Bhagyashree Shirvadkar

CLOUD MANAGEMENT (UNIT-4)

Q.85 What client management functionality is provided by configuration manager 2012 for managing end-user devices?

Ans:

Refer Pg. No 134

Q.89 What are the new system site roles in configuration manager? What are the enhancements to site system roles?

Ans:

- Configuration Manager 2012 includes a number of Site System role changes that simplify and improve operations.

➢ **New Site System roles include the following:**

1.Application Catalog Website Point and Web Services Point

- The Application Catalog Website Point is a new role that provides users with a list of available software.
- The Application Catalog Web Services Point provides software information to the Website Point from the new software library.

2. Enrollment Point

- The Enrollment Point uses certificates to complete the mobile device enrollment.

3. Endpoint Protection Point

- The Endpoint Protection Point implements the antimalware features of SCCM 2012, using the System Center 2012 Endpoint Protection.

➢ **Enhancements to Site System roles include the following:**

1. Management Points include automatic load balancing

- Management Points now include automatic load balancing within the primary site and dont use Network Load Balancing (NLB). This simplifies installation and allows for greater scalability.

2. Multiple Internet-based Management Point

- Sites can now be configured with multiple Internet—based Management Points. This allows clients to locate their closest Internet-based Management Point when on the Internet, allowing for greater fault tolerance and scalability.

3. Management Points include server locator functionality

- Including this functionality in the Management Points simplifies installation and administrative complexity, and now all Management Points include those capabilities.

4. Distribution Points include PXE functionality

- Distribution Points now incorporate the PXE Point functionality, which simplifies installation and administrative complexity.

5. Distribution Points supported on servers and workstations

- Installation of Distribution Points is now supported on both servers and workstations, eliminating the need for the Branch Distribution Point.

Q.92 Explain the configuration manager 2012 hierarchy.

Ans:

- The Site Server is the core component in the Configuration Manager hierarchy.
- The Site Server role manages the other roles that facilitate the different areas of client systems management, such as content provisioning and asset management.
- Site Servers can be configured in a hierarchical model.
- This parent/child relationship can be grown both horizontally and vertically for a high degree of scalahility.
- Each site in the hierarchy must be configured with a three-character site code.
- Site codes must be unique and shouldn’t be reused to avoid potential replication issues.
- Valid site codes contain letters and numbers.
- In a multisite hierarchy, Configuration Manager can be managed from any primary site.

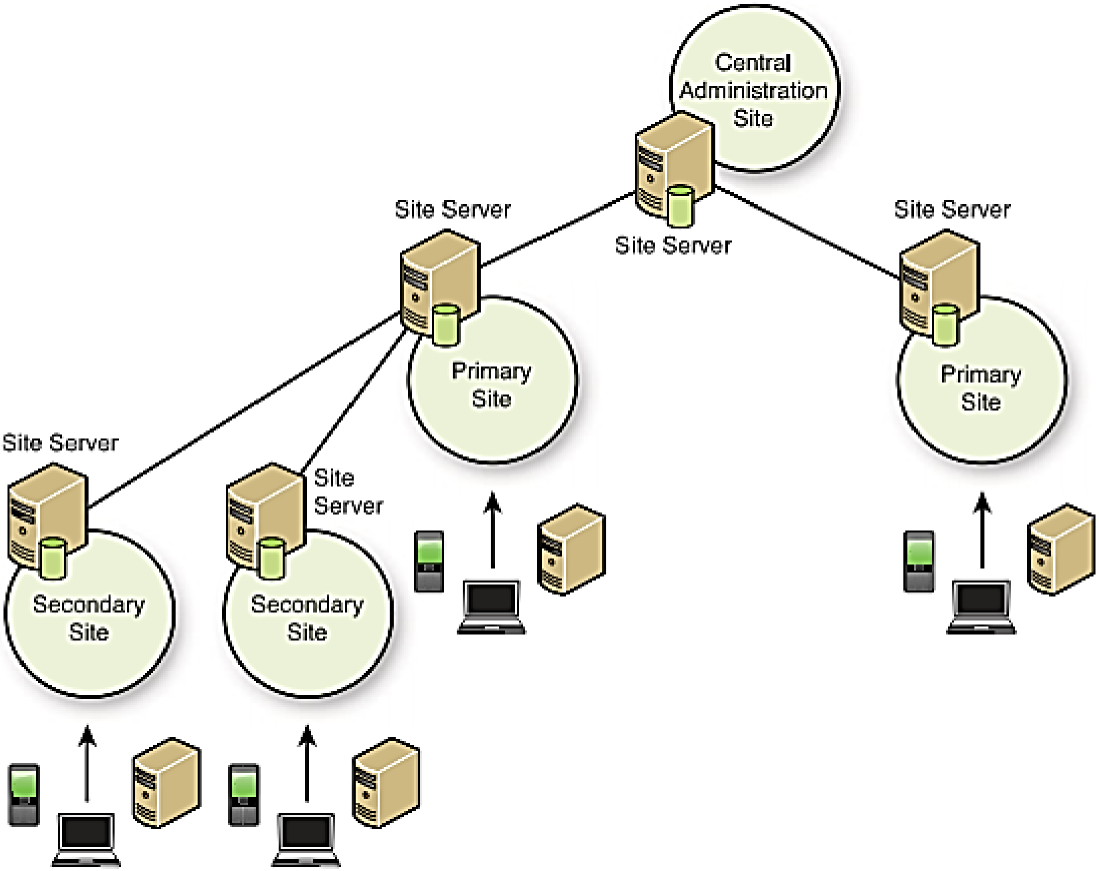

Figure: Configuration manager 2012 hierarchy

- The Configuration Manager hierarchy is typically managed from the central site as this provides access to the entire infrastructure and all managed systems. Opening a Configuration Manager Administration Console on a lower-level
- Site Servers in a parent/child relationship communicate with each other through Site Senders and Addresses, as well as database replication.
- The Site Sender controls how many processing threads can be active at any given time and how often to retry the delivery if a problem occurs.
- Site Addresses can be used to control the bandwidth utilization between sites.
- Addresses provide both a schedule and data rate limits to throttle communication between Site Servers.

Q.93 What is content distribution? Explain packages, applications, software update distribution and operating system deployment

Ans:

- Configuration Manager provides a highly scalable content distribution, execution, and reporting system.
- Several of Configuration Manager's key roles have been designed specifically to facilitate the provisioning of software, software updates, and operating systems.

➢ **Packages**

- The following distribution terminology are as follows:

1. Package

- The package consists of the software name, version number, and manufacturer.
- The package installation files defined source location and distribution settings within the package.
- Each package container holds the Access Account Distribution Points, and Programs subcontainers.

2. Program

- The program is a component of the package and defines how the content is executed on the target.
- A package can contain several programs, each with a unique configuration.

3. Deployment

- The deployment, formerly known as an advertisement, makes a package/program combination available on target systems.
- The deployment controls when and where the content is executed.

➢ **Applications**

- Applications in Configuration Manager 2012 are fundamentally usercentric, allowing users to he associated with devices and then targeting applications at users.
- The application terminology is similar to the package terminology:

1. Application

- The application consists of the software name, version number, and manufacturer.
- The application distribution settings are defined within the package, including additional information, such as references and superedence.

2. Deployment type

- The deployment type is a component of the applications and defines how the content is executed on the target.
- This includes settings such as content location, download behaviour, the command line to run the install, maximum runtime, disk space requirements, and execution environment
- An application can contain several deployment types, each with a unique configuration.

3. Deployment

- The deployment, formerly known as an advertisement, makes a package/program combination available on target systems.
- The deployment controls when and where the content is executed.

➢ **Software update distribution**

- Software update distribution terminology are as follows:

1. All Software Update

- The All Software Updates container shows all the metadata synchronized from Microsoft Update through the Windows Server Update Services(WSUS) component integration**.**

2. Software Update Groups

- A software update group, formerly update list.
- Individual updates are added from the All Software Updates container to the update list or automatically via an automatic deployment rule.
- If updates are added to an update group, these new updates are automatically deployed.

3. Automatic Deployment Rules

- An automatic deployment rule, formerly deployment template, is settings for deploying updates to a collection.
- The automatic deployment rule contains information such as the name of the collection, if updates should restart the target system, custom notification options, update deadlines etc.

Q.94 What is asset management? Explain asset intelligence, software metering and compliance management.

Ans:

- Asset management features help manage the environment by collecting granular details about the hardware and software running in the environment.
- The asset management functionality includes things like hardware inventory, software inventory, software metering, software and license management through Asset Intelligence, and Desired Configuration Management.

- **Asset Intelligence**
  - The Asset Intelligence (AI) functionality in Configuration Manager is used to identify and report software licensing and licensing compliance information for both Microsoft and non-Microsoft software.
- **Software Metering**
  - The software metering functionality provided with Configuration Manager simply tracks software usage on managed systems.
  - The creation of software metering rules can assist in identifying how often software is used.
- **Compliance Management**
  - Compliance Management allows an administrator to create configuration baselines to validate the settings of managed systems.
  - The validation of customizable settings determines the overall compliance of the target system.
  - Compliance Management provides many options for monitoring the state of both objects and settings on managed systems.
  - Compliance Management can monitor several types of objects, including Registry keys, files, and managed code assemblies.

Q.95 Explain the reporting feature of configuration 2012.
Ans:

- Configuration Manager includes a variety of preconfigured reports to show information about managed systems and the Configuration Manager infrastructure.
- These reports are run in the powerful Reporting Services Point, based on SQL Server Reporting Services.
- Report subscriptions can he created to deliver reports via email or to a file share On a regular basis, reducing the administrative effort needed to deliver reports.
- The reports can be found in the Monitoring space under the Reporting folder.
- Reports are important as they provide insight into the different functionality of Configuration Manager, including the health of the infrastructure and managed systems.
- For example, reports show client installation problems, the status of software distribution, the compliance of software updates, and many other things.

Q.96 Explain the architecture of configuration manager 2012 in detail.
Ans:

- Configuration Manager is composed of several basic roles: the Site Database, Site Server, SMS Provider, Management Point, Distribution Point, Clients, and Administration Console.

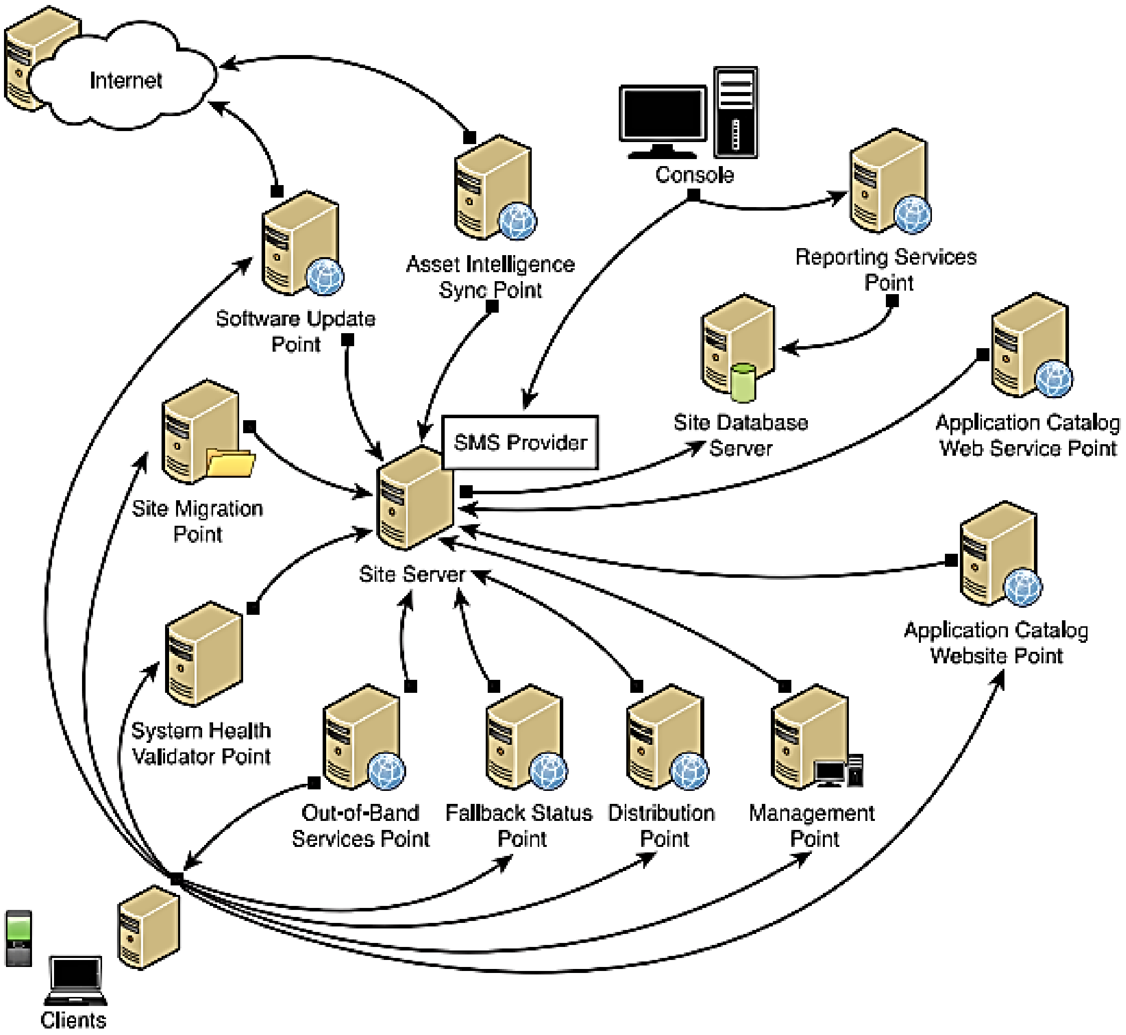

Figure: The Configuration Manager 2012 architecture

- The following list describes the different Configuration Manager components:

1. Clients

- Clients are installed on each managed system to provide efficient management of the environment.

2. Central Administration Site Servers

- The Central Administration Site Server is an optional parent site to all primary sites in the hierarchy.
- This server has the ability to manage all clients throughout the hierarchy.

3. Primary Site Servers

- A primary site server provides core functionality for Configuration Manager.

- This server manages Site Component Servers, provides an interface to manage systems.

4. SMS Provider

- The SMS Provider is a WMI provider that facilitates accessing and manipulating the Configuration Manager Site Database.
- All communication from the Site Server and the Configuration Manager Administration Console goes through the SMS Provider.

5. Site Server Database

- Each site requires a separate database.
- This database holds configuration settings and management data, such as hardware inventory for managed systems.

6. Wake On LAN

- The Wake On LAN (WOL) functionality provides a method to wake up client systems for deployments.

7. Distribution point

- Distribution Points are important for effectively deploying content.
- Content includes software, updates, and images used for OS deployment.
- Distribution Points can be deployed on servers and on clients, with the exact same functionality.

8. Health Validator Point

- The health Validator Point must be installed on a Windows server with the Network Access Protection (NAP) component installed.
- The health Validator simply tells NAP what software updates are required before the client can pass validation and communicate with the network.

9. Reporting Services Point

- The Reporting Services Point (RSP) provides an extensible reporting infrastructure based on SQL Reporting Services.

10. Mobile Device Management

- The Mobile Device Management features in Configuration Manager allow the management of mobile assets with the Configuration Manager infrastructure.

11. Out-of-Band Service Point

- Out-of-band management refers to the management of a system while the system has been turned off, or is otherwise not responding, such as when an operating system error has occurred.

- To support out-of-band management, the Intel vPRO chipset along with asupported version of the Active Management Technology (AMT) is required.

12. State Migration Point

- The State Migration Point (SMP) provides a secure location to store the user state from a client system during the OS deployment process.

13. Management Point

- The Management Point role is one of the first roles to move off the Site Server to improve performance.
- The Management Point can support 25,000 clients on a single server and as many as 100000 clients total when additional Management Points are added.

14. Fallback status Point

- The Fallback Status Point (FSP) provides a safety net for clients.

15. Asset Intelligence Synchronization Point

- The Asset Intelligence Synchronization Point communicates with System Center Online Services to retrieve updates to the asset catalog.

16. Reporting Services Point

- The Reporting Services Point (RSP) provides an extensible reporting infrastructure based on SQL Reporting Services.
- This provides a powerful way to access data in the Site Database and includes the ability to schedule reports through subscriptions.

17. Software Update Point

- The Software Update Point (SUP) communicates with the WSUS 3.() components receive data from Microsoft Update about patches and updates available for clients.

Q.97 . **What is wake-on-lan? Explain asset intelligence synchronization point, distribution point, fallback status point, health validator point, management point, out of band service point, state migration point, reporting services point, software update point and mobile device management for configuration manager 2012.**

Ans: Refer Question No:96

Q.98 Explain the security and management console of configuration manager 2012.

Ans:

- Configuration Manager 2012 introduces true role-based administration, allowing users and groups to be assigned roles in SCCM.
- Components of the role-based administration include the following:

1. Security Roles

- These are groups of security permissions that can be assigned to users to allow them to perform their administrative tasks.
- The security permissions define tasks that an administrator can perform and rights to particular object types.

2. Collectionsl

- These specify the users and devices that an administrator can view or manage.
- These collections can he based on geographic parameters, organizational parameters, or functional parameters. This allows very flexible division and organization of the resources to which administrators have access.

3. Security Scopes

- These provide administrative users with access-specific securable object instances, such as specific applications, configuration items, sites, and other objects.

- The difference between security roles arid security scopes can sometimes be difficult to distinguish.
- The bottom line is that security roles assigned rights to object types, such as all applications.
- Security scopes, on the other hand, assigned rights to specific object instances.
- Role-based administration in SCCM 2012 simplifies providing the correct least privilege access to administrators of SCCM.

Q.99 What are the service accounts needed to support basic deployment in configuration manager 2012?

Ans:

- The Configuration Manager servers use the Local System account for the majority of network authentication, moving the security boundary out to the operating system.
- When the Local System account is used, unauthorized users should not be allowed on the server.
- The Local System account has several benefits because the password is managed automatically with Active Directory membership.

➢ The following service accounts are needed to support basic deployments:

1. **Domain Join**
   - This account is used during OS deployments to join the system to the domain.
   - This should be a limited user account with the right to add new computers to a specific OU in which this account has been delegated the correct permissions.
2. **Network Access**
   - This account is used by non-domain members to access content and infrastructure components.
   - This scenario is common during OS deployment and when managing demilitarized zone (DMZ) systems.
   - This account should be a limited user account.
3. **Client Push Installation**
   - This account is used by the Site Server to connect to a remote system, copy required client files, and initiate the installation under the Local Service account.
   - This account requires administrative rights on managed systems to install the client.
4. **OS Capture Account**
   - This account provides access to the OS capture share.
   - This is the network share where OS images are copied during the OS capture process.

  - The captured image can be imported into Configuration Manager for delivery to client systems.
  - This account should be a limited user with only permissions on the OS capture location.

Q.100 Discuss the configuration manager 2012 design considerations.
Ans:

- Design Consideration includes how Configuration Manager handles data, how to connect Configuration Manager sites, and how Configuration Manager behaves over the WAN.

1. Designing Collections

- Collections provide a way to organize resources within the Configuration Manager console.
- A system can be part of many different collections. For example, a computer can be part of a location-specific collection and one or more functional collections.
- Each collection updates membership based on a predefined schedule. By default this is every 24 hours, based on the time the collection was created.
- Collection also provide security boundary for administration.

2. Discovering and Deploying Clients

- Potential client systems can be discovered through scheduled tasks available within the Configuration Manager console.
- The Active Directory system discovery is primarily used to locate systems.
- The groups to which a computer system belongs can also be discovered with the Active Directory System Group Discovery method.
- Configuration Manager can be set to automatically install the client on target systems.
- This is done by copying a small amount of code to the **\computername\ Admin$\ ccmsetup** folder on the system and then creating a service called **ccmsetup**.
- This service attempts to download the full client through BITS, for a more bandwidth-friendly installation.

- This service also manages the installation; if the installation fails or the computer reboots while the installation is being done, the service repairs and reinstalls the client correctly.
- This service is automatically removed once the installation has completed successfully.

3. Provisioning Content to Users and Groups

- Additional discovery methods are available to locate users and user groups within Active Directory.
- The Active Directory user discovery allows searches and creates **Data Discovery Records (DDRs)** for users. within the discovery, the groups of which the user is a member can be identified and added to the user as a searchable attribute.
- In addition, the Active Directory Security Group discovery locates groups within the domain.
- This allows collections of groups to be created for user-targeted provisioning.

4. Considerations for a Multisite Configuration Manager Hierarchy

- In Configuration Manager 2012, the site hierarchy has been simplified to a stratified three-tier site architecture.
- In a multisite SCCM 2012 architecture, there is a **Central Administration Site** at the top of the hierarchy.
- It cannot have clients report to it and does not support the Management Point role or the Distribution Point role.
- The next level of the hierarchy consists of the **primary sites,** which support agents and all system roles.
- All primary site are child sites off of the Central Administration Site.
- The third level of the hierarchy is **secondary sites,** which support a limited number of roles.
- All secondary sites are child sites of primary sites.

5. Placement of PXE-Enabled Distribution Points and StateMigration Points

- An important aspect in the design is the placement of the PXE-enahlcd Distribution Points and State Migration Points.
- A PXE-enahled Distribution Point is similar to DHCP where it responds to specific broadcast requests.

- Like a Distribution Point, the client will locate a SMP on the local subnet before choosing a remote SMP.
- Although the SMP can be located anywhere, depending on how much data needs to be captured from the client system.

6. Establishing Boundaries

- Establishing site boundaries is one of the most important aspects of Configuration Manager.
- Boundaries let managed systems receive content and communicate status to the closest server in the Configuration Manager hierarchy.

Q.101 What are the different storage considerations to be taken into account while deploying configuration manager 2012.

Ans:

- The two main contenders are a storage area network (SAN) disk subsystem and a direct attached storage (DAS) disk subsystem.
- The SAN is typically a switched-based, fiber-channel fabric and a large array of disks, which is managed by a dedicated storage team.
- The SAN provides high reliability and high performance, but also high cost.
- The DAS is a RAID subsystem of disks that are directly attached to the servers.
- Depending on the RAID configuration, this can have high reliability and high performance, hut costs less than a SAN.
- In general, a SAN provides better performance than a DAS.
- This is especially true for large, block-level data transfers, which is what the SQL database will he doing.
- The SAN provides a faster data transfer due to the higher MBps.
- If using DAS, the design of the DAS is critical to ensuring the performance of the disk subsystem.
- Choose the RAID appropriately, as not all RAIDs are created equal in terms of performance.

Q.102 Discuss the implementation of configuration manager 2012 components in small, medium and large enterprises.

Ans:

- **Small and Medium Enterprise**
  - In a small-sized implementation of Configuration Manager, all major components can be hosted on the same server.
  - For best performance, consider separating the following components onto separate physical drives:
    - Operating system
    - Configuration Manager installation
    - Site Database
    - Distribution Point content
- **Large Enterprise**
  - In a large-sized implementation of Configuration Manager, the Site Database and the Site Server component can likely be hosted on the same server but can be moved to a separate SQL server to improve performance or to meet business requirements.
  - For best performance, consider separating the following components onto separate physical drives:
    - Operating system
    - Configuration Manager installation
    - Backup location
    - VSS temporary location
    - Site Database
    - Site Database transaction log
    - SQL Temp DB
    - Distribution Point content

Q.103 What are the pre requisites for implementing configuration manager 2012?

Ans:

- Before implementing SCCM 2012, several prerequisite steps need to be taken to prepare Active Directory and the Site Servers.
- The required SCCM prerequisites are as follows:

- **Extending the Active Directory schema**
  - The Active Directory schema should he extended to support dynamic client assignment during Configuration Manager agent deployment and to assist clients with the location of Configuration Manager server infrastructure.
  - When the Active Directory schema is extended, clients can use the values provided through Active Directory to locate regional Site Servers and Distribution Points for package and content delivery.
  - To extend the Active Directory schema, execute the following steps:

    1. Log on to a domain controller with an administrative account that is a member of
       the Schema Admins group.
    2. Copy the EXTADSCH.exe from SMSSETUP\BIN\x64\ on the Configuration Manager installation media to a local folder on the Active Directory domain controller with the schema master FSMO role.
    3. Open a command window as an administrator and execute the EXTADSCH.
       Exe command with a Schema Admin account.
  - The command should report, “Successfully extended the Active Directory schema” when complete
- **Configuring the System Management container in Active Directory**
  - The System Management container holds the Configuration Manager objects in Active Directory.
  - This container can be created with the ADSI Edit console on the DC1 domain controller.
  - To create the System Management container with ADSI Edit, complete the following steps:

    1. Run ADSI Edit from DCL
    2. Right-click the ADSI Edit node and select Connect To.
    3. Type Domain in the Name field.
    4. Select default Naming Context from the list of well-known naming contexts.
    5. Click OK.
    6. Expand Default Naming Context.
    7. Expand DC=companyxyz, DC=com.

8. Select the CN=System container.
9. Right-click CN=System, click New, and then click Object.
10. Select Container from the list and click Next.
11. Enter System Management (or the CN attribute value, and then click Next.
12. Click Finish to complete the change.

- **Adding Windows roles and features on Site Servers**
  - The majority of client communications is over HTTP or HTTPS, which is serviced by the Windows lIS web server.
  - IIS is a key component of many Configuration Manager Site Systems roles.
  - This includes the Site Server itself in the following optional roles:
    - Application Catalog Web Service Point
    - Application Catalog website Point
    - Distribution Point
    - Enrollment Point
    - Enrollment Proxy Point
    - Failback Status Point
    - Management Point
    - Software Update Point

Q.104 How does the client agent locate the content? Explain.

Ans:

- An agent locates content in the following way:

  1. The client queries Active Directory to identify the closest Management Point in the hierarchy. The client will choose the Management Point based on the network boundaries in which the client currently resides.

  2. If a Resident Management Point is unavailable, the client will default to the Management Point in the site the client was originally assigned. The client communicates with the selected Management Point to locate content. The Management point provides the list of Distribution Points that contain the appropriate content. Only applicable DPs are provided.

3. If the client is within the boundaries of a fast site, the Management Point only provides a list of preferred DPs for the fast site, even if a slow Distribution Point with the content is available.

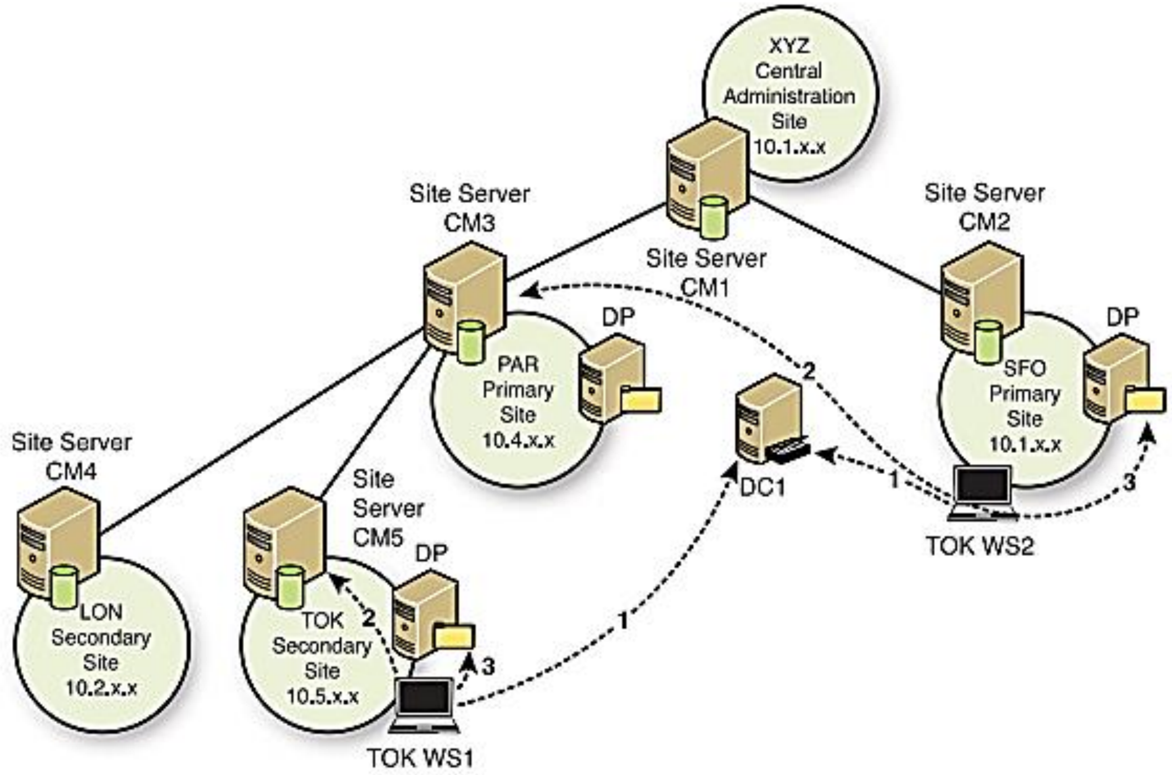

Figure: How Client Locate Content

- How a client locates content is shown in Figure. The figure shows two laptops from the Tokyo location (TOK), VS1 and WS2. The VS1 laptop is at the Tokyo location.
- The WS1 agent first checks with the domain controller to locate its Resident Management Point (step 1), contacts the Resident Management Point to locate its closest Distribution Point (step 2), and finally begins to download content from its local Distribution Point in TOK (step 3).
- The WS2 laptop is traveling and happens to he in the San Francisco location (SR).
  The WS2 agent first checks with the domain controller to locate its assigned Management Point (step 1), contacts the assigned Management Point in Paris (PAR) to locate its closest Distribution Point (step 2), and finally begins to download content from its local Distribution Point in SF0 (step 3).

Q.105 What is distribution point? How is it chosen?

Ans:

- **Distribution Point**
    - Distribution Points are important for effectively deploying content.
    - Content includes software, updates, and images used for OS deployment.
    - Distribution Points can be deployed on servers and on clients, with the exact same functionality.
    - The Distribution Point site role hosts content for clients in a specific location.
    - After the Management Point provides the list of available Distribution Points to the client, the client chooses the best-suited Distribution Point to receive content.
    - The order in which they are chosen is as follows:

  1. Distribution Points with the content that are located in a boundary group that contains a client’s boundary with fast connectivity.
  2. Distribution Points with the content that arc located in a boundary group that contains a client’s boundary with slow connectivity
  3. Distribution Points with the content that have the Allow Fullback option enabled.

Q.106 What are collection? Why are they used?

Ans:

- Collections are an important aspect of successfully delivering content.
- A collection defines a group of systems or users based on many different attributes.
- For example, all of the systems in a specific area can be part of a site-specific collection, or all the systems that share a common piece of software can be part of a software-specific collection.
- A system can be part of more than one collection.
- It is important to define collections based on our requirements.

- Collections can be created with static, manually added members. however, this type of management is not very scalable and should only be used when other means are not feasible.
- Designing collections based on queries is recommended for a much more scalable infrastructure.
- The query that defines a collection can be based on any hardware or software inventory data, along with information collected during the client discovery cycles.

➢ **Collections can he used for the following:**

- Targeting deployments
- Targeting client settings
- Targeting anti-malware settings
- Targeting firewall settings
- Power management settings
- Targeting content Distribution Points
- Reporting
- Administrative security scopes

Q.107 Explain the process of managing deployments .

Ans:

- The process of managing deployments includes targeting users and devices, configuring self-service and automatic deployments, and monitoring those deployments.

1. Targeting Users

- A key feature of Configuration Manager 2012 is the ability to target users.
- Previous versions had difficulty targeting the users or their associated systems, SO the targeting was mostly at systems independent of what user was assigned the system.

2. Deploying Software Self-Service

- When the Distribution Points have received the content, the software can be deployed to users as self-service applications.
- When software is deployed self-service, the user has the ability to execute the software when it’s convenient for him or her.
- To deploy the software, a deployment needs to be created.

3. Deploying Software Automatically

- Software can be installed automatically based on a required deadline.
- This is a convenient way to systematically update computers when the user is not using the system or during nonpeak hours.

4. Monitoring Software Deployment

- Monitoring the deployment of the software package is key to ensuring the environment is secure and maintained.
- Standardized software helps reduce the overhead of maintaining and managing the environment.
- From within the Configuration Manager console, an administrator can review the overall status of application deployment from the Deployments folder.
- The Deployments folder is located in the Monitoring space.

Q.108 How does configuration manager 2012 provide software update facility?

Ans:

Pg 232 (Refer Pg. No 187)

Q.109 What are the common operating systems deployment technologies?

Ans:

- The OS deployment functionality in Configuration Manager is highly modular. Each component is layered together to create a simple, effective system for distributing Windows operating systems.
- Common OS deployment technologies are as follows:

➢ **WinPE**

- The Windows Preinstallation Environment runs a small version Windows used to initiate the OS deployment.
- The WinPE environment is typically initiated over the network with the PXE-enabled Distribution Point.

➢ **Operating System Source**

- This is the location of the OS files.
- The OS media images are typically downloaded from Microsoft.
- The files are extracted and placed in the Operating System Source folder on the network.

➢ **Operating system installer**

  - This is the operating system package inside the Configuration Manager console that points to the Operating System Source folder on the network.
  - This allows operating systems to be created from scratch, as if booting to the original media.

- **Operating system image**
  - This is the capture of a prebuilt operating system into a Windows Imaging Format (WIM) file.
  - This allows an operating system to he built, applications to be installed, and configurations to be applied before capturing the image.
  - When the operating system is built starting from an operating system image, it saves a lot of time and ensures that the resulting systems are exactly the same.
- **Task sequence**
  - This set of tasks is used to execute the complete deployment.
  - This includes everything from configuring the hardware, installing the OS, and deploying the correct software packages.
  - Task sequences can also be used independent of operating system deployments to simply execute a series of steps, which is very useful for complex installations.
- **Drivers**
  - These are the drivers that have been uploaded to the Configuration Manager driver repository.
  - These drivers can be installed dynamically during the deployment process.
- **Driver packages**
  - Specific drivers are grouped together for easier management.
  - For example, all the drivers for a specific make and model of a server can he grouped together in a Driver package.

Q.110 How operating systems can be deployed using configuration manager 2012

Ans:

Pg 243

262