

All change please

Microsoft System Center Configuration Manager 2007 may mean you have to relearn old tricks, but it will make patch management easier, safer and more reliable. It will even help you patch in your sleep

If you're planning to roll out Microsoft System Center Configuration Manager 2007, beware: the Inventory Tool for Microsoft Updates (ITMU) is changing again. ITMU was never a core part of SMS; it was an add-on released roughly two years after SMS 2003 came out to replace the even clunkier Security Update Inventory and Microsoft Office Inventory tools.

The latest change will offer further improvements, including enhanced reporting and the ability to patch ConfigMgr clients that are Internet facing, assuming you are running ConfigMgr in its highest security mode with a Public Key Infrastructure (PKI).

ARCHITECTURE

One of the main changes from SMS 2003 is that the software update functionality is no longer an isolated component of ConfigMgr. Instead, ConfigMgr essentially assumes control of Windows Server Update Services (WSUS) and then delivers this to the down-level client via the use of a new site server role.

Metadata from Microsoft Update is synchronised with a WSUS server that could exist as a separate physical server, or be installed on the ConfigMgr server itself. If it is separate you would still need to install the WSUS administration console on the ConfigMgr server. However, for security reasons any server connecting to the Internet should be physically separate from the ConfigMgr server.

Either way, the ConfigMgr server will still control the settings on the WSUS server, such as

synchronisation times and update types. The Software Update Point (SUP) will then synchronise with Microsoft Update by using the WSUS server functionality as a sort of synchronisation proxy for the software update metadata, which is defined by the local administrator using the ConfigMgr console, rather than the WSUS console. It can then create a new object for each update within ConfigMgr, where it is then up to the administrator to decide what is done with it.

Once you have configured a WSUS server for an SUP then this WSUS server should not be used independently of ConfigMgr. An SUP will be required for each primary site server that will be handling updates. This can be configured on a separate physical server, if the load on the site server itself is a concern. Multiple WSUS servers can be configured at the different levels of the hierarchy with only the top level actually performing a synchronisation with Microsoft Update.

The software update information and the ConfigMgr objects are then replicated throughout the hierarchy to establish the foundations for deploying the required updates to the ConfigMgr clients. Now that the SUPs have the metadata regarding the software updates, this can be used to scan the clients using the ConfigMgr Software Updates Agent. This agent is a new addition to ConfigMgr. This scan is performed on a definable schedule and compliance information is written back to the database, allowing you to check the patch and security levels of

BY STEVE NEWBY

Senior Systems
Center Consultant
at IE

CONTACT

editorial@server-
management.co.uk

your infrastructure and take the appropriate measures.

DEPLOYING UPDATES

So, now that your infrastructure exists, what exactly is the process for getting the patches out to the clients? At first glance it may appear more complicated than the ITMU. It's no longer just a case of packages and advertisements. However, when you are talking about managing thousands of clients with differing operating systems and applications, the granular functionality of the process is a real benefit.

You no longer need to have one large deployment package containing all of the updates; instead multiple deployment packages can be used and the Software Updates Agent

“ When you have thousands of clients to manage, the granular functionality really helps

consolidates these into a single installation, causing less disruption to end users. The deployment process has a number of linked components.

Updates

These can be individual updates or lists can be created to group the updates for ease of use. For instance, you may want to have a list of all Internet Explorer updates or all Office 2007 updates. You may also want to assign security rights so that only certain administrators can configure deployments for certain types of update. The big advantage of using lists is that

you can simply drag-and-drop an update list into a deployment template to initiate the wizard.

Deployment templates

In SMS 2003 you had to specify such things as the collection to be targeted and client restart settings with every package. Now you can create a deployment template containing these common settings. An obvious use for this would be to have a separate deployment template for your test clients to drop in new updates in order to create a new deployment package for testing, prior to rolling them out to your live clients.

Deployments

Combining an update list with a deployment template creates a deployment object and it is this that delivers the updates to the clients you have targeted through the deployment template.

Deployment packages

These are the packages that contain the updates, which are then pushed out to the distribution points ready for downloading. The deployment package itself simply moves the updates to a distribution point; the client itself does not really care which package the required update is, so it will only download the update required, not the entire package. This means you can have a deployment package containing gigabytes of updates, without having to be worried that the clients will flood the network when they do an update.

CUSTOM UPDATES

Unfortunately, ConfigMgr can only deal natively with

Microsoft software, and unless you are running a very limited environment, the odds that you won't be using anything else are slim. SMS 2003 R2 included the Inventory Tool for Custom Updates (ITCU). This allowed third-party vendors to produce update definition catalogues for their products, taking advantage of the functionality to update non-Microsoft products. This functionality, provided by the System Center Updates Publisher, is now a core component of ConfigMgr. A number of software vendors have already created catalogues for their products that can be imported using this tool, such as 1E, Adobe and Citrix.

PATCH WHILE YOU SLEEP

In an ideal world the best time to patch a PC is when it is not being used. Unfortunately, the time when it is least likely to be used is the time it's most likely to be switched off. Wouldn't it be great if people could go home at night leaving their PCs turned off, only to come back the next day to find that their PCs have been patched to full compliance and are ready to use again straight away? Well, assuming that your PC supports Wake On LAN, this is now possible simply by selecting Enable Wake On LAN under the Schedule tab of the deployment.

While this is a great feature to have, there are a few caveats. The first is that ConfigMgr relies on being able to send the Wake On LAN magic packet across routers. This means that the router needs to be enabled for unicast or subnet-directed broadcasts. This is not something that is

usually very popular with network administrators.

Secondly, when waking up a PC from a powered off state it will only turn off again if the power management options have been set in Windows to turn it off after a specified period of inactivity. In my experience this is not something you would have set on corporate desktops. How thrilled would users

“ Even with gigabytes of updates, you needn't worry that clients will flood the network

be if their PCs turned themselves off every time they went to lunch or into a meeting? Probably about as thrilled as the support technician whose call volume would just have gone through the roof.

Thirdly, if you are waking up a PC that has been suspended or hibernating then the operating system will put it back into that state after two minutes, which is unlikely to be long enough even for the smallest patch to install.

These apart, the benefits of using Wake On LAN are compelling – especially in an organisation with tens of thousands of PCs, all of which need to be kept up to date. Third-party products, such as the Power & Patch Management Pack from 1E, ensure that network changes are not required and allow you to have a much tighter control over the wake up and shut down of your clients. This empowers you to further enhance the capabilities of ConfigMgr to give you a solution eminently suitable for managing most Windows client-based environments. ■