White Paper

Solving the Patch Management Dilemma Using SCCM 2007

Abstract

If you find it difficult to patch or update your enterprise computers, a Microsoft System Center Family product System Center Configuration Manager 2007 may be the solution you are looking for. In this white paper a strategy to solving the Software Update Management problem using SCCM will be presented.

Table of Contents

Introduction

System Center Configuration Manager (SCCM), formerly Systems Management Server (SMS), is a systems management software product by Microsoft for managing large groups of Windows-based computer systems. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory.

Configuration Manager also takes the step to standardize software updates. With Configuration Manager, we now use WSUS Server for software updates. Configuration Manager extends WSUS software update management functionality with advanced capabilities for patching (reporting, targeting, control of content, maintenance windows, delegated administration, 3rd-party updates, etc) while being integrated into a full configuration management offering. Now you can deploy, not just Windows updates. You can update bios and firmware for popular hardware vendors, download catalogs for popular third party software vendors, write catalogs for updating your internal custom applications, and receive your Forefront client updates.

Situation

A company has a multi DC enterprise infrastructure. With requirements for software update management for compliance assurance, security updates/ vulnerability assessment and application updates. The solution we present will address the software update/ patch Management problem and allow the customer to follow its compliance requirements with security policies.

Solution

Introduction

In SCCM 2007 Microsoft completely redesigned the Software update/ Patch Management operations.

Patch Management is inherently a risky activity. If you are installing software that changes basic functions of the operating system and key applications on every computer and server in the company. In such environments, there are no small errors. Even slight differences from intended options can cause serious problems. SCCM adds features that greatly reduce the need to select deployment options, once standards are developed and tested. Pre-selected sets of options can be used each month.

This solution takes into account that you already have SCCM with WSUS installed and the SUP working. If you need assistance with Patch Management, see the SCCM Installation and setup documentation available by Microsoft.

Solution Design

Sync with Microsoft
First you have to synchronize the WSUS server and SCCM with Microsoft Update on the desired schedule.

- The top-most server in the hierarchy synchronizes with Microsoft Update. All others synch that with top level server.
- Manual synchs only add new updates. Scheduled synchs also include changed and removed data.
- The first synch should be started in late afternoon. Monitor the wsyncmgr.log file until you see an entry saying "WSUS synchronizing categories, processed 0 of 820 items". The numbers may be different, of course. Allow the process to run overnight.
- Scheduled synchronization should run every evening, to detect any new or re-released updates.
- If multiple WSUS servers are running update the lower level ones from the top level after its synchronization has completed.

Scanning and Re-scanning
In this context, scanning refers to scanning for new updates. It checks the SUP and downloads any new update definitions. Rescanning is used to describe an activity totally within the client as it rescans for previous updates. This detects when older updates need to be applied or reapplied.

Scanning

- The scanning schedule is set globally, in the Software Updates Client Agent Properties, General tab
    - You can choose a simple schedule of once every X days, or a custom schedule
    - The custom schedule allows you to control time of day as well as the interval
- The scanning must be run on the client before new updates will be detected and can be deployed
    - The easiest way to assure that such is the case is to set a schedule of running daily, during the middle of the night after the Synch would be completed
    - If that imposes a load on the environment, set it to daily just before Patch Tuesday and reset it to weekly after all machines have been scanned at least once

Re-scanning

- The schedule is set globally, in the Software Updates Client Agent Properties, Deployment Re-evaluation tab
    - You can choose a simple schedule of once every X days, or a custom schedule
    - The custom schedule allows you to control time of day as well as the interval
- This is not needed frequently, weekly is probably good for most environments
- The load on the systems should be minimal

Selecting Updates

There are three basic steps to selecting updates:

- First, make sure you are downloading all of the updates you care about
    - Changes in your environment may require adding products such as a new version of Windows or SQL, so you should review this every month
- Second, review the newly available updates
    - Review all categories you have selected, not just security updates or critical updates
    - Compare to reports of installed products or other material to decide which are relevant to your environment
- Third, decide how you will deploy the updates
    - Separate deployments for workstations and servers are normal, so separate Update Lists would make that easier
    - Separate deployments for selected groups of machines may be needed to reduce the impact on network and DPs
    - Some non-security updates may require separate deployments because of testing and change management requirements
    - The goal is to minimize the chance of mistakes
    - All decisions are specific to your environment, deployment strategies, policies, organization, etc -- decide what's best for your environment, not someone else's

Deploying Updates

Creating Update List

Configuration Manager provides many ways to set up an update deployment. These sections reflect one way that I think should work well for many organizations. They will provide a good basis for understanding the process and make the alternative procedures clear. You should experiment in a lab setup to determine which is best for you.

The following steps create an Update List that is later used in one or more deployments. This procedure allows different individuals to select the updates to be applied, and also allows one Update List to be used in more than one deployment.

- Use Ctrl+click in a Search Folder to select the updates to be deployed, based on the previous analysis
- Right click and select Update List
- Select Create a new update list and enter the desired name, based on your naming standards
- Do *not* check the "Download the files..." box - that will be done as part of creating the deployment
- Update security permissions if needed, just as under SMS 2003
- A summary of the selected actions is displayed for your review - make sure it matches your intentions
- A final summary is displayed showing if the operation was successful - review any warnings or errors and correct as needed

Creating Deployments

Once the Update Lists are created, you need to set up the deployments. This is where you select the various deployment options and schedules. As explained in the Creating Update Lists section, Configuration Manager provides many ways to set up an update deployment. These sections reflect one way that I think should work well for many organizations. They will provide a good basis for understanding the process and make the alternative procedures clear. You should experiment in a lab setup to determine which is best for you.

- Expand the Update Lists section of the console, right click on the desired list, and choose Deploy Software Updates
- Select to create a new deployment package, and enter a name consistent with your standards
- If you have an existing Deployment Template that's appropriate, select it - otherwise select Create a new deployment definition
- The following steps assume you are creating a new definition, which can be saved as a template
    - Select the collection to receive this deployment
    - Select if users should be notified of the updates
    - Select whether to base schedule on client local time or GMT time (default is GMT)

    - Select the default postponement period, which can be overridden for any particular deployment
    - Specify if restarts are allowed or suppressed for servers and workstations, and whether to allow restarts outside of the maintenance windows
    - If you use MS Operations Manager, select actions you want taken - this is normally relevant only for updates to servers, and can enhance management reporting
    - Set client download settings, just as in an SMS 2003 advertisement. Note that the default is not to install over slow or unreliable networks
    - If desired, save these settings as a template using an appropriate name and description
    - Use of templates allows the preceding steps to be skipped and guarantees use of consistent settings
- Create a Deployment Package or update an existing one
    - This is what's copied to your DPs and deployed to the clients
    - Normally you select Create a new deployment package
    - Select a package name consistent with your naming standards
    - For the package source point to an existing share on any server where you want the downloaded files stored, with the name of the Deployment package appended as a sub-folder. Configuration Manager will create that sub-folder, but the share must already exist
    - Select enable binary differential replication if desired. This shouldn't hurt, but also is unlikely to normally be of use with updates
    - Select distribution points if desired. For large packages you may want to select just the location where they will be tested, and distribute to other DPs later
    - Select to download updates from the Internet if deploying from your central site server, otherwise point to the share location on the server containing the updates
    - Select the desired languages for the updates
- Set the deployment schedule
    - Clients will begin downloading updates from their DPs at the Time Available
    - If a deadline is set, updates will be applied automatically at that time if not scheduled earlier. If no deadline is set, updates will never be applied without user action
    - Enable Wake On LAN if your organization uses it and if it's appropriate for this deployment under your standards
    - Choose to ignore maintenance window if you want to override the deployment template setting
- Review the summary to be sure all actions are correct
- Updates are downloaded
- When the wizard is complete it reports success, warning or errors. Review and correct any warnings or errors as needed

Deployment Template
Deployment Templates are among the best innovations in Configuration Manager, because they allow a group of deployment settings to be stored and reused, thus eliminating one common source of problems.

Deployment templates can be created by themselves or the settings used in a new deployment can be saved as a template. The steps involved are identical. These steps are documented in the Creating Deployments above, and will not be repeated here.

The settings included in a deployment template are:

- Collection
- Allow or suppress notification on clients
- Base schedule on client local time or Greenwich Mean Time
- Default maximum postponement (can be overridden in a deployment)
- Restarts allowed or suppressed, separately for workstations and servers
- Allow restart outside of maintenance window (can be overridden in a deployment)
- Creating or suppression of MOM alerts
- Whether client should download and install updates on slow and unreliable networks, and from unprotected DPs

Separate templates are needed for any variations on settings that cannot be overridden in a deployment.

SCCM 2007 Software Update Standard Reports
Microsoft provides 34 standard reports, grouped in five categories.

Software Updates - A. Compliance
These reports show the degree to which portions or your entire network is in compliance. Reports can be based on Collections, Update Lists, Updates, Deployments, Vendors, or specific computers. They can provide high level summary data, and linked reports permits drilling down to details that can be used to increase the compliance rates.

Software Updates - B. Deployment Management
These reports are designed to help manage update deployments.

Software Updates - C. Deployment States
These reports help track the status and results of a Deployment.

Software Updates - D. Scan
These reports help manage scanning.

Software Updates - E. Troubleshooting
These reports help identify and troubleshoot problems.

Normal Monthly Activities

Preparation

Before beginning a monthly cycle, you'll usually have some cleanup to do from the previous month and activities to be sure you're ready for the next month. Details will always depend on how you manage updates at your company, but here are some possible activities.

Prior Month Cleanup Check the compliance rate for the prior month's updates, and address any significant issues.

If you roll each month's updates into a cumulative deployment package for baseline maintenance and reporting, you should do that after reaching an acceptable compliance rate. Ideally that's before starting the next month's cycle, but that won't always be true.

If you must continue monitoring last month's updates during the next cycle, identify the reports that will be appropriate to use. Identify the effect these ongoing activities might have on the reports you usually monitor for current month activities. Be certain you can produce the reports that may be needed for each separate month's activities or the combined total, based on your normal reporting.

Verify Pilot Test and Exception Lists If you have lists of pilot testers and/or exception machines that get special handling, make sure your data is current and reflects all changes during the last month.

Check Client Health Status Check the overall client health status, and assure that someone is following up on any issues. You may want to report the percentage to your management, as it establishes the maximum compliance rate possible.

Verify Server Data If you are responsible for patching servers, you're likely to have them divided into collections to reflect different deployment schedules or reboot handling. Make certain all servers are in the proper collections, particularly ones created during the past month.

Company-specific Testing Schedule

- Test the update deployments and updates per your company standards.
- After testing with VMs, it is common to test on computers belonging to the deployment team. You are most likely to recognize improper results.
- If pilot testers are used, create deployments specifying the appropriate collections, options and schedule. If templates do not exist they can be created while creating the deployments.

Follow Up

- Use standard reports to monitor deployment progress, detect issues, and resolve any issues.

- Provide periodic progress reports to appropriate management based on standard Compliance reports.
- Periodically review the Search Folder listing updates released during the latest month to see if any changes have been released. If so, decide what action is required.

Trouble Shooting software Updates
http://technet.microsoft.com/en-us/library/bb693492.aspx

About the Author

Nouman Khan is an Infrastructure Services Consultant presently working with expit. His expertise includes System Center Suite and Unified Communication design and implementation.

Resources and References

Microsoft System Center Configuration Manager
http://www.microsoft.com/systemcenter/configmgr/default.mspx

http://myitforum.com

Expit

http://www.expit.com