Cloud & Smarter Infrastructure Professional Certification Program

Study Guide Series

Exam C2010-521 - IBM Certified Deployment Professional - Endpoint Manager V9.2

Purpose of Exam Objectives

When an exam is being developed, the Subject Matter Experts work together to define the role the certified individual will fill. They define all of the tasks and knowledge that an individual would need to have in order to successfully implement the product. This creates the foundation for the objectives and measurement criteria, which are the basis for the certification exam.

The Tivoli Certification item writers use these objectives to develop the questions that they write and which will appear on the exam.

It is recommended that you review these objectives. Do you know how to complete the task in the objective? Do you know why that task needs to be done? Do you know what will happen if you do it incorrectly? If you are not familiar with a task, then go through the objective and perform that task in your own environment. Read more information on the task. If there is an objective on a task there is about a 95% chance that you WILL see a question about it on the actual exam.

After you have reviewed the objectives and completed your own research, then take the assessment exam. While the assessment exam will not tell you which question you answered incorrectly, it will tell you how you did by section. This will give you a good indication as to whether you are ready to take the actual exam or if you need to further review the materials.

Note: This is the high-level list of objectives. As you review these objectives, click for a more detailed level of how to perform the task.

High-level Exam Objectives

Section 1 - Planning	
1.1	Given the need to implement IBM Endpoint Manager (IEM) in a customer's network, and possessing an understanding of IEM, define IEM system requirements so that information about the customer's environment has been gathered to make system recommendation surrounding disaster recovery, remote database , and console requirements in order to meet the customer's uptime requirement.
1.2	Given the need to implement IEM in a distributed environment, plan and define the IEM relay architecture so that a IEM relay architecture has been designed which minimizes network impact and ensures the performance, reliability, and scalability of IEM is produced.
1.3	Given an upcoming IEM installation and knowledge about the network environment in which it will be installed, identify the best strategy for the installation so that there is a higher likelihood of a successful deployment.
1.4	Given having an understanding of IEM and the requirement to implement IEM, discuss the IEM security model so that the various options for security in IEM are understood.
1.5	Given an understanding of IEM and the requirement to integrate IEM with existing customer systems, discuss the IEM integration capabilities, so that the various APIs for IEM integration are understood.
Section 2 - Installation	
2.1	Given the appropriate server hardware and operating system, a IBM Endpoint Manager (IEM) license key and administrative permissions, install the IEM server and Web Reporting so that IEM has been installed on the appropriate server.
2.2	Given a functional IEM server installation and relay compatible agents checked into the IEM console, deploy the IEM relay so that load is distributed from the main IEM server and network traffic is reduced.
2.3	Given an operational IEM server, IEM console, a candidate computer in the DMZ to serve as a IEM relay, and coordination with the organization's networking and security teams, install an Internet facing relay so that IEM managed computers on the public Internet can still be actively managed.
2.4	Given an operational IEM server and console, install the IEM agent on computers so that they can be managed with the IEM environment.
2.5	Give the requirement to facilitate automation of processes that require communication with the IEM server and Web Reports, install the BES server Plugin service so that other IEM applications will be able to fully utilize IEM server functionality.
2.6	Given a functional IEM server, console, deployed agents and operator permissions, create manual or automatic computer groups so that computer target groups have been created based upon the customer's requirements.

2.7	Given functional IBM IEM relays, and deployed agents checked into the IEM console, configure relay affiliation so that agents report to the desired deployed IEM relays.
2.8	Given the appropriate server hardware and operating system, a IEM license key, and administrative permissions, install the replica IEM server and ensure Distributed Server Architecture (DSA) replication is functional so that there are two functional IEM servers replicating information between them.
2.9	Given an operational IEM Server with a local database, IEM Relay, IEM console, and IEM agent, perform a product upgrade from IEM 9.1 to IEM 9.2 using the IEM provided upgrade fixlets so that all of the latest IEM components are being used.
Section 3 - Componenent Configuration	
3.1	Given a functional IBM Endpoint Manager(TEM) server, and deployed agents checked into the IEM console, configure relay selection so that agents report to the desired deployed IEM relays.
3.2	Given that the IEM server is up and running, ensure that all endpoints are healthy and connected to the IEM server so that sufficient information has been gathered to determine whether the IEM endpoint agents are healthy and properly reporting into the IEM environment.
3.3	Given an IBM Endpoint Manager (IEM) server running on Windows needs to use an account other than SYSTEM for running the BES server services, and an account to run the service(s) as, configure the IEM service(s) to run as the different user so that the BES server services are running as an account other than SYSTEM.
3.4	Given a functional IBM Endpoint Manager (IEM) Server on a network that requires going through a proxy for Internet access, configure the IEM server to use the proxy so that content is successfully gathered and sites are successfully populated on the IEM server.
3.5	Given master operator access to the IEM environment and access to a console, manage roles and permissions within IEM so that users can effectively log in to the console and manage their endpoints.
3.6	Given an operational IEM server, console, master operator console account, and a valid IEM license, enable IEM content sites so that IEM solutions can be accessed from the console.
3.7	Given the reporting requirements of the customer, activate the appropriate set of analyses so that the IEM infrastructure will collect the desired data.
3.8	Given IEM components on a network infrastructure with bandwidth usage constraints, configure IEM agent and server settings so that TEM's bandwidth usage is controlled.
3.9	Given the requirement to remediate out of compliance agents, describe the settings available in an action so that proper options are used for making an action a policy.

3.10	Given the requirement to ensure actions are not performed on targets outside of maintenance windows, utilize the IEM Maintenance Window dashboard and client locking so that agents will automatically unlock at the beginning of the maintenance window and lock when the window is over.
3.11	Given an operational IEM server and IEM agent, deploy a custom agent setting so that all targeted IEM agents use the custom setting.
3.12	Given Web Report admin access and access to Web reports, manage roles and permissions within IEM so that users can effectively log in and use Web Reports.
3.13	Given an operational IEM server and console, use the IEM Administration Tool on Windows/Linux so that a user has the ability to administer masthead, system options, advanced options, replication and report encryption.
3.14	Given an operational IEM Administration Tool, IEM server, IEM relay, and IEM agent, configure report encryption and a decrypting relay so that all targeted IEM agents encrypt upstream data using Message Level Encryption and decryption occurs on a IEM relay instead of on the IEM server itself.
3.15	Given a functional IEM server on a network with no Internet access and an Internet-connected Windows machine on a different network, use the IEM Airgap tools to download IEM content on the Internet-connected computer so that site content and downloads are successfully populated on the IEM server.
3.16	Given a knowledge of the IEM platform components and content, describe the purpose and effect of IEM utilities, so that there is an understanding of how they an be used in management and troubleshooting of IEM deployment platform components and content.
Section 4 - Problem Determination and Performance Tuning	
4.1	Given that the IBM Endpoint Manager (IEM) server is up and running, use the IEM console to review the IEM Deployment Health Checks dashboard in conjunction with the Deployment Overview dashboard so that sufficient information has been gathered to properly gauge the health of the deployed components of a IEM installation.
4.2	Given an operational IEM server, IEM console, and a system running the IEM agent, enable debug logging so that all targeted IEM agents produce detailed logs for use in troubleshooting.
4.3	Given an operational IEM console, enable the IEM console debug menu so that a IEM console operator will have easy access to various tools useful in debugging IEM issues.
4.4	Given a IEM server with sub-optimal performance, identify the factors affecting performance so that they can be addressed.
4.5	Given a IEM server that is having issues gathering site content, troubleshoot the problem so it can gather site content and downloads.
4.6	Given a functional IEM server, console and relay, determine why IEM agent installations are failing by using the client deployment tool so that the source of the client deployment issue has been determined.

4.7	Given the requirement for IEM to efficiently transport large payloads, describe the steps required to troubleshoot an array of poorly performing IEM relays so that the issue with IEM relays can be diagnosed and resolved.
4.8	Given a functional IEM and a non-master operator in unable to see console content; determine the cause so that the issue can be resolved.
4.9	Given the need to manage an IEM environment by using Web Reports, describe how to resolve Web Reports technical issues so that Web Reports issues have been diagnosed and resolved.
4.10	Given an IEM agent that is not fully functional, perform the appropriate troubleshooting tasks so that the root cause can be identified and fixed appropriately leading to a functional agent.
4.11	Given an existing IEM deployment, troubleshoot and resolve issues related to filldb so that the data will be inserted into SQL/DB2 and inserted in to the console in a timely manner.
4.12	Given an issue with a fixlet/task not working as expected, troubleshoot the issue so that enough information has been gathered to determine the cause of the issue and resolve it.
4.13	Given that the new IEM server has already been set up, migrate all endpoints so that they are successfully reporting to the new IEM server.
Section 5	
5.1	Given the requirement to promote IBM Endpoint Manager to prospective customers, describe the purpose and capabilities of the IEM products, so that the customer understands the IEM product suite and how they can help with their business needs.
5.2	Given the need to install IBM Endpoint Manager (IEM) for Software Usage Analysis and that all pre-requirements including the database have been installed and configured, Install and configure IEM for Software Usage Analysis so that the desired reporting functionality will be fulfilled
5.3	Given a successfully installed IEM server, a master operator account and a license for IEM for Security Configuration Management, install IEM for Security Configuration Management so that endpoints' security configuration can be collected and measured.
5.4	Given a functional IEM server and a license from IBM for Patch Management functionality, configure the IEM server for patch management so that the IEM server is configured to deploy patches to endpoints.
5.5	Given that IEM is already installed and running, install and configure the Trend AntiVirus suite so that up to date virus patterns are automatically applied to the endpoints.
5.6	Given a functional IEM Server and a license from IEM for Server Automation, configure the IEM server for server automation, so that automation plans, middleware patching, and virtual host management can be enabled for endpoint management.
Section 6 - Custom Content	

6.1	Given the need to implement IBM Endpoint Manager (TEM) in a production environment, having an understanding of TEM, and having knowledge of the corporate organization in which IEM will be implemented it has been determined that a custom site will is required. Use the console to create a custom site ensuring that both operator accounts or roles and computers are subscribed appropriately so that the custom site is visible in the console with appropriate access granted to console operators and subscribed computers.
6.2	Given that IEM is installed, access to console and access to create custom content, create a custom fixlet so that a custom operation or package can be deployed.
6.3	Given a functional IEM console connected to the appropriate IEM server, create a property and a analysis so that custom information can be retrieved from an endpoint.
6.4	Given the requirement to maintain a consistent operating environment, create and maintain IEM baselines so that agents have the same operations and packages deployed.
6.5	Given a functioning Web Reports server, and a Web Reports user with appropriate permissions, create an explore data web report so that desired custom results can be retrieved.

Detailed Exam Objectives

Section 1 - Planning

1.1. Given the need to implement IBM Endpoint Manager (IEM) in a customer's network, and possessing an understanding of IEM, define IEM system requirements so that information about the customer's environment has been gathered to make system recommendation surrounding disaster recovery, remote database, and console requirements in order to meet the customer's uptime requirement.

SUBTASK(S):
1.1.1. Determine IEM server and database requirements.
1.1.2. Determine if database(s) will be local to application server or remote.
1.1.3. Determine application uptime and disaster recovery requirements.
1.1.4. Define requirements for remote databases.
1.1.5. Define replication frequency for Distributed Server Architecture.
1.1.6. Obtain necessary service accounts for database and internet access.
1.1.7. Determine number of console users.
1.1.8. Determine console requirements.
1.1.9. Gather a list of operating systems to be supported.

1.2. Given the need to implement IEM in a distributed environment, plan and define the IEM relay architecture so that a IEM relay architecture has been designed which minimizes network impact and ensures the performance, reliability, and scalability of IEM is produced.

SUBTASK(S):
1.2.1. Submit requests for network diagrams and other pertinent network architecture and configuration data.
1.2.2. Work with network and security teams to identify potential network port restrictions and firewall placement.
1.2.3. Submit requests to allow traffic on port 52311 between relay servers and upstream IEM relays and/or IEM servers.
1.2.4. Work with network team to analyze network topology and available bandwidth.
1.2.5. Determine where to place IEM relay servers and how many to deploy.
1.2.6. Work with server teams to identify or procure appropriate computer hardware to install the IEM relay servers on.
1.2.7. Determine relay selection techniques for each location.
1.2.8. Automatic vs Manual. Also consider the use of primary/secondary/tertiary relays and relay affiliation groups.
1.2.9. Consider relay selection for computers which move outside of the corporate network. Failover selection.
1.2.10. Document relay architecture and distribute for review and approval by all stakeholders.

1.3. Given an upcoming IEM installation and knowledge about the network environment in which it will be installed, identify the best strategy for the installation so that there is a higher likelihood of a successful deployment.

SUBTASK(S):

1.3.1. Determine appropriate IEM Server Platform

1.3.2. Determine agent deployment strategy.

- 1.3.2.1. Pre-existing software deployment tools - If a software deployment tool is already in use at an organization, leveraging it to install the IEM agent on all endpoints is generally the most effective deployment strategy.
- 1.3.2.2. IEM Client Deploy tool - The Client Deploy tool uses Active Directory or NT domain administrator credentials to push the agent to a list of computers via Windows SCM/RPC. If no existing software deployment tool is available, this is the easiest way to quickly and easily deploy a large number of agents. The Client Deploy tool directory is initially installed on the IEM server; however, it is self-contained and can be copied to any relay or other endpoint to allow further deployment into subnets not directly accessible from the IEM server.
- 1.3.2.3. Agent Deploy tool - The Agent Deploy tool connects to UNIX, Mac OS or Windows systems to deploy IEM agents to a set of systems at a time. It is a cross platform tool based on Java.
- 1.3.2.4. Login Script / GPO - The IEM agent can be run as a silent installation requiring no interaction with the end-user. This method can be used in any type of login script (Active Directory, NetWare, etc) to deploy the agent to end-user PCs at login time. Alternatively, a version of the IEM agent installer in MSI format is provided to allow installation of the agent by using an Active Directory GPO.
- 1.3.2.5. Manual / Other - The IEM agent can be installed manually as a last resort. The installer can also be put onto a Web server or Intranet server for one-click installation by end-users.
- 1.3.2.6. Define console connection method:
- 1.3.2.7. Remote console – console is installed on an administrator's computer on the same LAN as the IEM server.
- 1.3.2.8. Citrix / terminal server / remote desktop – console is installed on a virtual desktop on a terminal server on the same LAN as the IEM server.
- 1.3.2.9. Identify operator group requirements.
- 1.3.2.10. Identify required content/solutions.

1.3.3. Determine whether Message Level Encryption (MLE) is required for the network environment.

1.3.4. Determine whether Client Mailboxing is required to encrypt and sends data securely to individual computers.

1.4. Given having an understanding of IEM and the requirement to implement IEM, discuss the IEM security model so that the various options for security in IEM are understood.

SUBTASK(S):

1.4.1. There are two type of console users, local and remote.

- 1.4.1.1. Local console users can have password policies applied via IEM Administration Tool
  - 1.4.1.1.1. You can add LDAP associations to IEM. That allows you and other users to log in by using those credentials, piggybacking on your existing authentication scheme.
  - 1.4.1.1.2. You can use Microsoft Active Directory to handle authentication on IEM. That allows you and other users to log in to the console by using your Active Directory credentials, taking advantage of your existing authentication policies.
- 1.4.1.2. Client Authentication – Enables authentication on DMZ relays to manage roaming users more efficiently and prevent unauthorized access.
  - 1.4.1.2.1. Client MailBoxing – Encrypts and sends data securely to individual computers. This feature also enables actions to be sent directly to targeted endpoints rather then a broadcast over the deployment.
  - 1.4.1.2.2. MLE allows your agents to encrypt upstream data by using a combination of an RSA public/private key-pair and an AES session key.
  - 1.4.1.2.3. The RSA key-pair can be of 2048- or 4096-bit key length, with longer keys offering additional security, but requiring more processing power for decryption at the server. The AES session key uses the maximum FIPS-recommended length of 256 bits. You can configure your relays to reduce the load on the server by decrypting and repackaging the agent data before relaying it.
  - 1.4.1.2.4. The RSA public key encrypts the session key and adds it to the AES-encrypted report. At the IEM server (or a decrypting relay) the corresponding RSA private key is used to decrypt the AES session key, which is then used to decrypt the client report.
  - 1.4.1.2.5. Enhanced Security – Increases the cryptographic strength and communication protocol for the IEM Platform. This functionality allows the environment to disable SHA-1 signatures in favor of SHA-256, adds support for TLS 1.2, and increases the root certificate

key strength from 1024 to 4096 bits. **NOTE**: This feature will result in the loss of management of any agents or relays with version less than 9.1, including Proxy Agents.

1.4.2. There are three levels of report encryption:
   1.4.2.1. Required: clients require encryption of reports and uploads. The client does not report or upload files if it cannot find an encryption certificate or if its parent relay does not support receipt of encrypted documents.
   1.4.2.2. Optional: clients prefer, but do not require encryption of reports and uploads. If encryption cannot be performed, reports and uploads are done in clear-text.
   1.4.2.3. None: clients do not encrypt, even if an encryption certificate is present.

1.4.3. **Common Criteria Certification** – Allow IEM to meet the security certification by expanding the server audit logging functionality and adding configuration to the Console and Web Reports. These features include allowing the configuration of login banners and supporting an inactivity timeout.

1.5. Given an understanding of IEM and the requirement to integrate IEM with existing customer systems, discuss the IEM integration capabilities, so that the various APIs for IEM integration are understood.

SUBTASK(S):

1.5.1. Determine requirement of external product interactions with IEM data
1.5.2. Determine if IEM can provide access to his data to the external product via SOAP APIs, with WebReports scheduled CSV reports or with REST API.
1.5.3. Determine if external product is able to schedule or submit IEM task using REST API
1.5.4. Determine required interfaces
1.5.5. Determine if an existing integration already exists (eg. Connectors like Smartcloud Control Desk (SCCD) ITIC Adapter)
1.5.6. Determine if additional IEM solutions or components are required:
i.e. SCCD integration depends on availability and implementation of SUA
1.5.7. Determine required data workflows and interactions.

Section 2 - Installation

2.1. Given the appropriate server hardware and operating system, a IBM Endpoint Manager (IEM) license key and administrative permissions, install the IEM server and Web Reporting so that IEM has been installed on the appropriate server.

SUBTASK(S):

2.1.1. **For Windows Server Installation**

2.1.1.1. Obtain the latest version of IEM.

2.1.1.2. Run the installer (setup.exe), at the welcome screen, click Next.

2.1.1.3. You will see a dialog offering to install the Evaluation or Production version of IEM. Select Production and click Next.

2.1.1.4. After reading the license agreement, click Yes to accept it and continue.

2.1.1.5. Select the choice to install by using the IEM license authorization file from IBM then click Next.

2.1.1.6. The IEM Action Site Masthead Creation Wizard launches. It asks you for the location of your license authorization file. Click the Browse button to bring up a standard Windows open-file dialog. Navigate to your license authorization file, which has a name like CompanyName.BESLicenseAuthorization. Select the file and click **Open.**

2.1.1.7. A dialog appears displaying the current contents of your IEM license authorization. Click Next.

2.1.1.8. The next screen in the Wizard prompts you for the DNS name or IP address of your BES server. Type this in and click **Next**. Note: The DNS/IP address that you choose becomes a permanent part of your deployment and must never change. For the sake of flexibility, we strongly recommend using a DNS name instead of a static IP address.

2.1.1.9. The next screen in the Wizard prompts you for a site-level **password** so you can create a site admin key for your deployment. Type in your password twice (for verification), and specify a key size (from 2K- to 4K-bits) for the public/private key pair. Click **Next**.

2.1.1.10. From the **Save As** dialog, find a folder to save your private key file (license.pvk) to a secure location, such as a PGPDisk or a USB drive. Click **Save**.

2.1.1.11. The next screen in the Wizard prompts you to submit your masthead request to IBM. This request consists of your original authorization, your server DSN name and your public key, all packaged into a single file. Typically, you will select the first choice, **submit request**, to post the request via the Internet. Click **Next**. The Wizard will then retrieve your certificate (license.crt) from the License server.

2.1.1.12. Alternatively, the Wizard will let you save the request as a file named request.BESLicenseRequest. Then you can visit the IEM IBM Website, post your request and download your certificate.
2.1.1.13. Upon a successful request submission, the Wizard retrieves your license (license.crt) and prompts you to save it. Click **Save**. This action completes the Wizard, returning you to the **Setup Type** dialog. You are now ready to install the programs with your new production license.
2.1.1.14. If the installer is not already running, launch it. From the **Setup Type** dialog, select the second choice to **Install with a production license**. Click **Next**.
2.1.1.15. Browse to the location of your license key and click **Open**.
2.1.1.16. A dialog appears, prompting you for your private **site signing key** (license.pvk). This is typically stored in the same folder as the license.crt file. Browse to it and click **Open**.
2.1.1.17. A dialog prompts you for the **Site Admin Private Key Password**. Enter the password you selected to protect your private key (see the previous section) and click **OK**.
2.1.1.18. The program prompts for a server port number that IBM IEM will use for all its data transmissions. The default port is **52311**.
2.1.1.19. A standard Windows **Save As** dialog prompts you to save the **Masthead**. This is a public file that does not require protection. Navigate to the desired folder, name the file (e.g. actionsite.afxm), and click **Save**.
2.1.1.20. You are now ready to generate the **IEM suite installation components**. Select the default directory (BES Installers) or click **Browse** to choose a different folder. Click **Next**.
2.1.1.21. The Install Wizard will then generate and save various BigFix installation components. After saving the files, a dialog appears confirming the installation and reminding you of their location. Click **Finish** to exit and start the IEM **Installation Guide**.
2.1.1.22. If it is not already running, launch the IEM Installation Guide (**Start- > Programs - > BigFix Enterprise -> IBM Endpoint Manager Installation Guide**).
2.1.1.23. Select the button labeled **Install IBM Endpoint Manager Components**.
2.1.1.24. A dialog box appears, prompting you to select a BigFix component to install. Click the buttons on the left, in order from top to bottom, to install the BigFix components. The component installers include:
    2.1.1.24.1. Install IEM server.
    2.1.1.24.2. Install IEM console.
    2.1.1.24.3. Install IEM agents.
    2.1.1.24.4. Browse Installation folders.
2.1.1.25. Select install IEM server.

2.1.1.26. After reading the **License Agreement**, click **Yes** to accept it and continue.
2.1.1.27. A dialog prompts you to choose a **Master** or **Replicated** database. Click the first button to create a Master database for later replication – or if you only need a **Single** database in your deployment. Click the second button to create a Replica of an existing Master. If this is your initial installation, click the top button.
2.1.1.28. A dialog prompts you to select a **Local** or **Remote** database. If you want to use another computer to host the IEM database, it must have a SQL Server already installed. The most common choice is to use the local database.
2.1.1.29. A dialog displays a list of the IEM server components about to be installed. Accept the default components and click Next.
2.1.1.30. The installer prompts you for the desired destination of the BES server components. The default location is **C:\Program Files\BigFix Enterprise\BES Server**, but you can specify a different location by clicking the **Browse** button. Once you have decided on the destination, click **Next**.
2.1.1.31. The server properties dialog prompts you to enter a location for the BES server Web root folder (if different from the default). This is where downloaded files for the BES clients will be stored. The default URL is also available for editing, should you wish to change it.
2.1.1.32. Next a dialog prompts you for a location and port number for BES Web Reports. By default, it will use port 80. If IIS is installed, it will instead choose port 52312.
2.1.1.33. The IEM server installer then presents a window displaying the selected inventory of server components to be installed as well as some other installation programs to run. Click **Next** to continue the installation.
2.1.1.34. When the files have been properly installed, the program prompts you for specific information, depending on your installation parameters. The program will ask you to set a default ‗sa' password if the ‗sa' password for the SQL Server database is currently blank (this is done for security reasons).
2.1.1.35. The program then prompts you to locate the **Action Site Masthead**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where you stored your masthead, select it and click **Open**.
2.1.1.36. The program may prompt you for the location of your **license certificate**. Click **OK** to continue. At the Windows Open dialog, navigate to the folder where you stored your license (license.crt), select it and click **Open**.
2.1.1.37. Next, the program may prompt you for the location of your private key (license.pvk). Accept the default path (if specified) or click

the **Browse** button to find a different location. Finally, enter your password to initialize the database.

2.1.1.38. The program then prompts you to create an administrative user. Click **OK** to open the **BigFix Enterprise User Management** dialog.

2.1.1.39. Click **Add User** to enter each desired user.

2.1.1.40. For each user, enter the name, email, password and various permissions.

2.1.1.41. When you have finished entering users, click **Done**.

2.1.1.42. The IEM server installation is now complete. As the program exits, it gives you a chance to assess the installation. Make sure the box labeled **Run the IEM Diagnostic Tool** is checked and then click **Finish**. Click the **Full Interface** button to run the BES Diagnostics in order to ensure that the installation is functioning properly and to present a complete analysis for your inspection.

2.1.2. **For Linux Server Installation**

2.1.2.1. Obtain the latest version of IEM from IBM's Passport Advantage portal

2.1.2.2. Download IBM Endpoint Manager from IBM's Passport Advantage portal.

2.1.2.3. You can download IBM Endpoint Manager also from the support site athttp://support.bigfix.com/bes/install/downloadbes.html or from the DeveloperWorks trial site athttp://www.ibm.com/developerworks/downloads/tiv/endpoint/. The demonstration trial installer is the same installer program for a normal production installation.

2.1.2.4. To install the Endpoint Manager Server in your production environment, perform the following steps:

2.1.2.5. From the shell where you extract the server package, move to the installation directory, ServerInstaller_9.2.0.363-rhe6.x86_64 and enter the following command:./install.sh

2.1.2.6. After reading the License Agreement, enter 1 to accept it and continue.

2.1.2.7. To install the Production, enter 2: Select the type of installation

2.1.2.7.1. Evaluation: Request a free evaluation license from IBM Corp.
This license allows you to install a fully functional copy of the
IBM Endpoint Manager on up to 30 clients, for a period of 30 days.

2.1.2.7.2. Production: Install using a production license or an authorization for a production license.

2.1.2.8. Choose one of the options above or press <Enter> to accept the default value: [1] **Note:** If you enter 1 to run the evaluation installation, consider that this type of installation does not support the enhanced security option.

2.1.2.9. Select 1 if you want to install all the components:
2.1.2.10. Select the IBM Endpoint Manager features that you want to install:
    2.1.2.10.1. All components (server, client, and WebReports)
    2.1.2.10.2. Server and client only
    2.1.2.10.3. WebReports only
2.1.2.11. Choose one of the options above or press <Enter> to accept the default value:
    2.1.2.11.1. Enter 1 to create a Master database for later replication or single database if you need only one database in your deployment. Select the database replication:
    2.1.2.11.2. Single or master database
    2.1.2.11.3. Replicated database
2.1.2.12. Choose one of the options above or press <Enter> to accept the default: [1] If you enter 2, you create a replica of an existing master.
2.1.2.13. For additional information, see Using multiple servers (DSA).
2.1.2.14. To use a local database, enter 1:Select the database:
    2.1.2.14.1. Use a local database
    2.1.2.14.2. Use a remote database
2.1.2.15. Choose one of the options above or press <Enter> to accept the default:
2.1.2.16. The local database name of Endpoint Manager server is BFENT. The local database name of Web Reports is BESREPOR.
Note: To use an external database for IBM Endpoint Manager, you must perform the following steps:
2.1.2.17. Install the DB2® server on the remote workstation.
2.1.2.18. Install a DB2 client on the workstation from where you run the Endpoint Manager Server installation
2.1.2.19. Connect the DB2 server to the DB2 client installed on the workstation from where you run the installation, that is, the port of the DB2 database (default 50000) must be reachable by the workstation where the installation is running.
2.1.2.20. Provide the following information in the installation procedure:
    2.1.2.20.1. the remote DB2 node
    2.1.2.20.2. the DB2 port number
    2.1.2.20.3. the user name of the local DB2 instance owner
2.1.2.21. Enter the location where the downloaded files for the Clients are stored: Choose the web server's root folder:
2.1.2.22. Specify the location for the web server's root folder or press <Enter> to accept the default: /var/opt/BESServer
2.1.2.23. Enter the location where the WebReports Server stores its files: Choose the WebReports server's root folder:

2.1.2.24. Specify the location for the WebReports server's root folder or press <Enter> to accept the default: /var/opt/BESWebReportsServer
2.1.2.25. Enter the WebReports server's port number:Choose the WebReports server's port number:
2.1.2.26. Specify the port number or press <Enter> to accept the default: 80 The default is 80.
2.1.2.27. Enter the user name for the local DB2 Administrative user. The default is db2inst1.
2.1.2.28. Enter the DB2 Local Administrative user password.
2.1.2.29. Enter the DB2 instance configuration.
2.1.2.30. Enter the user ID and the password to define the IBM Endpoint Manager administrative user. The default user name is: IEMAdmin.
2.1.2.31. If the local firewall is running, the installation program asks to enter the Local firewall configuration.
2.1.2.32. To run the installation using a BES license authorization file, enter 1. Choose the setup type that best suits your needs:
    2.1.2.32.1. I want to install with a BES license authorization file
    2.1.2.32.2. I want to install with a production license that I already have
    2.1.2.32.3. I want to install with an existing masthead

    Note: If you already ran a first installation, or part of it, you can specify option 2 or 3, with an existing production license (license.crt, license.pvk) or an existing masthead (masthead.afxm) and perform only some of the installation steps.
2.1.2.33. Specify if a proxy must be used to communicate over the internet to external content sites or to Endpoint Manager subnetworks.
2.1.2.34. If your environment needs to use a proxy, specify the proxy hostname or IP Address and, optionally, the port number.
2.1.2.35. The installation procedure shows you the default configuration settings:
    2.1.2.35.1. Proxy user: none
    2.1.2.35.2. Proxy password:none
    2.1.2.35.3. Proxy tunneling capability: let proxy decide
    2.1.2.35.4. Authentication method: all methods allowed by the proxy
    2.1.2.35.5. Proxy exception list: localhost,127.0.0.1
    2.1.2.35.6. Use the proxy for downstream notification: false
2.1.2.36. You can accept the default settings or, alternatively, you can assign different values. These are thee settings that you can specify:
    2.1.2.36.1. Server port number
2.1.2.37. Specify the server port or press <Enter> to accept the default: 52311
2.1.2.38. Enable the use of FIPS 140-2 compliant cryptography

2.1.2.38.1. Use of FIPS enabled
2.1.2.38.2. Use of FIPS disabled

2.1.2.39. Choose one of the options above or press <Enter> to accept the default value: [2]

2.1.2.40. Gathering interval

2.1.2.41. Specify the time interval that you want to use. The default value is suitable for most of the IBM Endpoint Manager deployments.
2.1.2.41.1. Fifteen minutes
2.1.2.41.2. Half an hour
2.1.2.41.3. One hour
2.1.2.41.4. Eight hours
2.1.2.41.5. Half day
2.1.2.41.6. One day
2.1.2.41.7. Two days
2.1.2.41.8. One week
2.1.2.41.9. Two weeks
2.1.2.41.10. One month
2.1.2.41.11. Two months

2.1.2.42. Choose one of the options above or press <Enter> to accept the default value: Initial action lock
2.1.2.42.1. Locked
2.1.2.42.2. Lock duration
2.1.2.42.3. Unlocked

2.1.2.43. Choose one of the options above or press <Enter> to accept the default value:

2.1.2.44. Action lock controller
2.1.2.44.1. Console
2.1.2.44.2. Client
2.1.2.44.3. Nobody

2.1.2.45. Choose one of the options above or press <Enter> to accept the default value:

2.1.2.46. Enable lock exemptions
2.1.2.46.1. Lock exemption enabled (fairly unusual)
2.1.2.46.2. Lock exemption disabled

2.1.2.47. Choose one of the options above or press <Enter> to accept the default value:

2.1.2.48. Enable the use of Unicode filenames in archives
2.1.2.48.1. The use of Unicode filenames in archives is enabled.
2.1.2.48.2. The use of Unicode filenames in archives is disabled.

2.1.2.49. Choose one of the options above or press <Enter> to accept the default value: [1]

2.1.2.50. See Setting a proxy connection on the server for details about supported values and their usage.**Note:** If you want to enable FIPS mode, ensure that the proxy configuration is set up to use an authentication method other than digest, negotiate or ntlm. **Note:** If you specify to use the negotiate authentication method

on a server or relay, a different authentication method might be used. **Note:** The proxy configuration specified at installation time is saved in the server configuration file BESServer.config and it is used also at runtime.

2.1.2.51. Optionally you can test if the connection to the proxy can be successfully established. In particular you can select to:
    2.1.2.51.1. Test the connection
    2.1.2.51.2. Test the connection using FIPS
    2.1.2.51.3. Do not test the connection
2.1.2.52. If selected option 1 in the step 15, specify where the generated license authorization file is located:License Authorization Location
2.1.2.53. Enter the location of the license authorization file that you received from IBM or press <Enter> to accept the default: ./license/LicenseAuthorization.BESLicenseAuthorization
2.1.2.54. Specify the DNS name or ip address of the machine on which to install the server. This name is saved in your license and will be used by clients to identify the Endpoint Manager server. It cannot be changed after a license is created.
2.1.2.55. Specify the related Site Admin Private Key Password.
2.1.2.56. Specify the size in bits of the key used to encrypt the credentials:Key Size Level
2.1.2.57. Provide the key size that you want to use:
    2.1.2.57.1. 'Min' Level (2048 bits)
    2.1.2.57.2. 'Max' Level (4096 bits)
2.1.2.58. Choose one of the options above or press <Enter> to accept the default: [2]
2.1.2.59. Enter the License folder where the installation generates and saves license.crt, license.pvk and masthead.afxm.Choose License Folder:
2.1.2.60. Specify a folder for your private key (license.pvk), license certificate (license.crt), and site masthead (masthead.afxm) or press <Enter> to accept the default: ./license
2.1.2.61. After you specify where to save the files to be generated, you can submit the request to IBM for getting the license certificate by choosing one of the following options depending on if your machine is connected to Internet:
    2.1.2.61.1. Submit request from this machine over the Internet. The request will be redeemed for a license certificate (license.crt) and saved in your credential folder.
    2.1.2.61.2. Save request to a file and send it to IBM at the URL: 'http://support.bigfix.com/bes/forms/BESLicenseRequestHandler.html'.
    This method might be necessary if your deployment is isolated from the public Internet.

2.1.2.62. If you choose 1, you can continue with the next installation step. If you choose 2, the request.BESLicenseRequest request is generated. You can continue the installation by importing the certificate specifying the location of the license certificate (such as: ./license/license.crt) or exit from the installation and rerun it at a later time as described in the installation procedure:
Info: The following License Request file was successfully generated: ./license/request.BESLicenseRequest

2.1.2.63. Import License Certificate

2.1.2.63.1. Continue with the installation importing the certificate (license.crt).

2.1.2.63.2. Exit from the installation, I will import the certificate at a later time. If you exit the installation, you can rerun ./install.sh later and repeat all the steps specifying that you want to use the generated license with option 2: Choose the setup type that best suits your needs:

2.1.2.63.2.1. I want to install with a BES license authorization file

2.1.2.63.2.2. I want to install with a Production license that I already have

2.1.2.63.2.3. I want to install with an existing masthead

2.1.2.64. To import the files, you need to specify the license certificate file (./license/license.crt) and the Site Admin Private Key (./license/license.pvk) to administer the database:License Certificate Location

2.1.2.65. Enter the location of the license certificate file or press <Enter> to accept the default: ./license/license.crt

2.1.2.66. Site Admin Private Key:

2.1.2.66.1. Specify the site Level Signing Key file (license.pvk) for the database you want to administer or press <Enter> to accept the default: ./license/license.pvk

2.1.2.66.2. Accept the default masthead values: Server port number: 52311

2.1.2.66.3. Use of FIPS 140-2 compliant cryptography: Disabled

2.1.2.66.4. Gather interval: One Day

2.1.2.66.5. Initial action lock: Unlocked

2.1.2.66.6. Action lock controller: Console

2.1.2.66.7. Action lock exemptions: Disabled

2.1.2.66.8. Unicode filenames in archives: Enabled or change them by entering 2:

2.1.2.66.8.1. Use default values

2.1.2.66.8.2. Use custom values You can change the following masthead parameters: **Server port number** Specify the number of

the server port. The default value is: 52311. **Note:** Do not use port number 52314 for the network communication between the Endpoint Manager components because it is reserved for proxy agents.

2.1.2.67. **Enable use of FIPS 140-2 compliant cryptography** Use this setting to specify whether or not to be compliant with the Federal Information Processing Standard in your network. Enter 1 to enable it, 2 to disable it. The default value is 2.**Note:** Enabling FIPS mode prevents the use of some authentication methods when connecting to a proxy. If you selected to use a proxy to access the Internet or to communicate with IBM Endpoint Manager subcomponents, ensure that you selected an authentication method other than digest, negotiate or ntlm.

2.1.2.68. **Gathering interval** This option determines how long the clients wait without hearing from the server before they check whether new content is available. Specify the interval time to use by entering one of the following values:

2.1.2.68.1. Fifteen minutes
2.1.2.68.2. Half an hour
2.1.2.68.3. One hour
2.1.2.68.4. Eight hours
2.1.2.68.5. Half day
2.1.2.68.6. One day
2.1.2.68.7. Two days
2.1.2.68.8. One week
2.1.2.68.9. Two weeks
2.1.2.68.10. One month
2.1.2.68.11. Two months

The default value is: 6 (one day).

2.1.2.69. **Initial action lock** You can specify the initial lock state of all clients, if you want to lock a client automatically after installation. Locked clients report which Fixlet messages are relevant for them, but do not apply any actions. The default is to leave them unlocked and to lock specific clients later on. You can select one of the following values:

2.1.2.69.1. Locked
2.1.2.69.2. Lock duration
2.1.2.69.3. Unlocked The default value is: 3 (unlocked).

2.1.2.70. **Action lock controller** This parameter determines who can change the action lock state. You can select one of the following values:

2.1.2.70.1. Client
2.1.2.70.2. Console

2.1.2.70.3. Nobody

2.1.2.71. **Enable lock exemptions** In rare cases, you might need to exempt a specific URL from any locking actions. This setting allows you to disable or disable this function. You can select one of the following values:
2.1.2.71.1. Lock exemption enabled (fairly unusual)
2.1.2.71.2. Lock exemption disabled
The default value is 2 (disable lock exemption).

2.1.2.72. **Enable the use of Unicode filenames in archives** This setting specifies the codepage used to write filenames in the IBM Endpoint Manager archives. You can select one of the following values:
2.1.2.72.1. The use of Unicode filenames in archives is enabled.
2.1.2.72.2. The use of Unicode filenames in archives is disabled.

2.1.2.73. If you selected 1 in the previous step, you have now created the license files (license.pvk and license.crt files). After this step, the masthead.afxm file is created with the specified parameters.

2.1.2.74. Enter the port number for the DB2 connection to create the DB2 instance:

2.1.2.75. DB2 Connection:
2.1.2.75.1. Specify the DB2 Port Number or press <Enter> to accept the default: 50000
2.1.2.75.2. The installation program checks if a DB2 instance is already installed. If it is already installed, skip to step 5.If the database is not detected, enter 1 to specify the DB2 download package and install it:

2.1.2.76. DB2 Installation check

2.1.2.77. The installer does not detect DB2 as installed on the system. Determine which of the options corresponds to your installation:
2.1.2.77.1. DB2 is not installed, install it
2.1.2.77.2. DB2 is installed, use the installed instance
2.1.2.77.3. Exit from the installation

2.1.2.78. Choose one of the options above or press <Enter> to accept the default: [1]

2.1.2.79. If the user chooses the option1 then the user will be prompted with the following question with details of the settings that will be used.

2.1.2.80. Enter 1 to accept the DB2 default settings:
2.1.2.80.1. DB2 Installation
2.1.2.80.2. DB2 will be installed using the following settings:
2.1.2.80.3. DB2 Instance owner: db2inst1
2.1.2.80.4. DB2 Fenced user: db2fenc1
2.1.2.80.5. DB2 Administration Server user: dasusr1
2.1.2.80.6. DB2 communication port: 50000
2.1.2.80.7. DB2 Installation directory: /opt/ibm/db2/V10.5

2.1.2.81. If you need to use settings different from those proposed above, you can specify them in the installation response file. Refer to the product documentation for further details.
2.1.2.81.1. Proceed installing also DB2
2.1.2.81.2. Exit from the installation
2.1.2.82. Choose one of the options above or press <Enter> to accept the default: [1]
2.1.2.83. The IBM Endpoint Manager Server installation is now complete. You can now install the IBM Endpoint Manager Console on a Windows System and log on with the account you created during the installation of the server.

2.2. Given a functional IEM server installation and relay compatible agents checked into the IEM console, deploy the IEM relay so that load is distributed from the main IEM server and network traffic is reduced.

SUBTASK(S):
2.2.1. In the console, **open** the **Fixlets and Tasks** icon in the Domain Panel and then click **Tasks Only** to see a list of all Tasks.
2.2.2. Find the Task with the title Install IBM Endpoint Manager Relay (it might include a version number after it) for the appropriate operating system. These Tasks are relevant when there is at least one agent that meets the requirements for the relay.
2.2.3. Choose your deployment option by choosing one of the actions in the Task. You can target single or multiple computers with this action.
2.2.4. Click here to be prompted for a path where the IEM relay will be installed
2.2.5. Click here to install the IEM relay on the drive with the most space
2.2.6. Click here to install the IEM relay to the default location
2.2.7. Once the action completes, you'll have a functional IEM relay.

2.3. Given an operational IEM server, IEM console, a candidate computer in the DMZ to serve as a IEM relay, and coordination with the organization's networking and security teams, install an Internet facing relay so that IEM managed computers on the public Internet can still be actively managed.

SUBTASK(S):
2.3.1. Work with the organizations network and security teams to gain an understanding of the policies and configuration of the organizations DMZ. This information will assist in the configuration of IEM agent and IEM relay settings. The tasks outlined here will assume that ICMP traffic from the Internet to the DMZ is blocked and bi-directional HTTP traffic over port 52311 between the DMZ-based IEM relay and an internal IEM server or relay will be allowed.
2.3.2. Request that bi-directional HTTP traffic over port 52311 between the internal IEM server or IEM relay and the DMZ-based IEM relay be opened.

2.3.3. Request that at least inbound HTTP traffic over port 52311 between the DMZ-based IEM relay and the Internet be opened.
2.3.4. Request that a DNS alias (or IP address) for the DMZ-based IEM relay be assigned. The DNS-alias must be resolvable to a specific IP address.
2.3.5. Deploy the IEM relay to the DMZ-based computer.
2.3.6. Configure agent settings of computers which will be on the Internet to use the DNS-alias or IP address of the DMZ-based IEM relay as a fail-over relay. (Keep in mind that ICMP traffic coming in from the Internet is blocked, so the endpoints must be manually assigned).
2.3.7. Configure IEM agents to manually select the DMZ-based IEM relay's DNS-alias (or IP address) as the primary, secondary, or fail-over relay.
2.3.8. If a customer requirement – configure command polling interval.
2.3.9. If a customer requirement – use Task "BES Client Setting|Enable Relay Authentication. That relay will only communicate with authenticated agents.
2.3.10. If a customer requirement – Enable Client Encryption – This allows for Server and relay-bound communications from clients to be encrypted to prevent unauthorized access to sensitive information. On Windows Launch the IBM Endpoint Manager Adminstration Tool by selection Start >Programs>IBM Endpoint Manager>IBM Endpoint Manager Administration Tool. Select the Encryption tab. On Linux, run this command as super user "/opt/BESServer/bin/Besadmin.sh -reportencryption"
2.3.11. Available options can be retrieved from command help: "./BESAdmin.sh -reportencryption -h"

2.4. Given an operational IEM server and console, install the IEM agent on computers so that they can be managed with the IEM environment.

SUBTASK(S):
2.4.1. Use network shares to manually install the IEM agent (simply run the setup.exe from the IEM agent installation folder while logged in as a user with admin rights on that computer).- Msi silent installation
  2.4.1.1. msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi /qn
  2.4.1.2. -Client installer silent
  2.4.1.3. - setup.exe /s /v/l*voicewarmup \"C:\besclientinstall.log\" SETUPEXE=1 /qn"

  NOTE: full list of installation optionshttp://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp.
2.4.2. Deployment methods:
  2.4.2.1. For Windows domains or Windows Active Directory domains, you can use a domain administration user to deploy IEM agent by using the **IEM Client Deploy tool** located at Start -> All Programs -> IBM Endpoint Manager -> Endpoint Manager Client Deploy (on the computer that was used to run the IEM

Installation Generator). Note: You can add custom client settings under Advanced Options and Custom Settings.

2.4.2.2. You can use login scripts to automatically install the IEM agent on computers.

2.4.2.3. You can use package deployment applications (such as SCCM, etc.) to deploy IEM agent.

2.4.2.4. You can use any mechanism/procedure that you currently use to install applications within your network.

2.4.2.5. For non-Windows computers, you can leverage the UNIX/Linux/Mac Client Deploy tool, found on the Labs site.

2.4.2.6. You can enable the "Agent Deploy Tool" from the console in the BigFix Lab Domain, to deploy an agent deployment tool for Windows or for Linux, and then use fixlets to install the agent on additional systems

2.4.2.7. You can download the Agent Deployment Wizard (stand-alone) from the Developerworks site: https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/IEM%20Agent%20Deployment%20Wizard%20%28stand-alone%29 to install the agent on any supported endpoint system OS. You can add custom client setting

2.5. Give the requirement to facilitate automation of processes that require communication with the IEM server and Web Reports, install the BES server Plugin service so that other IEM applications will be able to fully utilize IEM server functionality.

SUBTASK(S):

2.5.1. **Install BES server plugin service:**

2.5.1.1. Log on to IEM console with master operator account.

2.5.1.2. Take action on Task 708 "Install BES Server Plugin Service" by using the IEM server as the target.

2.5.2. **Set up BigFix server plugin service to access Web Reports SOAP API**

2.5.2.1. Select Task 1295 "Configure SOAP API credentials for Server Plugin Service"

2.5.2.2. **in the Task description tab: enter Web Report User and Enter its password twice**

2.5.2.3. Set the name of your Web Reports server URL: e.g.: http://bigfix.company.com/webreports

2.5.3. **Submit the action by using the IEM server as the target.**

2.5.3.1. **On Windows only: Set up BES server plugin service to access IEM database. If the database is local or is remote with "SQL Server Authentication" these steps are not required**

2.5.3.2. Set up with database bu using NT Authentication:

2.5.3.3. Open the Windows Services dialog (Administrative Tools -> Services).
2.5.3.4. Open the BES server plugin service.
2.5.3.5. Click the Log On tab.
2.5.3.6. Select “This account”.
2.5.3.7. Set user to the same user as was used for the FillDb and GatherDb services.
2.5.3.8. Restart the service.

2.5.4. **Set up BigFix server plugin service to access REST API**
2.5.4.1. Select Task 1294 “Configure REST API credentials for Server Plugin Service” **in the Task description tab enter a Master operator user name , Enter its password twice.**
2.5.4.2. Verify the URL of your server API URL:
e.g.: http://bigfix.company.com:52311/api
2.5.4.3. **Submit the action by using the IEM server as the target.**

2.6. Given a functional IEM server, console, deployed agents and operator permissions, create manual or automatic computer groups so that computer target groups have been created based upon the customer’s requirements.

SUBTASK(S):

2.6.1. Create manual computer groups:
2.6.1.1. Click the ‘Computers’ icon in the All Content domain and in the resulting List Panel, Shift/Ctrl-click to select the computers you want grouped together.
2.6.1.2. Right-click the computers you've chosen and select ‘Add to Manual Group’ from the pop-up menu.
2.6.1.3. From the Select Manual Computer Group dialog, you can choose to add your selected computers to an existing group or create a new group for them.
2.6.1.4. Select an existing group or name a new one and click ‘OK’. If prompted, enter your password to propagate the new manual group.

2.6.2. Create automatic computer groups:
2.6.2.1. Click Tools -> Create New Automatic Group.
2.6.2.2. From the Create New Automatic Computer Group dialog, enter the name of your group and select the site and domain you want it to reside in.
2.6.2.3. Enter a property, a relation and a value into the three boxes at the bottom of the dialog. For instance to create a group that will automatically enlist Windows computers, select ‘OS contains Win’. Click the + button to add new properties that you can AND (include all properties) or OR (include any properties) together to identify group membership.

2.6.2.4. When you are done, click ‘OK’ and if prompted, enter your password to propagate the group settings.

2.7. Given functional IBM IEM relays, and deployed agents checked into the IEM console, configure relay affiliation so that agents report to the desired deployed IEM relays.

SUBTASK(S):

2.7.1. **Use relay affiliation.**
- 2.7.1.1. IEM relay fffiliation is intended to provide a more sophisticated control system for automatic relay selection.

2.7.2. **Create IEM agent affiliation groups .**
- 2.7.2.1. IEM agent is assigned to one or more Relay Affiliation Groups through the IEM agent setting: _BESClient_Register_Affiliation_SeekList
- 2.7.2.2. This IEM agent setting should be set to a semi-colon (;) delimited list of Relay Affiliation Groups, for example: AsiaPacific;Americas;DMZ

2.7.3. **Create IEM relay and server affiliation groups**
- 2.7.3.1. IEM relays and IEM servers can be assigned to one or more Affiliation Groups through the IEM agent setting:
- 2.7.3.2. _BESRelay_Register_Affiliation_AdvertisementList This IEM agent setting should also be set to a semi-colon (;) delimited list of Relay Affiliation Groups, for example: AsiaPacific;DMZ;* Note: IEM relays and IEM servers are not required to have a SeekList setting. The SeekList is only used by the IEM agent.

2.7.4. **IEM relay affiliation list information**
- 2.7.4.1. There are no pre-defined relay affiliation group names; you are free to pick group names that are logical to your deployment of TEM. There are some naming rules you should observe:
- 2.7.4.2. Do not use special characters (including —.ǁ) when picking names.
- 2.7.4.3. Group names are not case sensitive.
- 2.7.4.4. Leading and trailing whitespaces are ignored in comparisons.

2.8. Given the appropriate server hardware and operating system, a IEM license key, and administrative permissions, install the replica IEM server and ensure Distributed Server Architecture (DSA) replication is functional so that there are two functional IEM servers replicating information between them.

SUBTASK(S):

2.8.1. **Windows and MSSQL Server:**
- 2.8.1.1. Determine if you will be using SQL or NT authentication foe SQL.
- 2.8.1.2. Run the IEM server installer on the DSA server with admin and SA rights.

2.8.1.3. Select Replicated Database when prompted by installer.
2.8.1.4. Enter master server hostname and credentials with DBO rights to BFEnterprise on master server.
2.8.1.5. Run the IEM Administration Tool on newly configured server.
2.8.1.6. Configure replication cycle (5 minutes by default).
2.8.1.7. Run IEM Administration Tool on master server to ensure newly installed DSA server is available in drop-down list and set replication interval.
2.8.1.8. Check FillDB logs on master and replica server for replication information. (Default path C:\Program Files\BigFix Enterprise\BES Server\FillDBData)

2.8.2. **On Linux and DB2:**
2.8.2.1. Choose a single login name (for example, db2inst1), and a single password to be used by all servers in your deployment for db2 inter-server authentication.
2.8.2.2. On the Master Server, open the /var/opt/BESServer/besserver.config file.
2.8.2.3. Add or modify the following keywords in the [Software\BigFix\Enterprise Server\FillDB] section:
2.8.2.4. ReplicationUser = <login name>
2.8.2.5. ReplicationPassword = <password>
2.8.2.6. ReplicationPort = <DB2_port>
2.8.2.7. Restart the FillDB service.
2.8.2.8. copy the masthead file and the license.pvk file on the DSA server
2.8.2.9. Run the IEM server installer on the DSA server with root and DB2 administratator rights.
2.8.2.10. Select Replicated Database when prompted by installer.
2.8.2.11. Enter local DB2 administrator credentials when prompted.
2.8.2.12. Enter the folders of the Web Servers Root and WebReports Server Root
2.8.2.13. Enter the port number of the WebReports Server.
2.8.2.14. Define the credentials of the WebReports administrative user. The default is: IEMAdmin.
2.8.2.15. Specify the location of license.pvk and its password.
2.8.2.16. Specify the location of the existing masthead.afxm file that was generated when installing the master server.
2.8.2.17. On the Secondary Server DNS Name prompt, enter the DNS name of the new server. This name must be resolvable by other servers and by clients.
2.8.2.18. On the DB2 Connection prompt, enter the port number of the local DB2 instance where the installer is running.
2.8.2.19. Enter information about the master server DB2 instance to allow the new server to connect to DB2 on the master server

2.8.3. **On the Master Server Database Hostname prompt, specify the hostname of the system where the Master Server Database is located.**

2.8.3.1. On the Master Server Database Port prompt, specify the database port number of the system where the Master Server Database is located.
2.8.3.2. On the Master Server Database Administrative User prompt, specify the username of the DB2 Administrative user of the system where the Master Server Database is located.
2.8.3.3. On the Master Server Database Administrative User Password prompt, specify the password of the DB2 administrative user of the system where the Master Server Database is located.

2.9. Given an operational IEM Server with a local database, IEM Relay, IEM console, and IEM agent, perform a product upgrade from IEM 9.1 to IEM 9.2 using the IEM provided upgrade fixlets so that all of the latest IEM components are being used.

SUBTASK(S):
2.9.1. Carefully review all documentation for the new IEM version as well as all IEM upgrade instructions, change lists, and known issues. Also carefully review the information contained in the Description tab of all upgrade fixlets.
2.9.2. If possible, create a full backup of the IEM server. Always create full backups of all IEM Databases.
2.9.3. First upgrade the IEM Server, IEM Consoles and IEM installation components by running the task, IBM Endpoint Manager – Updated Platform Server Components version 9.2.0 Now Available!
2.9.4. Be sure when targeting to select Dynamically target by property and select All computers, this will ensure all components are upgraded on the server, any web reports servers, and all the consoles that are running in the environment.
2.9.5. The next step is to update all IEM relays in the environment. Run the appropriate relay update fixlets that will show up relevant under BigFix Management -> BES Deployment upgrade in the console
2.9.6. The final step is to upgrade all IEM agents in the environment. Run the appropriate client update fixlets the will show up relevant under BigFix Management -> BES Deployment upgrade in the console.

Section 3 - Component Configuration

3.1. Given a functional IBM Endpoint Manager(TEM) server, and deployed agents checked into the IEM console, configure relay selection so that agents report to the desired deployed IEM relays.

SUBTASK(S):

3.1.1. **Automatic relay selection**

3.1.1.1. Start up the IEM console and select the IEM Management domain. From the Computer Management folder, click the 'Computers' node to bring up a list of IBM IEM agents in the list panel.

3.1.1.2. Right-click on this highlighted set and choose 'Edit Computer Settings' from the pop-up menu. Depending on whether you selected one or more computers, the dialog boxes are slightly different. Typically, you will have selected all the IEM agent in your network, so you will see the multiple-select dialog. (if you selected one computer, you will need to select the “More Options” button before proceeding to step below)

3.1.1.3. Check the box marked 'Relay Selection Method'.

3.1.1.4. Click the button marked 'Automatically Locate Best Relay'.

3.1.1.5. Click 'OK'.

3.1.2. **Defaulting to automatic relay discovery:** As you install IEM agent, you may want them to automatically discover the closest IEM relay by default. Here is how to set this up:

3.1.2.1. As described in the previous section, open the 'Edit Computer Settings' dialog.

3.1.2.2. Select the 'Target' tab.

3.1.2.3. Click the button labeled 'All computers with the property'.

3.1.2.4. In the window below, select 'All Computers'.

3.1.2.5. Select the 'Constraints' tab.

3.1.2.6. Uncheck the 'Expires On' box.

3.1.2.7. Click 'OK'.

3.1.3. **Manually selecting relays:** You may have a reason to manually specify exactly which IEM agent should connect to which IEM relay. Here is how:

3.1.3.1. Start up the IEM console and select the IEM Management domain. From the Computer Management folder, click the 'Computers' node to bring up a list of IEM agent in the list panel.

3.1.3.2. Shift- and Ctrl-click to select the set of computers you want to attach to a particular IEM relay.

3.1.3.3. Right-click on this highlighted set and choose 'Edit Computer Settings' from the pop-up menu. As with creating the relays (above), the dialog boxes are slightly different if you have selected one or multiple computers.

3.1.3.4. Check the box labeled 'Primary IEM Relay' and then select a computer name from the drop-down list of available IEM relay servers.

3.1.3.5. Similarly, you can assign a ‘Secondary IEM Relay’, which will be the backup whenever the Primary relay server is unavailable for any reason.
3.1.3.6. Click the ‘OK’ button.

3.2. Given that the IEM server is up and running, ensure that all endpoints are healthy and connected to the IEM server so that sufficient information has been gathered to determine whether the IEM endpoint agents are healthy and properly reporting into the IEM environment.

SUBTASK(S):
3.2.1. Use the IEM console, navigate to BigFix Management domain.
3.2.2. Select the Deployment Health Check dashboard.
3.2.3. Navigate to the BES Client Health section.
3.2.4. Review the following guidelines:
3.2.5. Check agent distance from relays.
3.2.6. Agents should typically be less than 5 networks hops from relays.
3.2.7. Check Windows Management Interface (WMI) properties.
3.2.8. Try to leverage relevance inspectors other than WMI where possible.
3.2.9. Check Actions targeted by using lists.
3.2.10. Actions targeted at more than 50 computers should use lists.
3.2.11. Check Location properties.
3.2.12. Check the version level of the location properties wizard and ensure that it is the latest.
3.2.13. Check the total number of endpoints.
3.2.14. Ensure that the total number of installed IEM endpoint agents matches the number of physical machines that are managed by TEM.
3.2.15. Ensure that none of the computers are gray-out in the console computer site
3.2.16. If gray-out check, to ensure that the computer is properly booted and reachable by a ping.
3.2.17. Ensure that the computer properties are correctly reported.
3.2.18. Review core properties.
3.2.19. Review custom properties.
3.2.20. Check agent relay status.
3.2.21. Review Computer group memberships.
3.2.22. Review Subscribed site.
3.2.23. Review client settings.
3.2.24. Check Bandwidth Throttling status.
3.2.25. Check component version.
3.2.26. While still in the Deployment Health Check dashboard.
3.2.27. Navigate to the BES Console Health section.
3.2.28. Check the number of unreachable endpoints.
3.2.29. If a large number of endpoints are unreachable, it might indicate a problem.
3.2.30. Check number of stopped and expired actions.

3.2.31. Check number of stopped and expired hidden actions.
3.2.32. Check number of expired computers.
3.2.33. Expired computers have not reported in over a month.
3.2.34. Check Duplicate Computers.
3.2.35. Duplicate computers should be eliminated.
3.2.36. Navigate to Computers.
3.2.37. Select a computer of interest.
3.2.38. Expand the Relevant Messages.
3.2.39. Check every single non-compliance message.

3.3. Given an IBM Endpoint Manager (IEM) server running on Windows needs to use an account other than SYSTEM for running the BES server services, and an account to run the service(s) as, configure the IEM service(s) to run as the different user so that the BES server services are running as an account other than SYSTEM.

SUBTASK(S):
3.3.1. Identify or create an account that has appropriate permissions (for example, an Active Directory account that has DBO access to the IEM database but not Administrator permissions on the server).
3.3.2. Open the Services control panel. All the IEM service names begin with "BES": BES FillDB, BES GatherDB, BES Gather Service, BES Root server, and BES Web Reports server. The FillDB account requires DBO access to the BFEnterprise database.
3.3.3. Change the login account for the service by bringing up its Properties dialog and changing the "Log on as:" fields to use the chosen account name and password.
3.3.4. Restart the service to have it login by using the new account.
3.3.5. The services list should show the appropriate account in the "Log On As" column.

3.4. Given a functional IBM Endpoint Manager (IEM) Server on a network that requires going through a proxy for Internet access, configure the IEM server to use the proxy so that content is successfully gathered and sites are successfully populated on the IEM server.

SUBTASK(S):
3.4.1. Proxy does not require authentication
    3.4.1.1. Configure the Root Server computer Settings
        3.4.1.1.1. Enterprise Server_ClientRegister_ProxyServer (hostname or IP)
        3.4.1.1.2. Enterprise Server_ClientRegister_ProxyPort
    3.4.1.2. Configure the Exception List
        3.4.1.2.1. On Windows, configure the registry key, [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\Proxy]

"ProxyExceptionList"="localhost,127.0.0.1,ibm.com"
Values entered in this key are used for substring matching within URLs, so the value "ibm.com" will bypass the proxy for any URL that includes ibm.com (e.g. www.ibm.com and www.sfo.ibm.com)

3.4.1.2.2. On Linux, add the following to the [Software\BigFix\Enterprise Server\Proxy] section of /var/opt/BESServer/besserver.config
ProxyExceptionList=localhost,127.0.0.1,ibm.com

3.4.2. Proxy requires Basic or Digest Authentication

3.4.2.1. Configure the Root Server computer Settings

3.4.2.1.1. Enterprise Server_ClientRegister_ProxyUser

3.4.2.1.2. Enterprise Server_ClientRegister_ProxyPass

3.4.2.1.3. Enterprise Server_ClientRegister_ProxyServer (hostname or IP)

3.4.2.1.4. Enterprise Server_ClientRegister_ProxyPort

3.4.2.2. Configure the Exception List

3.4.2.2.1. On Windows, configure the registry key, [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\Proxy]
"ProxyExceptionList"="localhost,127.0.0.1,ibm.com"
Values entered in this key are used for substring matching within URLs, so the value "ibm.com" will bypass the proxy for any URL that includes ibm.com (e.g. www.ibm.com and www.sfo.ibm.com)

3.4.2.2.2. On Linux, add the following to the [Software\BigFix\Enterprise Server\Proxy] section of /var/opt/BESServer/besserver.config
ProxyExceptionList=localhost,127.0.0.1,ibm.com

3.4.3. Proxy require NTLM Authentication

3.4.3.1. Windows IEM Server

3.4.3.1.1. Run the following from the command prompt.
BESAdmin.exe /setproxy /user:<proxy user> /pass:<proxy password>

3.4.3.1.2. The user above, <proxy user> will need to login to the IEM server and configure Internet Options, in the Control Panel, to use the proxy

3.4.3.2. Linux IEM Server

3.4.3.2.1. On Linux, add the following to the [Software\BigFix\Enterprise Server\Proxy] section of /var/opt/BESServer/besserver.config
Proxy = http://username:passw0rd@proxyaddress:port
ProxyExceptionList=localhost,127.0.0.1,ibm.com

3.4.4. Proxy requires Kerberos Authentication (Windows IEM Server Only)

3.4.4.1. Run the following from the command prompt.

BESAdmin.exe /setproxy /user:<proxy user> /pass:<proxy password>

3.4.4.2. Configure the following key:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\Proxy]
"ProxyExceptionList"="localhost,127.0.0.1,ibm.com”

3.5. Given master operator access to the IEM environment and access to a console, manage roles and permissions within IEM so that users can effectively log in to the console and manage their endpoints.

SUBTASK(S):

3.5.1. **Create users and roles.**
- 3.5.1.1. Create **Non-Role users**
- 3.5.1.2. **Create Local Operator**
  - 3.5.1.2.1. Log in to IEM console.
  - 3.5.1.2.2. Browse to All Content -> Operators.
  - 3.5.1.2.3. Right Click in the main window and select Create Local Operator.
  - 3.5.1.2.4. Follow creation steps.
- 3.5.1.3. **Create Non-Role LDAP Operator.**
  - 3.5.1.3.1. Log in to IEM console.
  - 3.5.1.3.2. Browse to All Content -> Operators.
  - 3.5.1.3.3. Right Click in the main window and select Add LDAP Operator.
  - 3.5.1.3.4. Follow creation steps.
- 3.5.1.4. Create **roles.**
- 3.5.1.5. **Create actual role.**
  - 3.5.1.5.1. Log in to IEM console.
  - 3.5.1.5.2. Browse to All Content -> Roles.
  - 3.5.1.5.3. Right Click in the main window and select Create Role.
  - 3.5.1.5.4. Follow creation steps.

3.5.2. **Add to user or role.**
- 3.5.2.1. Add user to role.
  - 3.5.2.1.1. Log in to IEM console.
  - 3.5.2.1.2. Browse to All Content -> Operators.
  - 3.5.2.1.3. Select an Operator in the main window and browse to the Assigned Roles tab.
  - 3.5.2.1.4. Click Assign Role.
  - 3.5.2.1.5. Follow creation steps.
- 3.5.2.2. Add Content to user or role.
  - 3.5.2.2.1. Log in to IEM console.
  - 3.5.2.2.2. Browse to All Content -> Operators for a single user or All Content -> Roles for a role.
  - 3.5.2.2.3. Select an Operator or Role and browse to the Sites tab
  - 3.5.2.2.4. Click Assign Site.

3.5.2.2.5. Follow remaining Assignment Steps, including assigning Owner/Writer/Reader where appropriate.

3.5.2.3. Add Managed Computers to user or role.

3.5.2.3.1. Log in to IEM console.

3.5.2.3.2. Browse to All Content -> Operators for a single user or All Content -> Roles for a role.

3.5.2.3.3. Select an Operator or Role and browse to the Computer Assignments tab.

3.5.2.3.4. Click Add.

3.5.2.3.5. Follow remaining steps to add computers.

3.5.2.3.6. Sync Active Directory Group w/ Role

3.5.2.3.7. Set up LDAP Directory.

3.5.2.3.8. Log in to IEM console.

3.5.2.3.9. Browse to All Content -> LDAP Directories.

3.5.2.3.10. Right click on the Main Window and select Add LDAP Directory.

3.5.2.3.11. Follow remaining step to Add the LDAP Directory.

3.5.3. **Assign LDAP group to a role.**

3.5.3.1. After setting up an LDAP Directory

3.5.3.2. Log in to IEM console.

3.5.3.3. Browse to All Content -> Roles.

3.5.3.4. Select a role in the main window and browse to the LDAP Groups Tab.

3.5.3.5. Click Assign LDAP Group.

3.5.3.6. Follow remaining steps to add the LDAP group.

3.5.4. **Modify user or role.**

3.5.4.1. Modify user or role settings.

3.5.4.1.1. Log in to IEM console.

3.5.4.1.2. Browse to All Content -> Operators for a single user or All Content -> Roles for a role.

3.5.4.1.3. Select the Operator or Role you would like to change.

3.5.4.1.4. Click on the Details Tab.

3.5.4.1.5. Make any changes necessary.

3.5.4.1.6. Click Save Changes.

3.5.5. **Modify Content Assigned.**

3.5.5.1. Log in to IEM console.

3.5.5.2. Browse to All Content -> Operators for a single user or All Content -> Roles for a role.

3.5.5.3. Select the Operator or role you would like to change.

3.5.5.4. Click on the Sites tab.

3.5.5.5. Make any changes necessary.

3.5.5.6. Click Save Changes.

3.5.6. **Modify Computers Assigned.**

3.5.6.1. Log in to IEM console.

3.5.6.2. Browse to All Content -> Operators for a single user or All Content -> Roles for a role.

3.5.6.3. Select the Operator or Role you would like to change.
3.5.6.4. Click on the Computer Assignments Tab.
3.5.6.5. Make any changes necessary.
3.5.6.6. Click Save Changes.
3.5.6.7. Remove **user or role.**

3.5.7. **Delete user.**
3.5.7.1. Log in to IEM console.
3.5.7.2. Browse to All Content -> Operators.
3.5.7.3. Select the Operator you would like to remove,
3.5.7.4. Click Remove.

3.5.8. **Delete role**
3.5.8.1. Log in to IEM console.
3.5.8.2. Browse to All Content -> Roles.
3.5.8.3. Select the Role you would like to remove.
3.5.8.4. Click Remove.

3.6. Given an operational IEM server, console, master operator console account, and a valid IEM license, enable IEM content sites so that IEM solutions can be accessed from the console.

SUBTASK(S):

3.6.1. Enable Site:
3.6.1.1. Click on the BigFix Management domain icon in the domain panel of the IEM console.
3.6.1.2. Click on the ‘License Overview’ dashboard icon in the navigation pane.
3.6.1.3. Expand each software bundle to reveal a list of licensed content sites listed under the ‘Available Sites’ heading.
3.6.1.4. Click the ‘Enable’ link next to each site to which you want to subscribe.
3.6.1.5. The enabled sites will now appear in the list of ‘Licenses (Used / Allowed)’.

3.6.2. Enable Site Subscription:
3.6.2.1. For each site just enabled, click on the site name in the ‘License Overview’ and then select the 'Computer Subscriptions' tab.
3.6.2.2. Use the options on the 'Computer Subscriptions' tab to set which computers should gather the content from the enabled site. Computers that are not subscribed to a content site will not gather or evaluate the site’s content.
3.6.2.3. When you are finished setting the computer subscriptions, click the 'Save Changes' button to complete the subscription process for the site.

3.7. Given the reporting requirements of the customer, activate the appropriate set of analyses so that the IEM infrastructure will collect the desired data.

SUBTASK(S):

3.7.1. Log in to the IEM console as a master console operator.
3.7.2. Select the All Content Domain.
3.7.3. Select Analyses in the filter tree.
3.7.4. Highlight the desired analyses to activate within the list on the right (Ctrl-click to select multiple analyses).
3.7.5. Right-click and select Activate.
3.7.6. Repeat the previous 2 steps for any additional content that is required to be enabled.

3.8. Given IEM components on a network infrastructure with bandwidth usage constraints, configure IEM agent and server settings so that TEM's bandwidth usage is controlled.

SUBTASK(S):

3.8.1. Determine whether manual or dynamic bandwidth throttling is appropriate, and which traffic to throttle (outbound from the server/relay to endpoints, relays downloading from the server, and/or endpoints downloading from their server/relay), and how much bandwidth to allocate to the IEM traffic (which may vary per link).
3.8.2. To throttle outbound traffic from the server to the relays, use one of these tasks to configure the server settings:
    3.8.2.1. BES Server Setting: Throttle Outgoing Download Traffic
    3.8.2.2. BES Server Setting: Dynamically Throttle Outgoing Traffic
3.8.3. To throttle outbound traffic from relays to the endpoints, use one of these tasks to configure the relay settings:
    3.8.3.1. BES Relay Setting: Throttle Outgoing Download Traffic
    3.8.3.2. BES Relay Setting: Dynamically Throttle Outgoing Traffic
3.8.4. To throttle relays downloading from their upstream server/relay, use one of these tasks to configure the relay settings:
    3.8.4.1. BES Relay Setting: Download Throttling
    3.8.4.2. BES Relay Setting: Dynamic Download Throttling
3.8.5. To throttle endpoints downloading from their relay/server, use one of these tasks to configure the client settings:
    3.8.5.1. BES Client Setting: Download Throttling
    3.8.5.2. BES Client Setting: Dynamic Download Throttling
3.8.6. If using dynamic throttling instead of manual throttling, use these tasks to enable it:
    3.8.6.1. BES Client Setting: Enable/Disable Dynamic Throttling
    3.8.6.2. BES Relay/Server Setting: Enable/Disable Dynamic Throttling
3.8.7. Enable this analysis to verify the throttle settings (it is in the BES Support site, as are all the related tasks):
    3.8.7.1. Bandwidth Throttling Status

3.9. Given the requirement to remediate out of compliance agents, describe the settings available in an action so that proper options are used for making an action a policy.

SUBTASK(S):

3.9.1. Set policy expiry:
- 3.9.1.1. If setting a policy to never expire, uncheck the “Ends On” field.
- 3.9.1.2. If the policy is to only be active for a finite time, check the “Ends On” and set the date.

3.9.2. Set re-application policy:
- 3.9.2.1. Check the “Reapply this action”.
- 3.9.2.2. Choose “whenever it becomes relevant again” to immediately bring the system into compliance.
- 3.9.2.3. Choose “while relevant, waiting <interval> between reapplications” to wait for some interval before bringing the system into compliance.
- 3.9.2.4. Check the “Limit to <number> reapplications” to limit the number of times the policy will execute on a target.

3.10. Given the requirement to ensure actions are not performed on targets outside of maintenance windows, utilize the IEM Maintenance Window dashboard and client locking so that agents will automatically unlock at the beginning of the maintenance window and lock when the window is over.

SUBTASK(S):

3.10.1. Create Maintenance windows.
- 3.10.1.1. Log on to IEM console.
- 3.10.1.2. Navigate to All Content domain -> Dashboards- > BES Support -> Maintenance Window dashboard.
- 3.10.1.3. Activate the Maintenance Window Analysis.
- 3.10.1.4. Press the “Create New Maintenance Window” button.
- 3.10.1.5. Give the window a descriptive name.
- 3.10.1.6. Select length of time for the window to be open.
- 3.10.1.7. Set the start time for the window.
- 3.10.1.8. Select the frequency .
  - 3.10.1.8.1. Once: This will open the window on a specific date and time.
  - 3.10.1.8.2. Daily: Will occur every day interval at the specified time.
  - 3.10.1.8.3. Weekly: Will occur every week interval on the selected days at the specified time.
  - 3.10.1.8.4. Monthly: Will occur on a specific day of the month at the specified time.
- 3.10.1.9. Press the “Create Task” button. This will generate a task to set the registry settings on the agents.

3.10.1.10. Deploy Maintenance Window to agents.
3.10.1.11. Click on the desired maintenance window in the dashboard.
3.10.1.12. Press the “Take Action” button.
3.10.1.13. From the “Preset” select “Policy”.
3.10.1.14. In the Target tab, select the desired targets.
3.10.1.15. Press the OK button to submit the action and enter password.

3.10.2. Set client locking.
3.10.2.1. Navigate to All Content domain-> Dashboards-> BES Support -> Maintenance Window Dashboard, Click on the link for “Enforce Maintenance Window with Client Locking”.
3.10.2.2. Press the “Take Action” button.
3.10.2.3. From the “Preset” select “Policy”.
3.10.2.4. In the Target tab, select the desired targets.
3.10.2.5. Press the OK button to submit the action and enter password.

3.11. Given an operational IEM server and IEM agent, deploy a custom agent setting so that all targeted IEM agents use the custom setting.

SUBTASK(S):
3.11.1. Open the IEM console and go to the Computer section under the All Content domain.
3.11.2. Select the computer(s) that you would like to apply a custom agent setting to.
3.11.3. Right-click on the computer(s) and choose Edit Computer Settings -> More Options.
3.11.4. Under the Settings tab, check Custom Settings. Enter in a Name and Value for the new custom agent setting.
3.11.5. Click OK to send out the configuration setting, which will take effect immediately. You can view a computer's agent settings by selecting a computer and viewing the Client Settings section of the computers Summary page.

3.12. Given Web Report admin access and access to Web reports, manage roles and permissions within IEM so that users can effectively log in and use Web Reports.

SUBTASK(S):
3.12.1. **Non-Active Directory users**
3.12.1.1. **Create users:**
3.12.1.1.1. Log in to Web Reports.
3.12.1.1.2. Select Administration -> User Management -> Create User.
3.12.1.1.3. Fill in the appropriate information.
3.12.1.1.4. Click Create User.
3.12.1.2. **Edit user:**
3.12.1.2.1. Log in to Web Reports.

3.12.1.2.2. Select Administration -> User Management.
3.12.1.2.3. Check the user(s) to be changed.
3.12.1.2.4. (De)Select the new roles for the user in the Assign Roles pull- down menu.

3.12.1.3. **Delete user:**

3.12.1.3.1. Log in To Web Reports.
3.12.1.3.2. Select Administration -> User Management.
3.12.1.3.3. Check the user(s) to be deleted.
3.12.1.3.4. Click Delete.

3.12.2. **Active Directory users**

3.12.2.1. **Set up connection to Active Directory:**

3.12.2.1.1. Log in to Web Reports.
3.12.2.1.2. Select Administration -> User Management -> Active Directory Permissions.
3.12.2.1.3. If Active Directory credentials have not been entered a prompt will appear, enter valid Active Directory credentials.

3.12.2.2. **Create user:**

3.12.2.2.1. Log in to Web Reports.
3.12.2.2.2. Select Administration -> User Management -> Active Directory Permissions.
3.12.2.2.3. Ensure Names is selected.
3.12.2.2.4. Type in Active Directory account to use to create a new Web Reports user.
3.12.2.2.5. Click Search.
3.12.2.2.6. Once results have returned click the box next to the desired user to add.
3.12.2.2.7. Select the appropriate roles from the Assign Roles pull-down menu.

3.12.2.3. **Modify user:**

3.12.2.3.1. Log in to Web Reports.
3.12.2.3.2. Select Administration -> User Management -> Active Directory Permissions.
3.12.2.3.3. Ensure Assigned Web roles is selected.
3.12.2.3.4. Type in Active Directory account to use to modify, or leave blank to see all active users.
3.12.2.3.5. Click Search.
3.12.2.3.6. Once results have returned click the box next to the desired user to modify.
3.12.2.3.7. Select the appropriate roles to modify from the Assign Roles pull-down menu.

3.12.3. **Manage roles.**

3.12.3.1. **Create role:**

3.12.3.1.1. Log in To Web Reports.
3.12.3.1.2. Select Administration -> User Management -> Manage Roles.

3.12.3.1.3. Click Create Role.
3.12.3.1.4. Fill out the appropriate Information.
3.12.3.1.5. Click Create Role.

3.12.3.2. **Edit role:**

3.12.3.2.1. Log in To Web Reports.
3.12.3.2.2. Select Administration -> User Management -> Manage Roles.
3.12.3.2.3. Click on the name of the role to be changed.
3.12.3.2.4. Make the desired changes.
3.12.3.2.5. Click Update Role.

3.12.3.3. **Delete role:**

3.12.3.3.1. Log in To Web Reports.
3.12.3.3.2. Select Administration -> User Management -> Manage Roles.
3.12.3.3.3. Click the check box next to the role to be deleted.
3.12.3.3.4. Click Delete.

3.13. Given an operational IEM server and console, use the IEM Administration Tool on Windows/Linux so that a user has the ability to administer masthead, system options, advanced options, replication and report encryption.

SUBTASK(S):

3.13.1. Masthead Management
3.13.2. Edit, export, **request**, or activate a masthead.
3.13.3. System options:
3.13.4. Minimum **refresh** interval
3.13.5. Default **Fixlet** Visibility
3.13.6. Client UI **Icon**
3.13.7. Advanced options:
3.13.7.1. Special name/value pairs that allow you to customize the behavior of IEM deployment.
3.13.8. Replication:
3.13.8.1. This dialog helps to visualize your replication servers.
3.13.9. Encryption:
3.13.9.1. This dialog allows you to manage encryption keys.
3.13.10. Security:
3.13.10.1. This dialog allows you to enforce enhanced security with SHA-256 digital signatures.

3.14. Given an operational IEM Administration Tool, IEM server, IEM relay, and IEM agent, configure report encryption and a decrypting relay so that all targeted IEM agents encrypt upstream data using Message Level Encryption and decryption occurs on a IEM relay instead of on the IEM server itself.

SUBTASK(S):

3.14.1. Windows:

- 3.14.1.1. Launch the IEM Administration Tool.
- 3.14.1.2. Go to the Encryption tab and click on Generate Key.
- 3.14.1.3. Select the desired Key Size by selecting an option from the Key Size dropdown.
- 3.14.1.4. Uncheck the box for “Begin encrypting using this key immediately (uncheck if you need to distribute this key to decrypting relays)”.
- 3.14.1.5. Save the encryption key.
- 3.14.1.6. Securely copy the saved encryption key to all desired decrypting IEM relays. The key should be placed in “Program Files\BigFix Enterprise\BES Relay\Encryption Keys\”.
- 3.14.1.7. Access the Encryption tab of the IEM Administration Tool. Select Enable Encryption and click OK.
- 3.14.1.8. Select Yes to propagate the action site.
- 3.14.1.9. Deploy the task titled “BES Client Setting: Encrypted Reports” using an appropriate setting of either required, if possible, or disabled.

3.14.2. Linux:

- 3.14.2.1. Run the IEM Administration Tool with proper values.
- 3.14.2.2. BESAdmin.sh -reportencryption -generatekey [-privateKeySize=<min|max>] -deploynow=no -outkeypath=<path> -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>]
- 3.14.2.3. Generate Key with option -generatekey.
- 3.14.2.4. Select the desired Key Size by setting min or max for -privateKeySize.
- 3.14.2.5. Begin encrypting using this key immediately with option -deploynow=yes (if you need to distribute this key to decrypting relays use option -deploynow=no).
- 3.14.2.6. Save the encryption key to specific path with option -outkeypath=<path>
- 3.14.2.7. Securely copy the saved encryption key to all desired decrypting IEM relays. The key should be placed in “/var/opt/BESRelay/Encryption Keys”.
- 3.14.2.8. To enable Encryption run IEM Administration Tool: BESAdmin.sh –reportencryption -enablekey -sitePvkLocation=<path+license.pvk> [-sitePvkPassword=<password>]
- 3.14.2.9. Deploy the task titled “BES Client Setting: Encrypted Reports” using an appropriate setting of either required, if possible, or disabled.

3.15. Given a functional IEM server on a network with no Internet access and an Internet-connected Windows machine on a different network,

use the IEM Airgap tools to download IEM content on the Internet-connected computer so that site content and downloads are successfully populated on the IEM server.

SUBTASK(S):

3.15.1. Windows:

- 3.15.1.1. Identify a Windows machine with Internet access to act as the air-gap gather server (it does not have to be an IEM server).
- 3.15.1.2. Run the Air-gap tool on the IEM server to put the IEM server's gather requests and a copy of the Air-gap tool onto a storage device.
- 3.15.1.3. Run the Air-gap tool from the storage device, on the air-gap gather server, to copy the results of the gather request onto a storage device.
- 3.15.1.4. Run the Air-gap tool from the storage device, on the IEM server, to copy the results of the gather request onto the IEM server.
- 3.15.1.5. Verify that the sites were gathered properly by checking that the aggregate fixlet count increased as a result.
- 3.15.1.6. Run the BESDownloadCacher tool on the air-gap gather server for each site with download content to be gathered.
- 3.15.1.7. Copy the cached downloads to the IEM server's cache directory (using a thumb drive or other method).
- 3.15.1.8. Verify that the download content was downloaded by deploying a fixlet that depends on one of the cached downloads.

3.15.2. Linux:

- 3.15.2.1. Identify a Windows machine with Internet access to act as the air-gap gather server (it does not have to be an IEM server).
- 3.15.2.2. Download the Windows Endpoint Manager Airgap utility (BESAirgapTool.exe), from the Utilities page. https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Endpoint Manager/page/Utilities
- 3.15.2.3. From your Windows IEM Console system get the following two libraries libBEScrypto.dll and libBEScryptoFIPS.dll. Put them in the same storage device as the BESAirgapTool.exe
- 3.15.2.4. Run the Air-gap tool on the IEM server. From the generated airgap.tar file extract the AirgapRequests.xml file. Place it on the same storage device where you have copied the Windows Airgap Tool executable and libraries.
- 3.15.2.5. Plug the storage device on the Windows machine with internet access.
- 3.15.2.6. Run the Air-gap tool from the storage device.
- 3.15.2.7. Plug the storage device on the IEM server and copy the AirgapResponse file in to the airgap folder on the Linux IEM server directory.
- 3.15.2.8. Run the Air-gap tool from the IEM server and copy the results of the gather request onto the storage device.

3.15.2.9. Verify that the sites were gathered properly by checking that the aggregate fixlet count increased as a result.
3.15.2.10. Download the Windows BESDownloadCacher tool (BESDownloadCacher-5.8.3.exe), from the Utilities page. https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Endpoint Manager/page/Utilities
3.15.2.11. Copy the BESDownloadCacher to the storage device and place it where the gather request is stored
3.15.2.12. Plug the storage device to the Windows machine again
3.15.2.13. Run the BESDownloadCacher tool on the Windows machine for each site with download content to be gathered.
3.15.2.14. Copy the cached downloads to the IEM server's cache directory (using a thumb drive or other method).
3.15.2.15. Verify that the download content was downloaded by deploying a fixlet that depends on one of the cached downloads.

3.16. Given a knowledge of the IEM platform components and content, describe the purpose and effect of IEM utilities, so that there is an understanding of how they an be used in management and troubleshooting of IEM deployment platform components and content.

SUBTASK(S):
3.16.1. Describe purpose, capabilities, and function of each supported utility:
3.16.2. PropertyIDMapper – Creates a PropertyIDMap table within the BFEnterprise database to link properties with their corresponding names.
3.16.3. Remove Utility – Identifies installed components software on host computer and allows uninstall of one or all components and related configuration data. Note: Installation and upgrade keys in Windows registry remain.
3.16.4. CleanupIEMRegistryKeys – Removes Windows registry keys from product installation or upgrade. Note: Presence of these keys prevents Client Deploy Tool from installing a new client on the computer.
3.16.5. Computer Remover – Removes all specified computer data from database.
3.16.6. Audit Trail Cleaner Reclaim database space – Removes previous and deleted versions of custom Fixlets, properties, analyses and actions from database.
3.16.7. Download Cacher – Prefetches software files required to apply all Fixlets in a specified content site.
3.16.8. Client Diagnostics – Uploads logs and diagnostics from a specified client.
3.16.9. Fixlet Debugger (QnA) – Performs Relevance Language queries and Action Script commands on host computer. Note: Action Script can be destructive to files and computer configuration; Relevance is not destructive.

3.16.10. SHA1 Tool – Returns SHA1 checksum value and has option to generate Action Script “download” statement for specified file.
3.16.11. Make-Prefetch Tool – Generate Action Script "Prefetch" statement for specified file. Note: Supports SHA1 and SHA256 hashes.
3.16.12. BFArchive Tool – Compresses specified file or folder for efficient downloading and extraction through Action Script commands.
3.16.13. Relays.dat Parser – Inspect relays.dat file on the host computer, to display the computers list of known relays in the deployment.
3.16.14. BES Client Refresher – Forces specified client to report all state data.
3.16.15. Airgap Tool – Updates content on a server in an isolated network.
3.16.16. Server Signing Key Tool – Enables specific maintenance operations (such as preparation of existing 8.2 server to recognize console operators from LDAP.
3.16.17. BESRegistrationListCleaner – Removes child registrations over 24 hours old from relay registration list, effectively un-registering them.
3.16.18. RESTAPI CLI – Processes REST (Representable State Transfer) commands. Note: Web Reports service is required to run REST API (Application Programming Interface) and REST CLI (Command-line Interface)
3.16.19. Identify which of the supported utilities can be destructive where IEM data, or managed computer files or configuration is concerned:
3.16.20. Remove Utility – Can remove IEM software components from host computer.
3.16.21. CleanupIEMRegistryKeys – Removes Windows registry keys.
3.16.22. Computer Remover – Removes all specified computer data from database.
3.16.23. Audit Trail Cleaner Reclaim database space – Removes previous and deleted versions of custom Fixlets, properties, analyses and actions from database.
3.16.24. Fixlet Debugger (QnA) – Action Script commands run on host computer can be destructive to files and computer configuration.
3.16.25. BESRegistrationListCleaner – Removes child registrations over 24 hours old from relay registration list, effectively un-registering them.

Section 4 - Problem Determination and Performance Tuning

4.1. Given that the IBM Endpoint Manager (IEM) server is up and running, use the IEM console to review the IEM Deployment Health Checks dashboard in conjunction with the Deployment Overview dashboard so that sufficient information has been gathered to properly gauge the health of the deployed components of a IEM installation.

SUBTASK(S):

4.1.1. Using the IEM console, navigate to the BigFix Management domain.
4.1.2. Select the Deployment Overview dashboard
4.1.3. Check BES agents reported in the last day
4.1.4. Check BES relays reported in the last day
4.1.5. Check average number of BES clients per relay
4.1.6. Select the Deployment Health Check dashboard.
4.1.7. Perform a quick scan of the status of the health checks to verify they are all “Passed” (Green)
4.1.8. Gather information of IEM environment by initiating a Collect Deployment information function located in the Deployment Information section.
4.1.9. Check number of computers.
4.1.10. Check numbers of active computers.
4.1.11. Check relay information.
4.1.12. Number of relays
4.1.13. Maximum distance to relays
4.1.14. Check console information.
4.1.15. Check number of console computers.
4.1.16. Check number of console operators.
4.1.17. Check license information.
4.1.18. Check license site number.
4.1.19. Check license expiration date.
4.1.20. Check action information.
4.1.21. Number of actions
4.1.22. Number of top level actions
4.1.23. Number of open actions
4.1.24. Check fixlets information.
4.1.25. Relevant fixlets
4.1.26. Non-relevant fixlets
4.1.27. Number of hidden fixlets
4.1.28. Check tasks information.
4.1.29. Relevant tasks
4.1.30. Non-relevant tasks
4.1.31. Number of hidden tasks
4.1.32. Check analyses information.
4.1.33. Relevant Analyses
4.1.34. Non-relevant Analyses
4.1.35. Number of hidden Analyses
4.1.36. Review BES relay health section.

4.1.37. Download folders.
4.1.38. Number of clients per relay
4.1.39. relay service stopped.
4.1.40. Review BES Console Health section.
4.1.41. Too Many Offline computers
4.1.42. Stopped And Expired Actions
4.1.43. Stopped And Expired Actions Hidden Actions
4.1.44. Expired computers
4.1.45. Duplicate computers.
4.1.46. Review BES server health section.
4.1.47. BES server free disk space
4.1.48. Number of clients on main BES server
4.1.49. Number of relays on main BES server
4.1.50. SQL Server service pack
4.1.51. Review BES client health.
4.1.52. BES client distance from BES relays
4.1.53. WMI properties
4.1.54. Actions targeted using lists
4.1.55. Location properties
4.1.56. Review Deployment Optimization section.
4.1.57. Support analysis activation
4.1.58. Open actions.
4.1.59. Open hidden actions.
4.1.60. Operators by using Policy Actions
4.1.61. Statistical Property evaluation period
4.1.62. ICMP settings Controls
4.1.63. Components per baseline
4.1.64. Action applicability too large
4.1.65. Policy actions not targeted by property
4.1.66. Superseded fixlets
4.1.67. Support analysis removal
4.1.68. Efficient MIME
4.1.69. Office deployment control initial assignment
4.1.70. Deprecated fixlet sites
4.1.71. Console operators have never logged in.
4.1.72. Console operator accounts not being used
4.1.73. License expiration

4.2. Given an operational IEM server, IEM console, and a system running the IEM agent, enable debug logging so that all targeted IEM agents produce detailed logs for use in troubleshooting.

SUBTASK(S):
4.2.1. Take action with the fixlet titled “BES Client Setting: Enable Debug Logging”.

4.2.2. Enter in an appropriate value in the Action Parameter dialogue and click OK.
4.2.3. Deploy the action.

4.3. Given an operational IEM console, enable the IEM console debug menu so that a IEM console operator will have easy access to various tools useful in debugging IEM issues.

SUBTASK(S):
4.3.1. Open the IEM console and hold down the following keys at the same time: **Ctrl + Alt + Shift + D.**
4.3.2. In the dialogue box select the checkbox **"Display Debug Menu"**.

4.4. Given a IEM server with sub-optimal performance, identify the factors affecting performance so that they can be addressed.

SUBTASK(S):
4.4.1. In the console, pull down File -> Preferences to inspect the length of time between heartbeats and the amount of time to wait before marking a computer offline.
4.4.2. By default the IEM agents "check in" to the IEM server on a regular interval known as a "heartbeat". When the IEM agents send in a heartbeat to the IEM server, they will update their "Last Report Time" property along with any other properties that have changed since the last heartbeat. In medium to large IEM deployments, processing the heartbeats can consume significant IEM server resources. To ensure optimal performance, the heartbeat should be raised from the default 15 minutes to 1 hour or even 2-6 hours for larger IEM deployments. The heartbeat can be changed under the File > Preferences menu in the IEM console.
4.4.3. When the IEM console is being used, the IEM console will query the IEM server database and cache the results locally. The cache is updated according to the IEM console refresh period. The more IEM agents, the more data is transferred to the IEM console using database resources and network bandwidth. The IEM console refresh period should be raised to from its default of 15 seconds to 30 seconds, 60 seconds, or even 120 seconds for large deployments with lots of simultaneous IEM console users. The refresh rate can be changed under the File > Preferences menu in the IEM console (note that this setting is per IEM console.
4.4.4. If endpoints are not reachable via UDP (e.g. clients in a DMZ behind a firewall that blocks UDP), they will not receive real-time notifications of new content and will instead check in at the clients' command poll interval, which is 24 hours by default. Use this task to change the command poll interval for such clients:
    4.4.4.1. BES Client Setting: Enable Command Polling
    4.4.4.2. IEM agent CPU utilization settings can affect IEM agent performance significantly. These settings adjust it:

4.4.4.3. _BESClient_Resource_WorkIdle (milliseconds; range 1-500; default 10): The IEM agent will do work (evaluate relevance) for a designated amount of time then go to sleep for a designated amount of time. This setting controls how many milliseconds to work before going to sleep in each cycle. If this number is high in comparison to the _BESClient_Resource_SleepIdle setting, then the IEM agent will evaluate fixlet relevance faster, but the CPU usage will be higher.

4.4.4.4. _BESClient_Resource_SleepIdle (milliseconds; range 1-500; default 480): The IEM agent will do work (evaluate relevance) for a designated amount of time then go to sleep for a designated amount of time. This setting controls how many milliseconds to sleep after working in each cycle. If this number is high in comparison to the _BESClient_Resource_WorkIdle setting, then the IEM agent will take longer to evaluate fixlet relevance, but the CPU usage will be lower.

4.4.4.5. The IEM server and IEM relay's normal operations involve creating and processing a lot of temporary files. This activity is essential for good performance of IEM, but can be slowed down dramatically if a virus scanner is scanning each file. To address this issue, configure your virus scanner on the IEM server and IEM relay computers to exclude the IEM server folder and all subfolders or the IEM relay and its subfolders. Refer to instructions from your virus scanner for more information on how to set this exclusion rule.

4.4.4.6. The IEM server and IEM relay's normal operations involve creating and processing a lot of temporary files. This activity is essential for good performance of IEM, but can be slowed down dramatically if Windows file indexing is turned on or if the drive is set to use file compression. If these computers have indexing or compression enabled, you should disable them.

4.5. Given a IEM server that is having issues gathering site content, troubleshoot the problem so it can gather site content and downloads.

SUBTASK(S):

4.5.1. Browse to http://MyIEMServerURL:52311/rd for the Relay Diagnostics page. Click the “Gather Status” link to verify that sites are in the “Failed” state.

4.5.2. Windows:

4.5.2.1. Use Internet Explorer on the IEM server to browse to http://sync.bigfix.com and http://gatherer.bigfix.com. If they are not both reachable, a proxy server may need to be configured and/or the sites may need to be unblocked at the network’s firewall.

4.5.2.2. Go into the Services control panel to restart the Gather Service. Check the Gather Status on the Relay Diagnostics page to see if the issue is resolved.
4.5.2.3. In the IEM console, pull down File -> Preferences and click the "Clear Cache" button, then restart the console. Check the Gather Status on the Relay Diagnostics page to see if the issue is resolved.
4.5.2.4. Use the Air-gap method and tool to attempt to gather the site(s) manually. (See "Gather IEM Content on an Air-gapped Network".)
4.5.2.5. Perform a gather state refresh to completely reset the gather status. Click the Gather button on the site.
4.5.2.6. Review the gather.db log file. C:\Program Files\BigFix Enterprise\BES Server\GatherDBData

4.5.3. Linux
4.5.3.1. Use wget on the IEM server to request data from http://sync.bigfix.com and http://gatherer.bigfix.com. If they are not both reachable, a proxy server may need to be configured and/or the sites may need to be unblocked at the network's firewall.
4.5.3.2. Restart the Gather Service "/etc/init.d/besgatherdb restart" as rootuser. Check the Gather Status on the Relay Diagnostics page to see if the issue is resolved.
4.5.3.3. In the IEM console, pull down File -> Preferences and click the "Clear Cache" button, then restart the console. Check the Gather Status on the Relay Diagnostics page to see if the issue is resolved.
4.5.3.4. Use the Air-gap method and tool to attempt to gather the site(s) manually. (See "Gather IEM Content on an Air-gapped Network".)
4.5.3.5. Perform a gather state refresh to completely reset the gather status. Click the Gather button on the site.
4.5.3.6. Review the gather.db log file. /var/opt/BESServer/GatherDBData/

4.6. Given a functional IEM server, console and relay, determine why IEM agent installations are failing by using the client deployment tool so that the source of the client deployment issue has been determined.

SUBTASK(S):
4.6.1. Determine if the necessary tool requirements have been met:
4.6.2. You are logged in with an account that has admin rights on the targeted computers
4.6.3. The targeted computers meet the OS requirements (2000, W2K3, XP, Win7, Vista, W2K8, W2K8R2)
4.6.4. The targeted computers must have the following services running (workstation, server, net logon, remote registry)
4.6.5. The targeted computers must have "File and Print" sharing enabled
4.6.6. There are no firewall policies that block RPC connections

4.6.7. Use the Net use command to check for errors the client deployment tool may be encountering (net use *\\targetname\admin$ /user:domain\user password
4.6.8. Error codes and there meaning
4.6.9. System error 53 has occurred. The network path was not found. ADMIN$ is not available
4.6.10. System error 1219 has occurred. Multiple connections to a server or shared resource by the same user, using more than one user name, not allowed. Disconnect all previous connections to the server or shared resource and try again. If the machine used to run the BES client deployment tool already has a connection to remote machine ADMIN$ share, using a different credential, this error will occur.
4.6.11. System error 1311 has occurred. There are currently no logon servers available to service the logon request. The Domain server is not available for authentication.
4.6.12. System error 1326 has occurred. Logon failure: unknown user name or bad password.
4.6.13. System error 5 has occurred. Access is denied user name/password correct, but account does not have permission to ADMIN$ share.
4.6.14. No network provider accepted the given network path. The agent or the server could not be resolved during the client deployment tool process.

4.7. Given the requirement for IEM to efficiently transport large payloads, describe the steps required to troubleshoot an array of poorly performing IEM relays so that the issue with IEM relays can be diagnosed and resolved.

SUBTASK(S):
4.7.1. Ensure that enough relays have been installed and configured for the environment.
4.7.2. Check that the IEM relay service/process is started on all relays.
4.7.3. Check the number of hops between a agent and its closest relay.
4.7.4. Ensure all relays are available by using the Deployment Health Checks on the Bigfix Management domain
4.7.5. Review the BES Relay Service Stopped check.
4.7.6. Review the BES Relay Free Disk Space check.
4.7.7. Determine problems with automatic relay selection.
4.7.8. Endpoint to relay.
4.7.9. relay to relay.
4.7.10. Review the agent list of relays in relays.dat.
4.7.11. Review relay affiliation.
4.7.12. Check the relay selection frequency.
4.7.13. Follow relay selection through hierarchy of relays: primary, secondary, fail-over and finally IEM server.
4.7.14. Check whether relays are set to manual configuration or automatic configuration.

4.7.15. Ensure that Relay to Relay configuration was manually configured.
4.7.16. Ensure that relays are up and running 24/7.
4.7.17. Check the relay automatic selection settings.
4.7.18. Tune the settings if required.
4.7.19. Identify relay lack of disk space issues.
4.7.20. Calculate theoretical amount of disk space required on each relay.
4.7.21. Build different size Payload.
4.7.22. Do performance testing to identify bottlenecks.
4.7.23. Review the logs: C:\Program Files\BigFix Enterprise\BES Relay\logfile.txt.

4.8. Given a functional IEM and a non-master operator in unable to see console content; determine the cause so that the issue can be resolved.

SUBTASK(S):
4.8.1. Log in to the console as the master operator
4.8.2. Go to Operator under the BigFix Management domain.
4.8.3. Select the user name that is having the issue.
4.8.4. Verify that the user is subscribed to sites.
4.8.5. Right-click a single operator in question from the list and select Assign User Management Rights from the pop-up menu
4.8.6. Click the Add button to verify management rights are assigned to the selected operator.
4.8.7. Log in as the Non-master operator and verify console content is now visible.

4.9. Given the need to manage an IEM environment by using Web Reports, describe how to resolve Web Reports technical issues so that Web Reports issues have been diagnosed and resolved.

SUBTASK(S):
4.9.1. Ensure that the Web browser installed and used is fully supported by IEM.
4.9.2. Ensure that Web Reports is the right version for your IEM environment.
4.9.3. Check to ensure that SSL connectivity was properly configured.
4.9.4. Check that there is a proper SSL certificate.
4.9.5. Should be in OpenSSL *.pem file format.
4.9.6. For HTTPS configuration refer to the IEM Web Reports user's guide.
4.9.7. Check message indicating whether or not the certificate can be trusted.
4.9.8. Check to see if certificate is issued by a trusted certificate authority (CA).
4.9.9. Check to see whether the correct fully qualified host name is specified.
4.9.10. Check to see if the certificate has not expired.
4.9.11. Check a stand-alone Web Reports server configuration.
4.9.12. Check the requirements in the technical documentation.
4.9.13. Check memory requirements for the number of IEM agent in the IEM environment.
4.9.14. Check CPU size of a stand-alone Web Reports server.

4.9.15. Make changes if necessary.
4.9.16. Check the configuration of Web Reports running on the database server.
4.9.17. Refer to documentation to ensure that it was properly configured.
4.9.18. Check that Emails can be sent.
4.9.19. Check your Email accounts and server.
4.9.20. Ensure that the SMTP server is up and running.
4.9.21. Check the Database server cache settings.
4.9.22. Fine-tune the default length of 15 seconds if required.
4.9.23. Run reports to see if Web Reports work correctly.
4.9.24. Run a prepackaged report.
4.9.25. Identify missing data in reports.
4.9.26. Ensure that all required databases have been added.
4.9.27. Export Reports to PDF function does not work.
4.9.28. Check documentation to understand what is required to be done for the configuration.
4.9.29. Ensure that the export to PDF function was properly configured.
4.9.30. Review specific log files for Web Reports.
4.9.31. Ensure that the log file feature is enabled.

4.10. Given an IEM agent that is not fully functional, perform the appropriate troubleshooting tasks so that the root cause can be identified and fixed appropriately leading to a functional agent.

SUBTASK(S):

4.10.1. **"Troubleshoot why the agent does not appear in the console"**
- 4.10.1.1. Determine whether or not the agent exists in a master operator's console view.
- 4.10.1.2. If not, validate that:
- 4.10.1.3. The endpoint has the IEM agent software installed.
- 4.10.1.4. The IEM agent service/agent is in a running state.
- 4.10.1.5. The IEM agent has the appropriate masthead/license for the appropriate IEM Server instance/deployment.
- 4.10.1.6. The IEM agent is connected to the network, and is able to communicate (register, gather, and post reports) with its relay or the main IEM server.
- 4.10.1.7. If it does, proceed to next step.
- 4.10.1.8. Ensure that the console operator has management rights over the agent in question, by launching the IEM console as a master operator, select the All Content domain, select Operators, find the Operator in question, then validate that the endpoint/agent is listed within their Administered Computers tab.

4.10.2. **"Troubleshoot why the agent appears unresponsive to actions"**
- 4.10.2.1. Some common reasons why this might occur:
- 4.10.2.2. IEM agent is off or not connected to the network - The IEM agent obviously cannot report if the computer is off or if the

IEM agent cannot connect to the IEM server or IEM relays. It is easy to see the last report time of the IEM agent in the IEM console to see if the computer has reported recently.

4.10.2.3. IEM agent did not receive UDP 'ping' - Whenever there is a new action, new fixlets available, or new downloads available, the IEM server and IEM relays send a UDP 'ping' on the IEM port number (by default it is 52311) to the last known IEM agent IP. If this message is not received, the IEM agent will not know there is a new action to report on. By default, the IEM agent will automatically gather once per day to see if there are any new actions or fixlets available. At this time, they will notice any actions sent out. You can test if the IEM agent can receive UDP 'pings' by right-clicking on the computer in the IEM console and sending a refresh. If the IEM agent receives the UDP message, it will shortly update its last report time (within a minute or two usually). If it doesn't update that time, it indicates it didn't receive the UDP message.

4.10.2.4. Note: The IEM agent will report in normally on their heartbeat interval so make sure that the IEM agent was responding to the refresh and wasn't reporting on its normal schedule. The IEM agent will not receive their UDP messages if there is a firewall blocking UDP packets on the IEM port (52311 by default), if there is a NAT translator between the IEM server and the IEM agent (or IEM relays and IEM agent), if the computers are running personal firewalls like Zone Alarm, Black Ice, or the XP firewall, or if the IEM agent have switched IP addresses since the last time it registered (by default the IEM agent registers every 6 hours).

4.10.2.5. Note: Another simple test from the IEM console can help determine if UDP messages are being blocked. On the Computers tab in the IEM console select a computer and then right-click to select the option 'Send Refresh'. If UDP messages are able to get to the IEM agent you will see an entry similar to 'ForceRefresh command received' in the agent's log file.

4.10.3. **“Determine why agents appear gray in the console”**

4.10.3.1. Computers that are grayed out in the IEM console are considered to be offline. Computers will be considered offline if the IEM agent has not reported in a specified amount of time. By default, the IEM agent sends a heartbeat every 15 minutes and if the IEM server has not received a heartbeat in 45 minutes from a particular IEM agent, the computer will be marked offline. The length of time between heartbeats and the amount of time to wait before marking a computer offline are

both configurable in the IEM console under File -> Preferences.

4.10.3.2. There are several reasons why a agent's reports may not have reached the IEM console within the time that the IEM console is configured to mark them as gray/offline:
4.10.3.3. The agent is legitimately offline or off the network.
4.10.3.4. The agent is having network connectivity issues with its relay.
4.10.3.5. Check the agent logs for indications of network connectivity issues with its relay, such as failed registration attempts, failed father attempts, or failures to post reports .
4.10.3.6. The agent is having performance issues, and is unable to consistently report in a timely manner on the defined heartbeat.
4.10.3.7. Check the agent logs for indications of reporting performance issues by comparing the intervals between Report Posted Successfully entries and the defined heartbeat.
4.10.3.8. Send the agent a refresh through the console. If it responds relatively quickly, but hadn't been posting reports on a consistent basis previously, it is typically an indication of a long running relevance expression causing the agent to appear 'hung'. Enable the agent's debug log and the Usage Profiler to identify the potentially problematic relevance expression or content item.
4.10.3.9. The relay is not properly forwarding the agent's reports up the relay hierarchy to the main IEM server.
4.10.3.10. Check the relay's forwarding BufferDIR for the existence of agent reports.
4.10.3.11. The main IEM server is not processing the incoming agent reports, or not processing them in a sufficiently quick manner.
4.10.3.12. Ensure that the FillDB service is running.
4.10.3.13. The IEM console is not properly updating its session cache from the information available in the IEM Database.
4.10.3.14. Validate ODBC connectivity.
4.10.3.15. Ensure that there are no database locks.
4.10.3.16. Duplicate computer object.
4.10.3.17. Delete old computer objects.

4.11. Given an existing IEM deployment, troubleshoot and resolve issues related to filldb so that the data will be inserted into SQL/DB2 and inserted in to the console in a timely manner.

SUBTASK(S):

4.11.1. Determine if **issues** with filldb are related to data/connection problems or if issues are performance related.
4.11.2. Connection Issues- FillDB Debug Log -- Used to troubleshoot issues with agent reports or FillDB connection errors common on remote database deployments.

4.11.3. Enable Debug log
4.11.4. Windows: by setting registry key. HKLM\Software\Bigfix\Enterprise Server\FillDB default value is “critical” change to “critical;debug” by default log will be in the FillDBData folder on the IEM server.
4.11.5. Linux: by setting configuration entry. [Software\BigFix\Enterprise Server\FillDB] default value is “critical” change to “critical;debug” by default log will be in the FillDBData folder on the IEM server.
4.11.6. Check filldb service logon account and reset password.
4.11.7. Check Database:
4.11.8. Windows: Check SQL to ensure filldb service account has access to SQL server and to BFEnterprise database.
4.11.9. Linux: Check DB2 to ensure filldb service account has access to DB2 server and to BFEnterprise database.
4.11.10. Restart filldb service on IEM server.
4.11.11. Performance Issues - FillDB Performance Log -- Used to measure and troubleshoot FillDB performance issues with the server/database Disabled by default.
4.11.12. Enable performance log –
4.11.13. Windows: HKLM\Software\BigFix\Enterprise server\FillDB set “PerformanceDataPath” for example c:\program files\BigFix Enterprise\BES Server\FillDBData\FillDBPerf.log
4.11.14. Linux: [Software\BigFix\Enterprise Server\FillDB] set “PerformanceDataPath” for example /var/opt/BESServer/FillDBData/FillDBPerf.log
4.11.15. Restart Filldb service on IEM server.
4.11.16. Windows
    4.11.16.1. Check SQL transaction log and shrink if over 2GB.
    4.11.16.2. Ensure SQL is set to use simple mode.
    4.11.16.3. Check SQL for memory issues – run the query “DBCC MEMORYSTATUS” look at the Buffer Pool section. If the Committed value is greater than the Target, that is an indication of internal memory pressure. A high percentage (greater than 75-80%) of stolen pages relative to Target is an indicator of the internal memory pressure.
    4.11.16.4. Check to make sure the default reindexing job is running in SQL daily.
4.11.17. Linux
    4.11.17.1. DB2 Check size of DB2DIAG.LOG to avoid the system to run out of space on hard drive
    4.11.17.2. Make yourself familiar with db2dp tool to retrieve informatione from DB2 about database transactions, tablespaces, table statistics, dynamic SQL, database configurations, and many other database details.

4.12. Given an issue with a fixlet/task not working as expected, troubleshoot the issue so that enough information has been gathered to determine the cause of the issue and resolve it.

SUBTASK(S):
4.12.1. Troubleshoot Relevance statements.
4.12.2. Identify the problem relevance statement.
4.12.3. Launch Fixlet Debugger and insert relevance statement.
4.12.4. Press CTRL+Enter to execute the statement.
4.12.5. Identify problem and correct.
4.12.6. Copy fixed relevance statement to source.
4.12.7. Troubleshoot ActionScripts.
4.12.8. Identify the problem fixlet/task.
4.12.9. Identify ActionScript line.
4.12.10. By using the Status information from a completed action, find the failed line
4.12.11. Open the <date stamp>.log file in the client directory (Windows: C:\Program Files\BigFix Enterprise\BES Client__BESData__Global\Logs) and search for failures.
4.12.12. Determine issue in the action line.
4.12.13. If program execution failing, manually execute command line
4.12.14. Correct issue with command line in ActionScript.
4.12.15. If relevance issue, copy to Fixlet Debugger running on problem system .
4.12.16. Correct issue with relevance statement.

4.13. Given that the new IEM server has already been set up, migrate all endpoints so that they are successfully reporting to the new IEM server.

SUBTASK(S):
4.13.1. Determine the operating systems of the endpoints to be Migrated.
4.13.2. If migrating only Windows, decide if the migration strategy will be to migrate via a URL or via a network share.
4.13.3. If using a network share determine if a null share needs to be created.
4.13.4. Based on the instructions in the migration fixlet, make the masthead from the NEW IEM server accessible to the infrastructure. This is generally accomplished by copying it to the OLD IEM server.
4.13.5. Uninstall all relays from the OLD IEM infrastructure.
4.13.6. Migrate the Endpoints via the following fixlets:
    4.13.6.1. Switch BES Client Action Site Masthead – BES >= 7
    4.13.6.2. TROUBLESHOOTING: Switch ActionSite Masthead on Solaris
    4.13.6.3. TROUBLESHOOTING: Switch ActionSite Masthead on Max OS X
    4.13.6.4. TROUBLESHOOTING: Switch ActionSite Masthead on RHEL/SUSE

4.13.6.5. TROUBLESHOOTING: Switch ActionSite Masthead on VMware ESX server
4.13.6.6. TROUBLESHOOTING: Switch ActionSite Masthead on AIX
4.13.6.7. TROUBLESHOOTING: Switch ActionSite Masthead on HP-UX
Note: Be sure to not run the migration fixlet against the OLD IEM server

4.13.7. Once the endpoint runs the above fixlet, it's relay settings will be removed, and it will be repointed to the new server. NOTE: The action on the OLD IEM Infrastructure will not report back as completed.

4.13.8. Redeploy the relay as appropriate.

Section 5 - Application Configuration

5.1. Given the requirement to promote IBM Endpoint Manager to prospective customers, describe the purpose and capabilities of the IEM products, so that the customer understands the IEM product suite and how they can help with their business needs.

SUBTASK(S):

5.1.1. Describe purpose of each IEM product (sales bundle) in the product family:

- 5.1.1.1. Core Protection – Helps protect physical and virtual endpoints from malware and malicious threats before they can exploit vulnerabilities.
- 5.1.1.2. Datacenters – Enables users to perform advanced automation tasks across servers, including task sequencing.
- 5.1.1.3. Lifecycle Management – Provides near time visibility into the state of endpoints, giving administrators advanced functionality for managing OS deployment and migrations, software installations and updates, and remote administration.
- 5.1.1.4. IBM MaaS360 (Formerly Mobile Device Management) -- Delivers a complete enterprise data loss prevention solution with consistent and seamless workflows, and empowers your users by giving them access to business documents on mobile devices while providing total manageability and control in a secure, encrypted container, and simplifies mobile application management by delivering an easy-to-use enterprise app catalog with full security and operational lifecycle management of apps across mobile device platforms.
- 5.1.1.5. Patch Management – Allows you to assess, deploy and manage patches for operating systems and applications throughout heterogeneous environments.
- 5.1.1.6. Power Management – Enables enforcement of granular, highly targeted energy conservation policies throughout your organization without impacting employee productivity or security requirements.
- 5.1.1.7. Security and Compliance – Provides unified, near real-time visibility and enforcement of patches, configuration baselines and multiple third-party anti-malware systems. Compliance analytics and host-based vulnerability reporting provides assurance to internal and external auditors.
- 5.1.1.8. Server Automation – Enables users to perform advanced application deployment throughout servers, including task sequencing—without the need for programming skills.
- 5.1.1.9. Software Use Analysis – Identifies licensed and unlicensed software with in-depth granularity. It tracks software usage patterns and trends to support better planning, budgeting and vendor license compliance.

5.1.2. Identify computer management applications within each IEM product:

5.1.2.1. Core Protection includes the following computer management applications: Anti-Malware, Firewalls, Data Loss Prevention, and Device Control.
5.1.2.2. Datacenters includes the following computer management applications: OS & App Patching, Basic HW & SW Inventory, Software Distribution, OS Deployment, Remote Control, Security Configuration Management, Vulnerability Assessment, Compliance Analytics, 3rd Party Endpoint Protection Mgmt, and Self-Quarrantine.
5.1.2.3. Lifecycle Management includes the following computer management applications: Patch Management, Basic HW & SW Inventory, Software Distribution, OS Deployment, and Remote Control.
5.1.2.4. IBM MaaS360 (Formerly Mobile Device Management) includes the following computer management applications: Application Security, Threat Management, Secure Mail, Secure Document Sharing (Secure Browser, Mobile Enterprise Gateway, Mobile Expense Management, MaaS360 On-Premises, Laptop Management), Application Management, and Compliance.
5.1.2.5. Patch Management) includes the following computer management applications: OS Patching, Application Patching, and Offline Patching.
5.1.2.6. Power Management) includes the following computer management applications: Power Management with Carbon and cost reduction reports, plus End-user Dashboard.
5.1.2.7. Security and Compliance) includes the following computer management applications:Patch Management, Security Configuration Management, Vulnerability Assessment, Compliance Analytics, 3rd Party Endpoint Protection Management, and Self-Quarantine.
5.1.2.8. Server Automation) includes the following computer management applications: Advanced Server Management & Task Automation, Physical & Virtual Server Management, and Middleware Management.
5.1.2.9. Software Use Analysis) includes the following computer management applications: SW Inventory, SW Usage Reporting, and SW Catalog Correlation.

5.2. Given the need to install IBM Endpoint Manager (IEM) for Software Usage Analysis and that all pre-requirements including the database have been installed and configured, Install and configure IEM for Software Usage Analysis so that the desired reporting functionality will be fulfilled

SUBTASK(S):
5.2.1. Deploy the rpm package to the target SUA server

5.2.1.1. In the console, select the Systems Lifecycle domain and from the navigation tree expand Software Use Analysis and then Server Setup. Select the Software Use Analysis 9.1 dashboard
5.2.1.2. Select the target system from the list in the dashboard and click the Deploy Installer button
5.2.1.3. Once the download has completed, the installer package will be found on the endpoint under /root/IEMInstaller with the name SUA-server-9.1.tar.gz.
5.2.1.4. Run the following to decompress and unzip the file, tar -zxvf SUA-server-9.1.tar.gz

5.2.2. Run the installer
5.2.2.1. Run the following command to being the installation process and invoke the gui based installer, ./setup-server-linux-x86_64.sh
5.2.2.2. Click ***Ok*** after selecting the correct language
5.2.2.3. Click ***Next***
5.2.2.4. Accept the IBM and non-IBM terms and click ***Next***
5.2.2.5. Specify the SUA installation directory, and click ***Next,*** note the DB will be installed in the home directory of the database instance.
5.2.2.6. Specify the web console port and click ***Next***
5.2.2.7. Confirm the install summary and click ***Install***
5.2.2.8. While installing the tool will give the opportunity to correct any issues, if there are none, click ***Next***
5.2.2.9. Once the install is complete click ***Done*** and a web browser will open to finish configuration

5.2.3. Configure SUA
5.2.3.1. Enter all configuration data about the new database and click ***Create***
5.2.3.2. The next screen will prompt to create the admin user, enter the credentials and click ***Create***
5.2.3.3. The next screen will prompt for connection credentials for the IEM server, Web Reporting Server, and an IEM Master Operator account. Note if the IEM server is using a SQL database, SQL server authentication must be selected, click ***Create***
5.2.3.4. The next step is to do the initial import, once this is completed the SUA application will be completely installed. Click ***Import Now***

5.3. Given a successfully installed IEM server, a master operator account and a license for IEM for Security Configuration Management, install IEM for Security Configuration Management so that endpoints' security configuration can be collected and measured.

SUBTASK(S):
5.3.1. Log on to the IEM console with a master operator account.
5.3.2. Navigate to the BigFix Management domain.
5.3.3. Open the License Overview Dashboard.

5.3.4. Find the newly licensed site within the dashboard, and click the Enable link. If you do not see your newly licensed site, click the Check for license update button, which will tell the server to look for newly licensed sites.
5.3.5. To subscribe agents to the site, follow the link in the site name. You can also access the site document through the Manage Sites node within the IEM Management Domain.
5.3.6. Define your computer subscription rules in the Computer Subscriptions tab of the site document

5.4. Given a functional IEM server and a license from IBM for Patch Management functionality, configure the IEM server for patch management so that the IEM server is configured to deploy patches to endpoints.

SUBTASK(S):
5.4.1. In the License Overview Dashboard in the BES Support site, enable the following sites:
5.4.2. Patching Support – Provides supporting tools for the patch process.
5.4.3. Enable OS and application patching sites as appropriate.
5.4.4. Subscribe endpoints to appropriate sites.
5.4.5. Grant operators appropriate permissions.
5.4.6. Activate analyses for the appropriate platform sites.
5.4.7. Some OS vendors require authentication for patches to be downloaded from the OS vendor's site, such as Red Hat, SUSE, and Solaris. In these cases a server plugin must be used to automate the downloading of patches from the OS vendor's site. To configure it:
5.4.8. Navigate to the "All patch management " Node and expand Dashboads
5.4.9. Select "Manage Download Plugin" dashboard
5.4.10. On the Dashboard select your server
5.4.11. In the work panel, select the desired plugin (e.g. Solaris plugin) and click on the "Register" button
5.4.12. the action : "BES Relay/Server: Register Download Plug-in for <OS>" (e.g. "BES Relay/Server: Register Download Plug-in for Solaris") will pop-up . Submit the action to your Server.
5.4.13. When the action is completed the dashboard will show the possibility to configure the plugin
5.4.14. Select the plugin and click the "configure" button
5.4.15. The task will prompt for the login name and password to the OS vendor's site.

5.5. Given that IEM is already installed and running, install and configure the Trend AntiVirus suite so that up to date virus patterns are automatically applied to the endpoints.

SUBTASK(S):
5.5.1. Enable Trend Antivirus Content.

5.5.1.1. In the IEM console, navigate to BigFix Management -> License Overview.
5.5.1.2. Confirm the Trend Micro Sites are Enabled, there are 4 of them, Trend Micro Common Firewall, Trend Micro Core Protection Module, Trend Micro Core Protection Module for Mac, and Trend Micro Reporting.
5.5.1.3. Subscribe the endpoints to the new Trend Micro content as appropriate.
5.5.1.4. Install server component. **(Does not apply for Linux)**
5.5.1.5. In the IEM console , navigate to Endpoint Protection -> Core Protection Module -> Quick Start -> Automatic Update or navigate to Endpoint Protection -> Core Protection Module -> Deployment
5.5.1.6. Run the fixlet, *Core Protection Module – Install Server Component,* against your IEM server. This will install the actual Trend Micro Server Components on your IEM server.

5.5.2. Install update script. **(Does not apply for Linux)**
5.5.2.1. Once the server component is installed, the fixlet *Core Protection Module – Download CPMAu*toUpdateSetup Script will become relevant.
5.5.2.2. Run this fixlet, it will automatically download and run an installer from Trend Micro. This installer will prompt you for your admin password as well as the location of your license.pvk file. It will not store this information. It will however use it to create the account the IEM server will use to run the auto updater.

5.5.3. Deploy Antivirus to endpoints.
5.5.3.1. All competing antivirus may need to be uninstalled before the Trend Micro client can be uninstalled, run the appropriate Core Protection Module – Uninstall fixlet under Endpoint Protection -> Core Protection Module -> Deployment -> Uninstall.
5.5.3.2. Run the appropriate Core Protection Module – Endpoint Deploy fixlet from Endpoint Protection -> Core Protection Module -> Deployment -> Install. The current version at the time of writing this is 10.6.

5.5.4. Additional Setup fixlets/tasks **(Does not apply for Linux)**
5.5.4.1. Fixlets/tasks to be run once, both appearing under Endpoint Protection -> Core Protection Module -> Updates -> Automatic Update Tasks
5.5.4.2. Run *Core Protection Module – Enable Automatic Updates – Server* against the IEM server.
5.5.4.3. Run *Core Protection Module – Enable Automatic Updates – Endpoint* against each endpoint you will be managing once the AV client is installed. It is suggested to run this as a policy so it applies to every new endpoint that installed.
5.5.4.4. Fixlet/tasks to be setup to run as a policy. appearing under Endpoint Protection -> Core Protection Module -> Updates -> Automatic Update Tasks

5.5.4.5. Run Core *Protection Module – Set ActiveUpdate Server Pattern Update Interva*l as a policy against the IEM server based on the information provided on the Description Tab of the fixlet
5.5.4.6. Run Core Protection Module – Apply Automatic Updates as a policy against all endpoints that are running Trend based on the information provided on the Description Tab of the fixlet.

5.5.5. Additional Tasks to Consider
5.5.5.1. Set up virus scans.
5.5.5.2. Enable Web Reputation.
5.5.5.3. Enable the clientUI.

5.6. Given a functional IEM Server and a license from IEM for Server Automation, configure the IEM server for server automation, so that automation plans, middleware patching, and virtual host management can be enabled for endpoint management.

SUBTASK(S):

5.6.1. Enable the Server Automation and Virtual Endpoint Manager sites, and subscribe the appropriate computers
5.6.1.1. For the following steps, run the fixlets in the order mentioned if they are relevant

5.6.2. Install and configure Server Automation
5.6.2.1. Under Server Automation -> Automation -> Setup and Maintenance -> Fixlets and Tasks, run Install BES Server Plugin Service against the IEM root server.
5.6.2.2. Under Server Automation -> Automation -> Setup and Maintenance -> Fixlets and Tasks, run Configure REST API credentials for BES Server Plugin Service against the IEM root server.
5.6.2.3. Under Server Automation -> Automation -> Setup and Maintenance -> Fixlets and Tasks, run Install Latest Automation Plan Engine against the IEM root server.

5.6.3. Install and configure Virtualization
5.6.3.1. Under Server Automation -> Virtualization -> Setup and Maintenance -> Activate Analyses and activate VMWare VM Overview, VMWare Host Overview, Management Extender Status, and SSL Encryption Analysis for Management Extender analyses
5.6.3.2. Under Server Automation -> Virtualization -> Setup and Maintenance -> Setup and Configuration Wizard, click ***Activate*** to enable any remaining analyses needed
5.6.3.3. Under Server Automation -> Virtualization -> Setup and Maintenance -> Setup and Configuration Wizard, click the link to ***Deploy Management Extender for VMware vCenter*** and then run the fixlet targeting the relay that will facilitate the communications to vCenter.

5.6.3.4. Under Server Automation -> Virtualization -> Setup and Maintenance -> Configure VMware Management Extender for Windows Templates, click ***Activate*** to enable and remaining analyses needed

5.6.3.5. Under Server Automation -> Virtualization -> Setup and Maintenance -> Configure VMware Management Extender for Windows Templates, enter the correct configuration information, click ***Take Action***, ensuring to target the correct endpoint.

Section 6 - Custom Content

6.1. Given the need to implement IBM Endpoint Manager (TEM) in a production environment, having an understanding of TEM, and having knowledge of the corporate organization in which IEM will be implemented it has been determined that a custom site will is required. Use the console to create a custom site ensuring that both operator accounts or roles and computers are subscribed appropriately so that the custom site is visible in the console with appropriate access granted to console operators and subscribed computers.

SUBTASK(S):

6.1.1. **Create Custom site**

- 6.1.1.1. Log in to the IEM console as a master operator.
- 6.1.1.2. Select the All Content domain.
- 6.1.1.3. Select tools > Create Custom site
- 6.1.1.4. Assign a name to the custom site – (Note once the name is assigned it cannot be changed).
- 6.1.1.5. Define Computer Subscriptions and/or Operator Permissions as required:
- 6.1.1.6. Assign Computer Subscriptions to custom site
- 6.1.1.7. Select - Computer Subscription Tab (Note there are four choices)
- 6.1.1.8. All computers: all computers will subscribe to the site in question.
- 6.1.1.9. No computers: no computers will subscribe to the site in question.
- 6.1.1.10. Computers subscribed via ad-hoc custom site subscription actions
- 6.1.1.11. Computers which match the condition below: computer subscription will be based on the set of criteria defined which can include any combination of the following:
- 6.1.1.12. Make appropriate selection and click “Save Changes”.
- 6.1.1.13. Assign Operator Permissions to custom site.
- 6.1.1.14. Select - The Operators Permission Tab (Note there are five choices)
- 6.1.1.15. Grant read permissions globally – All console operators will have read access to site content
- 6.1.1.16. Owner - selected console operator will have owner rights to custom site
- 6.1.1.17. Writer - selected console operator will have ability to add custom content to the custom site
- 6.1.1.18. Reader – selected console operator will have ability to read content in custom site
- 6.1.1.19. None – Remove assigned permissions from console operator
- 6.1.1.20. Make appropriate selection and click “Save Changes”
- 6.1.1.21. Assign permissions based on predefined roles (Note there are four choices).
- 6.1.1.22. Owner – console operators assigned to a selected role will be granted owner permissions to the custom site

6.1.1.23. Writer – console operators assigned to a selected role will be granted write permissions to the custom site
6.1.1.24. Reader - console operators assigned to a selected role will be granted read permissions to the custom site
6.1.1.25. None – Selected role will remove all permissions from console operators assigned to the selected role
6.1.1.26. Make appropriate selection and click “Save Changes”

6.2. Given that IEM is installed, access to console and access to create custom content, create a custom fixlet so that a custom operation or package can be deployed.

SUBTASK(S):

6.2.1. Decide whether a fixlet or a task better suits the requirement. Both fixlets and tasks consist of Relevance clauses, which are evaluated to determine the applicability of the fixlet or task to the endpoint, and ActionScript commands, which perform actions on the endpoint. They differ in their success criteria:
6.2.1.1. A task is considered “complete” if it runs its component commands successfully.
6.2.1.2. A fixlet is considered “fixed” only if it runs its component commands successfully AND is no longer relevant after completing them.
6.2.1.3. In the console, pull down Tools -> Create New Task or Tools -> Create New Fixlet, and write the Relevance clause(s) and ActionScript by using the guides at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Fixlet%20Authoring

6.2.2. The Custom Authoring Training Guide gives an overview of the authoring process and includes strategies for creating tasks/fixlets.
6.2.2.1. The Relevance Quick Reference and Core Inspectors Reference explain the Relevance functions and objects that are common across all IEM platforms.
6.2.2.2. The Windows Inspector Guide explains the Relevance functions and objects that are specific to Windows clients; the Linux Inspector Guide explains the Relevance functions and objects that are specific to Linux; etc.
6.2.2.3. The Action Guide and the Action Guide and Examples explain the commands that are available to use in ActionScripts.
6.2.2.4. Test the task/fixlet using the Fixlet Debugger, available for Windows at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Fixlet%20Authoring and instructions for non-Windows systems at

http://www-01.ibm.com/support/docview.wss?uid=swg21506026

6.2.2.5. Deploy the task/fixlet by taking action on it. Full details of how to deploy tasks and fixlets are included in the IEM Console Operator's Guide at http://support.bigfix.com/resources.html

6.3. Given a functional IEM console connected to the appropriate IEM server, create a property and a analysis so that custom information can be retrieved from an endpoint.

SUBTASK(S):

6.3.1. Create a new property:
- 6.3.1.1. In the IBM console navigate to Tools -> Manage Properties
- 6.3.1.2. Click on the 'Add New' button to create a new property.
- 6.3.1.3. You can select which category you would like to create your new property by clicking on the 'Category' button.
- 6.3.1.4. Give your new property a name in the 'Name' field.
- 6.3.1.5. Populate the relevance field with the appropriate relevance to match with your property.
- 6.3.1.6. Choose the Evaluate period by clicking on the drop-down menu called 'Evaluate' select which period you would like.
- 6.3.1.7. Click the 'OK' button to finish creating your property
  NOTE: If there are errors in your relevance statement you are using in your new property it will save it but give a syntax error.

6.3.2. Create a new analysis:
- 6.3.2.1. To create a new analysis you can create it from a number of places. The simplest way is to click on the 'Tools' menu and select 'Create New Analyses…'
- 6.3.2.2. Provide a name for the new analysis.
- 6.3.2.3. Select which site from the drop-down menu to create your new Analysis in.
- 6.3.2.4. Select which domain from the drop-down menu you would like to create the domain in.
- 6.3.2.5. On the first tab 'Description' enter a description of what your new analysis will do.
- 6.3.2.6. On the second tab 'Properties' select 'Add Property'.
- 6.3.2.7. Give your property a name in the ' Name' field.
- 6.3.2.8. Enter your relevance statement for the property in the relevance field below.
- 6.3.2.9. Select the period in the 'Evaluate' drop-down window.

6.3.3. On the 'Relevance' tab Select one of the following:
- 6.3.3.1. All computers
- 6.3.3.2. Computers that match the condition below
- 6.3.3.3. Select a property, clause and value to match.
- 6.3.3.4. Computers which match all of the relevance clauses below
- 6.3.3.5. Enter in a relevance statement to match.

6.3.3.6. On the bottom of the main page deselect the check box to ‘Automatically activate this analysis after it is created’

6.4. Given the requirement to maintain a consistent operating environment, create and maintain IEM baselines so that agents have the same operations and packages deployed.

SUBTASK(S):

6.4.1. Create baseline:
- 6.4.1.1. Select Tools -> Create New Baseline from the menu.
- 6.4.1.2. Set baseline name.
- 6.4.1.3. Set description (optional).
- 6.4.1.4. Select site to create the baseline in.
- 6.4.1.5. Select the domain to create the baseline in.
- 6.4.1.6. Set relevance conditions in the “Relevance” tab.

6.4.2. Add fixlets/tasks to baseline:
- 6.4.2.1. Select desired fixlet(s)/task(s).
- 6.4.2.2. Right click and select “Add to New Baseline” or “Add to Existing Baseline”.
- 6.4.2.3. If adding to a new baseline set properties required to create new baseline.
- 6.4.2.4. If adding to existing baseline, select the baseline.
- 6.4.2.5. On “Components” tab, select the desired action.
- 6.4.2.6. Press “OK” and enter password to save baseline.

6.4.3. Remove components from baseline:
- 6.4.3.1. Open desired baseline to “Components” tab.
- 6.4.3.2. Click on red circle with the “X” to delete from the baseline.
- 6.4.3.3. Press “OK” and enter password to save baseline.
- 6.4.3.4. Modify component order in baseline.
- 6.4.3.5. Open desired baseline to “Components” tab.
- 6.4.3.6. Select single up arrow to move the component to be installed earlier or single down arrow to move later.
- 6.4.3.7. Select double up arrow to move to a previous component group or double down arrow to move to a later component group.
- 6.4.3.8. Press “OK” and enter password to save baseline.

6.4.4. Delete baseline:
- 6.4.4.1. Select desired baseline.
- 6.4.4.2. Right click on baseline and select “Remove”.
- 6.4.4.3. Press “OK” and enter password to delete the baseline.

6.5. Given a functioning Web Reports server, and a Web Reports user with appropriate permissions, create an explore data web report so that desired custom results can be retrieved.

SUBTASK(S):

6.5.1. Enter the Web Reports URL in your browser:
http://hostname.domain.com:80/webreports
6.5.2. Log in to the Web Reports server with your user ID.
6.5.3. Click on the Explore Data link at the top of the page on the left side.
6.5.4. Select the data category you wish to use.
6.5.5. Select the Results to match ‘Any’ or ‘All”.
6.5.6. Apply filters to produce the report results you are looking for.
6.5.7. Apply more filters by selecting the ‘-‘ or ‘+’ key.
6.5.8. If you wish to add a clause to the same filter click on the ‘add clause’.
6.5.9. If you wish to remove a clause click on the ‘X’ button to the left of it.
6.5.10. Click ‘Apply Filter’ button to see the results bellow.
6.5.11. To create a chart for your report click on the ‘Add Chart’ button
6.5.12. Give the chart a title, typically describes your chart data
6.5.13. Pick a computer property to populate your chart with.
6.5.14. Modify the chart by dragging lines on top of each other to form groups.
6.5.15. Click the ‘Create Chart’ button.
6.5.16. Click the ‘Save Report’ button.
6.5.17. Give your New report a descriptive name.
6.5.18. Click on the ‘Save Button’.
6.5.19. To Find your new report, click on the ‘Report List’ button.
6.5.20. Type in the partial or full name of the report you just created in the filter box at the top of the page to filter the list.

Next Steps

1. Take the IBM Certified Deployment Professional - Endpoint Manager V9.2 assessment test using the promotion code *csistudy* for $10 ($20 USD savings).

2. If you pass the assessment exam, visit pearsonvue.com/ibm to schedule your testing sessions. Use the promotion code *tivguide* to receive 20% off.

3. If you failed the assessment exam, review how you did by section. Focus attention on the sections where you need improvement. Keep in mind that you can take the assessment exam as many times as you would like ($10 per exam), however, you will still receive the same questions only in a different order.