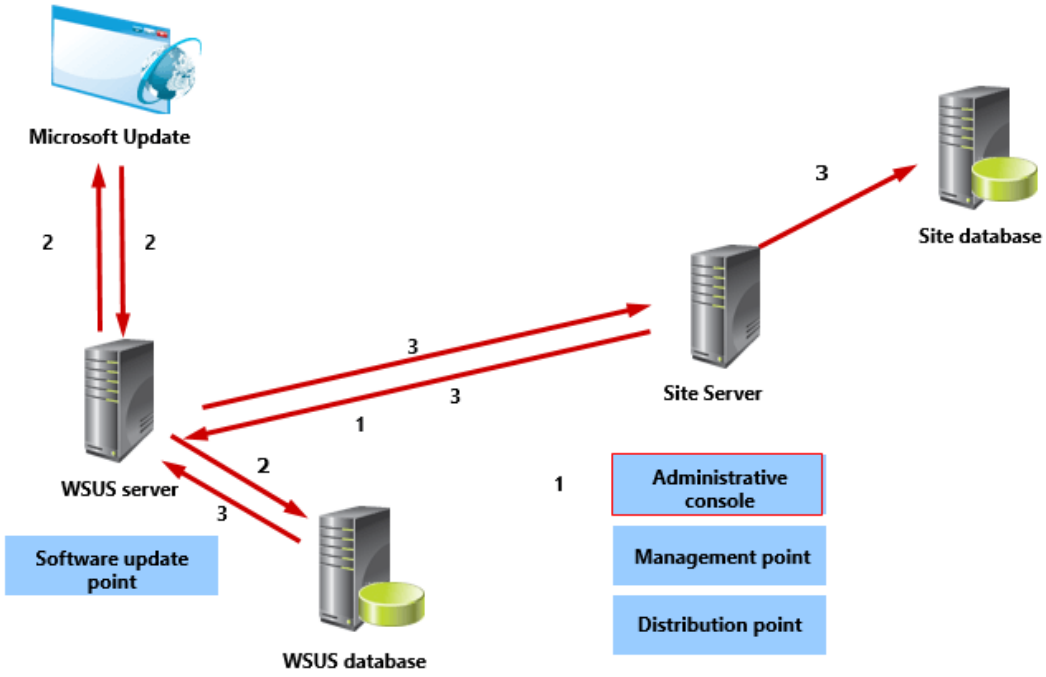
Synchronizing the Software Update Catalog Metadata

The software update process begins at the top-level site (central administration site or standalone primary site). You can configure synchronization settings, by defining products and classification. You can also schedule or manually initiate the synchronization process. Step by step process is defined below.



1. On schedule or on manual trigger, a component on site server called *WSUS Synchronization Manager* calls an application programming interface (API) which requests the WSUS server to initiate synchronization from Microsoft Update.
2. WSUS server connects Microsoft Update to download metadata and stores it in its database. On scheduled trigger it will do full download and in event of manual trigger, only delta download is done which is faster.
3. WSUS Synchronisation Manager keeps on polling WSUS and once it detects metadata download completion at WSUS server, it requests the software update metadata from the WSUS server and inserts it into the Configuration Manager site database.

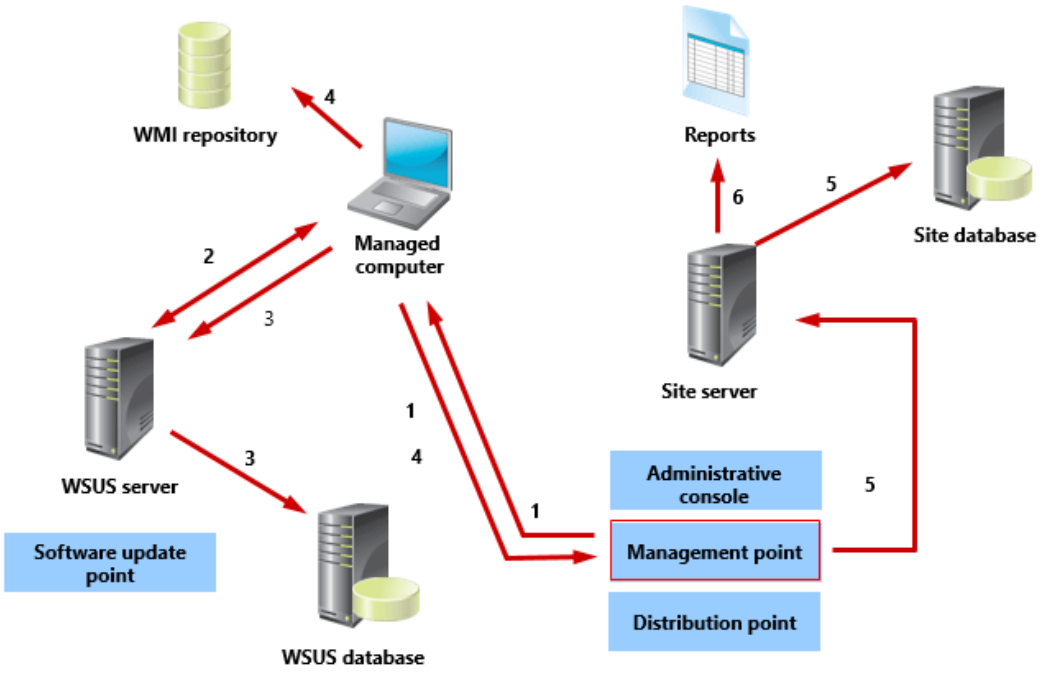
Once this process is completed you can check updates on site server.

Note: Only metadata is downloaded at this point, not the actual update data.

Compliance scan

Once metadata is synchronized at site server, clients will scan their compliance status and send it to site server. Lets discuss this process now.

Software Updates Agent (SUA) at client side is responsible for checking compliance and to deploy updates that are applicable for client. It gets enabled by default due to D*efault Client Policy*.When you install and synchronize a software update point in a site, Configuration
Manager creates a site-wide machine policy that informs client computers that software update metadata is available. The client computers then initiate a scan for compliance with software updates. Step by step process is mentioned below.



1. On schedule or when you initiate the scan manually, the client receives machine policy from the Management point. Software updates agent submits a request to the management point to find the WSUS server. After the management point provides the WSUS server location, the agent enables the **Specify intranet Microsoft update service location** this is a *local Group Policy* setting, and then configures the policy setting with the URL of the server that is running the software update point/WSUS. The machine policy also provides the schedule for scanning and re-evaluation.

Note: AD based GPO will override local GPO setting, so make it sure that you don't have any WSUS server defined in AD based GPO.

2. Software update agent gives control to Windows Update Agent which connects to the WSUS server, retrieves the software update metadata, and initiates the compliance scan. The client returns a list that reflects the compliance state for every update evaluated.

3. If configured, WSUS stores the scan results in the WSUS database. This is not enabled by default.

4. The client stores the compliance scan results in Windows Management Instrumentation (WMI), and then sends the results to the management point as state messages, every 15 minutes, by default.

5. The management point sends the results to the site server, which enters them into the site database.

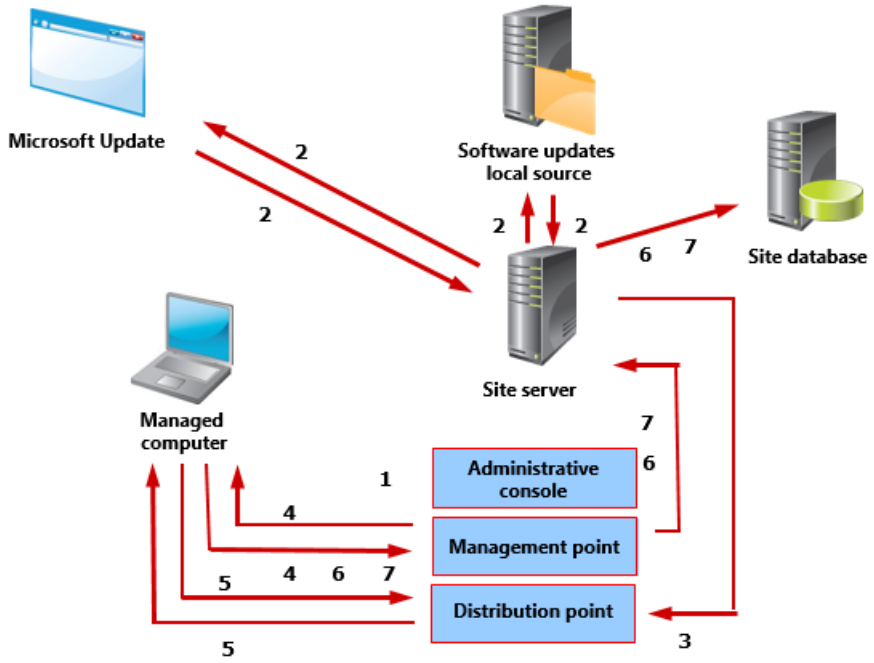
6. You can run reports to check compliance scan results.

Compliance state of client can be in either of 4 states:

1. Installed
2. Required
3. Not required
4. Unknown

Software Updates Deployment Process

Once you deploy software from server side, client will get it on policy evaluation cycle and deployment will start.



1. Use SCCM console to deploy updates using *Deploy Software Updates Wizard* which will create a package for it. There are various settings in this wizard.
2. The updates are not yet downloaded on site server rather it has only metadata as explained by me earlier. The site server requests the software updates from the download location that you define in the deployment. These updates can come from Microsoft Update or a local source.
   The metadata is downloaded by WSUS while actual update binaries are downloaded by site server.
3. The site server copies the software update binaries to the content library on the distribution point. The site server adds the new software update deployment to the machine policy.
4. At the client policy-polling interval, the client retrieves the machine policy from the management point and receives the new deployment information.
5. When a client receives a policy containing a new update deployment, WUA initiates a software update evaluation scan once again that evaluates all the newly assigned updates for applicability. Client won't download all the updates rather only those which are applicable for it. If you configure the software update deployment type as *Required*, the client requests the binaries from the distribution point for each required update, and

then stores them in the local cache. If you configure the deployment type as *Available*, the updates download when the user invokes the installation manually.

6. The client sends a state message to the management point that reports that the software update was downloaded. The management point forwards the state message to the site server, which then enters the message into the database.
7. If the deployment has a deadline, clients trigger another update scan by the WUA at that defined deadline to ensure that nothing has changed since the last update scan. The client installs the software update, performs another scan on the client to verify that the update is no longer required, and then sends a state message to the management point that indicates the update has been installed. If a restart is necessary, the state message indicates that the client computer is pending a restart. After the restart, a scan begins to verify that the software update is not required and to create a state message which indicate that the update has installed. For each software update that fails to install, an error message is sent to the management point, which forwards the messages to the site server. The site server inserts status messages into the database.

You can run reports at server side for consolidated information.

Many thanks to Vinit Pandey

https://vinitpandey.com/2017/03/23/troubleshooting-software-update-using-sccm-2012-part-1/