IBM TIVOLI ENDPOINT MANAGER V8.2 IMPLEMENTATION COURSE CONTENT

❖ SECTION 1:PLANNING:

A. Given the need to implement IBM Tivoli Endpoint Manager (TEM) in a customer's network, and possessing an understanding of TEM, define TEM 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.

With emphasis on performing the following tasks:

a) Determine TEM server and database requirements.
b) Determine if database(s) will be local to application server or remote.
c) Determine application uptime and disaster recovery requirements.
d) Define requirements for remote databases.
e) Define replication frequency for Distributed Server Architecture.
f) Obtain necessary service accounts for database and internet access.
g) Determine number of console users.
h) Determine console requirements.
i) Gather list of operating system to be supported.

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

With emphasis on performing the following tasks:

a) Submit requests for network diagrams and other pertinent network architecture and configuration data.
b) Work with network and security teams to identify potential network port restrictions and firewall placement.
    1) Submit requests to allow traffic on port 52311 between relay servers and upstream TEM relays and/or TEM servers.
c) Work with network team to analyze network topology and available bandwidth.
    1) Determine where to place TEM relay servers and how many to deploy.
d) Work with server teams to identify or procure appropriate computer hardware to install the TEM relay servers on.
e) Determine relay selection techniques for each location.
    1) Automatic vs Manual. Also consider the use of primary/secondary/tertiary relays and relay affiliation groups.
    2) Consider relay selection for computers which move outside of the corporate network. Failover selection.
f) Document relay architecture and distribute for review and approval by all stakeholders.

C. Given an upcoming TEM 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.

With emphasis on performing the following tasks:

a) Determine agent deployment strategy.
    1) Pre-existing software deployment tools - If a software deployment tool is already in use at an organization, leveraging it to install the TEM agent on all endpoints is generally the most effective deployment strategy.
    2) TEM Client Deploy tool - The Client Deploy tool uses Active Directory or NT domain administrator credentials to push the agent to a list of computers (Windows 2000 and above) 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 TEM 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 TEM server.

3) TEM Unix/Mac Client Deploy tool - The Unix/Mac Client Deploy tool uses SSH and root/su/sudo credentials to deploy TEM agents to entire groups of Macintosh, UNIX, and Linux endpoints at a time. (The tool itself runs on Windows.)
4) Login Script / GPO - The TEM 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 TEM agent installer in MSI format is provided to allow installation of the agent by using an Active Directory GPO.
5) Manual / Other - The TEM 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.

b) Define console connection method:
1) Remote console - console is installed on an administrator's computer on the same LAN as the TEM server.
2) Citrix / terminal server / remote desktop - console is installed on a virtual desktop on a terminal server on the same LAN as the TEM server.

c) Identify operator group requirements.
d) Identify required content/solutions.
e) Determine whether Message Level Encryption (MLE) is required for the network environment.

D. Given having an understanding of TEM and the requirement to implement TEM, discuss the TEM security model so that the various options for security in TEM are understood.
With emphasis on performing the following tasks:

a) There are two type of console users, local and remote.
1) Local console users can have password policies applied via TEM Administration Tool
2) You can add LDAP associations to TEM. That allows you and other users to log in by using those credentials, piggybacking on your existing authentication scheme.
3) You can use Microsoft Active Directory to handle authentication on TEM. 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.

b) 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) 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.
2) The RSA public key encrypts the session key and adds it to the AES-encrypted report. At the TEM 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.
3) There are three levels of report encryption:-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.-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.-None: clients do not encrypt, even if an encryption certificate is present.

❖ SECTION 2:INSTALLATION:

A. Given the appropriate server hardware and operating system, a IBM Tivoli Endpoint Manager (TEM) license key and administrative permissions, install the TEM server and Web Reporting so that TEM has been installed on the appropriate server.
With emphasis on performing the following tasks:

a) Obtain the latest version of TEM.
b) Run the installer (setup.exe), at the welcome screen, click Next.
c) You will see a dialog offering to install the Evaluation or Production version of TEM. Select Production and click Next.
d) After reading the license agreement, click Yes to accept it and continue.
e) Select the choice to install by using the TEM license authorization file from IBM then click Next.
f) The TEM 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.
g) A dialog appears displaying the current contents of your TEM license authorization. Click Next.
h) 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.
i) 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.
j) 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.
k) 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. Alternatively, the Wizard will let you save the request as a file named request.BESLicenseRequest. Then you can visit the TEM IBM Website, post your request and download your certificate.
l) 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.
m) 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.
n) Browse to the location of your license key and click Open.
o) 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.
p) 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.
q) The program prompts for a server port number that IBM TEM will use for all its data transmissions. The default port is 52311.
r) 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.
s) You are now ready to generate the TEM suite installation components. Select the default directory (BES Installers) or click Browse to choose a different folder. Click Next.
t) 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 TEM Installation Guide.
u) If it is not already running, launch the TEM Installation Guide (Start- > Programs - > BigFix Enterprise -> Tivoli Endpoint Manager Installation Guide).
v) Select the button labeled Install Tivoli Endpoint Manager Components.
w) 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:

1) Install TEM server.
2) Install TEM console.
3) Install TEM agents.
4) Browse Installation folders.

x) Select install TEM server.
y) After reading the License Agreement, click Yes to accept it and continue.
z) 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.
aa) A dialog prompts you to select a Local or Remote database. If you want to use another computer to host the TEM database, it must have a SQL Server already installed. The most common choice is to use the local database.
bb) A dialog displays a list of the TEM server components about to be installed. Accept the default components and click Next.
cc) 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.
dd) 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.
ee) 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.
ff) The TEM 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.
gg) 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 □a□ password if the □a□ password for the SQL Server database is currently blank (this is done for security reasons).
hh) 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.
ii) 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.
jj) 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.
kk) The program then prompts you to create an administrative user. Click OK to open the BigFix Enterprise User Management dialog. Click Add User to enter each desired user. For each user, enter the name, email, password and various permissions. When you have finished entering users, click Done.
ll) The TEM 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 TEM 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.

B. Given a functional TEM server installation and relay compatible agents checked into the TEM console, deploy the TEM relay server so that load is distributed from the main TEM server and network traffic is reduced.
With emphasis on performing the following tasks:
a) 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.

b) Find the Task with the title Install Tivoli Endpoint Manager Relay (it might include a version number after it). This Task is relevant when there is at least one agent that meets the requirements for the relay.
c) Choose your deployment option by choosing one of the actions in the Task. You can target single or multiple computers with this action.
    1) Click here to be prompted for a path where the TEM relay will be installed
    2) Click here to install the TEM relay on the drive with the most space
    3) Click here to install the TEM relay to the default location
d) Once the action completes, you'll have a functional TEM relay.

C. Given an operational TEM server, TEM console, a candidate computer in the DMZ to serve as a TEM relay, and coordination with the organization's networking and security teams, install an Internet facing relay so that TEM managed computers on the public Internet can still be actively managed.
With emphasis on performing the following tasks:
a) 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 TEM agent and TEM 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 TEM relay and an internal TEM server or relay will be allowed.
    1) Request that bi-directional HTTP traffic over port 52311 between the internal TEM server or TEM relay and the DMZ-based TEM relay be opened.
    2) Request that bi-directional HTTP traffic over port 52311 between the DMZ-based TEM relay and the Internet be opened.
    3) Request that a DNS alias (or IP address) for the DMZ-based TEM relay be assigned. The DNS-alias must be resolvable to a specific IP address.
b) Deploy the TEM relay to the DMZ-based computer.
c) The TEM relay must be made aware of the DNS-alias (or IP address). Do so by deploying the TEM Support site task ﷺBigFix Relay Setting: Name Override' to the DMZ-based TEM relay.
d) Configure agent settings of computers which will be on the Internet to use the DNS-alias or IP address of the DMZ-based TEM relay as a fail-over relay. (Keep in mind that ICMP traffic coming in from the Internet is blocked)
e) With the entire TEM communication path established from the Internet through the DMZ-based TEM relay and ultimately to the main TEM server, the next step depends on the various relay selection methods available in a given TEM infrastructure/instance. Since inbound ICMP traffic is blocked, Manual Relay Selection should be used.
f) Configure TEM agents to manually select the DMZ-based TEM relay's DNS-alias (or IP address) as the primary, secondary, or fail-over relay.
g) Dynamic Policy Settings can be applied to Internet-based TEM agents to allow for configurations better suited to external agents. For example, since the normal notification method (a UDP ping on port 52311) for new content will likely not reach external TEM agents, dynamic settings can be used to have TEM agents to check for new content more frequently than the default period of 24 hours.

D. Given an operational TEM server and console, install the TEM agent on computers so that they can be managed with the TEM environment.
With emphasis on performing the following tasks:
a) Use network shares to manually install the TEM agent (simply run the setup.exe from the TEM agent installation folder while logged in as a user with admin rights on that computer).- Msi silent installation msiexec.exe /i c:\BESInstallers\ClientMSI\BESClientMSI.msi /qn- Client installer silent- 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.
b) Deployment methods:
    1) For Windows domains or Windows Active Directory domains, you can use a domain administration user to deploy TEM agent by using the TEM Client Deploy tool located at

Start -> All Programs -> Tivoli Endpoint Manager -> Tivoli Endpoint Manager Client Deploy (on the computer that was used to run the TEM Installation Generator). Note: You can add custom client settings under Advanced Options and Custom Settings.-You can use login scripts to automatically install the TEM agent on computers.-You can use package deployment applications (such as SCCM, etc.) to deploy TEM agent.-You can use any mechanism/procedure that you currently use to install applications within your network.-For non-Windows computers, you can leverage the UNIX/Linux/Mac Client Deploy tool, found on the Labs site.

E. Given the requirement to facilitate automation of processes that require communication with the TEM server and Web Reports, install the BES server Plugin service so that other TEM applications will be able to fully utilize TEM server functionality.
With emphasis on performing the following tasks:
   a) Install BES server plugin service:
      1) Log on to TEM console with master operator account.
      2) Take action on Task 708 "Install BES Server Plugin Service" by using the TEM server as the target.
   b) Set up BigFix server plugin service to access Web Reports SOAP API
      1) Set up Windows registry values with Web Reports user information and Web Reports server.
      2) 32-Bit:[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports] SOAPUsername (String)Set with the name of your Web Reports user as its value.[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports]SOAPPassword (String)Set with the users password as its value.[HKEY_LOCAL_MACHINE\SOFTWARE\BigFix\Enterprise Server\BESReports]WRHTTP (String)Set with the name of your Web Reports server url:e.g.: http://bigfix.company.com/webreports
      3) 64-Bit:[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports] SOAPUsername (String)Set with the name of your Web Reports user as its value.[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports]SOAPPassword (String)Set with the users password as its value.[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BigFix\Enterprise Server\BESReports]WRHTTP (String)Set with the name of your Web Reports server URL:e.g.: http://bigfix.company.com/webreports
   c) Set up BES server plugin service to access TEM database. If the database is local or is remote with "SQL Server Authentication" these steps are not required
      1) Set up with database bu using NT Authentication:-Open the Windows Services dialog (Administrative Tools -> Services).-Open the BES server plugin service.-Click the Log On tab.-Select "This account".-Set user to the same user as was used for the FillDb and GatherDb services.-Restart the service.

F. Given a functional TEM 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.
With emphasis on performing the following tasks:
   a) Create manual computer groups:
      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) Right-click the computers you've chosen and select ?Add to Manual Group' from the pop-up menu.
      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.
      4) Select an existing group or name a new one and click ?OK'. If prompted, enter your password to propagate the new manual group.
   b) Create automatic computer groups:

1) Click Tools -> Create New Automatic Group.
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.
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.
4) When you are done, click 'OK' and if prompted, enter your password to propagate the group settings.

G. Given functional IBM TEM relays, and deployed agents checked into the TEM console, configure relay affiliation so that agents report to the desired deployed TEM relays.
With emphasis on performing the following tasks:
   a) Use relay affiliation.
      1) TEM relay fffiliation is intended to provide a more sophisticated control system for automatic relay selection.
   b) Create TEM agent affiliation groups .
      1) TEM agent is assigned to one or more Relay Affiliation Groups through the TEM agent setting: _BESClient_Register_Affiliation_SeekList
      2) This TEM agent setting should be set to a semi-colon (;) delimited list of Relay Affiliation Groups, for example: AsiaPacific;Americas;DMZ
   c) Create TEM relay and server affiliation groups
      1) TEM relays and TEM servers can be assigned to one or more Affiliation Groups through the TEM agent setting: -_BESRelay_Register_Affiliation_AdvertisementList This TEM agent setting should also be set to a semi-colon (;) delimited list of Relay Affiliation Groups, for example: AsiaPacific;DMZ;*-Note: TEM relays and TEM servers are not required to have a SeekList setting. The SeekList is only used by the TEM agent.
   d) TEM relay affiliation list information
      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: -Do not use special characters (including □□) when picking names.-Group names are not case sensitive. -Leading and trailing whitespaces are ignored in comparisons.

H. Given the appropriate server hardware and operating system, a TEM license key, and administrative permissions, install the replica TEM server and ensure Distributed Server Architecture (DSA) replication is functional so that there are two functional TEM servers replicating information between them.
With emphasis on performing the following tasks:
   a) Determine if you will be using SQL or NT authentication foe SQL.
   b) Run the TEM server installer on the DSA server with admin and SA rights.
   c) Select Replicated Database when prompted by installer.
   d) Enter master server hostname and credentials with DBO rights to BFEnterprise on master server.
   e) Run the TEM Administration Tool on newly configured server.
   f) Configure replication cycle (5 minutes by default).
   g) Run TEM Administration Tool on master server to ensure newly installed DSA server is available in drop-down list and set replication interval.
   h) Check FillDB logs on master and replica server for replication information. (Default path C:\Program Files\BigFix Enterprise\BES Server\FillDBData)

I. Given an operational TEM server with a local database, TEM relay, TEM console, and TEM agent, perform a product upgrade from TEM 8.1 to TEM 8.2 using TEM provided upgrade fixlets so that all of the latest TEM components are being used.
With emphasis on performing the following tasks:
   a) Carefully review all documentation for the new TEM version as well as all TEM upgrade instructions, change lists, and known issues. Also carefully review the information contained in the Description tab of all upgrade fixlets.

b) If possible, create a full backup of the TEM server. Always create full backups of all TEM databases.
c) First, upgrade the TEM server and TEM console(s) as well as all installation components by taking action with the fixlet titled "Updated Windows Server/Console Components - Tivoli Endpoint Manager version 8.2.xxxx.0 Now Available!". Choose the option to "upgrade all Tivoli Endpoint Manager Server, Console, and Installation Components installed on the target computers". Note that the TEM server and all TEM consoles must be upgraded at the same time. Older TEM consoles cannot connect to newer TEM servers.
d) Second, upgrade the TEM Web Reports server by taking action with the fixlet titled "Updated Windows Web Reports server - Tivoli Endpoint Manager version 8.2.xxxx.0 Now Available!". It is recommended that you run this upgrade immediately after the TEM server and consoles are upgraded. Web Reports servers that are not upgraded at the same time as the TEM server will be unable to communicate with the upgraded server.
e) Third, upgrade all TEM relays. For Windows TEM relays, take action with the fixlet titled "Updated Windows Relay - Tivoli Endpoint Manager version 8.2.xxxx.0 Now Available!". All TEM relays must be upgraded before TEM agents.
f) Finally, upgrade all TEM agents. For Windows TEM agents, take action with the fixlet titled "Updated Windows Client - Tivoli Endpoint Manager version 8.2.xxxx.0 Now Available!". Using a policy action is recommended.

❖ SECTION 3:COMPONENT CONFIGURATION:

A. Given a functional IBM Tivoli Endpoint Manager(TEM) server, and deployed agents checked into the TEM console, configure relay selection so that agents report to the desired deployed TEM relays.
With emphasis on performing the following tasks:
a) Automatic relay selection
1) Start up the TEM console and select the TEM Management domain. From the Computer Management folder, click the 'Computers' node to bring up a list of IBM TEM agents in the list panel.
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 TEM 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) Check the box marked 'Relay Selection Method'.
4) Click the button marked 'Automatically Locate Best Relay'.
5) Click 'OK'.
b) Defaulting to automatic relay discovery: As you install TEM agent, you may want them to automatically discover the closest TEM relay by default. Here is how to set this up:
1) As described in the previous section, open the 'Edit Computer Settings' dialog.
2) Select the 'Target' tab.
3) Click the button labeled 'All computers with the property'.
4) In the window below, select 'All Computers'.
5) Select the 'Constraints' tab.
6) Uncheck the 'Expires On' box.
7) Click 'OK'.
c) Manually selecting relays: You may have a reason to manually specify exactly which TEM agent should connect to which TEM relay. Here is how:
1) Start up the TEM console and select the TEM Management domain. From the Computer Management folder, click the 'Computers' node to bring up a list of TEM agent in the list panel.
2) Shift- and Ctrl-click to select the set of computers you want to attach to a particular TEM relay.

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.
4) Check the box labeled 'Primary TEM Relay' and then select a computer name from the drop-down list of available TEM relay servers.
5) Similarly, you can assign a ◆Secondary TEM Relay', which will be the backup whenever the Primary relay server is unavailable for any reason.
6) Click the ◆OK' button.

B. Given that the TEM server is up and running, ensure that all endpoints are healthy and connected to the TEM server so that sufficient information has been gathered to determine whether the TEM endpoint agents are healthy and properly reporting into the TEM environment.
With emphasis on performing the following tasks:
   a) Use the TEM console, navigate to BigFix Management domain.
      1) Select the Deployment Health Check dashboard.
   b) Navigate to the BES Client Health section.
   c) Review the following guidelines:
      1) Check agent distance from relays.-Agents should typically be less than 5 networks hops from relays.
      2) Check Windows Management Interface (WMI) properties.-Try to leverage relevance inspectors other than WMI where possible.
      3) Check Actions targeted by using lists.-Actions targeted at more than 50 computers should use lists.
      4) Check Location properties.-Check the version level of the location properties wizard and ensure that it is the latest.
   d) Check the total number of endpoints.
      1) Ensure that the total number of installed TEM endpoint agents matches the number of physical machines that are managed by TEM.
   e) Ensure that none of the computers are gray-out in the console computer site
      1) If gray-out check, to ensure that the computer is properly booted and reachable by a ping.
   f) Ensure that the computer properties are correctly reported.
      1) Review core properties.
   g) Review custom properties.
      1) Check agent relay status.
      2) Review Computer group memberships.
      3) Review Subscribed site.
      4) Review client settings.
      5) Check Bandwidth Throttling status.
      6) Check component version.
   h) While still in the Deployment Health Check dashboard.
      1) Navigate to the BES Console Health section.
      2) Check the number of unreachable endpoints.-If a large number of endpoints are unreachable, it might indicate a problem.
      3) Check number of stopped and expired actions.
      4) Check number of stopped and expired hidden actions.
      5) Check number of expired computers.
      6) Expired computers have not reported in over a month.
   i) Check Duplicate Computers.
      1) Duplicate computers should be eliminated.
   j) Navigate to Computers.
      1) Select a computer of interest.
      2) Expand the Relevant Messages.
      3) Check every single non-compliance message.

C. Given a TEM server that 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 TEM service(s) to run as the different user so that the BES server services are running as an account other than SYSTEM.
With emphasis on performing the following tasks:
   a) Identify or create an account that has appropriate permissions (for example, an Active Directory account that has DBO access to the TEM database but not Administrator permissions on the server).
   b) Open the Services control panel. All the TEM 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.
   c) 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.
   d) Restart the service to have it login by using the new account.
   e) The services list should show the appropriate account in the "Log On As" column.

D. Given a functional TEM Server on a network that requires going through a proxy for Internet access, configure the TEM server to use the proxy so that content is successfully gathered and sites are successfully populated on the TEM server.
With emphasis on performing the following tasks:
   a) Create an account for proxy access.
      1) Determine whether the proxy requires authentication through Active Directory.
      2) If authentication is required, create a generic Active Directory account with a non-expiring password for proxy access.
      3) If no authentication is required, create a local account in the Administrators group for proxy access.
   b) Log in as the newly created account and configure proxy settings in Internet Explorer (Tools -> Internet Options -> Connections -> LAN Settings). Check the "Bypass proxy server for local addresses" box in the proxy settings.
   c) Verify that http://sync.bigfix.com and http://gatherer.bigfix.com are reachable through the proxy by accessing it with Internet Explorer.
   d) Go to the Services control panel (Start -> Control Panel -> Administrative Tools -> Services) and edit the properties for the BES Gather Service. Set the service to "Log on as:" the newly created account.
   e) Verify that sites are gathering properly on the TEM server.
      1) Browse to http://MyTEMServerURL:52311/rd and click the "Gather Status" link to verify that no sites are in a "Failed" state.
      2) Verify that the aggregate fixlet count increases (may require that the "Show Not Relevant" toggle is depressed).

E. Given master operator access to the TEM environment and access to a console, manage roles and permissions within TEM so that users can effectively log in to the console and manage their endpoints.
With emphasis on performing the following tasks:
   a) Create users and roles.
      1) Create Non-Role users-Create Local Operator-Log in to TEM console.-Browse to All Content -> Operators.-Right Click in the main window and select Create Local Operator.-Follow creation steps.-Create Non-Role LDAP Operator.-Log in to TEM console.-Browse to All Content -> Operators.-Right Click in the main window and select Add LDAP Operator.-Follow creation steps.
      2) Create roles.-Create actual role.-Log in to TEM console.-Browse to All Content -> Roles.-Right Click in the main window and select Create Role.-Follow creation steps.
   b) Add to user or role.
      1) Add user to role.-Log in to TEM console.-Browse to All Content -> Operators.-Select an Operator in the main window and browse to the Assigned Roles tab.-Click Assign Role.-Follow creation steps.

2) Add Content to user or role.-Log in to TEM console.-Browse to All Content -> Operators for a single user or All Content -> Roles for a role.-Select an Operator or Role and browse to the Sites tab-Click Assign Site.-Follow remaining Assignment Steps, including assigning Owner/Writer/Reader where appropriate.
3) Add Managed Computers to user or role.-Log in to TEM console.-Browse to All Content -> Operators for a single user or All Content -> Roles for a role.-Select an Operator or Role and browse to the Computer Assignments tab.-Click Add.-Follow remaining steps to add computers.
4) Sync Active Directory Group w/ Role-Set up LDAP Directory.-Log in to TEM console.-Browse to All Content -> LDAP Directories.-Right click on the Main Window and select Add LDAP Directory.-Follow remaining step to Add the LDAP Directory.-Assign LDAP group to a role.-After setting up an LDAP Directory-Log in to TEM console.-Browse to All Content -> Roles.-Select a role in the main window and browse to the LDAP Groups Tab.-Click Assign LDAP Group.-Follow remaining steps to add the LDAP group.

c) Modify user or role.
1) Modify user or role settings.-Log in to TEM console.-Browse to All Content -> Operators for a single user or All Content -> Roles for a role.-Select the Operator or Role you would like to change.-Click on the Details Tab.-Make any changes necessary.-Click Save Changes.
2) Modify Content Assigned.-Log in to TEM console.-Browse to All Content -> Operators for a single user or All Content -> Roles for a role.-Select the Operator or role you would like to change.-Click on the Sites tab.-Make any changes necessary.-Click Save Changes.
3) Modify Computers Assigned.-Log in to TEM console.-Browse to All Content -> Operators for a single user or All Content -> Roles for a role.-Select the Operator or Role you would like to change.-Click on the Computer Assignments Tab.-Make any changes necessary.-Click Save Changes.

d) Remove user or role.
1) Delete user.-Log in to TEM console.-Browse to All Content -> Operators.-Select the Operator you would like to remove,-Click Remove.
2) Delete role-Log in to TEM console.-Browse to All Content -> Roles.-Select the Role you would like to remove.-Click Remove.

F. Given an operational TEM server, console, master operator console account, and a valid TEM license, enable TEM content sites so that TEM solutions can be accessed from the console.
With emphasis on performing the following tasks:

a) Enable Site:
1) Click on the BigFix Management domain icon in the domain panel of the TEM console.
2) Click on the License Overview' dashboard icon in the navigation pane.
3) Expand each software bundle to reveal a list of licensed content sites listed under the Available Sites' heading.
4) Click the Enable' link next to each site to which you want to subscribe.
5) The enabled sites will now appear in the list of Licenses (Used / Allowed)'.

b) Enable Site Subscription:
1) For each site just enabled, click on the site name in the License Overview' and then select the 'Computer Subscriptions' tab.
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) When you are finished setting the computer subscriptions, click the 'Save Changes' button to complete the subscription process for the site.

G. Given the reporting requirements of the customer, activate the appropriate set of analyses so that the TEM infrastructure will collect the desired data.
With emphasis on performing the following tasks:

a) Log in to the TEM console as a master console operator.
b) Select the All Content Domain.
c) Select Analyses in the filter tree.
d) Highlight the desired analyses to activate within the list on the right (Ctrl-click to select multiple analyses).
e) Right-click and select Activate.
f) Repeat the previous 2 steps for any additional content that is required to be enabled.

H. Given TEM components on a network infrastructure with bandwidth usage constraints, configure TEM agent and server settings so that TEM's bandwidth usage is controlled.
With emphasis on performing the following tasks:
a) 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 TEM traffic (which may vary per link).
b) To throttle outbound traffic from the server to the relays, use one of these tasks to configure the server settings:
1) 151 - BES Server Setting: Throttle Outgoing Download Traffic
2) 462 - BES Server Setting: Dynamically Throttle Outgoing Traffic
c) To throttle outbound traffic from relays to the endpoints, use one of these tasks to configure the relay settings:
1) 163 - BES Relay Setting: Throttle Outgoing Download Traffic
2) 459 - BES Relay Setting: Dynamically Throttle Outgoing Traffic
d) To throttle relays downloading from their upstream server/relay, use one of these tasks to configure the relay settings:
1) 152 - BES Relay Setting: Download Throttling
2) 458 - BES Relay Setting: Dynamic Download Throttling
e) To throttle endpoints downloading from their relay/server, use one of these tasks to configure the client settings:
1) 167 - BES Client Setting: Download Throttling
2) 457 - BES Client Setting: Dynamic Download Throttling
f) If using dynamic throttling instead of manual throttling, use these tasks to enable it:
1) 605 - BES Client Setting: Enable/Disable Dynamic Throttling
2) 702 - BES Relay/Server Setting: Enable/Disable Dynamic Throttling
g) Enable this analysis to verify the throttle settings (it is in the BES Support site, as are all the related tasks):
1) 218 - Bandwidth Throttling Status

I. 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.
With emphasis on performing the following tasks:
a) Set policy expiry:
1) If setting a policy to never expire, uncheck the "Ends On" field.
2) If the policy is to only be active for a finite time, check the "Ends On" and set the date.
b) Set re-application policy:
1) Check the "Reapply this action".-Choose "whenever it becomes relevant again" to immediately bring the system into compliance.-Choose "while relevant, waiting between reapplications" to wait for some interval before bringing the system into compliance.-Check the "Limit to reapplications" to limit the number of times the policy will execute on a target.

J. Given the requirement to ensure actions are not performed on targets outside of maintenance windows, utilize the TEM 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.
With emphasis on performing the following tasks:
a) Create Maintenance windows.

1) Log on to TEM console.
2) Navigate to All Content domain -> Dashboards- > BES Support -> Maintenance Window dashboard.
3) Activate the Maintenance Window Analysis.
4) Press the "Create New Maintenance Window" button.
5) Give the window a descriptive name.
6) Select length of time for the window to be open.
7) Set the start time for the window.
8) Select the frequency .-Once: This will open the window on a specific date and time.-Daily: Will occur every day interval at the specified time.-Weekly: Will occur every week interval on the selected days at the specified time.-Monthly: Will occur on a specific day of the month at the specified time.
9) Press the "Create Task" button. This will generate a task to set the registry settings on the agents.

b) Deploy Maintenance Window to agents.
1) Click on the desired maintenance window in the dashboard.
2) Press the "Take Action" button.
3) From the "Preset" select "Policy".
4) In the Target tab, select the desired targets.
5) Press the OK button to submit the action and enter password.

c) Set client locking.
1) Navigate to All Content domain -> Dashboards- > BES Support- > Maintenance Window Dashboard, Click on the link for "Enforce Maintenance Window with Client Locking".
2) Press the "Take Action" button.
3) From the "Preset" select "Policy".
4) In the Target tab, select the desired targets.

d) Press the OK button to submit the action and enter password.

K. Given an operational TEM server and TEM agent, deploy a custom agent setting so that all targeted TEM agents use the custom setting.
With emphasis on performing the following tasks:
a) Open the TEM console and go to the Computer section under the All Content domain.
b) Select the computer(s) that you would like to apply a custom agent setting to.
c) Right-click on the computer(s) and choose Edit Computer Settings -> More Options.
d) Under the Settings tab, check Custom Settings. Enter in a Name and Value for the new custom agent setting.
e) 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.

L. Given Web Report admin access and access to Web reports, manage roles and permissions within TEM so that users can effectively log in and use Web Reports.
With emphasis on performing the following tasks:
a) Non-Active Directory users
1) Create users:-Log in to Web Reports.-Select Administration -> User Management -> Create User.-Fill in the appropriate information.-Click Create User.
2) Edit user:-Log in to Web Reports.-Select Administration -> User Management.-Check the user(s) to be changed.-(De)Select the new roles for the user in the Assign Roles pull-down menu.
3) Delete user:-Log in To Web Reports.-Select Administration -> User Management.-Check the user(s) to be deleted.-Click Delete.

b) Active Directory users
1) Set up connection to Active Directory:-Log in to Web Reports.-Select Administration -> User Management -> Active Directory Permissions.-If Active Directory credentials have not been entered a prompt will appear, enter valid Active Directory credentials.

2) Create user:-Log in to Web Reports.-Select Administration -> User Management -> Active Directory Permissions.-Ensure Names is selected.-Type in Active Directory account to use to create a new Web Reports user.-Click Search.-Once results have returned click the box next to the desired user to add.-Select the appropriate roles from the Assign Roles pull-down menu.
3) Modify user:-Log in to Web Reports.-Select Administration -> User Management -> Active Directory Permissions.-Ensure Assigned Web roles is selected.-Type in Active Directory account to use to modify, or leave blank to see all active users.-Click Search.-Once results have returned click the box next to the desired user to modify.-Select the appropriate roles to modify from the Assign Roles pull-down menu.

c) Manage roles.
1) Create role:-Log in To Web Reports.-Select Administration -> User Management -> Manage Roles.-Click Create Role.-Fill out the appropriate Information.-Click Create Role.
2) Edit role:-Log in To Web Reports.-Select Administration -> User Management -> Manage Roles.-Click on the name of the role to be changed.-Make the desired changes.-Click Update Role.
3) Delete role:-Log in To Web Reports.-Select Administration -> User Management -> Manage Roles.-Click the check box next to the role to be deleted.-Click Delete.

M. Given an operational TEM server and console, use the TEM Administration Tool so that a user has the ability to administer masthead, system options, advanced options, replication and report encryption.
With emphasis on performing the following tasks:
a) Masthead Management
1) Edit, export, request ,or activate a masthead.
b) System options:
1) Minimum refresh interval
2) Default Fixlet Visibility
3) Client UI Icon
c) Advanced options:-special name/value pairs that allow you to customize the behavior of TEM deployment.
d) Replication:-this dialog helps to visualize your replication servers.
e) Encryption:-This dialog allows you to manage encryption keys.

N. Given an operational TEM Administration Tool, TEM server, TEM relay, and TEM agent, configure report encryption and a decrypting relay so that all targeted TEM agents encrypt upstream data using Message Level Encryption and decryption occurs on a TEM relay instead of on the TEM server itself.
With emphasis on performing the following tasks:
a) Launch the TEM Administration Tool.
b) Go to the Encryption tab and click on Generate Key.
c) Select the desired Key Size by selecting an option from the Key Size dropdown.
d) Uncheck the box for "Begin encrypting using this key immediately (uncheck if you need to distribute this key to decrypting relays)".
e) Save the encryption key.
f) Securely copy the saved encryption key to all desired decrypting TEM relays. The key should be placed in "Program Files\BigFix Enterprise\BES Relay\Encryption Keys\".
g) Access the Encryption tab of the TEM Administration Tool. Select Enable Encryption and click OK.
h) Select Yes to propagate the action site.
i) Deploy the task titled "BES Client Setting: Encrypted Reports" using an appropriate setting of either required, if possible, or disabled.

O. Given a functional TEM server on a network with no Internet access and an Internet-connected Windows machine on a different network, use the TEM Airgap tools to download TEM content on the Internet-connected computer so that site content and downloads are successfully populated on the TEM server.
With emphasis on performing the following tasks:
a) Identify a Windows machine with Internet access to act as the air-gap gather server (it does not have to be a TEM server).

b) Run the Air-gap tool on the TEM server to put the TEM server's gather requests and a copy of the Air-gap tool onto a storage device.
c) 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.
d) Run the Air-gap tool from the storage device, on the TEM server, to copy the results of the gather request onto the TEM server.
e) Verify that the sites were gathered properly by checking that the aggregate fixlet count increased as a result.
f) Run the BESDownloadCacher tool on the air-gap gather server for each site with download content to be gathered.
g) Copy the cached downloads to the TEM server's cache directory (using a thumb drive or other method).
h) Verify that the download content was downloaded by deploying a fixlet that depends on one of the cached downloads.

❖ **SECTION 4:PROBLEM DETERMINATION AND PERFORMANCE TUNING:**

A. Given that the IBM Tivoli Endpoint Manager (TEM) server is up and running, use the TEM console to review the TEM 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 TEM installation.
With emphasis on performing the following tasks:
a) Using the TEM console, navigate to the BigFix Management domain.
b) Select the Deployment Overview dashboard
    1) Check BES agents reported in the last day
    2) Check BES relays reported in the last day
    3) Check average number of BES clients per relay
c) Select the Deployment Health Check dashboard.
d) Perform a quick scan of the status of the health checks to verify they are all "Passed" (Green)
e) Gather information of TEM environment by initiating a Collect Deployment information function located in the Deployment Information section.
    1) Check number of computers.-Check numbers of active computers.
    2) Check relay information.-Number of relays-Maximum distance to relays
    3) Check console information.-Check number of console computers.-Check number of console operators.
    4) Check license information.-Check license site number.-Check license expiration date.
    5) Check action information.-Number of actions-Number of top level actions-Number of open actions
    6) Check fixlets information.-Relevant fixlets-Non-relevant fixlets-Number of hidden fixlets
    7) Check tasks information.-Relevant tasks-Non-relevant tasks-Number of hidden tasks
    8) Check analyses information.-Relevant Analyses-Non-relevant Analyses-Number of hidden Analyses
f) Review BES relay health section.
    1) Download folders.
    2) Number of clients per relay
    3) relay service stopped.
g) Review BES Console Health section.
    1) Too Many Offline computers
    2) Stopped And Expired Actions
    3) Stopped And Expired Actions Hidden Actions
    4) Expired computers
    5) Duplicate computers.
h) Review BES server health section.
    1) BES server free disk space

2) Number of clients on main BES server
3) Number of relays on main BES server
4) SQL Server service pack

i) Review BES client health.
1) BES client distance from BES relays
2) WMI properties
3) Actions targeted using lists
4) Location properties

j) Review Deployment Optimization section.
1) Support analysis activation
2) Open actions.
3) Open hidden actions.
4) Operators by using Policy Actions
5) Statistical Property evaluation period
6) ICMP settings Controls
7) Components per baseline
8) Action applicability too large
9) Policy actions not targeted by property
10) Superseded fixlets
11) Support analysis removal
12) Efficient MIME
13) Office deployment control initial assignment
14) Deprecated fixlet sites
15) Console operators have never logged in.
16) Console operator accounts not being used
17) License expiration

B. Given an operational TEM server, TEM console, and a Windows computer with the TEM agent, enable debug logging so that all targeted TEM agents produce detailed logs for use in troubleshooting.
With emphasis on performing the following tasks:
a) Take action with the fixlet titled "BES Client Setting: Enable Debug Logging".
b) Enter in an appropriate value in the Action Parameter dialogue and click OK.
c) Deploy the action.

C. Given an operational TEM console, enable the TEM console debug menu so that a TEM console operator will have easy access to various tools useful in debugging TEM issues.
With emphasis on performing the following tasks:
a) Open the TEM console and hold down the following keys at the same time: Ctrl + Alt + Shift + D.
b) In the dialogue box select the checkbox "Display Debug Menu".

D. Given a TEM server with sub-optimal performance, identify the factors affecting performance so that they can be addressed.
With emphasis on performing the following tasks:
a) 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.
1) By default the TEM agents "check in" to the TEM server on a regular interval known as a "heartbeat". When the TEM agents send in a heartbeat to the TEM 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 TEM deployments, processing the heartbeats can consume significant TEM 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 TEM deployments. The heartbeat can be changed under the File > Preferences menu in the TEM console.
2) When the TEM console is being used, the TEM console will query the TEM server database and cache the results locally. The cache is updated according to the TEM console refresh period. The more TEM agents, the more data is transferred to the TEM

console using database resources and network bandwidth. The TEM 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 TEM console users. The refresh rate can be changed under the File > Preferences menu in the TEM console (note that this setting is per TEM console.

b) 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:
    1) 157 - BES Client Setting: Enable Command Polling
c) TEM agent CPU utilization settings can affect TEM agent performance significantly. These settings adjust it:
    1) _BESClient_Resource_WorkIdle (milliseconds; range 1-500; default 10): The TEM 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 TEM agent will evaluate fixlet relevance faster, but the CPU usage will be higher.
    2) _BESClient_Resource_SleepIdle (milliseconds; range 1-500; default 480): The TEM 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 TEM agent will take longer to evaluate fixlet relevance, but the CPU usage will be lower.
d) The TEM server and TEM relay's normal operations involve creating and processing a lot of temporary files. This activity is essential for good performance of TEM, but can be slowed down dramatically if a virus scanner is scanning each file. To address this issue, configure your virus scanner on the TEM server and TEM relay computers to exclude the TEM server folder and all subfolders (default is "C:\program files\bigfix enterprise\bes server") or the TEM relay and its subfolders (default is "C:\program files\bigfix enterprise\bes relay"). Refer to instructions from your virus scanner for more information on how to set this exclusion rule.
e) The TEM server and TEM relay's normal operations involve creating and processing a lot of temporary files. This activity is essential for good performance of TEM, 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.

E. Given a TEM server that is having issues gathering site content, troubleshoot the problem so it can gather site content and downloads.
With emphasis on performing the following tasks:
a) Browse to http://MyTEMServerURL:52311/rd for the Relay Diagnostics page. Click the "Gather Status" link to verify that sites are in the "Failed" state.
b) Use Internet Explorer on the TEM 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.
c) 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.
d) In the TEM 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.
e) Use the Air-gap method and tool to attempt to gather the site(s) manually. (See "Gather TEM Content on an Air-gapped Network".)
f) Perform a gather state refresh to completely reset the gather status. Click the Gather button on the site.
g) Review the gather.db log file. C:\Program Files\BigFix Enterprise\BES Server\GatherDBData

F. Given a functional TEM server, console and relay, determine why TEM agent installations are failing by using the client deployment tool so that the source of the client deployment issue has been determined. With emphasis on performing the following tasks:
   a) Determine if the necessary tool requirements have been met:
      1) You are logged in with an account that has admin rights on the targeted computers
      2) The targeted computers meet the OS requirements (2000, W2K3, XP, Win7, Vista, W2K8, W2K8R2)
      3) The targeted computers must have the following services running (workstation, server, net logon, remote registry)
      4) The targeted computers must have "File and Print" sharing enabled
      5) There are no firewall policies that block RPC connections
   b) Use the Net use command to check for errors the client deployment tool may be encountering (net use *\\targetname\admin$ /user:domain\user password
   c) Error codes and there meaning
      1) System error 53 has occurred. The network path was not found. ADMIN$ is not available
      2) 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.
      3) 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) System error 1326 has occurred. Logon failure: unknown user name or bad password.
      5) System error 5 has occurred. Access is denied user name/password correct, but account does not have permission to ADMIN$ share.
      6) No network provider accepted the given network path. The agent or the server could not be resolved during the client deployment tool process.

G. Given the requirement for TEM to efficiently transport large payloads, describe the steps required to troubleshoot an array of poorly performing TEM relays so that the issue with TEM relays can be diagnosed and resolved.
With emphasis on performing the following tasks:
   a) Ensure that enough relays have been installed and configured for the environment.
      1) Check that the TEM relay service/process is started on all relays.
      2) Check the number of hops between a agent and its closest relay.
   b) Ensure all relays are available by using the Deployment Health Checks on the Bigfix Management domain
      1) Review the BES Relay Service Stopped check.
      2) Review the BES Relay Free Disk Space check.
   c) Determine problems with automatic relay selection.
      1) Endpoint to relay.
      2) relay to relay.
      3) Review the agent list of relays in relays.dat.
      4) Review relay affiliation.
      5) Check the relay selection frequency.
      6) Follow relay selection through hierarchy of relays: primary, secondary, fail-over and finally TEM server.
   d) Check whether relays are set to manual configuration or automatic configuration.
      1) Ensure that Relay to Relay configuration was manually configured.
   e) Ensure that relays are up and running 24/7.
   f) Check the relay automatic selection settings.
      1) Tune the settings if required.
   g) Identify relay lack of disk space issues.

1) Calculate theoretical amount of disk space required on each relay.-Build different size Payload.-Do performance testing to identify bottlenecks.
2) Review the logs: C:\Program Files\BigFix Enterprise\BES Relay\logfile.txt.

H. Given a functional TEM and a non-master operator in unable to see console content; determine the cause so that the issue can be resolved.
With emphasis on performing the following tasks:
   a) Log in to the console as the master operator
   b) Go to Operator under the BigFix Management domain.
   c) Select the user name that is having the issue.
   d) Verify that the user is subscribed to sites.
   e) Right-click a single operator in question from the list and select Assign User Management Rights from the pop-up menu
   f) Click the Add button to verify management rights are assigned to the selected operator.
   g) Log in as the Non-master operator and verify console content is now visible.

I. Given the need to manage a TEM environment by using Web Reports, describe how to resolve Web Reports technical issues so that Web Reports issues have been diagnosed and resolved.
With emphasis on performing the following tasks:
   a) Ensure that the Web browser installed and used is fully supported by TEM.
   b) Ensure that Web Reports is the right version for your TEM environment.
   c) Check to ensure that SSL connectivity was properly configured.
      1) Check that there is a proper SSL certificate.-Should be in OpenSSL *.pem file format.
      2) For HTTPS configuration refer to the TEM Web Reports user's guide.
   d) Check message indicating whether or not the certificate can be trusted.
      1) Check to see if certificate is issued by a trusted certificate authority (CA).
      2) Check to see whether the correct fully qualified host name is specified.
      3) Check to see if the certificate has not expired.
   e) Check a stand-alone Web Reports server configuration.
      1) Check the requirements in the technical documentation.-Check memory requirements for the number of TEM agent in the TEM environment.-Check CPU size of a stand-alone Web Reports server.
      2) Make changes if necessary.
   f) Check the configuration of Web Reports running on the database server.
      1) Refer to documentation to ensure that it was properly configured.
   g) Check that Emails can be sent.
      1) Check your Email accounts and server.
      2) Ensure that the SMTP server is up and running.
   h) Check the Database server cache settings.
      1) Fine-tune the default length of 15 seconds if required.
   i) Run reports to see if Web Reports work correctly.
      1) Run a prepackaged report.
   j) Identify missing data in reports.
      1) Ensure that all required databases have been added.
   k) Export Reports to PDF function does not work.
      1) Check documentation to understand what is required to be done for the configuration.
      2) Ensure that the export to PDF function was properly configured.
   l) Review specific log files for Web Reports.
      1) Ensure that the log file feature is enabled.

J. Given a TEM 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.
With emphasis on performing the following tasks:
   a) "Troubleshoot why the agent does not appear in the console"
      1) Determine whether or not the agent exists in a master operator's console view.-If not, validate that:-The endpoint has the TEM agent software installed.-The TEM agent

service/agent is in a running state.-The TEM agent has the appropriate masthead/license for the appropriate TEM Server instance/deployment.-The TEM agent is connected to the network, and is able to communicate (register, gather, and post reports) with its relay or the main TEM server.-If it does, proceed to next step.-Ensure that the console operator has management rights over the agent in question, by launching the TEM 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.

b) "Troubleshoot why the agent appears unresponsive to actions"
   1) Some common reasons why this might occur:-TEM agent is off or not connected to the network - The TEM agent obviously cannot report if the computer is off or if the TEM agent cannot connect to the TEM server or TEM relays. It is easy to see the last report time of the TEM agent in the TEM console to see if the computer has reported recently.-TEM agent did not receive UDP 'ping' - Whenever there is a new action, new fixlets available, or new downloads available, the TEM server and TEM relays send a UDP 'ping' on the TEM port number (by default it is 52311) to the last known TEM agent IP. If this message is not received, the TEM agent will not know there is a new action to report on. By default, the TEM 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 TEM agent can receive UDP 'pings' by right-clicking on the computer in the TEM console and sending a refresh. If the TEM 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. -Note: The TEM agent will report in normally on their heartbeat interval so make sure that the TEM agent was responding to the refresh and wasn't reporting on its normal schedule. The TEM agent will not receive their UDP messages if there is a firewall blocking UDP packets on the TEM port (52311 by default), if there is a NAT translator between the TEM server and the TEM agent (or TEM relays and TEM agent), if the computers are running personal firewalls like Zone Alarm, Black Ice, or the XP firewall, or if the TEM agent have switched IP addresses since the last time it registered (by default the TEM agent registers every 6 hours). -Note: Another simple test from the TEM console can help determine if UDP messages are being blocked. On the Computers tab in the TEM console select a computer and then right-click to select the option 'Send Refresh'. If UDP messages are able to get to the TEM agent you will see an entry similar to 'ForceRefresh command received' in the agent's log file.

c) "Determine why agents appear gray in the console"
   1) Computers that are grayed out in the TEM console are considered to be offline. Computers will be considered offline if the TEM agent has not reported in a specified amount of time. By default, the TEM agent sends a heartbeat every 15 minutes and if the TEM server has not received a heartbeat in 45 minutes from a particular TEM 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 TEM console under File -> Preferences.
   2) There are several reasons why a agent's reports may not have reached the TEM console within the time that the TEM console is configured to mark them as gray/offline:-The agent is legitimately offline or off the network.-The agent is having network connectivity issues with its relay.-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 . -The agent is having performance issues, and is unable to consistently report in a timely manner on the defined heartbeat.-Check the agent logs for indications of reporting performance issues by comparing the intervals between Report Posted Successfully entries and the defined heartbeat.-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.-The relay is not properly forwarding the agent's reports up the relay hierarchy to the main TEM server.-Check the relay's forwarding BufferDIR for the existence of agent reports.-The main TEM server is not processing the incoming agent reports, or not processing them in a sufficiently quick manner.-Ensure that the FillDB service is running.-The TEM console is not properly updating its session cache from the information available in the TEM Database.-Validate ODBC connectivity.-Ensure that there are no database locks.-Duplicate computer object.-Delete old computer objects.

K. Given an existing TEM deployment, troubleshoot and resolve issues related to filldb so that the data will be inserted into SQL and inserted in to the console in a timely manner.
With emphasis on performing the following tasks:
   a) Determine if issues with filldb are related to data/connection problems or if issues are performance related.
      1) Connection Issues- FillDB Debug Log -- Used to troubleshoot issues with agent reports or FillDB connection errors common on remote database deployments.
      2) Enable Debug log 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 TEM server.
      3) Check filldb service logon account and reset password.
      4) Check SQL to ensure filldb service account has access to SQL server and to BFEnterprise database.
      5) restart filldb service on TEM server.
   b) Performance Issues - FillDB Performance Log -- Used to measure and troubleshoot FillDB performance issues with the server/database Disabled by default.
      1) Enable performance log - HKLM\Software\BigFix\Enterprise server\FillDB set "PerformanceDataPath" for example c:\program files\BigFix Enterprise\BES Server\FillDBData\FillDBPerf.log
      2) Restart Filldb service on TEM server.
      3) Check SQL transaction log and shrink if over 2GB.
      4) Ensure SQL is set to use simple mode.
      5) 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.
      6) Check to make sure the default reindexing job is running in SQL daily.

L. 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.
With emphasis on performing the following tasks:
   a) Troubleshoot Relevance statements.
      1) Identify the problem relevance statement.
      2) Launch Fixlet Debugger and insert relevance statement.
      3) Press CTRL+Enter to execute the statement.
      4) Identify problem and correct.
      5) Copy fixed relevance statement to source.
   b) Troubleshoot ActionScripts.
      1) Identify the problem fixlet/task.
      2) Identify ActionScript line.-By using the Status information from a completed action, find the failed line-Open the .log file in the client directory (Windows: C:\Program Files\BigFix Enterprise\BES Client__BESData__Global\Logs) and search for failures.

3) Determine issue in the action line.-If program execution failing, manually execute command line-Correct issue with command line in ActionScript.-If relevance issue, copy to Fixlet Debugger running on problem system .-Correct issue with relevance statement.

M. Given that the new TEM server has already been set up, migrate all endpoints so that they are successfully reporting to the new TEM server.
With emphasis on performing the following tasks:
   a) Determine the operating systems of the endpoints to be Migrated.
   b) If migrating only Windows, decide if the migration strategy will be to migrate via a URL or via a network share.
   c) If using a network share determine if a null share needs to be created.
   d) Based on the instructions in the migration fixlet, make the masthead from the NEW TEM server accessible to the infrastructure. This is generally accomplished by copying it to the OLD TEM server.
   e) Uninstall all relays from the OLD TEM infrastructure.
   f) Migrate the Endpoints via the following fixlets:Switch BES Client Action Site Masthead - BES >= 7TROUBLESHOOTING: Switch ActionSite Masthead on SolarisTROUBLESHOOTING: Switch ActionSite Masthead on Max OS XTROUBLESHOOTING: Switch ActionSite Masthead on RHEL/SUSETROUBLESHOOTING: Switch ActionSite Masthead on VMware ESX serverTROUBLESHOOTING: Switch ActionSite Masthead on AIXTROUBLESHOOTING: Switch ActionSite Masthead on HP-UXNote: Be sure to not run the migration fixlet against the OLD TEM server
   g) 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 TEM Infrastructure will not report back as completed.
   h) Redeploy the relay as appropriate.

❖ **SECTION 5:ADMINISTRATION:**

A. Given the need to install Software Usage Analysis with IBM Tivoli Endpoint Manager (TEM) and that all pre-requirements have been installed and configured, Install and configure TEM for Software Usage Analysis so that the desired reporting functionality will be fulfilled.
With emphasis on performing the following tasks:
   a) Save the installer on the computer you have designated to be your SUA Application Server.
      1) This launches the InstallShield Wizard. When the Welcome panel opens, click Next.
   b) Follow the prompts through the License Agreement and Destination Folder panels.
   c) Select a location for your SUA application, and then click Next.
   d) When the Completed window opens, click Finish.
   e) Configuring the Application.
      1) The next task is to configure the SUA application by using the SUA Configuration Wizard. When the Welcome panel opens, click Next.
      2) Enter the domain, username, and password for the user under which the core SUA application services is to run, and then click Next. .
      3) If you want your current Web Reports users to also be SUA users, select the I have Web Reports box and then click Next.
      4) If you selected the I have Web Reports box, a dialog box opens where you set up your data settings for Web Reports.
      5) A dialog box opens where you can set up data settings for SUA. Select from the server drop-down menu or manually enter the database server name. -This is where the database tables for the inventory will be created. This can also be the same database server where your TEM server database is located. If your server is on a non-standard port, you can enter this by putting a comma and the port number after the server name (localhost,1433).
      6) Select your connection method to either "SQL Server Authentication" or "NTAuthorization". SQL Server authentication requires your SQL Server ID and password.

-For NT Authorization, use the user information that was specified on the Authorization Credentials panel. Be certain that this user has at least "dbcreator" permissions to create new databases and tables on the database server.

7) Click Next. -Note: The Server Port Configuration is set with a default of 80 for HTTP or 443 for HTTPS.
8) Click Next. -Note: The database for the SUA application is created on your SQL server computer and services are installed and enabled.
9) In the Completing the SUA Configuration Wizard window, click Finish.-Note: You have now completed the installation of the TEM SUA application and configured the SUA application database. The tables have been created on your database server.

f) Enable all SUA Analysis.

B. Given an installed and functional TEM server with administrative permissions and a licensed and fully gathered Power Management module, enable and configure Power Management so that historical monitoring and power profiles can be generated.
With emphasis on performing the following tasks:

a) Within the Power Management module navigate to Setup and Configuration.
b) Select the Quick Start folder.
c) Activate all Power Analyses.
d) Within the Manage Power Tracking folder, enable Power Tracking with Default Assumptions.
e) Select the Manage Assumptions folder and select Manage Custom Assumptions Tasks.
f) Create a new General Assumption if needed otherwise use the default.
g) Navigate to the Configure Historical Reporting folder.
h) Within the Configure Historical Reporting folder, configure Historical Reporting Groups using the define Policy Wizard.
i) Enable Store Power Data utility.
j) Enable Client-side Dashboard if required.
k) Manage power profiles, pc insomnia, power state, and wakeup behavior as needed.

C. Given the need to deploy Asset Discovery & Inventory functionality within a completed TEM infrastructure, subscribe to and configure the Asset Discovery and Inventory & License Fixlet Sites so that the desired functionality and reporting capabilities may be provided to the customer.
With emphasis on performing the following tasks:

a) Define Asset Discovery:
1) TEM for Asset Discovery ensures organizations truly identify all IP-addressable devices quickly, with minimal network impact. Any TEM-managed Windows device can be used to initiate the discovery process, allowing each subnet to be scanned by using Nmap(Network Mapper) in parallel or independently with results analyzed locally and consolidated for reporting back to the central management server. This allows for frequent scans and provides unmatched accuracy.
2) TEM for Asset Inventory enables deep software and hardware property inventory capabilities for TEM-managed devices.

b) High-level configuration tasks to enable Asset Discovery:
1) Enable to the Asset Discovery site.
2) Subscribe computers to the Asset Discovery site.
3) Install and configure the Nmap Asset Discovery Import service.-Deploy the Task called 'Install Nmap Asset Discovery Import Service - BES >= 7.0' from the Asset Discovery Site.-Note that you can specify the frequency by which the service imports data with this Task.
4) Deploy the Asset Discovery Scan Points.-Deploy the Task(s) starting with the name 'Designate Nmap Scan Point'.
5) Run a Network Scan: you can leverage either of the two mechanisms described below:-Deploy the Task(s) starting with 'Run Nmap Scan'.-Leverage the 'BigFix Asset Discovery Nmap Scan Wizard' to schedule and configure a network scan with advanced options and parameters.-Some of the advanced options/parameters include:-Scanning

local subnet versus specific hosts or IP/subnet ranges-TCP ports to scan-Scan Timing-OS/version Detection-Host exclusions-Scheduling and scan frequency

c) High-level configuration tasks to enable Asset Inventory and License:
   1) Enable the Inventory and License site.
   2) Subscribe computer to the Inventory and License site.
   3) Deploy the desired/appropriate Hardware probe actions.-Hardware probe actions will collect the appropriate information from the selected platforms: Linux, HP-UX, AIX, Solaris, Virtual Machines.
   4) Activate the desired Analyses to have the endpoints report inventory information.-In the TEM console, right-click on the desired Analysis, right-click, and select ⁄Activate'.-If prompted, type in the private key password, and click OK.-Some notable analyses include information that collects:-Cross platform application information (installed applications/packages, services, etc.)-Cross platform hardware information (ex: CPU of processors, hard disk info, RAID, network adapters, video controllers, audio devices, device model, device manufacturer, asset tag)-Hypervisor host information: name(s) of VM(s) on the Hypervisor, state(s) of VM(s), GUID(s) of VM(s)-Cross platform OS information (ex: full name, version, type, uptime, system language, architecture)-USB Device Detection (Windows)

D. Given a functional TEM server, a functional relay infrastructure, a subscription to TEM Lifecycle management, install and configure TEM software distribution for native and legacy processes so that users can create and deploy software packages using TEM.
With emphasis on performing the following tasks:
   a) Enable software distribution from License Overview Dashboard.
   b) Subscribe both computers and operators to the site by using the standard methodology.
   c) Find fixlet ID 708 (install BES server plugin service) under fixlets and tasks. If relevant deploy the fixlet to the TEM server.
   d) Go to the System Lifecycle domain in the console.
   e) Once site has gathered open software distribution under the system lifecycle domain.
   f) Expand the setup tasks.
   g) Run the task to install the TEM Upload Maintenance service for Software Distribution.
   h) Run the task to register the Download plug-in for software distribution.
   i) Import legacy packages by using the Software Distribution Upload Manager tool.
   j) Test the updated software distribution site by deploying a native and a legacy package.

E. Given a successfully installed TEM server, a master operator account and a license for TEM for Security Configuration Management, install TEM for Security Configuration Management so that endpoints' security configuration can be collected and measured.
With emphasis on performing the following tasks:
   a) Log on to the TEM console with a master operator account.
   b) Navigate to the BigFix Management domain.
   c) Open the License Overview Dashboard.
   d) 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.
   e) 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 TEM Management Domain.
   f) Define your computer subscription rules in the Computer Subscriptions tab of the site document

F. Given a functional TEM server and a license from IBM for Patch Management functionality, configure the TEM server for patch management so that the TEM server is configured to deploy patches to endpoints.
With emphasis on performing the following tasks:
   a) In the License Overview Dashboard in the BES Support site, enable the following sites:
      1) Patching Support - Provides supporting tools for the patch process.
      2) Enable OS and application patching sites as appropriate.
   b) Subscribe endpoints to appropriate sites.

c) Grant operators appropriate permissions.
d) Activate analyses for the appropriate platform sites.
e) 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:
    1) Navigate to the content site (e.g. Patches for Solaris) and run the task: "BES Relay/Server: Register Download Plug-in for " (e.g. "BES Relay/Server: Register Download Plug-in for Solaris").
    2) The task will prompt for the login name and password to the OS vendor's site.

G. Given that TEM 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.
With emphasis on performing the following tasks:
    a) Enable Trend Antivirus Content.
        1) In the TEM console, navigate to BigFix Management -> License Overview.
        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.
        3) Subscribe the endpoints to the new Trend Micro content as appropriate.
    b) Install server component.
        1) In the TEM console , navigate to Endpoint Protection -> Core Protection Module -> Quick Start -> Automatic Update or navigate to Endpoint Protection -> Core Protection Module -> Deployment
        2) Run the fixlet, Core Protection Module - Install Server Component, against your TEM server. This will install the actual Trend Micro Server Components on your TEM server.
    c) Install update script.
        1) Once the server component is installed, the fixlet Core Protection Module - Download CPMAutoUpdateSetup Script will become relevant.
        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 TEM server will use to run the auto updater.
    d) Deploy Antivirus to endpoints.
        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.
        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.
    e) Additional Setup fixlets/tasks
        1) Fixlets/tasks to be run once, both appearing under Endpoint Protection -> Core Protection Module -> Updates -> Automatic Update Tasks-Run Core Protection Module - Enable Automatic Updates - Server against the TEM server.-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.
        2) Fixlet/tasks to be set up to run as a policy. appearing under Endpoint Protection -> Core Protection Module -> Updates -> Automatic Update Tasks-Run Core Protection Module - Set ActiveUpdate Server Pattern Update Interval as a policy against the TEM server based on the information provided on the Description Tab of the fixlet-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.
    f) Additional Tasks to Consider
        1) Set up virus scans.

2) Enable Web Reputation.
3) Enable the clientUI.

❖ **SECTION 6:TROUBLESHOOTING AND PERFORMANCE TUNING:**

A. Given the need to implement IBM Tivoli Endpoint Manager (TEM) in a production environment, having an understanding of TEM, and having knowledge of the corporate organization in which TEM 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.
With emphasis on performing the following tasks:
   a) Log in to the TEM console as a master operator.
   b) Select the All Content domain.
   c) Select tools > Create Custom site
   d) Assign a name to the custom site - (Note once the name is assigned it cannot be changed).
      1) Define Computer Subscriptions and/or Operator Permissions as required:
      2) Assign Computer Subscriptions to custom site-Select - Computer Subscription Tab (Note there are four choices)-All computers: all computers will subscribe to the site in question.-No computers: no computers will subscribe to the site in question.-Computers subscribed via ad-hoc custom site subscription actions-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:-Make appropriate selection and click "Save Changes".-Assign Operator Permissions to custom site.-Select - The Operators Permission Tab (Note there are five choices)-Grant read permissions globally - All console operators will have read access to site content-Owner - selected console operator will have owner rights to custom site-Writer - selected console operator will have ability to add custom content to the custom site-Reader - selected console operator will have ability to read content in custom site-None - Remove assigned permissions from console operator-Make appropriate selection and click "Save Changes"-Assign permissions based on predefined roles (Note there are four choices).-Owner - console operators assigned to a selected role will be granted owner permissions to the custom site-Writer - console operators assigned to a selected role will be granted write permissions to the custom site-Reader - console operators assigned to a selected role will be granted read permissions to the custom site -None - Selected role will remove all permissions from console operators assigned to the selected role-Make appropriate selection and click "Save Changes"

B. Given that TEM 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.
With emphasis on performing the following tasks:
   a) 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:
      1) A task is considered "complete" if it runs its component commands successfully.
      2) A fixlet is considered "fixed" only if it runs its component commands successfully AND is no longer relevant after completing them.
   b) 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
      1) The Custom Authoring Training Guide gives an overview of the authoring process and includes strategies for creating tasks/fixlets.

2) The Relevance Quick Reference and Core Inspectors Reference explain the Relevance functions and objects that are common across all TEM platforms.
3) 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.
4) The Action Guide and the Action Guide and Examples explain the commands that are available to use in ActionScripts.

c) Test the task/fixlet using the Fixlet Debugger, available at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Fixlet%20Authoring
d) Deploy the task/fixlet by taking action on it. Full details of how to deploy tasks and fixlets are included in the TEM Console Operator's Guide at http://support.bigfix.com/resources.html

C. Given a functional TEM console connected to the appropriate TEM server, create a custom Property and a custom Analysis so that custom information can be retrieved from an endpoint.
With emphasis on performing the following tasks:

a) Create a new property:
1) In the TEM console navigate to Tools -> Manage Properties
2) Click on the ⬚Add New' button to create a new property.
3) You can select which category you would like to create your new property by clicking on the ⬚Category' button.
4) Give your new property a name in the ⬚Name' field.
5) Populate the relevance field with the appropriate relevance to match with your property.
6) Choose the Evaluate period by clicking on the drop-down menu called ⬚Evaluate' select which period you would like.
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.

b) Create a new analysis:
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⬚'-Provide a name for the new analysis.-Select which site from the drop-down menu to create your new Analysis in.-Select which domain from the drop-down menu you would like to create the domain in.-On the first tab ⬚Description' enter a description of what your new analysis will do.-On the second tab ⬚Properties' select ⬚Add Property'.-Give your property a name in the ⬚ Name' field.-Enter your relevance statement for the property in the relevance field below.-Select the period in the ⬚Evaluate' drop-down window.-On the ⬚Relevance' tab Select one of the following:-All computers-Computers that match the condition below-Select a property, clause and value to match.-Computers which match all of the relevance clauses below-Enter in a relevance statement to match.-On the bottom of the main page deselect the check box to ⬚Automatically activate this analysis after it is created'

D. Given the requirement to maintain a consistent operating environment, create and maintain TEM baselines so that agents have the same operations and packages deployed.
With emphasis on performing the following tasks:

a) Create baseline:
1) Select Tools -> Create New Baseline from the menu.-Set baseline name.-Set description (optional).-Select site to create the baseline in.-Select the domain to create the baseline in.-Set relevance conditions in the "Relevance" tab.

b) Add fixlets/tasks to baseline:
1) Select desired fixlet(s)/task(s).

2) Right click and select "Add to New Baseline" or "Add to Existing Baseline".-If adding to a new baseline set properties required to create new baseline.-If adding to existing baseline, select the baseline.-On "Components" tab, select the desired action.-Press "OK" and enter password to save baseline.

c) Remove components from baseline:
   1) Open desired baseline to "Components" tab.
   2) Click on red circle with the "X" to delete from the baseline.
   3) Press "OK" and enter password to save baseline.

d) Modify component order in baseline.
   1) Open desired baseline to "Components" tab.
   2) Select single up arrow to move the component to be installed earlier or single down arrow to move later.
   3) Select double up arrow to move to a previous component group or double down arrow to move to a later component group.
   4) Press "OK" and enter password to save baseline.

e) Delete baseline:
   1) Select desired baseline.
   2) Right click on baseline and select "Remove".
   3) Press "OK" and enter password to delete the baseline.

E. Given a functioning Web Reports server, and a Web Reports user with appropriate permissions, create a custom Web Report so that desired custom results can be retrieved.
With emphasis on performing the following tasks:

a) Enter the Web Reports URL in your browser: http://hostname.domain.com:80/webreports
   1) Log in to the Web Reports server with your user ID.
   2) Click on the Explore Data link at the top of the page on the left side.
   3) Select the data category you wish to use.
   4) Select the Results to match ?Any' or ?All".
   5) Apply filters to produce the report results you are looking for.
   6) Apply more filters by selecting the ?-? or ?+' key. -If you wish to add a clause to the same filter click on the ?add clause'.-If you wish to remove a clause click on the ?X' button to the left of it.
   7) Click ?Apply Filter' button to see the results bellow.
   8) To create a chart for your report click on the ?Add Chart' button-Give the chart a title, typically describes your chart data-Pick a computer property to populate your chart with.-Modify the chart by dragging lines on top of each other to form groups.-Click the ?Create Chart' button.
   9) Click the ?Save Report' button.
   10) Give your New report a descriptive name.
   11) Click on the ?Save Button'.

b) To Find your new report, click on the ?Report List' button.
   1) 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.