CONCENTRATED TECH

ProductScope™

Goverlan v8 as a Companion to System Center Configuration Manager (SCCM)

October 2014

commissioned by

GOVERLAN®

manage IT complexity simply

Executive Overview

An increasing number of organizations are turning to Microsoft System Center Configuration Manager (SCCM) to manage the computers in their environments. SCCM offers a broad range of capabilities intended to centralize management and to facilitate remote support of users. In this paper, we examine the real-world experience organizations are having with these features, explore missing capabilities, and examine the role that a standalone remote-support solution like Goverlan Remote Administration Suite v8 can have in an SCCM-managed environment.

Overview and Methodology

SCCM is a large-scale configuration management solution that can support up to 400,000 managed nodes in a site hierarchy. It provides a number of useful features, which are generally categorized as follows:

- Collection of software and hardware inventory
- Monitoring and collection of software usage ("metering")
- Remotely controlling computers
- Reporting on various collected data

In addition, the product (referring to SCCM 2012 R2) has very basic configuration auditing and remediation capabilities. These capabilities overlap lightly with Windows' native Group Policy functionality.

For this paper, we interviewed 11 customers using SCCM 2012 and updated to SCCM 2012 R2 in their environments. 4 of these customers already use a supplemental remote support solution, which helped highlight capabilities that they found missing in SCCM. We also conducted two focus groups. The first consisted of 27 IT professionals actively engaged in day-to-day support of managed nodes, and the other consisted of 8 IT managers who rely on SCCM in their environments.

Problem Domain

As previously mentioned, SCCM is designed for massive levels of scale. A single multi-site hierarchy can support up to 400,000 managed nodes. Given the amount of data collected from those nodes, and the frequency with which it is collected, it would be impractical, if not impossible, for SCCM to operate in "real time." The primary means by which SCCM achieves that level of scale is by operating extremely asynchronously. In other words, almost nothing in SCCM happens immediately. An administrator tells SCCM to do something, and that instruction flows through several stages before arriving at a managed node. This means that actions can take anywhere from 15 minutes or more to complete, using SCCM's default settings. SCCM's default schedule means inventory information can be up to a week old at any given moment. Again, the scale that SCCM must support necessitates these delays.

The problem is that organizations often have more immediate needs, particularly in break/fix scenarios. For example, when a technician needs to deploy a tool to diagnose a problem, they can't wait the time needed for the managed node to "check in" with SCCM, process the revised policy, contact a Distribution Point, download the software in the background (which happens on a low-priority thread), install the application, convey status information back to the SCCM hierarchy, process that status information into the database, and finally confirm to the technician that the deployment was successful. That entire process will almost always take 15-30 minutes, if not longer in some scenarios.

This lack of immediacy is what would seem to open the door for supplemental solutions that do operate in real-time.

In speaking with customers and our focus groups, we identified several specific functional areas where SCCM created frustrating situations, and where IT teams needed to work with greater immediacy:

- Software deployment. Not for end-user applications, in many cases, but rather for deploying tools, patches, fixes, and other software, typically on a one-off, ad-hoc basis.

- Software and hardware inventory. In many cases, this was to confirm that the information in the SCCM database was still accurate, so that a technician could confidently proceed with a given task or the reporting of needed information.

- Reconfiguration. SCCM's ability to manage configuration settings is fairly weak, necessitating different approaches.

- Remote control. SCCM's native remote control capabilities have, for some organizations, several downsides.

After discussing the problem areas with customers and focus groups, we asked them to consider specific features of the Goverlan product, and evaluate how well those features supplemented SCCM's native functionality.

Software Deployment

This was perhaps the most convoluted set of functionality to discuss with customers and focus groups.

Invariably, managers who we spoke with felt that all software should be deployed through, and managed by, SCCM. This is understandable as their primary investment in SCCM was to control and manage software, and they wanted to utilize that investment. Deploying software outside SCCM makes that software less manageable; it is more difficult to later manage via SCCM in terms of removal, retirement, updating, reporting, and so forth. Change control and documentation were additional concerns in using other alternatives to SCCM.

Just as invariably, support technicians frequently need ad-hoc access to utilities that help them diagnose and fix problems, and often need to deploy software patches or fixes immediately in order to solve a user problem. Some organizations address this in part by building "super utility" packages that are deployed to all computers as part of a base operating system deployment, the idea being to have all necessary utilities available locally, at all times. Less than half of the individuals we spoke to found these "super utilities" to be sufficient; others stated that they still often needed to deploy small pieces of software ad-hoc. Without a managed system in place to do so, they often maintained a file share of utilities, and used remote control to install those, on-demand, on managed nodes.

This contention between managers desiring complete control with SCCM and support technicians faced with the immediate need of real-time control functionality creates an on going management issue inside many organizations. We feel that there is a management issue that needs to be addressed in advance of the functional question. Simply put, organizations must recognize the need for ad-hoc, out-of-band software deployments. They should develop guidelines for what can be deployed this way and how such software is to be managed, and provide a solution that enables such deployment efficiently and effectively. This would not be complete without guidelines for documenting ad-hoc management and the notification chain to ensure smooth transition from a one-off solution that may impact other systems. Failing to provide the solution does not remove the need for the functionality; it simply forces technicians to waste time with less-efficient mechanisms for accomplishing the deployment and risking incidents due to a lack of well-understood and documented processes.

For example, of the customers who already had a supplemental remote support solution in place, 3 used the Goverlan product. They estimated that they could deploy permitted ad-hoc tools to an affected client in under 3 minutes, with no impact to, or visibility by, the end user. Customers without a supplemental solution needed to interrupt the end user by remotely controlling the client computer, and typically needed 15-20 minutes to deploy the ad-hoc tool. Clearly, this is an area where a supplemental product can provide a marked gain in efficiency, lowering IT costs and increasing end user satisfaction.

One Goverlan customer also noted that it was his organization's practice to also use Goverlan to un-install ad-hoc tools once they were no longer needed. As a usual part of their support procedure, they would complete a ticket by using Goverlan to remove whatever tool they had just deployed and used. The process added less than 3 minutes to the overall ticket time, and could be accomplished after the end user had been satisfied and gone back to work.

Another customer suggested that SCCM could also be used to ensure the removal of ad-hoc tools, if desired, by simply having a standing deployment to uninstall them. As tools are installed, SCCM would eventually realize that through updated software inventory, which in turn could trigger the deployment of an uninstalling package. Regardless of the approach used, it's clear that there is a need for ad-hoc software deployment, and that organizations should provide that capability so that it can be managed and efficient.

Another problem exists with regard to software deployment through SCCM, and that is the need to construct packages or applications, the two units of management supported by SCCM. The actual, physical software installers can be complex to build, often requiring hours of analysis, building, testing, and revision. Organizations can attempt to address this by committing the time needed to properly package all of their support tools (again, leading back to the "super utility" package), but maintaining that over time as new tools are added can create a great deal of overhead. There is an argument that SCCM is a less-appropriate solution for the deployment of ad-hoc tools, and that a real-time, supplemental solution like Goverlan, combined with an effective management process, provides better capability with less overhead. Every organization will arrive at their own answer for this question, but it is a question organizations should discuss.

Organizations are also extremely unlikely to open up the SCCM infrastructure so that support technicians can create package deployments – the opportunity for costly, impactful errors is simply too high and has resulted in negative situations for several of the interviewed organizations. Instead, technicians needing a deployment would typically open a ticket with an SCCM administrator, or would schedule the deployment. That business process, of course, can add significant time and overhead negatively impacting the user and their work. Again, the Goverlan solution seems ideally positioned – along with appropriate business policies and procedures – to enable these support technicians to work independently of the SCCM infrastructure when needed.

Software and Hardware Inventory

By default, SCCM managed nodes report hardware and software inventory every 7 days, and there are some additional minor delays in that inventory being processed into the SCCM database.

Once in the database, inventory is used for two major purposes:

- Reporting, which may be full, formal inventory reports, or may simply be ad-hoc lookups of information by technicians.

- Targeting, wherein inventory information is used to define collections, which are in turn used to target specific computers for configuration settings, software deployments, and other activities.

For the most part, organizations are comfortable with the delays involved. SCCM continually re-evaluates collection membership on a scheduled basis, which means that eventually, it will have updated inventory and will properly consider a managed node for targeting. For normal day-to-day tasks like deploying major application updates, this is more than sufficient.

It is not uncommon, however, for a technician to need more timely information, and like software deployment this need often comes in conjunction with a break/fix scenario. For example, a technician may have an immediate need to check the processes running on a managed node, or to confirm the amount of disk space free on a disk, or to confirm the current configuration of a critical background service. SCCM's inventory information is rarely "current." One interviewed customer described the immediate need to verify service state condition on several servers and resorted to scripting a solution to overcome the stale data in SCCM.

Many organizations try to better accommodate this need by moving SCCM's inventories to 24 hours instead of 7 days, something SCCM can readily handle even in very large environments. However, that still involves some lag time – for some information, such as processes, values are constantly changing and nothing short of real-time may be acceptable, especially in a break/fix scenario. In addition, many organizations are less-than-comfortable providing their lower-level technicians with any access to the SCCM management console.

The Goverlan solution provides a unique hybrid solution in that it first gathers its information in real-time, then optionally storing this information (using SURE-DATA technology) to a local file or central SQL database. This contrasts from SCCM by providing immediate real-time information as the technician is working and displaying stored information for systems that may be offline, permitting more accurate queries for actions and reports. Inventory collection may also be scheduled, but the importance of having real-time information immediately available is the foremost concern. While it would not scale to inventorying the 400,000 clients supported by an SCCM site hierarchy, it can offer the immediate "inventory check" that technicians often need in a break/fix situation. Much of Goverlan's inventory information is gathered from Windows Management Instrumentation, which is the same source SCCM itself uses; Goverlan simply queries less information at once (only what is requested), and it does so immediately from a single computer or a group of computers. It can produce reports based on that information, but again does so immediately. Because the Goverlan tool has no connection or dependency to the SCCM infrastructure, and because it is more purpose-designed for support technicians, organizations are more likely to feel comfortable deploying the solution to those technicians.

The customers we spoke to almost universally acknowledged a need for ad-hoc, immediate inventory information. Recognizing that SCCM could not provide the immediacy needed, these customers often resorted to home-grown scripts and tools, which they acknowledged were inconsistent and not usable by

less-experienced technicians in their environment. Our focus groups in particular felt that the Goverlan product did an "excellent" job of making these ad-hoc inventory checks more accessible to a broader set of IT workers.

A number of our focus group participants pointed out that, in some instances, organizations were willing to bypass SCCM in an emergency. For example, one participant described a situation where the network had been infected by malware that was targeting a line-of-business application. An application patch was available, and needed to be deployed immediately to about 50 affected computers. SCCM was deemed too slow given the emergency nature of the problem: our participant estimated that it would have taken several hours to build the package, along with the usual SCCM delays involved in deploying it and then verifying that deployment. We asked our participants to use the Goverlan solution in a virtual lab to create a similar deployment, using real-time inventory information to identify the computers needing the patch. After receiving a basic orientation with the Goverlan product, participants averaged under 14 minutes to create the necessary ad-hoc deployment.

It seems clear, then, that the Goverlan Remote Administration Suite product provided another valuable supplementary capability within the environment. Even when used in a way that seems to overlap SCCM functionality, immediacy was the key in making it useful for the customers we spoke with.

Reconfiguration

SCCM 2012 R2 includes a "configuration baseline and auditing" capability that, in limited scenarios, supports configuration remediation. In other words, SCCM can report on selected configuration items and in some cases reset them to a desired state.

The weakness in this feature is that it is fairly limited in reach. It works primarily for registry keys in terms of remediation, and in checking things like files or Active Directory attributes for non-remediable settings. It can run arbitrary scripts to both check and remediate configurations, but that requires fairly extensive programming skills. None of the customers we spoke with were actively using this SCCM feature for general configuration auditing or enforcement. The desire for remediation was conveyed, but until SCCM better utilizes Desired State Configuration (DSC) implemented with PowerShell v4, the investment wasn't warranted.

Group Policy also offers a configuration enforcement mechanism, although it is primarily limited to the Windows registry. While the registry is the source for much of Windows' configuration, it can be difficult to use. For example, if a technician needs to reconfigure a computer to enable Remote Desktop, where in the registry would they go? Will they have permission to edit a GPO for that one computer? Can they wait the 30-90 minutes needed for the new GPO to take affect? Will the computer immediately use the new configuration, or will it take affect only after a restart?

The SCCM's configuration auditing feature, DSC, and Group Policy is made for long-term management of baseline configuration settings. Neither is intended for real-time configuration fixes. Most of the SCCM customers we spoke with were accustomed to remotely controlling the desired computer, and simply using its native graphical user interface (such as the Control Panel applets) to reconfigure whatever needed reconfiguring.

At this point in our customer discussions, the issue of user impact was raised. A benefit of both Group Policy and SCCM is that they happen entirely in the background. Settings change without the user being visually impacted or interrupted. Remotely controlling a computer, on the other hand, interrupts and impacts the person using that computer. The Goverlan solution, however, was specifically designed for this use case. It replicates many of the Windows GUI screens for configuration. In other words, a technician can use a familiar-looking GUI, such as Task Manager or the Services console, while in fact targeting a remote computer. This combines the "best of both worlds:" users are not impacted or interrupted, and technicians can work almost as they would if they were actually remote controlling the targeted computer.

It should be noted that many of Windows' native Microsoft Management Console (MMC) snap-ins can already be pointed to a remote computer, but it should also be noted that many Windows configuration settings aren't accessed via one of these snap-ins. The Goverlan solution provides a unified way of accessing many of the most common configuration elements in a single, consistent location.

Both of our focus groups saw immediate value in using this aspect of the Goverlan Remote Administration Suite feature set. Our management-based focus group felt that the remote reconfiguration features would help reduce IT's impact on end users while accomplishing needed work in less time; they also felt there was an opportunity to reduce the number of snap-ins and tools that needed to be deployed to technicians' workstations. Our technician-based focus group felt the remote configuration features of Goverlan would make their jobs easier and faster, and that the consistency of the tool would make it easier to onboard and train new technicians coming into the environment.

It is important to understand that "configuration management" has two aspects. There is the long-term view, where a set of standardized configuration policies are created, deployed, and enforced over time. There is

also the short-term view, which often involves per-machine settings that relate to a particular problem. The actual configuration settings involved in these two views seldom overlap. For example, the long-term view might focus on firewall standards and other security configuration issues; the short-term view might focus on stopping a particular runaway process or fixing a network adapter configuration. SCCM and, to a greater degree Group Policy, take the long-term view; the Goverlan solution focuses more on the short-term view. That, we feel, is how SCCM and Goverlan complement each other.

Remote Control

SCCM supports three methods for remote control:

- *Remote Assistance*, a native Windows feature that allows remote screen sharing with the end user.
- *Remote Desktop*, a native Windows feature that allows for remote control, but not screen sharing; an administrator must force the user to log off in order to initiate this connection.
- *Remote Control,* a feature of the SCCM software that allows for screen sharing and is more tightly integrated into the SCCM console.

Goverlan Remote Administration Suite also supports both Remote Assistance and Remote Desktop, and adds its own remote control capability. We, and our focus groups, found its remote control to be superior to SCCM's in almost every way. It offers in-session text chat with the user of the remote computer, and facilitates file transfers between computers using a simple drag-and-drop mechanism or via clipboard integration. Technicians can create "dashboards" showing remote control sessions to multiple computers at once – ideal for managing a small "farm" of servers, for example. Technicians have the ability to lock out the local user and blank their local screen, often necessary when performing sensitive tasks that the organization does not want the user attempting to replicate. Technicians can also capture screen shots and video snippets of remote control sessions.

Goverlan provides a unique feature named fastConnect that is especially useful to support technicians. This feature allows the support professional to find and target a computer by searching for the username of the currently logged on user. As an example, when a user contacts support, they rarely know their computer name, forcing the support technician to spend several minutes helping the user discover and report the computer name for a remote connection. With fastConnect, the technician can query for the username and see the corresponding computer, allowing for an immediate connection without further involving the user.

Goverlan's remote control also offered a wider array of bandwidth-control options, such as color depth reduction and a range of visual options to help conserve bandwidth over slow links.

It should be noted that Goverlan's improvement and integrated support for cross-platform clients, VNC for Mac and Telnet/SSH for Linux, satisfied the ongoing needs of both focus groups.

Our management-based focus group expressed concern over auditing, citing the need to balance user privacy and organizational needs against support conveniences like remote control. Both SCCM and Goverlan rely on Windows' native auditing for Remote Assistance and Remote Desktop; both SCCM and Goverlan (through its Central Server option) support extensive activity auditing for their respective remote control features.

Both SCCM and Goverlan offer user notification options for their respective remote control features. Organizations can take an "always get user permission" position, move to the opposite end of the spectrum with "the user doesn't need to know they're being monitored," or adopt a position somewhere in between. One focus group participant noted that Goverlan's "monitor only" option, where a technician can see what a remote user is doing but not take control of the computer, would be useful as part of her organization's quality control procedures (which also entails recording phone calls with customers).

Unlike SCCM, Goverlan also supports having multiple administrators participate in the same remote control session, enabling collaboration and consulting-style approaches. Several focus group participants stated

that this feature would find heavy use in their environments, given the composition of their IT teams and the processes by which they worked. One such example involved server administrators along with Exchange managers to troubleshoot an outage, taking advantage of both teams' unique knowledge of the system.

We should point out that there are technically two distinct approaches to remote control. In-band control is the traditional remote control discussed in this section. Another approach, out-of-band control, utilizes hardware-based redirection of the keyboard, mouse, and monitor. This type of control is primarily for the support technician dealing with break/fix scenarios of target computers in an unknown state. Both SCCM and Goverlan support the common features of out-of-band management such as complete power options, the ability to mount ISO images for diagnostics or OS repair, and KVM sessions. This type of support requires the computer motherboard to include the technology, and the most popular today is Intel vPro-based remote control. Goverlan provides a cleaner unified GUI approach over SCCM and offers the support technician rapid and easy access to the Intel vPro features.

Potential Barriers

Like SCCM, the Goverlan solution requires a small piece of agent software to be installed on managed nodes. We discussed this need with customers and our focus groups, well aware of the fact that "yet another agent" might present a barrier for some organizations to using the Goverlan solution. It should be noted that many technicians find the "no new agent" rule an almost absolute, but when taken with the organization's agreed adoption of a product, such as Goverlan, this no longer poses an issue.

Approximately 70% of the feedback we received was that the Goverlan agent would not present a challenge, and that SCCM would provide a good way of deploying the agent to existing machines and as part of new OS deployments. Another 20% of the feedback indicated optimism, noting that any such deployment would be a change management discussion in their organizations but not identifying any specific show-stopping issues. Only 10% of our participants indicated that deploying "yet another agent" might present issues in their environment, and that further piloting, testing, and discussion would be needed in order for them to do so.

The Goverlan agent is small (under 5MB) and when not being used consumed no significant observable system resources (including under 2MB of system memory). The agent does not monitor process starts, nor does it monitor disk activity, which serves to further reduce its potential impact. The agent is available as a Windows Installer package (MSI), which facilitates its deployment as an SCCM package or application. When deployed in this fashion, the agent has no dependencies or pre-requisites apart from its basic system requirements.

Conclusion

Based on our own analysis and customer discussions, we feel that SCCM environments can benefit from a supplemental remote support and control solution that offers better immediacy and support for ad-hoc operations.

With regard to Goverlan Remote Administration Suite, we feel it would be an excellent candidate for such a solution in any SCCM environment.

- Its ability to quickly deploy tools almost immediately to remote computers, with little or no user impact, is valuable in a number of scenarios.
- Its ability to quickly verify hardware inventory details, and to use those in an SCCM-like fashion for small-scale tool deployment or reconfiguration, is very complementary to SCCM.
- Its support for remote, GUI-based, non-interruptive reconfiguration is of significant value.
- Its remote control offers features that are superior to those found in SCCM.
- Target discovery by username using fastConnect demonstrated a deeper understanding of the challenges faced by support professionals.
- Its SURE-DATA technology to provide real-time and the most up-to-date inventory information, including offline systems.

Most of the customers we spoke with felt that, in general, they would rather deploy a purpose-built tool like Goverlan Remote Administration Suite to their front-line technicians than provide those technicians with the full SCCM console. They acknowledged the need to revisit some of their business processes and procedures to fully embrace this level of technician empowerment, but felt broadly that Goverlan Remote Administration Suite filled in many of the gaps – particularly with regard to immediacy – that they had experienced thus far with SCCM.

During our discussions, we kept coming back to two particular terms. The customers we spoke with tended to use management with regard to long-term, lifecycle-based issues, and turned to SCCM to help facilitate those. Managing the overall software library of the organization, auditing key configuration settings related to security and compliance, monitoring inventory over the long term. They began to use the word support, and to consider solutions like Goverlan Remote Administration Suite, to refer to lower-level, more-granular, real-time issues like fixing configuration problems, quickly resolving operational issues, and helping educate users on specific tasks. Those two terms reinforce our belief that SCCM and Goverlan Remote Administration Suite play complementary roles within an organization.

We feel that SCCM and Goverlan Remote Administration Suite also map to different job roles within the organization. SCCM tends to be managed by higher-level members of the IT team, along with other major infrastructure components like messaging and databases. They take the long-term perspective, while the Goverlan solution is targeted more toward support technicians working from a more immediate, short-term view. The fact that the Goverlan solution can be deployed easily without the extensive back-end infrastructure required by SCCM further emphasizes this focus. It enables those support technicians, without providing potential exposure and possible error that would come from opening up the SCCM console to a wider IT audience within the organization.