



# **Cloud & Smarter Infrastructure Professional Certification Program**

Study Guide Series

**Exam C2010-507 - IBM Tivoli Monitoring  
V6.3 Implementation**

**Purpose of Exam Objectives..... 3**

**High-level Exam Objectives ..... 4**

**Detailed Exam Objectives ..... 9**

    Section 1 - Planning..... 9

    Section 2 - Installation ..... 18

    Section 3 - Configuration ..... 23

    Section 4 - Administration ..... 31

    Section 5 - Performance Tuning and Problem Determination ..... 37

**Next Steps..... 43**

## Purpose of Exam Objectives

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

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

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

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

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

## High-level Exam Objectives

Section 1 - Planning	
1.1	<u>Given a customer with a timeline, determine the scope of a monitoring project so that a Statement of Work and project plan are created.</u>
1.2	<u>Given the requirements to implement ITM 6.3 and the knowledge of the customer's organization, determine what is to be monitored so that there is an understanding of customer's monitoring requirements.</u>
1.3	<u>Given the customer network diagram and a basic ITM 6.3 architecture, identify network ports and request to open and test the networking so that firewall requirements are outlined and verified.</u>
1.4	<u>Given the customer's operating environment and monitoring requirements, determine the OS agent platforms so that corresponding OS agents can be deployed.</u>
1.5	<u>Given the ITM High Availability (HA) Guide and the customer's business needs, determine the customer's requirement for a high availability environment so that an ITM 6.3 HA design plan is created.</u>
1.6	<u>Given the sizing and the architecture of the monitoring environment, determine how many Hub Tivoli Enterprise Monitoring Server (Hub TEMS) and RTEMS are necessary to support the monitoring environment so that an initial version of an ITM V6.3 solution architecture document is created.</u>
1.7	<u>Given the customer's monitoring and reporting requirements and the ITM 6.x Warehouse Load Projections spreadsheet, determine the length of historical data collection and size the data warehouse so that historical configuration parameters have been defined and the required storage capacity for historical data is identified.</u>
1.8	<u>Given the ITM 6.3 architecture document with estimated agents to be deployed, define the size of the ITM 6.3 environment so that the appropriate hardware will be deployed.</u>
1.9	<u>Given the LDAP or Active Directory server to authenticate, define the authentication method so that the authentication method is defined.</u>
1.10	<u>Given an understanding of customer's monitoring requirements, review authorization options and define TEPS user groups as required so that TEPS users will have access and permissions required to perform assigned monitoring functions.</u>
1.11	<u>Given a basic understanding of ITM software implementation and knowledge of the ITM installation documentation, review the ITM Installation and Setup Guide and run the prerequisite scanner so that ITM prerequisites are determined.</u>
1.12	<u>Given a basic knowledge of ITM architecture concepts, ITM deployment, and the customer's monitoring requirements, determine the most appropriate installation methods so that an implementation and deployment plan for Tivoli Monitoring infrastructure and monitoring agents is developed.</u>

1.13	<u>Given the scope of the monitoring project and a knowledge of the customer's monitoring environment, review available event management facilities and document any need for ITM event integration so that ITM events can be displayed on an event management console if required.</u>
1.14	<u>Given knowledge of customer's monitoring requirements and knowledge of what is to be monitored, assess whether there is a need for agentless monitoring, as well as or instead of standard OS agents, in the ITM environment so that requirements for agentless monitoring can be included in the ITM architecture diagram and hardware resources to support agentless monitoring can be sized appropriately.</u>
1.15	<u>Given experience and knowledge with ITM, describe the features and functions that allow ITM agents to run independently of the TEMS so that the features and functions of Agent Autonomy have been described.</u>
1.16	<u>Given a knowledge of ITM concepts and the customer's operating environment, determine what type(s) of the TEP client will be used so that ITM users can be provided with accurate instructions on accessing the TEP client.</u>
1.17	<u>Given the dashboard requirements for an organization, describe requirements for JAZZ and Dash so that business needs are met.</u>
1.18	<u>Given the data reporting requirements for an organization, describe requirements for Jazz and Tivoli Common Reporting (TCR) so that business needs are met.</u>
<b>Section 2 - Installation</b>	
2.1	<u>Given the scope of the monitoring project and a statement of what is to be monitored, verify the compatibility of IBM Tivoli Monitoring (ITM) and customer software components and download required ITM software install media so that correct version of each required ITM component is available to install.</u>
2.2	<u>Given an ITM Installation and Deployment Guide, an action plan to address any inadequate or missing requirements and a basic knowledge of the ITM deployment and the servers where each component is to be installed, install the OS, hardware and software prerequisites so that requirements for all ITM infrastructure components are fulfilled</u>
2.3	<u>Given the installation media and the host system, install and configure the supporting RDBMS so that it supports the TDW and/or the TEPS.</u>
2.4	<u>Given the ITM 6.3 architecture, take the required actions for Hub TEMS, RTEMS, TEPS, Tivoli Enterprise Portal (TEP) client, TDW and the agents so that the components of ITM environment are installed.</u>
2.5	<u>Given the storage capacity and installation media, populate the depot so that the remote installation of OS and non OS agent can be completed.</u>
2.6	<u>Given an installed ITM environment at required version level, the knowledge of the ITM tool, the target business requirement and enabled self describing feature on TEPS, supported agents, and any remote TEMS, take the required actions so that self-describing agent capability can be deployed.</u>

2.7	<a href="#">Given basic knowledge of ITM and agent installation, use the self-describing agent feature correctly and install application support at the TEMS and TEPS as required so that agent monitoring data will be displayed correctly in the TEP.</a>
<b>Section 3 - Configuration</b>	
3.1	<a href="#">Given installed base components of the IBM Tivoli Monitoring (ITM) and the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Tivoli Enterprise Monitoring Server (TEMS) so that TEMS can run according to required business needs.</a>
3.2	<a href="#">Given installed base components of the ITM and installed DBMS for Tivoli Enterprise Portal Server (TEPS) and Tivoli Data Warehouse (TDW), the IBM Tivoli Monitoring installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the TEPS so that the ITM environment can run according to required business needs.</a>
3.3	<a href="#">Given installed base components of the ITM and installed DBMS for TDW, the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Summarization and Pruning Agent (SPA) so that the SPA can run according to required business needs.</a>
3.4	<a href="#">Given installed base components of the ITM and installed DBMS for Data Warehouse, the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Warehouse Proxy so that the Warehouse Proxy can run according to required business needs.</a>
3.5	<a href="#">Given installed base components of the ITM and the ITM installation guide, the deployment architecture and basic knowledge of the IBM Tivoli Monitoring Solution, configure the OS monitoring agent so that the OS monitoring agent can run according to required business needs.</a>
3.6	<a href="#">Given installed base components of the ITM and the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Tivoli Enterprise Portal (TEP) so that the TEP can run according to required business needs.</a>
3.7	<a href="#">Given a working ITM environment, configure components so that ITM is highly available</a>
3.8	<a href="#">Given access to event management system, TEMS, and installation guides, configure the integration with event management so that ITM integration to the Event Management System can be completed.</a>
3.9	<a href="#">Given a deployed and running ITM Infrastructure (TEP, TEPS, TEMS and/or secondary TEMS), configure agents so that they are correctly connected to a TEMS.</a>
3.10	<a href="#">Given a working ITM environment, installed and configured WPA and SPA and Application Support for selected agents, and a customer's historical data collection and reporting requirements, configure historical data collection so that required historical data can be collected, summarized and pruned correctly.</a>

3.11	<u>Given an installed ITM environment at required version level, the knowledge of the ITM tool, the target business requirement, take the required actions so that range partitioning for TDW can be completed.</u>
3.12	<u>Given a working ITM environment describe the functions of Agent Management Services (AMS) so that it can be used to monitor and manage agents.</u>
<b>Section 4 - Administration</b>	
4.1	<u>Given an installed and running IBM Tivoli Monitoring (ITM) environment, and the knowledge of the ITM products, verify the installed components are running appropriately so that their connection status to the Hub can be confirmed.</u>
4.2	<u>Given a running ITM V6.3 Infrastructure that is installed and configured correctly and ITM administrator User ID, use the TEP interface so that users are created with appropriate access rights and roles.</u>
4.3	<u>Given an installed, configured and running ITM environment, and knowledge of the IBM Tivoli Monitoring product, access the TEP so that data visibility for monitored items can be demonstrated and confirmed.</u>
4.4	<u>Given a working ITM environment, create custom views and workspaces so that data is displayed in a customized way.</u>
4.5	<u>Given a working ITM environment and the authority to create situations, examine the product provided situations and create a custom situation so that customer requirements can be met.</u>
4.6	<u>Given a working ITM environment, periodically verify ITM disk space so that normal operation and file growth are accommodated</u>
4.7	<u>Given a working ITM failover configuration, perform required actions so that correct functionality of the failover can be verified.</u>
4.8	<u>Given access to an implemented ITM system, back up the TEPS database so that a restore of the TEPS database can be successfully performed, if required.</u>
4.9	<u>Given a working ITM environment, back up the Hub TEMS objects so that after restoration, the Hub TEMS is fully operational at the state in which the backup was taken.</u>
<b>Section 5 - Performance Tuning and Problem Determination</b>	
5.1	<u>Given access to IBM Tivoli Monitoring (ITM), review the installation logs so that errors or failures can be identified.</u>
5.2	<u>Given access to a correctly implemented ITM, set the Java Heap Size so that the Tivoli Enterprise Portal Server (TEPS) can handle multiple concurrent logins.</u>
5.3	<u>Given access to the application and system log, review and analyze the logs so that any issues or error are identified.</u>
5.4	<u>Given access to the server, enable user and component auditing so that all changes are tracked</u>
5.5	<u>Given access to the TEP with permission to modify situations, ensure that monitoring situations are running at an appropriate frequency so that the correct sampling frequency is entered per the customer requirements.</u>

5.6	<u>Given the customer requirements and TEP access, review the self-monitoring topology so that the agents are distributed appropriately across the monitoring infrastructure.</u>
5.7	<u>Given the number of concurrent users on an HTTP, Apache, or IIS Web server, tune the Web server so that concurrent users connectivity is optimized.</u>
5.8	<u>Given access to the server, configure logging so that logging levels and parameters are set appropriately for the production environment</u>



## **Detailed Exam Objectives**

### **Section 1 - Planning**

#### **1.1. Given a customer with a timeline, determine the scope of a monitoring project so that a Statement of Work and project plan are created.**

##### **SUBTASK(S):**

- 1.1.1. Schedule a meeting with the stakeholders.
- 1.1.2. Discuss customer requirements and expectations.
  - 1.1.2.1. Return on investment (time to value)
  - 1.1.2.2. Data retention
- 1.1.3. Obtain a list of licensed software.
- 1.1.4. Obtain knowledge of customer's monitoring environment and available hardware.
  - 1.1.4.1. Determine the number of servers to be monitored.
  - 1.1.4.2. Determine operating system platforms.
  - 1.1.4.3. Determine what the customer will monitor (logs, applications and databases).
- 1.1.5. Obtain knowledge of customer's IT operational procedures and event management system.
  - 1.1.5.1. Review Service Level Agreements (SLAs)
  - 1.1.5.2. Determine how the operators will be using IBM Tivoli Monitoring (ITM).
  - 1.1.5.3. Determine the operational queues (where the event goes).

#### **1.2. Given the requirements to implement ITM 6.3 and the knowledge of the customer's organization, determine what is to be monitored so that there is an understanding of customer's monitoring requirements.**

##### **SUBTASK(S):**

- 1.2.1. Identify key project sponsors, participants, and stakeholders.
  - 1.2.1.1. Management sponsorship
  - 1.2.1.2. departmental management and/or technical leads for business applications
  - 1.2.1.3. those that have responsibility for the success of the solution
  - 1.2.1.4. personnel charged with the technical support of ITM.
- 1.2.2. Determine which business components are required to be monitored.
  - 1.2.2.1. Types of servers
  - 1.2.2.2. Applications
  - 1.2.2.3. Databases
  - 1.2.2.4. Determine which custom solutions will be required so appropriate timing and resources can be planned.
  - 1.2.2.5. Agent Builder
    - 1.2.2.5.1. Scripting

- 1.3. Given the customer network diagram and a basic ITM 6.3 architecture, identify network ports and request to open and test the networking so that firewall requirements are outlined and verified.**

SUBTASK(S):

- 1.3.1. Identify network ports.
  - 1.3.1.1. Verify if firewall gateways need to be used.
  - 1.3.1.2. Verify if IP.SPIPE is used.
- 1.3.2. Request to open ports to network team .
- 1.3.3. Test flow across the network ports.

- 1.4. Given the customer's operating environment and monitoring requirements, determine the OS agent platforms so that corresponding OS agents can be deployed.**

SUBTASK(S):

- 1.4.1. List and identify required OS agents.
  - 1.4.1.1. Identify Linux OS agent.
  - 1.4.1.2. Identify UNIX OS agent.
  - 1.4.1.3. Identify Windows OS agent.
  - 1.4.1.4. Identify IBM i OS agent.
- 1.4.2. List and Identify agentless for monitoring, if required.
  - 1.4.2.1. Identify agentless Monitoring for AIX
  - 1.4.2.2. Identify agentless Monitoring for HP-UX
  - 1.4.2.3. Identify agentless Monitoring for Linux
  - 1.4.2.4. Identify agentless Monitoring for Solaris
  - 1.4.2.5. Identify agentless Monitoring for Windows

- 1.5. Given the ITM High Availability (HA) Guide and the customer's business needs, determine the customer's requirement for a high availability environment so that an ITM 6.3 HA design plan is created.**

SUBTASK(S)

- 1.5.1. Determine method of HA that will be implemented.
  - 1.5.1.1. Hot Standby
  - 1.5.1.2. OS Cluster
  - 1.5.1.3. Other
- 1.5.2. Determine if the Portal Server requires HA.
- 1.5.3. Determine if IBM Dashboard Application services requires HA.
- 1.5.4. Determine if the Tivoli Enterprise Monitoring Server (TEMS) or remote Tivoli Enterprise Monitoring Server (RTEMS) requires HA.
- 1.5.5. Determine configuration of the agents for HA.

- 1.6. Given the sizing and the architecture of the monitoring environment, determine how many Hub Tivoli Enterprise Monitoring Server (Hub TEMS) and RTEMS are necessary to support the monitoring**

**environment so that an initial version of an ITM V6.3 solution architecture document is created.**

**SUBTASK(S):**

- 1.6.1. Define how many servers will be monitored.
- 1.6.2. Define how many applications will run in each server.
  - 1.6.2.1. Every server has one OS agent running.
  - 1.6.2.2. Define number of agents per application. Ex:(one for DB2, one for Lotus Domino)
- 1.6.3. Establish the limit of 1500 agent running on each RTEMS.
- 1.6.4. Establish the limit of 20.000 maximum agents running on ITM environment.
- 1.6.5. Define the number of RTEMS running.
  - 1.6.5.1. Grant that each RTEMS support up to 1500 managed systems.
  - 1.6.5.2. Define if there are any standby RTEMS and configure it.
- 1.6.6. Define the number of Hub TEMS.
  - 1.6.6.1. Determine if there is HA and increase the number of HTEMS accordingly.

**1.7. Given the customer's monitoring and reporting requirements and the ITM 6.x Warehouse Load Projections spreadsheet, determine the length of historical data collection and size the data warehouse so that historical configuration parameters have been defined and the required storage capacity for historical data is identified.**

**SUBTASK(S):**

- 1.7.1. Define the metrics to be collected.
- 1.7.2. Define the retention length.
- 1.7.3. Define the level of summarization.
- 1.7.4. Define the frequency of collection.
- 1.7.5. Identify the number and types of agents in the ITM environment.
- 1.7.6. Use the IBM Tivoli Monitoring 6.x Warehouse Load Projections spreadsheet to estimate the required space.

**1.8. Given the ITM 6.3 architecture document with estimated agents to be deployed, define the size of the ITM 6.3 environment so that the appropriate hardware will be deployed.**

**SUBTASK(S):**

- 1.8.1. Identify the size of the ITM 6.3 environment.
  - 1.8.1.1. Large and medium-sized environments >1500 agents, the Hub TEMS should have at least 2 processors and 3 GB of RAM and the usage of RTEMS are necessary.
  - 1.8.1.2. Small environments <1000 agents The system should have at least 2 processors and 4 GB of RAM.
  - 1.8.1.3. Remote monitoring server can support up to 1500 managed systems, a server with 4 GB of memory is typically sufficient.

**1.9. Given the LDAP or Active Directory server to authenticate, define the authentication method so that the authentication method is defined.**

**SUBTASK(S):**

- 1.9.1. Discuss with the LDAP administrators the required parameters to be configured:
  - 1.9.1.1. LDAP server and port
  - 1.9.1.2. CN, DC, OU
  - 1.9.1.3. Auditor credentials
- 1.9.2. Define the authentication method.
  - 1.9.2.1. Hub TEMS
    - 1.9.2.1.1. Local Operational system
    - 1.9.2.1.2. External LDAP server
  - 1.9.2.2. Tivoli Enterprise Portal Server (TEPS)
    - 1.9.2.2.1. External LDAP server
- 1.9.3. Determine communication between TEMS and LDAP server.

**1.10. Given an understanding of customer's monitoring requirements, review authorization options and define TEPS user groups as required so that TEPS users will have access and permissions required to perform assigned monitoring functions.**

**SUBTASK(S):**

- 1.10.1. Review administrator's guide sections regarding:
  - 1.10.1.1. Enable user authentication.
  - 1.10.1.2. Tivoli Enterprise Portal (TEP) user authorization
  - 1.10.1.3. Role-based authorization policies
- 1.10.2. Determine how TEP users will be authenticated:
  - 1.10.2.1. Through the Hub TEMS
    - 1.10.2.1.1. Local account
    - 1.10.2.1.2. LDAP
  - 1.10.2.2. LDAP through the TEPS
  - 1.10.2.3. Other
- 1.10.3. Determine what TEP user groups and special permissions will be required
  - 1.10.3.1. Define what roles TEP users are expected to fulfill within ITM.
  - 1.10.3.2. Review TEP user permissions to map groups of users to the appropriate permissions.
  - 1.10.3.3. Design a number of user groups that will contain appropriate permissions, for example, default ITM user groups include:
    - 1.10.3.3.1. \*ADMINISTRATOR
    - 1.10.3.3.2. \*OPERATOR
    - 1.10.3.3.3. \*USERS
  - 1.10.3.4. Determine if specific users will require additional permissions not satisfied by their group permissions.

- 1.10.4. Determine if role-based authorization policies will be required to protect against unauthorized access by users of IBM Dashboard Application Services Hub. If so, determine if one of the many pre-defined roles and permissions will fit the requirements
- 1.10.5. Document all these finding in an ITM infrastructure access and user roles document for use in ITM configuration and administration steps.

**1.11. Given a basic understanding of ITM software implementation and knowledge of the ITM installation documentation, review the ITM Installation and Setup Guide and run the prerequisite scanner so that ITM prerequisites are determined.**

**SUBTASK(S):**

- 1.11.1. Review section of the ITM Installation and Setup Guide regarding Hardware and Software Requirements.
- 1.11.2. Review section of the ITM Installation and Setup Guide regarding the Prerequisite Scanner.
- 1.11.3. Run the Prerequisite Scanner on servers where OS agents are going to be installed.
- 1.11.4. Review the Prerequisite Scanner reports.
- 1.11.5. Given the results of the review of hardware and software requirements, and the Prerequisite Scanner reports, generate a plan of action required to address deficiencies, if any.

**1.12. Given a basic knowledge of ITM architecture concepts , ITM deployment, and the customer's monitoring requirements, determine the most appropriate installation methods so that an implementation and deployment plan for Tivoli Monitoring infrastructure and monitoring agents is developed.**

**SUBTASK(S):**

- 1.12.1. Determine where the ITM components should be installed based on existing hardware and software resources in the customer environment.
  - 1.12.1.1. The IT staff's familiarity and expertise level with each of the available platforms for the deployment should be considered.(i.e. For a shop with limited Windows expertise, Linux or AIX might be the best deployment platform)
- 1.12.2. Identify the number and types of agents to be deployed.
- 1.12.3. Verify that the intended hardware deployment platform has the necessary resources. (CPU, memory, disk, network)
  - 1.12.3.1. Determine the amount of data to be warehoused as well as the summarization and pruning schedules.
  - 1.12.3.2. Refer to "sizing guidelines" in the ITM Installation & Deployment Guide Redbooks.
- 1.12.4. Verify if the necessary access to the deployment platform is available.

- 1.12.4.1. A Windows deployment must be done with administrator privileges, and the monitoring components must run as a user with administrator privileges.
- 1.12.4.2. It is recommended that a UNIX deployment should be done as the root user. If a UNIX deployment must be done as a non-root user due to security guidelines, there are some additional steps that must be performed during the installation.
  - 1.12.4.2.1. Use the same user to install all components.
  - 1.12.4.2.2. Some file permissions will be required to be changed for every agent installation.
- 1.12.5. If a firewall gateway is required, meet with network administrators to discuss ports to be utilized and finalize detailed design.
- 1.12.6. Document the order of installation of each of the ITM components.
  - 1.12.6.1. Hub TEMS
  - 1.12.6.2. RTEMS (if required)
  - 1.12.6.3. TEPS
  - 1.12.6.4. Tivoli Enterprise Portal desktop client (if required)
  - 1.12.6.5. Tivoli Data Warehouse – Warehouse Proxy agent and Summarization & Pruning agent
- 1.12.7. Determine how monitoring agents can best be deployed.
  - 1.12.7.1. In most cases the creation of an agent depot for remote deployment of agents will be sufficient.
  - 1.12.7.2. If an enterprise-class software distribution product (for example, Tivoli Configuration Manager or Tivoli Provisioning Manager) is already being used, it might be more efficient to utilize it for distribution of agents and patches.
  - 1.12.7.3. If a remote TEMS will be installed, the use of an NFS share can minimize the amount of administrative overhead to maintain the agent depot.

**1.13. Given the scope of the monitoring project and a knowledge of the customer's monitoring environment, review available event management facilities and document any need for ITM event integration so that ITM events can be displayed on an event management console if required.**

**SUBTASK(S):**

- 1.13.1. Determine if ITM event integration with an event management product is required.
  - 1.13.1.1. If the event management product is IBM Tivoli Netcool/OMNIBus (Netcool/OMNIBus) , review the sections of the Installation Guide: Integrating event management systems and set up event forwarding to Netcool/Omnibus.
    - 1.13.1.1.1. Bi-directional or uni-directional integration (Situation Update Forwarder)

- 1.13.1.2. If the event management system is Tivoli Event Console (TEC), review the sections of the Installation Guide: Integrating event management systems and set up event forwarding to Tivoli Enterprise Console.
- 1.13.1.3. If a different event management product is being used, review additional options for forwarding ITM events. These may include:
  - 1.13.1.3.1. Use ITM workflow automation (policies) to send an SNMP alert to an event console.
  - 1.13.1.3.2. Use features of the ITM Autonomous agent to emit SNMP alerts, as discussed in the Administrator's Guide, section on Agent autonomy.
  - 1.13.1.3.3. Create a custom event receiver that integrates with the event management product.
- 1.13.1.4. Create an event integration planning document that contains the selected event integration strategy, if any, as input to the ITM configuration and administration processes.

**1.14. Given knowledge of customer's monitoring requirements and knowledge of what is to be monitored, assess whether there is a need for agentless monitoring, as well as or instead of standard OS agents, in the ITM environment so that requirements for agentless monitoring can be included in the ITM architecture diagram and hardware resources to support agentless monitoring can be sized appropriately.**

**SUBTASK(S):**

- 1.14.1. Review agentless monitoring documentation.
- 1.14.2. Discuss with customer the features of agentless monitoring and determine if there is a need for agentless monitoring in the ITM environment, Considerations will include:
  - 1.14.2.1. Determine if remote servers need to be monitored from a central location, rather than having an OS agent installed.
  - 1.14.2.2. Determine if SNMP, WMI (Windows) or CIM (Solaris) is available for collection of metrics on the remote server.
  - 1.14.2.3. Compare the attributes and attribute groups collected by agentless monitoring against those collected by the standard OS agents to determine whether agentless monitoring will meet requirements.
  - 1.14.2.4. If agentless monitoring is required, identify the number of servers where agentless agents for collecting monitoring information will be installed and plan for additional server resources within the ITM infrastructure to support the required agentless agents.

**1.15. Given experience and knowledge with ITM, describe the features and functions that allow ITM agents to run independently of the TEMS so**

**that the features and functions of Agent Autonomy have been described.**

**SUBTASK(S):**

- 1.15.1. The Tivoli Enterprise Monitoring Agent (TEMA) :
  - 1.15.1.1. TEMA can run independently of the TEMS.
  - 1.15.1.2. Collects data, run situations and register events when they are disconnected from the TEMS.
- 1.15.2. The TEMA can be configured to run autonomously.
- 1.15.3. The TEMA can use rules defined in an XML file so that:
  - 1.15.3.1. Situations can be defined and run locally.
  - 1.15.3.2. Events can be sent as SNMP alerts or Event Integration Facility (EIF) events to a receiver.
  - 1.15.3.3. Collect and save historical data locally.
  - 1.15.3.4. The TEMA will store situation events that will be forwarded to the TEMS upon reconnection.
  - 1.15.3.5. Situations that require evaluation at the TEMS are unable to run if there is no connection.
- 1.15.4. The Tivoli System Monitor agent:
  - 1.15.4.1. Is installed where there is no Tivoli Management Services or TEMA installed, except for Agent Builder agents.
  - 1.15.4.2. Is an OS agent that never connects to a TEMS.
  - 1.15.4.3. Uses the same code as a TEMA.
  - 1.15.4.4. Does not use Java for installation.
  - 1.15.4.5. Has a smaller software footprint than a TEMA.
  - 1.15.4.6. Uses XML files for situation and SNMP alert definitions.
- 1.15.5. Both agents can run private situations.

**1.16. Given a knowledge of ITM concepts and the customer's operating environment, determine what type(s) of the TEP client will be used so that ITM users can be provided with accurate instructions on accessing the TEP client.**

**SUBTASK(S):**

- 1.16.1. Review the section of the Administrator's Guide that discusses "Preparing your Tivoli Enterprise Portal environment".
- 1.16.2. Review the information in the TEP User's Guide that discusses Browser client differences
- 1.16.3. Evaluate the customer technical environment compared to the requirements, and the differences, for each of the TEP client choices. Items to be considered may include:
  - 1.16.3.1. Ease of installation and ongoing maintenance requirements
  - 1.16.3.2. Workspaces that are referenced by unique URLs
  - 1.16.3.3. Availability of tabbed workspaces
  - 1.16.3.4. Which browser and Java products are supported in the environment and at which versions.



- 1.16.4. Determine how many and which of the TEP client choices will be recommended and supported within this ITM environment:
  - 1.16.4.1. Desktop client
  - 1.16.4.2. Browser client
  - 1.16.4.3. Java Web Start client
- 1.16.5. Prepare a document that instructs TEP users on accessing the version(s) of the TEP client that are recommended and supported.

**1.17. Given the dashboard requirements for an organization, describe requirements for JAZZ and Dash so that business needs are met.**

**SUBTASKS:**

- 1.17.1. Meet with the customer of the solution to determine requirements.
- 1.17.2. Document the integration points with third party tools.
- 1.17.3. Determine the sign on method.
- 1.17.4. Determine if you are going to use an existing or install a new WebSphere server.
- 1.17.5. Determine if the installation will be FIPS Compliant.
- 1.17.6. Review custom installations to support business policies.
- 1.17.7. Choose the installed topology.
- 1.17.8. Determine Hardware requirements.
- 1.17.9. Determine if an existing or new DB2 instance will be used.

**1.18. Given the data reporting requirements for an organization, describe requirements for Jazz and Tivoli Common Reporting (TCR) so that business needs are met.**

**SUBTASK(S):**

- 1.18.1. Meet with the customer of the solution to determine requirements.
- 1.18.2. Document the integration points with third party tools.
- 1.18.3. Determine the sign on method.
- 1.18.4. Determine if you are going to use an existing or install a new WebSphere server.
  - Review custom installations to support business policies.
- 1.18.5. Choose the installed topology.
- 1.18.6. Determine Hardware requirements.
- 1.18.7. Determine if an existing or new DB2 instance will be used.

## **Section 2 - Installation**

- 2.1. Given the scope of the monitoring project and a statement of what is to be monitored, verify the compatibility of IBM Tivoli Monitoring (ITM) and customer software components and download required ITM software install media so that correct version of each required ITM component is available to install.**

**SUBTASK(S):**

- 2.1.1. Review the scope of the monitoring project and the customer monitoring requirements to create a complete list of what ITM components are required to be installed on what operating platform.
- 2.1.2. Access and review the Software Product Compatibility Reports to ensure that all required versions of ITM products are compatible with each other and with the available operating platforms.
  - 2.1.2.1. Software Product Compatibility Reports are currently available at <http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.html>
- 2.1.3. If installation media for each required ITM component is not already available, perform the following:
  - 2.1.3.1. Access the ITM download instructions document on the ITM documentation Website to determine the correct eAssembly and/or Part number to download for each required ITM product.
  - 2.1.3.2. Access Passport Advantage and use it to download all required eAssemblies and/or Parts.

- 2.2. Given an ITM Installation and Deployment Guide, an action plan to address any inadequate or missing requirements and a basic knowledge of the ITM deployment and the servers where each component is to be installed, install the OS, hardware and software prerequisites so that requirements for all ITM infrastructure components are fulfilled**

**SUBTASK(S):**

- 2.2.1. Install any required OS, hardware or software prerequisites for:
  - 2.2.1.1. the Hub Tivoli Enterprise Monitoring Server (Hub TEMS)
  - 2.2.1.2. each remote Tivoli Enterprise Monitoring server (RTEMS)
  - 2.2.1.3. the Tivoli Enterprise Portal Server (TEPS)
  - 2.2.1.4. the Tivoli Data Warehouse (TDW)
  - 2.2.1.5. the Summarization and Pruning agent (SPA)
  - 2.2.1.6. each Warehouse Proxy Agent (WPA)
- 2.3. Given the installation media and the host system, install and configure the supporting RDBMS so that it supports the TDW and/or the TEPS.**

**SUBTASK(S):**

2.3.1. Select the RDBMS for TEPS

2.3.1.1. DB2

2.3.1.2. MS-SQL

Embedded TEPS Database (Derby)

Select the RDBMS for TDW

Oracle

DB2

MS-SQL

2.3.2. Install and configure the RDBMS.

**2.4. Given the ITM 6.3 architecture, take the required actions for Hub TEMS , RTEMS, TEPS, Tivoli Enterprise Portal (TEP) client, TDW and the agents so that the components of ITM environment are installed.**

SUBTASK(S):

2.4.1. Install the components in the following order:

2.4.1.1. Hub TEMS

2.4.1.2. RTEMS (if required)

2.4.1.3. RDBMS if required

2.4.1.4. TEPS

2.4.1.5. TEP desktop client

2.4.1.6. TDW

2.4.1.6.1. RDBMS if required

2.4.1.6.2. SPA

2.4.1.6.3. WPA

2.4.1.7. Tivoli Enterprise Monitoring Agents (TEMAs)

**2.5. Given the storage capacity and installation media, populate the depot so that the remote installation of OS and non OS agent can be completed.**

SUBTASK(S):

2.5.1. Verify the capacity of the filesystem or directory.

2.5.2. Use the installation media to populate the depot.

2.5.2.1. For Linux/Unix use tacmd addBundles command.

2.5.2.2. Use installation Wizard.

2.5.3. Check and test the installation components inside the depot.

2.5.4. Check depot contents in the Deploy Depot Package list.

2.5.5. Use tacmd createnode command to remotely install a OS agent .

2.5.6. Deploy non OS agent.

2.5.6.1. Use TEPS to create by using Add Managed System.

2.5.6.2. Use tacmd addSystem command line.

**2.6. Given an installed ITM environment at required version level, the knowledge of the ITM tool, the target business requirement and enabled self describing feature on TEPS, supported agents, and any**

**remote TEMS, take the required actions so that self-describing agent capability can be deployed.**

**SUBTASK(S):**

- 2.6.1. Enabling the self-describing agent capability at the Hub monitoring server
  - 2.6.1.1. On Windows systems :
    - 2.6.1.1.1. In the Manage Tivoli Enterprise Monitoring Services application, right-click Tivoli Enterprise Monitoring Server and select Advanced-> Edit ENV file. The component environment variable file is displayed.
    - 2.6.1.1.2. Change the variable KMS\_SDA=N to KMS\_SDA=Y and save the file.
    - 2.6.1.1.3. Recycle the TEMS to have your changes take effect.
  - 2.6.1.2. On Linux and Unix systems
    - 2.6.1.2.1. Change to the <install\_dir>/config directory and open the coordinating file for the monitoring server: <hostname>\_ms\_<tems\_name>.config.
    - 2.6.1.2.2. Change the variable KMS\_SDA=N to KMS\_SDA=Y and save the file
    - 2.6.1.2.3. Recycle the Tivoli Enterprise Monitoring Server to have your changes take effect.
- 2.6.2. Configure self-describing agent seeding.
  - 2.6.2.1. Use the tacmd editSdaOptions command to configure how the self-describing agent feature seeds product definitions.

**2.7. Given basic knowledge of ITM and agent installation, use the self-describing agent feature correctly and install application support at the TEMS and TEPS as required so that agent monitoring data will be displayed correctly in the TEP.**

**SUBTASK(S):**

- 2.7.1. Review the sections of the Installation Guide regarding “Enabling self-describing agent capability at the Hub TEMS” and “Dynamically controlling the Hub TEMS self-describing agent capability”.
- 2.7.2. If self-describing agents will be used for this ITM implementation, perform the documented steps to ensure that it is configured and enabled.
- 2.7.3. Use the cinfo command, or the kincinfo command (Windows), to verify whether or not all required application support has been installed on the Hub TEMS, all RTEMS and TEPS servers.
- 2.7.4. If additional application support is required to be installed, review the sections of the Installation Guide regarding installation of application support for the TEMS, TEPS and TEP desktop client. The following guidelines may be helpful in understanding how to manually install application support:

- 2.7.4.1. Download the installation files for each required agent/ product if they are not found on the ITM Media DVD. (z/OS, ITCAM, MQ Series are examples of files that are not on the DVDs).
- 2.7.4.2. URL for Locating ITM Workspace Application Support Files for z/OS agents – this site contains Application Support files for most if not all Tivoli agents:  
<http://www-01.ibm.com/support/docview.wss?uid=swg21255545>
- 2.7.4.3. Extract the downloaded files (these can be placed into a temporary directory) and follow the install and enablement step below: (read the readme to determine the specific installation requirements).
- 2.7.4.4. Add Application Support for Windows TEMS and TEPS
  - 2.7.4.4.1. Execute the setup.exe file in the Windows sub-directory.
  - 2.7.4.4.2. Select the agent products for each of the display components. (TEMS, TEPS, TEP client).
    - 2.7.4.4.2.1. Verify that application support has been installed correctly. Note: Next 4 steps require the user log in to the TEP.
  - 2.7.4.4.3. Open the product HELP and verify the agent/ product help has been loaded.
  - 2.7.4.4.4. Open the Situation Editor and verify that the agent/ product provided situations are loaded.
  - 2.7.4.4.5. Open the QUERY editor and verify that the agent/ product provided queries are loaded.
  - 2.7.4.4.6. If possible, NAVIGATE the PHYSICAL topology, locate an agent instance and verify the agent/ product provided workspaces are loaded.
- 2.7.4.5. Add Application Support for non-Windows TEMS and TEPS
  - 2.7.4.5.1. Launch the install.sh script and follow the steps described in the ITM Install Guide by using the Installing and enabling Application Support section. An additional step is required for each of the ITM components (TEMS, TEPS, and TEP client).
  - 2.7.4.5.2. Execute the commands by using the ITM CLI depending on the ITM component:
    - 2.7.4.5.2.1. For the TEMS: itmcmd support
    - 2.7.4.5.2.2. For the TEPS and TEP client: itmcmd config
    - 2.7.4.5.2.3. Verify that application support has been installed correctly. Note: Next 4 steps require the user log in to the TEP.
  - 2.7.4.5.3. Open the product HELP and verify the agent/ product help has been loaded.
  - 2.7.4.5.4. Open the Situation Editor and verify that the agent/ product provided situations are loaded.

- 2.7.4.5.5. Open the QUERY editor and verify that the agent/  
product provided queries are loaded.
- 2.7.4.5.6. If possible, NAVIGATE the PHYSICAL topology, locate  
an agent instance and verify the agent/ product  
provided workspaces are loaded.

## Section 3 - Configuration

- 3.1. Given installed base components of the IBM Tivoli Monitoring (ITM) and the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Tivoli Enterprise Monitoring Server (TEMS) so that TEMS can run according to required business needs.**

### SUBTASK(S):

- 3.1.1. Configure the Hub Tivoli Enterprise Monitoring Server (Hub TEMS) and remote Tivoli Enterprise Monitoring server (RTEMS) :
- 3.1.1.1. Access the installed Hub TEMS or RTEMS component.
  - 3.1.1.2. Use the GUI or the command line to configure the TEMS or RTEMS component.
  - 3.1.1.3. Select configuration options in line with business needs recorded in the plan.
  - 3.1.1.4. Start the Hub TEMS and RTEMS.
  - 3.1.1.5. Verify that the Hub TEMS or RTEMS is running without failure.

- 3.2. Given installed base components of the ITM and installed DBMS for Tivoli Enterprise Portal Server (TEPS) and Tivoli Data Warehouse (TDW), the IBM Tivoli Monitoring installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the TEPS so that the ITM environment can run according to required business needs.**

- 3.2.1. Configure the TEPS
- 3.2.1.1. Access the installed TEPS component.
  - 3.2.1.2. Use the GUI or the command line to configure the TEPS.
  - 3.2.1.3. Select configuration options in line with business needs recorded in the plan.
  - 3.2.1.4. Configure a database connection to the TDW.
  - 3.2.1.5. Start the TEPS.
  - 3.2.1.6. Verify that the TEPS is running without failure.

- 3.3. Given installed base components of the ITM and installed DBMS for TDW, the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Summarization and Pruning Agent (SPA) so that the SPA can run according to required business needs.**

- 3.3.1. Configure the SPA.
- 3.3.1.1. Access the installed SPA component.
  - 3.3.1.2. Use the GUI or the command line to configure the SPA component.

- 3.3.1.3. Select configuration options in line with business needs recorded in the plan.
- 3.3.1.4. Configure a JBDC or ODBC connection to the TDW.
- 3.3.1.5. Start the SPA.
- 3.3.1.6. Verify that the SPA is running without failure.
- 3.4. Given installed base components of the ITM and installed DBMS for Data Warehouse, the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Warehouse Proxy so that the Warehouse Proxy can run according to required business needs.**
  - 3.4.1. Configure the Warehouse Proxy agent (WPA)
    - 3.4.1.1. Access the installed WPA.
    - 3.4.1.2. Use the GUI or the command line to configure the WPA.
    - 3.4.1.3. Select configuration options in line with business needs recorded in the plan
    - 3.4.1.4. Configure a JBDC or ODBC connection to the TDW.
    - 3.4.1.5. Start the WPA.
    - 3.4.1.6. Verify that the WPA is running without failure.
- 3.5. Given installed base components of the ITM and the ITM installation guide, the deployment architecture and basic knowledge of the IBM Tivoli Monitoring Solution, configure the OS monitoring agent so that the OS monitoring agent can run according to required business needs.**
  - 3.5.1. Configure the OS monitoring agent:
    - 3.5.1.1. Access the installed OS monitoring agent.
    - 3.5.1.2. Use the GUI or the command line to configure the OS monitoring agent.
    - 3.5.1.3. Select configuration options in line with business needs recorded in the plan.
    - 3.5.1.4. Start the OS monitoring agent .
    - 3.5.1.5. Verify that the OS monitoring agent is running without failure and connecting to the Hub or Remote Hub.
- 3.6. Given installed base components of the ITM and the ITM installation guide, the deployment architecture and basic knowledge of the ITM solution, configure the Tivoli Enterprise Portal (TEP) so that the TEP can run according to required business needs.**
  - 3.6.1. Configure the TEP:
    - 3.6.1.1. Decide on one of the three options for TEP. ( Desktop or Browser or Web Start )
    - 3.6.1.2. Access the installed desktop TEP.



- 3.6.1.2.1. Use the GUI or the command line to configure the desktop TEP.
- 3.6.1.2.2. Select configuration options in line with business needs recorded in the plan.
- 3.6.1.2.3. Start the desktop TEP.
- 3.6.1.2.4. Verify that the desktop TEP allows the user to view the ITM Navigators and Workspaces.
- 3.6.1.3. For the Browser and Web Start TEP, Use the required steps to download Java and configure them.

### **3.7. Given a working ITM environment, configure components so that ITM is highly available**

#### **SUBTASK(S):**

- 3.7.1. Determine which method will be used for High Availability (HA):
- 3.7.2. If TEMS Hot Standby
  - 3.7.2.1. Install a second Hub TEMS by following the standard TEMS installation procedures.
  - 3.7.2.2. Define one Hub TEMS as the primary Hub TEMS and the other Hub TEMS as the secondary TEMS.
  - 3.7.2.3. Configure the primary Hub TEMS to take the secondary TEMS as the Hot Standby Hub TEMS.
  - 3.7.2.4. Configure the secondary Hub TEMS to take the primary TEMS as the Hot Standby Hub TEMS.
- 3.7.3. Configure all RTEMS to specify the primary Hub TEMS and the secondary Hub TEMS.
- 3.7.4. Configure all monitoring agents that are connected directly to the Hub TEMS by specifying the primary Hub TEMS and the secondary TEMS.
- 3.7.5. Configure the WPA and the SPA to connect to the primary Hub TEMS and the secondary TEMS.
- 3.7.6. Certain degree of high availability for TEPS can be achieved by the following without using cluster technology.
  - 3.7.6.1. Install a second TEPS as a backup TEPS.
  - 3.7.6.2. Users are only allowed to update ITM objects on the primary TEPS.
  - 3.7.6.3. Develop some procedures to synchronize the primary and the backup TEPS databases.
  - 3.7.6.4. When the primary TEPS goes down, direct users to log in the backup TEPS.
- 3.7.7. If third-party, non-ITM clustering solution, consult vendor specific documentation.
- 3.7.8. Generic HUB TEMS clustering instructions:
  - 3.7.8.1. Set up the basic cluster resource group with a shared persistent storage and virtual IP address.
  - 3.7.8.2. Install the monitoring server on the first node of the cluster (shared persistent storage).

- 3.7.8.3. Remove automatic startup of the monitoring server service (if applicable to your platform).
- 3.7.8.4. Bind the monitoring server to the virtual IP address.
- 3.7.8.5. Set up the monitoring server on the second node of the cluster (depending on the platform, this might involve copying registry keys, environment variables, or both to the second node).
- 3.7.8.6. Add the monitoring server as a resource to the resource group.
- 3.7.9. Generic TEPS clustering instructions:
  - 3.7.9.1. Install the database middleware locally on both nodes.
  - 3.7.9.2. Set up the database users and groups to be exactly the same on both nodes.
  - 3.7.9.3. Remove automatic startup of the monitoring server service (if applicable to your platform).
  - 3.7.9.4. Set up the basic cluster resource group with shared persistent storage, virtual IP address, and the database middleware.
  - 3.7.9.5. Create the portal server database on the first node of the cluster (shared persistent storage).
  - 3.7.9.6. Catalog the portal server database on the second node of the cluster.
  - 3.7.9.7. Install the portal server on the first node of the cluster (shared persistent storage).
  - 3.7.9.8. Disable autostart of the portal server service (if applicable to your platform).
  - 3.7.9.9. Bind the portal server to the virtual IP address.
  - 3.7.9.10. Set up the monitoring server on the second node of the cluster (depending on the platform, this might involve copying registry keys, environment variables, or both to the second node).
  - 3.7.9.11. Add the portal server as a resource to the resource group.

**3.8. Given access to event management system, TEMS, and installation guides, configure the integration with event management so that ITM integration to the Event Management System can be completed.**

**SUBTASK(S):**

- 3.8.1. Determine event management systems to integrate with:
  - 3.8.1.1. For Tivoli Enterprise Console:
    - 3.8.1.1.1. Install event synchronization with TEC.
      - 3.8.1.1.1.1. Install by using wizard.
      - 3.8.1.1.1.2. Install from the command line.
      - 3.8.1.1.1.3. Install from command line by using a silent installation.
      - 3.8.1.1.1.4. Install and configure EIF Probe.
  - 3.8.1.2. For IBM Tivoli Netcool/OMNIBus (Netcool/OMNIBus):
    - 3.8.1.2.1. Install event synchronization with Netcool/OMNIBus.
      - 3.8.1.2.1.1. Install by using wizard.
      - 3.8.1.2.1.2. Install from the command line.

- 3.8.1.2.1.3. Install from command line by using a silent installation.
- 3.8.1.2.1.4. Install and configure EIF Probe.
  - 3.8.1.2.1.4.1. If Situation Update Forwarder is used, verify data is synchronized correctly.
- 3.8.1.2.2. Configure the Netcool/OMNIbus server for program execution from scripts.
- 3.8.1.2.3. Update the Netcool/OMNIbus database schema.
- 3.8.2. Configure TEMS to forward events.
- 3.8.3. Open Manage Tivoli Enterprise Monitoring services.
- 3.8.4. Click the monitoring server and click Reconfigure.
- 3.8.5. On the configuration options window, select Tivoli® Event Integration Facility. Click OK and OK.
- 3.8.6. Complete the following fields on the Event Server: Location and Port Number window and click OK.

**3.9. Given a deployed and running ITM Infrastructure (TEP, TEPS, TEMS and/or secondary TEMS), configure agents so that they are correctly connected to a TEMS.**

**SUBTASK(S):**

- 3.9.1. Configure the agents.
- 3.9.2. Access the configuration interface (Command line or GUI).
- 3.9.3. Run the Agent Configuration command or click to start the Agents Configuration process.
- 3.9.4. Determine that the agent is correctly configured.
- 3.9.5. Start the agent.
- 3.9.6. Test that the agent is connected to the TEMS or secondary TEMS.

**3.10. Given a working ITM environment, installed and configured WPA and SPA and Application Support for selected agents, and a customer's historical data collection and reporting requirements, configure historical data collection so that required historical data can be collected, summarized and pruned correctly.**

**SUBTASK(S):**

- 3.10.1. Configure data collection.
  - 3.10.1.1. Start History Configuration tool from TEP.
  - 3.10.1.2. Create a new collection setting – Enter name, select Monitored Applications and Attribute Group.
  - 3.10.1.3. From the Basic tab, select Collection Interval, Collection Location and Warehouse Interval.
  - 3.10.1.4. From the Distribution tab, select the target system or managed systems group.

- 3.10.2. Configure data summarization and pruning.
  - 3.10.2.1. Start History Configuration tool from TEP.
  - 3.10.2.2. Select a monitored application, such as Windows OS -> select an Attribute Group.
  - 3.10.2.3. Select Summarization interval.
  - 3.10.2.4. Select Pruning interval.

**3.11. Given an installed ITM environment at required version level, the knowledge of the ITM tool, the target business requirement, take the required actions so that range partitioning for TDW can be completed.**

SUBTASK(S):

- 3.11.1. Configure range partitioning for the WPA.
  - 3.11.1.1. Connect and gain access to the WPA.
  - 3.11.1.2. Use the GUI or command line to configure the WPA.
  - 3.11.1.3. Select required options to configure range partitioning for the WPA.
  - 3.11.1.4. Set required parameters in the WPA environment file.
  - 3.11.1.5. Start the WPA.
- 3.11.2. Configure range partitioning for the SPA.
  - 3.11.2.1. Connect and gain access to the SPA.
  - 3.11.2.2. Use the GUI or command line to configure the SPA.
  - 3.11.2.3. Select required options to configure range partitioning for the SPA.
  - 3.11.2.4. Set required parameters in the SPA environment file.
  - 3.11.2.5. Start the SPA.

**3.12. Given a working ITM environment describe the functions of Agent Management Services (AMS) so that it can be used to monitor and manage agents.**

SUBTASK(S):

- 3.12.1. The OS agent for Windows, UNIX, or Linux includes a feature called AMS. The main feature of AMS is the “Watchdog”. AMS will watch any agent, if the agent terminates the agent will be restarted.
- 3.12.2. If an agent is being watched, it is said to have a status of “Managed”, if it is not being watched it has a status of “unmanaged”.
- 3.12.3. AMS components include:
  - 3.12.3.1. An “Agent Watchdog” running inside the OS agent :
    - 3.12.3.1.1. Runs inside the OS agent.
    - 3.12.3.1.2. Can monitor non-OS agents running on the same server, if they have terminated they will be restarted.
    - 3.12.3.1.3. AMS allows non-OS agents to be either managed or unmanaged.

- 3.12.3.1.4. AMS provides commands to turn on and off the management of an agent.
- 3.12.3.1.5. It will not restart agents that were manually stopped.
- 3.12.3.1.6. By default, non-OS agents are not managed.
- 3.12.3.2. An “Agent Management Services Watchdog” running as a separate process:
  - 3.12.3.2.1. Runs as a separate process.
  - 3.12.3.2.2. Monitors only the OS agent on the same server, if the OS agent terminates it is restarted.
  - 3.12.3.2.3. AMS provides commands to turn this off and on.
  - 3.12.3.2.4. It will not restart the OS agent if it is manually stopped.
  - 3.12.3.2.5. By default, the OS agent is managed.
- 3.12.3.3. Commands to control the Agent Management Services Watchdog. This Watchdog only watches the OS agent. These commands are system commands and executed on the server.
  - 3.12.3.3.1. Windows:
    - 3.12.3.3.1.1. <Install-Dir>\tmaitm6\disarmWatchDog.bat
    - 3.12.3.3.1.2. <Install-Dir>\tmaitm6\rearmWatchDog.bat
  - 3.12.3.3.2. Linux
    - 3.12.3.3.2.1. <InstallDir>/bin/itmcmd execute lz disarmWatchdog.sh
    - 3.12.3.3.2.2. <InstallDir>/bin/itmcmd execute lz rearmWatchdog.sh
  - 3.12.3.3.3. UNIX
    - 3.12.3.3.3.1. <InstallDir>/bin/itmcmd execute ux disarmWatchdog.sh
    - 3.12.3.3.3.2. <InstallDir>/bin/itmcmd execute ux rearmWatchdog.sh
- 3.12.3.4. Commands to control the Agent Watchdog. This is the watchdog running inside the OS agent and monitors non-OS agents. These commands are executed by using the ITM Take Action facility. They can be run with a TEP “Take Action”, by using the tacmd executeAction command, or as the action of a situation. Product provided take action commands will appear when the Application Support of the OS agent is installed. The Commands are:
  - 3.12.3.4.1. AMS Start Management - Start managing any agent.
  - 3.12.3.4.2. AMS Stop Management - Stop managing any agent.
  - 3.12.3.4.3. AMS Start Agent instance - Start a non-OS agent.
  - 3.12.3.4.4. AMS Stop Agent instance - Stop a non-OS agent.
  - 3.12.3.4.5. AMS Recycle Agent instance - Cycle a non-OS agent

- 3.12.3.4.6. AMS Reset Agent Daily Restart Count - Reset the daily restart count to zero.
- 3.12.3.4.7. Security Caution: Any TEP user whose user ID has access to the OS agent and his/her user ID has view access for the “Action” permission, will be able to execute these commands.
- 3.12.3.5. AMS has its own attribute groups, navigational items, workspaces, queries, and situations. These allow a TEP user to easily see the status of agents, their version, fix level, install directory, etc.
  - 3.12.3.5.1. AMS attribute groups included within the OS agent are:
    - 3.12.3.5.1.1. Agent Active Runtime Status
    - 3.12.3.5.1.2. Agent Availability Management Status
    - 3.12.3.5.1.3. Alerts Table
    - 3.12.3.5.1.4. Configuration Information
  - 3.12.3.5.2. Navigational items:
    - 3.12.3.5.2.1. Physical view for an OS agent now contains an AMS navigational item.
    - 3.12.3.5.2.2. Additional items can be customized.
  - 3.12.3.5.3. Workspaces. Within the Physical view, two workspaces are provided:
    - 3.12.3.5.3.1. Agents Management Log
    - 3.12.3.5.3.2. AMS
  - 3.12.3.5.4. Situations: One situation called AMS Alert Critical monitors the Alerts Table attribute group.
  - 3.12.3.5.5. Queries: One query is provided for each AMS attribute group.

## Section 4 - Administration

- 4.1. Given an installed and running IBM Tivoli Monitoring (ITM) environment, and the knowledge of the ITM products, verify the installed components are running appropriately so that their connection status to the Hub can be confirmed.**

**SUBTASK(S):**

- 4.1.1. Extract the list of installed components.
  - 4.1.1.1. Connect and gain access to the Hub.
  - 4.1.1.2. Run commands to extract the list of installed components known to the Hub.
  - 4.1.1.3. Run commands to verify that the components are running.
  - 4.1.1.4. Gain access to the Tivoli Enterprise Portal (TEP).
  - 4.1.1.5. Use the GUI (TEP) to verify that components are connected to the Hub (Offline Managed Systems).
- 4.1.2. Verify that installed components are connecting to the Hub.
  - 4.1.2.1. Gain access to the target component.
  - 4.1.2.2. Run commands to see that the component is running.
  - 4.1.2.3. Read log files to see that the component is connected to the Hub.

- 4.2. Given a running ITM V6.3 Infrastructure that is installed and configured correctly and ITM administrator User ID, use the TEP interface so that users are created with appropriate access rights and roles.**

**SUBTASK(S):**

- 4.2.1. Create user groups.
  - 4.2.1.1. Log on to the Tivoli Enterprise Portal Server (TEPS) with a valid administrator ID.
  - 4.2.1.2. Open the Administer User Accounts dialog.
  - 4.2.1.3. Create needed user groups.
- 4.2.2. Select a user group(s) and validate (verify and update) the following:
  - 4.2.2.1. Permissions – validate each permission setting.
  - 4.2.2.2. Applications – validate the applications accessible by the group.
  - 4.2.2.3. Navigator Views – validate the Navigator views assigned to the group.
- 4.2.3. Create users:
  - 4.2.3.1. Log on to the TEPS with a valid administrator ID.
  - 4.2.3.2. Open the Administer User Accounts dialog.
  - 4.2.3.3. Create needed users
  - 4.2.3.4. Assign a user to the appropriate user group.
  - 4.2.3.5. If a user requires permissions additional to group permissions, then assign:
    - 4.2.3.5.1. Permissions – validate each permission setting.

- 4.2.3.5.2. Applications – validate the applications accessible by the group.
    - 4.2.3.5.3. Navigator Views – validate the Navigator views assigned to the group.
  - 4.2.4. Validate users:
    - 4.2.4.1. Log on to the TEPS with a valid administrator ID.
    - 4.2.4.2. Open the Administer User Accounts dialog.
    - 4.2.4.3. Select a user and validate (verify and update) the following:
      - 4.2.4.3.1. Permissions – Validate each permission setting.
      - 4.2.4.3.2. Applications – Validate the applications accessible by the user.
      - 4.2.4.3.3. Navigator Views – Validate the Navigator views assigned to the user.
      - 4.2.4.3.4. Member of – Validate the groups to which the user is a member.
  - 4.2.5. Validate the TEPS LDAP authentication:
    - 4.2.5.1. Perform only if using LDAP for ITM user authentication.
      - 4.2.5.1.1. Verify that the TEPS LDAP server is running.
      - 4.2.5.1.2. Verify or Add the LDAP Repository.

**4.3. Given an installed, configured and running ITM environment, and knowledge of the IBM Tivoli Monitoring product, access the TEP so that data visibility for monitored items can be demonstrated and confirmed.**

**SUBTASK(S):**

- 4.3.1. Access the IBM Tivoli environment through TEP.
  - 4.3.1.1. Use one of the methods to connect to TEP ( browser, desktop or Web start).
  - 4.3.1.2. Access the ITM Workspaces with correct credentials.
- 4.3.2. Certify that data is visible from TEP.
  - 4.3.2.1. Select target Navigator items for the verification.
  - 4.3.2.2. Navigate between workspaces to confirm that real time data displays changes.
  - 4.3.2.3. Refresh workspaces to reload monitored data metrics.
  - 4.3.2.4. Request historical data, if configured, by expanding the time span and display changes.

**4.4. Given a working ITM environment, create custom views and workspaces so that data is displayed in a customized way.**

**SUBTASK(S):**

- 4.4.1. Describe ITM workspace.
  - 4.4.1.1. A workspace consists of different views. The two major view categories are Query based views and Event views.



- 4.4.1.2. Query based views include: Table, Pie chart, Bar chart, Plot chart, Circular gauge and Linear gauge.
- 4.4.1.3. The most popular event views include: Situation event console view, Message log view, Graphic view, Tivoli Event Console view and Common event console view.
- 4.4.2. Create or select a blank workspace.
  - 4.4.2.1. Select a monitoring resource from the Navigator.
  - 4.4.2.2. Select an existing blank workspace or create a new blank workspace by splitting an existing workspace.
- 4.4.3. Create objects in the workspace.
  - 4.4.3.1. Select a graphic type.
  - 4.4.3.2. Assign a query.
    - 4.4.3.2.1. Click assign a query button.
    - 4.4.3.2.2. In Query Editor, select a default query.
    - 4.4.3.2.3. Select the display columns.
    - 4.4.3.2.4. Note: The larger the number of queries and/or the higher the number of managed systems for which data is retrieved from the higher the cost to the ITM infrastructure.
- 4.4.4. Edit a workspace.
  - 4.4.4.1. Select the workspace to be edited -> Click the edit icon (pencil icon).
  - 4.4.4.2. In the Query tab: Assign a query.
  - 4.4.4.3. In the Filters tab: Select the columns to be displayed in the workspace.
  - 4.4.4.4. Note: Do not grab data or refresh your screen more than necessary.
  - 4.4.4.5. Click Ok.

**4.5. Given a working ITM environment and the authority to create situations, examine the product provided situations and create a custom situation so that customer requirements can be met.**

**SUBTASK(S):**

- 4.5.1. Log in to the TEP with authority to Edit, Modify, and Start/Stop situations.
- 4.5.2. Open the Situation Editor.
- 4.5.3. Examine product-provided situations and determine what custom situations should be created.
- 4.5.4. Create custom situations:
  - 4.5.4.1. Right-click Windows OS in the left panel. Select "Create new Situation".
  - 4.5.4.2. Fill out the dialog window with: Name = CustomerName\_Windows\_Restart\_Service & Description= This Situation will alert for any service that is not running and has a start type of Automatic
    - 4.5.4.2.1. Monitored Application = Windows OS

- 4.5.4.2.2. Type – Standard Situation
- 4.5.4.2.3. Click OK.
- 4.5.4.3. The “Select Condition” dialog box appears next.
  - 4.5.4.3.1. First select the attribute group. Note: You are required to know which attribute group in which your situations attributes reside. This can often be guessed from the attribute group names.
  - 4.5.4.3.2. Select Attribute Group “Services”.
  - 4.5.4.3.3. In the same window, select the needed attributes then click on OK: Multiple attributes can be selected by using the Ctrl or shift keys.
    - 4.5.4.3.3.1. Current State
    - 4.5.4.3.3.2. Start Type
- 4.5.4.4. Now back on the Situation’s main page, stay on the Formula tab.
  - 4.5.4.4.1. Enter Conditions
    - 4.5.4.4.1.1. In current status column, change operator to Not Equal and type in Running for the value to be compared.
    - 4.5.4.4.1.2. In the Start Type column, leave operator as Equal. For this attribute, typing a value is not required, use the drop-down and select Automatic.
    - 4.5.4.4.1.3. Select a sample interval, use 5 minutes.
    - 4.5.4.4.1.4. Leave the Run at Startup checked.
  - 4.5.4.4.2. Go to Distribution tab:
    - 4.5.4.4.2.1. Decide which Windows managed systems which run this situation. Select a managed system, in the Available managed systems frame and then click on the appropriate arrow to put it in the Assigned frame.
- 4.5.4.5. Click Ok.
- 4.5.4.6. In the navigator, right click the managed node you want to associate with the situation, then selection “Situations”.
- 4.5.4.7. Select the “Situation Filter” button, then check “Eligible for Association”.
- 4.5.4.8. Right click on the situation that was just created and Select “Associate”.
- 4.5.4.9. Click Ok.

#### **4.6. Given a working ITM environment, periodically verify ITM disk space so that normal operation and file growth are accommodated**

##### **SUBTASK(S):**

- 4.6.1. Identify the ITM System OS
- 4.6.2. If Windows:
  - 4.6.2.1. Access the server where ITM is installed.

- 4.6.2.2. On the task manager, click Start then "Computer".
- 4.6.2.3. Observe the disk space utilization for the drive where \$ITMHOME is located.
- 4.6.2.4. Verify if space remaining is less than 1GB.
- 4.6.3. If Linux/Unix:
  - 4.6.3.1. Access the server where ITM is installed.
  - 4.6.3.2. From the command prompt, execute df -h.
  - 4.6.3.3. Observe the disk space utilization for the directory where \$ITMHOME is located.
  - 4.6.3.4. Verify if space remaining is less than 1GB.

**4.7. Given a working ITM failover configuration, perform required actions so that correct functionality of the failover can be verified.**

**SUBTASK(S):**

- 4.7.1. Determine method of Failover utilized.
  - 4.7.1.1. If TEMS Hot Standby is used
    - 4.7.1.1.1. Stop Acting Primary Hub TEMS.
    - 4.7.1.1.2. This will cause failover of agents to Standby Hub.
    - 4.7.1.1.3. Reconfigure the TEPS and point to Now Acting TEMS.
    - 4.7.1.1.4. Restart TEPS.
    - 4.7.1.1.5. Open up TEP Client and login to TEPS.
    - 4.7.1.1.6. Verify that all agents have connected to the 'new' TEMS.
  - 4.7.1.2. If a proprietary solution (Windows clustering, System Automation for Multi-platform, etc) is used.
    - 4.7.1.2.1. Take desired resource offline (This resource can be a TEMS, TEPS, TDW, WPA, S&P or TEMA).
    - 4.7.1.2.2. This will cause automatic failover of the product to backup resource.
    - 4.7.1.2.3. Log in to the TEP and ensure no ITM functionality has been lost.

**4.8. Given access to an implemented ITM system, back up the TEPS database so that a restore of the TEPS database can be successfully performed, if required.**

**SUBTASK(S):**

- 4.8.1. Access the system where the TEPS is deployed.
- 4.8.2. If Host OS is Linux/Unix:
  - 4.8.2.1. Open a terminal.
  - 4.8.2.2. Navigate to \$ITMHOME/bin .
  - 4.8.2.3. Execute ./itmcmd execute cq "runscript.sh migrate-export.sh".
  - 4.8.2.4. The output, an export of the entire TEPS database, will be found in \$ITMHOME/<platform>/cq/sqllib/saveexport.sql.
- 4.8.3. If Host OS is Windows:

- 4.8.3.1. Open a command prompt.
  - 4.8.3.2. Navigate to \$ITMHOME\CNPS.
  - 4.8.3.3. Enter migrate-export.
- The output, an export of the entire TEPS database, will be found in \$ITMHOME\CNPS\sql\lib\saveexport.sql.

**4.9. Given a working ITM environment, back up the Hub TEMS objects so that after restoration, the Hub TEMS is fully operational at the state in which the backup was taken.**

**SUBTASK(S):**

- 4.9.1. Identify the ITM System OS.
- 4.9.2. If Windows:
  - 4.9.2.1. Access the server where ITM is installed.
  - 4.9.2.2. Launch the Manage Tivoli Enterprise Monitoring Services (MTEMS) (KinConfig.exe).
  - 4.9.2.3. Stop all running ITM componets.
  - 4.9.2.4. Record any configuration settings, if required.
  - 4.9.2.5. Right click each ITM component, then select "Advanced" and "Unconfigure".
  - 4.9.2.6. Copy directories in \$ITMHOME to backup location.
  - 4.9.2.7. On the Windows Taskbar, click Start then Run.
  - 4.9.2.8. Type regedit and hit enter.
  - 4.9.2.9. Select the MyComputer node at the top of the registry.
  - 4.9.2.10. Select File, then Export.
  - 4.9.2.11. Name the backup registry file and save it to the same backup location from 4.10.2.6.
- 4.9.3. If Linux/Unix:
  - 4.9.3.1. Access the server where ITM is installed.
  - 4.9.3.2. Stop all running ITM componets.
  - 4.9.3.3. Use the tar command to compress \$ITMHOME.
  - 4.9.3.4. Run a command to add the following files to the tar file from.
    - 4.10.3.4 To include additional files, execute the appropriate command depending on host OS.
    - 4.9.3.4.1. AIX: /etc/rc.itm\* tar -uvf /tmp/CANDLE\_HOME.backup.tar /etc/rc.itm\*
    - 4.9.3.4.2. HP-UX: /sbin/init.d/ITMAgents\* tar -uvf /tmp/ITMinstall\_dir.backup.tar /etc/init.d/ITMAgents\*
    - 4.9.3.4.3. Unix/Linux: /etc/initd/ITMAgents\* tar -uvf /tmp/CANDLE\_HOME.backup.tar /etc/init.d/ITMAgents\*
  - 4.9.3.5. Copy resulting tar file to backup location

## Section 5 - Performance Tuning and Problem Determination

### 5.1. Given access to IBM Tivoli Monitoring (ITM), review the installation logs so that errors or failures can be identified.

#### SUBTASK(S):

- 5.1.1 Access the system where the ITM is deployed.
- 5.1.2 If Host OS is Linux/Unix:
  - 5.1.2.1. Navigate to \$ITMHOME/logs/.
  - 5.1.2.2. Review contents of candle\_installation.log.
  - 5.1.2.3. Review contents of itm\_install.log.
  - 5.1.2.4. Observe any errors contained in the logs to begin troubleshooting process.
- 5.1.3 If Host OS is Windows:
  - 5.1.3.1. Navigate to \$ITMHOME\InstallITM\.
  - 5.1.3.2. Review contents of productname\_timestamp.log.
  - 5.1.3.3. Observe any errors contained in the logs to begin troubleshooting process.

### 5.2. Given access to a correctly implemented ITM, set the Java Heap Size so that the Tivoli Enterprise Portal Server (TEPS) can handle multiple concurrent logins.

#### SUBTASK(S):

- 5.2.1 Access the system where the TEPS is deployed.
- 5.2.2 Shut down the TEPS.
- 5.2.3 If Host OS is Linux/Unix:
  - 5.2.3.1. Navigate to \$ITMHOME/<arch>/iw/bin.
  - 5.2.3.2. Access the wasadmin script via ./wsadmin.sh -conntype none -lang jython.
  - 5.2.3.3. Set the proper JVM variable via `jvm = AdminConfig.list("JavaVirtualMachine").split("\n")[0]`.
  - 5.2.3.4. Verify proper JVM set via `print jvm`.
  - 5.2.3.5. Increase the initial Heap Size via `AdminConfig.modify(jvm, [{"initialHeapSize", 512}])`.
  - 5.2.3.6. Increase the maximum Heap Size via `AdminConfig.modify(jvm, [{"maximumHeapSize", 1024}])`.
  - 5.2.3.7. Save the new values with `AdminConfig.save()`.
  - 5.2.3.8. Exit with `exit`.
- 5.2.4 If Host OS is Windows:
  - 5.2.4.1. Navigate to \$ITMHOME\CNPSJ\bin.
  - 5.2.4.2. Access the wasadmin script via `wsadmin.bat -conntype none -lang jython`.
  - 5.2.4.3. Set the proper JVM variable via `jvm = AdminConfig.list("JavaVirtualMachine").split("\n")[0]`.
  - 5.2.4.4. Verify proper JVM set via `print jvm`.

- 5.2.4.5. Increase the initial Heap Size via AdminConfig.modify(jvm, ["initialHeapSize", 512]) .
- 5.2.4.6. Increase the maximum Heap Size via AdminConfig.modify(jvm, ["maximumHeapSize", 1024]) .
- 5.2.4.7. Save the new values with AdminConfig.save().
- 5.2.4.8. Exit with exit.
- 5.2.5 Restart the TEPS .

### **5.3. Given access to the application and system log, review and analyze the logs so that any issues or error are identified.**

#### **SUBTASK(S):**

- 5.3.1 Examine first failure data capture log directory.
- 5.3.2 Review Tivoli Enterprise Portal (TEP) client logs for errors
  - 5.3.2.1. Tivoli Enterprise Server
    - 5.3.2.1.1. For UNIX/Linux, logs are in \$CANDLEHOME/logs/\*cq\* .
    - 5.3.2.1.2. For Windows , logs are in %CANDLEHOME%\logs\\*cq\*
  - 5.3.2.2. TEP Java Web Start:
    - 5.3.2.2.1. For a TEP Java Web Start - the trace has the form javawsNNNNN.trace and is in the following directory C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log .
  - 5.3.2.3. TEP browser client :
    - 5.3.2.3.1. For a TEP Browser client - the trace has the form plugin150.trace and is in the same directory C:\Documents and Settings\Administrator\Application Data\IBM\Java\Deployment\log.
  - 5.3.2.4. TEP desktop client:
    - 5.3.2.4.1. For a TEP desktop client - the traces are in <install\_dir>\CNP\logs\kcjerror.log and <install\_dir>\CNP\logs\kcjras1.log .
- 5.3.3 Review Tivoli Enterprise Management Server (TEMS) logs for errors
  - 5.3.3.1. TEMS Operation Log:
    - 5.3.3.1.1. UNIX Installation \$CANDLEHOME/logs
      - 5.3.3.1.1.1. File name should look like <hostname>\_ms\_<epoch>.log.
    - 5.3.3.1.2. Windows Installation % CANDLEHOME%\logs
      - 5.3.3.1.2.1. File name should look like kdsmain.msg
  - 5.3.3.2. TEMS Diagnostic log:
    - 5.3.3.2.1. UNIX Installation \$CANDLEHOME/logs
      - 5.3.3.2.1.1. File name should look like <hostname>\_ms\_<epoch\_hex>-NN.log.
    - 5.3.3.2.2. Windows Installation % CANDLEHOME%\logs
      - 5.3.3.2.2.1. File name should look like <hostname>\_ms\_<epoch\_hex>-NN.log.

- 5.3.4 Review agent logs for errors.
  - 5.3.4.1. ITM agent operation log:
    - 5.3.4.1.1. UNIX Installation \$CANDLEHOME/logs
      - 5.3.4.1.1.1. File name should look like  
<agent\_name>.LG0.
    - 5.3.4.1.2. Windows Installation % CANDLEHOME%\logs
      - 5.3.4.1.2.1. File name should look like  
<agent\_name>.LG0.
  - 5.3.4.2. ITM agent TEMS diagnostic log:
    - 5.3.4.2.1. UNIX Installation \$CANDLEHOME/logs
      - 5.3.4.2.1.1. File name should look like  
<hostname>\_<product\_code>\_<process\_name>\_<epoch\_hex>-NN.log.
    - 5.3.4.2.2. Windows Installation % CANDLEHOME%\logs
      - 5.3.4.2.2.1. File name should look like  
<<hostname>\_<product\_code>\_<process\_name>\_<epoch\_hex>-NN.log.

#### **5.4. Given access to the server, enable user and component auditing so that all changes are tracked**

##### **SUBTASK(S):**

- 5.4.1 Review ITM administration document and audit requirements and parameters.
  - 5.4.1.1. Determine requirement for level of logging.
  - 5.4.1.2. Determine requirement for Maximum number of log files.
  - 5.4.1.3. Determine requirement for log file of size.
- 5.4.2 Modify the appropriate Audit environment variables.
- 5.4.3 Review audit log output to ensure information is populated.


#### **5.5. Given access to the TEP with permission to modify situations, ensure that monitoring situations are running at an appropriate frequency so that the correct sampling frequency is entered per the customer requirements.**

##### **SUBTASK(S):**

- 5.5.1 Log in to TEP as a user with permission to modify situation.
- 5.5.2 Click the situation editor icon at the top of the page.
- 5.5.3 Navigate to the situation group.
  - 5.5.3.1. Select the situation in question and ensure the Sampling interval is set appropriately per the customer requirements.
- 5.5.4 Ensure the option to apply the changes is selected.
- 5.5.5 Stop and start the situation to ensure the changes are picked up immediately.

**5.6. Given the customer requirements and TEP access, review the self-monitoring topology so that the agents are distributed appropriately across the monitoring infrastructure.**

**SUBTASK(S):**

- 5.6.1 Log in to TEP accessing the self-monitoring topology workspace.
  - 5.6.1.1. Click the  Enterprise Navigator item to open its default workspace.
  - 5.6.1.2. Either right-click the Enterprise Navigator item or open the View menu, then select workspace - Self-Monitoring Topology.
- 5.6.2 Review the Managed Systems per TEMS chart displaying the number of managed systems reporting to each monitoring server and ensure the agents are spread appropriately across the monitoring infrastructure.

**5.7. Given the number of concurrent users on an HTTP, Apache, or IIS Web server, tune the Web server so that concurrent users connectivity is optimized.**

**SUBTASK(S):**

- 5.7.1 Configure IBM HTTP Server or Apache HTTP Server with the default settings. See the product documentation ([www-306.ibm.com/software/webserver/httpserver/library](http://www-306.ibm.com/software/webserver/httpserver/library)) for additional information.
  - 5.7.1.1. Open the httpd.conf file in a text editor.
    - 5.7.1.1.1. For the Apache server, the file is typically located in the /etc/httpd/conf/ directory.
  - 5.7.1.2. Find the line that begins with DocumentRoot.
    - 5.7.1.2.1. For Linux and UNIX computers:
      - 5.7.1.2.1.1. Change the value between the double quotation marks (""") to itm\_installdir/os\_dir/cw, where itm\_installdir is the directory where IBM Tivoli Monitoring is installed and os\_dir is the operating system type (li6263 for SLES9 for Intel systems, li3263 SLES9).
    - 5.7.1.2.2. Windows computers:
      - 5.7.1.2.2.1. Change the value between the double quotation marks (") to itm\_installdir/CNB where itm\_installdir is the directory where IBM Tivoli Monitoring is installed. Use forward slashes for the path. For example: DocumentRoot "C:/IBM/ITM/CNB".
  - 5.7.1.3. Find the line that begins with <Directory docRoot>. Change the path to the value used for DocumentRoot.
  - 5.7.1.4. Save and close the file.



- 5.7.1.5. Open the mime.types file in a text editor and make the following changes.
  - 5.7.1.5.1. If the following lines are not in the file, add them:  
application/java-archive jar, image/icon ico
  - 5.7.1.5.2. If you will be using Java Web Start and the following lines are not in the file, add them: application/x-java-jnlp-file jnlp, image/x-icon ico
- 5.7.1.6. Modify the line that begins with application/octet-stream to include  
ior ser at the end.
- 5.7.1.7. Save and close the file.
- 5.7.1.8. Stop the IBM HTTP Server or Apache HTTP Server services, then  
start it again to enable the configuration changes.
- 5.7.2 Alternative option for Windows would be to configure Internet Information  
Server.
  - 5.7.2.1. Start IIS Manager.
  - 5.7.2.2. Right-click Web Sites and click New->Web Site.
  - 5.7.2.3. Click Next.
  - 5.7.2.4. Type the name of a Web site (for example "Tivoli") and click Next.  
Chapter 12. Additional Tivoli Enterprise Portal configuration 273
  - 5.7.2.5. Type the IP address for the Tivoli Enterprise Portal Server  
computer (this should be the same computer where IIS 6.0 is  
running) and click Next.
  - 5.7.2.6. Type the path to the IBM Tivoli Monitoring home directory that is  
the root of the Web Contentsubdirectories. The default path is  
C:\IBM\ITM\CNB. Click Next.
  - 5.7.2.7. Select Read, Run scripts, and Execute. Click Next.
  - 5.7.2.8. Click Finish.
  - 5.7.2.9. Right-click the new Web site and click Properties.
  - 5.7.2.10. Click the Documents tab.
  - 5.7.2.11. In the Add Content Page field, type index.html. This is the main  
page for the Tivoli Enterprise Portal.
  - 5.7.2.12. Click the Move Up button to move index.html to the top of the list.
  - 5.7.2.13. Click the HTTP Headers tab.
  - 5.7.2.14. Click MIME Types.
  - 5.7.2.15. Click New next to MIME Types.
  - 5.7.2.16. Type \*.asp in the Extension field.
  - 5.7.2.17. Type application/x-asp in the MIME Type field.
  - 5.7.2.18. Click OK.
  - 5.7.2.19. Repeat Steps 15 to 18 for each of the following:
    - 5.7.2.19.1. .class application/java-class
    - 5.7.2.19.2. .ior application/octet-stream
    - 5.7.2.19.3. .jar application/java-archive
    - 5.7.2.19.4. .jks application/octet-stream
    - 5.7.2.19.5. .jnlp application/x-java-jnlp-file
    - 5.7.2.19.6. .js application/x-javascript
    - 5.7.2.19.7. .lser application/octet-stream

- 5.7.2.19.8. .pl application/x-perl
- 5.7.2.19.9. .ser application/java-serialized-object
- 5.7.2.19.10..txt text/plain
- 5.7.2.19.11..zip application/zip
- 5.7.2.20. Click OK.
- 5.7.2.21. Click Apply.
- 5.7.2.22. Click OK.

**5.8. Given access to the server, configure logging so that logging levels and parameters are set appropriately for the production environment**

**SUBTASK(S):**

- 5.8.1 Review ITM administration document and audit requirements and parameters
  - 5.8.1.1. Verify level of logging is set to Disable or BASIC.
  - 5.8.1.2. Determine requirement for maximum number of log files.
  - 5.8.1.3. Determine requirement for log file of size.
  - 5.8.1.4. Recycle the component to have your changes take effect.
- 5.8.2 Review audit log output to ensure information is populated.
  - 5.8.2.1. Access component server.
  - 5.8.2.2. Open audit logs directory under the <install\_dir> directory.
  - 5.8.2.3. View log file each process has its own log file formatted in XML.
    - 5.8.2.3.1. For single-instance:  
<UserID>.<hostname>\_<pc>\_audit.log
    - 5.8.2.3.2. For multi-instance:  
<UserID>.<hostname>\_<pc>\_<instance>\_audit.log

## Next Steps

1. Take the [IBM Tivoli Monitoring V6.3 Implementation](#) assessment test using the promotion code *csistudy* for \$10 (\$20 USD savings).
2. If you pass the assessment exam, visit [pearsonvue.com/ibm](https://pearsonvue.com/ibm) to schedule your testing sessions. Use the promotion code *tivguide* to receive 20% off.
3. If you failed the assessment exam, review how you did by section. Focus attention on the sections where you need improvement. Keep in mind that you can take the assessment exam as many times as you would like (\$10 per exam), however, you will still receive the same questions only in a different order.