

Build Vs. Buy

Mass Management Solutions for Windows Systems



Executive Summary

When it comes to the mass management of the Windows workstations in your network, you have two alternatives: use third party products or roll out your own solution, such as writing scripts or using the Group Policies feature of Active Directory. This paper presents recommendations for using each solution and describes the benefits that you can receive.



Contents

Executive Summary.....	1
Introduction	3
Are Group Policies or Scripts the Way To Go?.....	4
What Is the Right Mass Management Application For Me?.....	6
Third Party Products for Different Needs	7
Next Steps	10
Summary	10
About Lieberman Software.....	10



Introduction

“I only need to change a few things on all of my Windows workstations...should I write something using a script or should I purchase a third party product?”

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

There are many different ways to create scripts that 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.

Go to the technical section of any bookstore and you can find a wide range of excellent books on writing scripts. Many of these books contain a large number of pre-written scripts that you can easily implement in your network. There are also many books about using the Windows Management Interface (WMI). And as an added dimension to mass management, you can utilize Group Policies to implement a wealth of changes using the Active Directory function of Windows.

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 product to do mass management of their Windows workstations?

For some IT administrators, scripts (with or 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”. For more advanced administrators with large, complex IT environments, a third party solution is mandatory for accomplishing vital configuration changes.



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 IT administrators turn to scripts. However, before you opt for scripts you must consider the following issues. 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 update 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?
- Handle the "gotcha" cases where the scriptable interface behaves differently depending on the target system (i.e. XP, 2003, Vista, Server 2008 all with varying levels of hot fixes/service packs)?
- Force the change in managed systems immediately (no coding, propagation delay, development time)?
- Handle scalability to manage more than 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 the 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. However, most overworked IT administrators don't have the luxury of being able to consider all of the security implications of deploying a script to run enterprise-level management projects. It is practical to ask yourself whether your 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 product specifically designed for that purpose.

It is difficult to convince an IT administrator who has just learned how to write scripts that a third party option 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.



What Is the Right Mass Management Application For Me?

If you are interested in acquiring a third party mass management solution, ask yourself a series of questions:

- How large is my environment?
- Is there any sensitive information on my machines which requires that I take periodic, proactive steps to report on and fix the security configurations of my Windows workstations?
- 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 even a few minutes could cause my organization serious damage?
- Will the product work on just a few machines at a time or must it hit all of the systems with the same change?
- Is the product for the Help Desk or a domain-wide administrator?
- Do I need the program to do per-machine logic such as “move all users except the following to a special group”?
- 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?
- Will I need to manage systems in multiple domains and different workgroups?
- Is there a need to manage machines by NETBIOS, DNS, and IP identities?
- How important is auditing/logging to my situation?
- Do I need auto-retry of off-line systems as well as scheduled operations?
- Does my list of machines change constantly and do I need the product to automatically adapt to the “current” list?
- Do I care if errors occur in operations and there is no feedback as to why the error took place?
- Is it important to me to see the internal technical details of all operations that are performed on my systems?
- 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?



Third Party Products for Different Needs

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

Freeware/Shareware Applications

These tools 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
- Limited machine list management



Low-End Commercial Machine Management Applications

Most of these tools 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 limited. Designed to provide a broad view of a network and to allow a drill down to a specific machine, these products 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 have 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 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
- 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
- Limited support and training



Dedicated Mass Management Applications

These high-performance products 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 products is somewhat fewer than those of the low-end commercial management applications, but each area is handled in a more comprehensive manner. These products are specifically designed for high-end domain administrators, rather than day-to-day help desk users.

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

Pros:

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

Cons:

- Per-managed node cost makes it more expensive than shareware or low-end mass management products
- Powerful solutions that require extensive planning regarding the exact nature of the change being put into effect
- Logging details may intimidate some administrators; product can be set to output simple success/failure, or all technical details of changes



Next Steps

Lieberman Software's User Manager Pro Suite can help you modify and report on all of the groups, users, passwords, registries, policies, audit settings, and rights in your Windows network en masse. Please contact us for more information on this mass management solution, or to request a fully functional evaluation. Trial software is available at no cost to qualified organizations. For more information, email info@Liebsoft.com.

Summary

The decision of how to mass manage Windows workstation environments depends on the complexity of your enterprise, as well as your stamina and level of interest. Can you handle the tedious process of physically visiting each system or use Microsoft's built-in GUI tools to make changes?

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

In deciding which third party product is right for you, examine the complexity of your requirements, the importance of the feature sets of each product and, of course, your budget.

It is also wise to investigate the internal architecture of the products you are considering to assure yourself that you are acquiring enough horsepower for your needs and that the quality of the product matches the value of the systems you are protecting.

About Lieberman Software

Lieberman Software Corporation, established in 1978 as a software consultancy, has been a profitable, management-owned organization since its inception. The company provides privileged identity management and security management solutions that secure the multi-platform enterprise. By automating time-intensive IT administration tasks, Lieberman Software increases control over the computing infrastructure, reduces security vulnerabilities, improves productivity, and helps ensure regulatory compliance.

Lieberman Software is a Microsoft Gold Certified Partner and has technical partnerships with other industry leaders such as Cisco, Novell, Red Hat, Hewlett-Packard, IBM, RSA, Oracle and Intel. The company is headquartered in Los Angeles, CA, and maintains a regional office in Austin, TX. All product development, testing, and support operations are based in the United States.

For more information, visit www.liebsoft.com
or call 800-829-6263 (USA and Canada) or 01-310-550-8575 (International).