

White Paper: Build vs. Buy: Mass Management Tools for Your Workstations

Rev 0 - 12/8/03

Written by Philip Lieberman (phil@lanicu.com)
Lieberman & Associates
<http://www.lanicu.com>

Abstract

This whitepaper examines the pros and cons of mass managing workstations with either third party tools or roll your own solutions such as writing scripts or using the Group Policies feature of Active Directory in Windows 2000/2003. Recommendations are made for the most appropriate use of each method.

Contents

1. Introduction	3
2. Are Group Policies or Scripts the Way to Go?	4
3. What is the Right Mass Management Application for Me?	5
4. Third Party Tools for Different Needs	6
5. Summary	7
6. About the Author	8

1. Introduction

“I only need to change a few things on all of my workstations...should I write something using scripts or should I buy a third party tool?”

This is a question that faces almost every administrator responsible for sets of workstations both large and small.

There are many different ways to create scripts to make changes to workstations. If you look at the Microsoft Resource Kit for Windows, you will find a wealth of pre-written scripts that address many issues ranging from managing user accounts on Active Directory to group management. By going to any technical bookstore you can find a wide range of excellent books on writing scripts. Many of these books will contain a very large number of pre-written scripts. There are also many books on using the Windows Management Interface (WMI). As an added dimension to mass management, you can also use Group Policies to implement a wealth of changes using Active Directory in Windows 2000/2003.

So, with all of this easily available free code, built-in Group Policies and massive documentation already in place, why would anybody need to purchase a third party tool to do mass management of their workstations?

For some customers, scripts (with/without WMI) and Group Policies are a perfect solution—they cost nothing to buy and do everything that the administrator needs them to do. On the other hand, there is some truth to the saying that the “devil is in the details,” and for more advanced administrators with large or complex environments, a third party tool is mandatory for getting vital changes accomplished.

2. Are Group Policies or Scripts the Way to Go?

Group Policies provide a very limited range of changeable options; there is no conditional logic with policies (i.e. you can't change the policy per machine depending on the conditions within the machine) and propagation delays can be significant. There is also the classic problem of determining the 'effective setting' of a policy, if more than one policy is in effect.

Because Group Policies has these limitations, many administrators switch to scripts. However, you must consider the following issues that need to be addressed with any script you write. Can you:

- Constantly maintain an accurate list of machines to process?
- Deal with off-line systems (auto-retry list management)?
- Schedule operations on a one-time/periodic basis?
- Handle multiple domains/workgroups and credentials?
- Log successes/failures in a human readable/Event Log format?
- Document the code and operating procedures of the scripts?
- Find the time to keep updating the scripts?
- Find the time to learn all of the scriptable interfaces?
- Prepare a wide range of reports of system settings?
- Handle the programming of situations where there are no scriptable interfaces - requiring a C programmer to add essential functionality to the scripts?
- Handle the 'gotcha' cases where the scriptable interface behaves differently depending on the target system (i.e. NT, 2000, XP, 2003 all with different levels of hot fixes/service packs)?
- Force the change in managed systems immediately without delay (no coding, propagation delay, development time)?
- Handle scalability where you need to manage over 10,000 systems at a time?
- Deal with a topology of LAN/WANs with varying speed connections in which scripts completely stop and wait for the slowest system in list?
- Handle both ASCII and UNICODE data as well multiple languages on different systems?
- Handle the storage/retrieval/editing of cryptographically sensitive credentials needed for script execution?

It is definitely a lot of fun to write scripts and see them work. But, it is also a good idea to ask yourself whether the time might be better spent developing applications that are unique to the business needs of the organization; leaving the general purpose mass management tasks to a third party tool specifically designed for that purpose.

It is very difficult to convince an administrator that has just learned how to write scripts that a third party tool would be a wise investment--that is, until the administrator has written, deployed, debugged, and supported the suite of created scripts for a period of time.

The question to ask is: "What added functionality or convenience do I get with a third party solution that I would be missing if I did it myself?"

The general rule of thumb is as follows: Purchase a third party mass management application if it contains the functionality that is needed to manage an area of the organization that is extremely critical, but is impossible to practically reproduce with scripts or Group Policies.

3. What is the Right Mass Management Application for Me?

If you are interested in buying a third party mass management application, you need to ask yourself a series of questions:

- 1) How big is my environment?
- 2) Is there any sensitive information on my machines that requires that I take periodic proactive steps to report on and secure or fix the security configurations of my workstations?
- 3) Am I ever in the situation where I need to get a security configuration report or make a change on all of my systems immediately, and a delay of minutes to hours could cost my organization serious damage?
- 4) Will the tool work on just a few machines at a time or must it hit all of the systems with the same change?
- 5) Is the tool for the Help Desk or a domain wide administrator?
- 6) Do I need the program to do per-machine logic such as “move all users except the following to a special group”?
- 7) Do I need per-machine wild card operators such as “change the name/password of the built-in administrator account,” no matter what its current name is?
- 8) Will I need to manage systems in multiple domains and different workgroups?
- 9) Is there a need to manage machines by NETBIOS, DNS, and IP identities?
- 10) How important is auditing/logging to my situation?
- 11) Do I need auto-retry of off-line systems as well as scheduled operations?
- 12) Does my list of machines to manage change constantly and do I need the tool to automatically adapt to the “current” list?
- 13) Do I care if errors occur in operations and there is no feedback as to why the error took place?
- 14) Is it important to me to see the internal technical details of all operations that are performed on my systems?
- 15) Do I need all operations as well as who performed them, when, and from where recorded in both the local and remote systems event logs?

4. Third Party Tools for Different Needs

The arena of third party mass management tools can be broken down into the following three groups:

Freeware/Shareware Applications

These applications are typically written as scripts (PERL, VBScript) and may have a simple GUI interface.

Pros:

- Free or inexpensive
- No per-node cost

Cons:

- Limited/no support
- Slow when handling more than a handful of machines
- Limited or no logging
- Limited to no error recovery
- Limited functionality
- No or limited machine list management

Low-end Commercial Machine Management Applications

Most of these applications are written as Visual Basic applications with a tree-view screen paradigm. They have a wide scope of functionality, but the depth of capabilities in each area is very limited. Designed to provide a broad view of an enterprise and to allow a drill down to a specific machine, these tools provide a significant improvement over the built-in tools provided by Microsoft.

The tools in this area represent a very good value for the customer that does not need a tool for a large number of systems or sophisticated features such as encryption, wild cards, logging, auditing, recovery, scheduling, or operation logic per systems.

Pros:

- Wide functional ability from a single consistent interface
- Very good value for the scope of functionality
- Excellent tool for Help Desk staff needing to poke around one machine at a time
- Low cost - priced by administrator, or by node

Cons:

- Not designed for concurrent mass management (some tools can generate one-time mass management scripts that use resource kit tools)
- Primitive error recovery/logging (if any)
- Very slow operation due to design constraints of Visual Basic language and UI elements chosen
- Only basic add/delete operations of single objects are supported
- Large organizations may be disappointed by the lack of error handling/recovery and limited options within any one area of the tool
- Limited support and training

Dedicated Mass Management Applications

These high-performance tools are typically written in C/C++ and are designed to handle complex management scenarios on large groups of systems. The number of areas managed by these tools is somewhat fewer than those of the low-end commercial management applications, but each area is handled in a more comprehensive manner. These tools are specifically designed for high-end domain administrators, rather than day-to-day help desk users.

The typical purchaser of dedicated mass management tools handles large groups of systems that need the same concurrent changes. These tools appeal to the administrator that is seeking auditing, recovery, scheduling, cryptography, and complex update case support. These tools handle multiple languages, varying operating system versions, patch levels, and network speeds smoothly, while maintaining a high throughput rate.

Pro:

- Appeals to power administrator looking for all of the bells and whistles in an industrial strength mass management tool
- Easily handles large environments and complex security situations
- Stable and consistent performance with comprehensive customer support
- User interface may be utilitarian in design, but it is optimized for administrator looking to perform changes with a minimal number of mouse clicks

Cons:

- Per-managed node cost makes it more expensive than shareware or low end mass management applications
- Because these powerful tools are very sharp and fast an administrator needs to think through the exact nature of the change put into effect. It is best to try out the change on a few machines before sending it off to the entire organization.
- Logging details may intimidate some administrators - tool can be set to output simple success/failure, or all technical details of changes

5. Summary

The decision of how to mass manage workstation environments depends on your stamina and boredom level. Can you handle the tedious process of having to physically visit each system or use Microsoft's own built-in GUI tools to make a change?

If you don't mind writing a script, you can automate many necessary changes. As the nature of your changes becomes more sophisticated and the size of the list of systems increase, you may decide that a third party mass management tool can make your life a lot easier and give you more power and control than any tool you might write yourself.

In deciding which third party tool is right for you, you will need to examine the complexity of your requirements, how important the features of each product are to you and, of course, your budget. It is also wise to investigate the internal architecture of the tools you are considering to assure yourself that you are buying enough horsepower for your needs and that the quality of the tool matches the value of the systems you are protecting.

6. About the Author

Philip Lieberman is a well known lecturer and award winning author of many articles, books, hardware products, software programs, and technical courses. He has been a developer for a very long time spanning technologies from IBM 360 punch cards to the latest Microsoft Longhorn operating system release. He can be found at all hours of the day and night happily coding away in C++ creating and updating the suite of mass management, migration and security products sold by his company, Lieberman Software Corporation.

Please feel free to contact us for technical questions on this process whether you are a customer or not.

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)
Web: www.lanicu.com Email: support@lanicu.com

