to unleash the power of BigFix
- F. Get organized with Content Sites!
- G. Learn how to secure your BigFix Environment using Roles and Users
- H. Minimize administrative overhead using Computer Groups!

VI. Patches
- A. Structure of a Patch in BigFix
- B. Patch-specific Features and how to use them
- C. Where do patches come from?
- D. Are patches for all operating systems created equal?
- E. Patch Process: Is there a method to the madness?
- F. How are patches deployed?
- G. Customizing deployments to fit any situation

VII. Advanced Patch Management
- A. To Deploy or not to deploy: Superseded Fixlets
- B. Blacklisting: Hiding undesirable content
- C. Whitelisting: Showing only what you want them to see
- D. Automating deployments using execution parameters
- E. Configuring and deploying non-Windows patches
- F. Set and Forget: WebUI Patch Policies
- G. Patch Sequencing across multiple endpoints
- H. Troubleshooting

VIII. Everything you need to know about Web Reports
- A. Configure and use web reporting
- B. How to access the Web Reports Interface
- C. List and generate existing reports
- D. Explore and Filter Data
- E. Create Custom Reports
- F. Export Report Data

Schedule Reports to be automatically generated and mailed

Course Outline

HCL BigFix Operator Fundamentals + Compliance

Course Outline (cont'd)

IX. Overview

A. Introduction, covering: benefits and advantages; the BigFix portfolio and adjacent products; roles and responsibilities; compliance motivators (Business Needs, IT Needs)
B. Key Concepts, including: security vs. compliance; checklists and parameters; reporting; and enforcement
C. Features and Functions, such as: enforcing compliance rules; reporting on compliance; and automation of process

X. Plan and Install

A. Architecture of Compliance, including: Scalability (BigFix architecture, checklists, data import); network design; firewalls, proxy servers, and ports; network planning; and reporting groups
B. BigFix Platform and Compliance Infrastructure, covering: server and database requirements; disk space; permissions; licensing & masthead; installing BigFix Server, relays, and clients; security and access
C. Implementation of Compliance, including: installing the Compliance analytics server; subscribing systems to checklists; configuring data source connection; mail server settings; roles; server settings; session settings; and user provisioning

XI. Configure and Operate

A. Navigation, such as: interface navigation and customization, setting default views, creating custom views
B. Using checks and checklists, including: check Fixlets; modifying check parameters; activating Measured Value Analyses; creating and managing Custom Checklists; using the Synchronize Custom Checks wizard; taking a remediation action; importing SCAP content; using OVALDI and viewing Windows Vulnerabilities for Oval bulletins
C. Exception management
D. Reporting, including: running and exporting reports; reviewing existing built in overview and list reports; and customizing reports
E. Computer Grouping, covering: creating computer groups for reporting; checklist targeting and exception; computer properties from BigFix

XII. Maintain

A. Compliance Application management, such as: Extract, Transform, Load monitoring and management; and database management
B. BigFix Platform management, including: Fixlet site version; Platform updates and upgrades; process start and stop procedures; and backup & restore

XIII. Troubleshoot

A. Disaster Recovery planning, covering: backing up the Application Server; and successful recovery from a failure
B. Support resources, including log locations; VM Manager command line options; manual catalog updates; support; Forums and self-help