**A Feature-Based Analysis & Comparison of IT Automation Tools:**

**Comparing Kaseya to Windows Server 2003**

**Developed by:**Timothy Cruz

Flavio Suguimitzu

**Advisor:**
Dr. S. Masoud Sadjadi

School of Computing and Information Sciences

Florida International University

**Contact Information:**

sadjadi@cs.fiu.edu,

<http://www.cs.fiu.edu/~sadjadi>

(305)348-1835

**Spring 2010**

**1. Introduction**

**Overview:** Microsoft’s Windows Server 2003 (W2K3) is the sole foundation of every business cyber-infrastructure. Whether it is a school operating with as little as one hundred computers, or a corporation serving one thousand computers, W2K3 is implemented one way or another. The power that can be harnessed by a system administrator is without a doubt worth its price per license. W2K3 has become the industry standard server platform that even Kaseya requires it in order to be used effectively. Although it is unfair to compare Kaseya to a server Operating System, W2K3 is equipped with enough programs to effectively replicate almost 80% of Kaseya’s IT Management and Automation services to such an extent that depending on the client’s need, it can be the logical choice for their business environment. The rest of this report will comprise of in-depth summary and analysis of W2K3’s capability in comparison to Kaseya’s VSA modules.

**Background:** Microsoft is one of the world’s leading computer technology corporations that develops and supports a wide range of software products. They were established in Albuquerque, New Mexico, prior to moving to Redmond, Washington in 1986, on April 4, 1975 by William Henry Gates III (known as Bill Gates). They were first known for selling B.A.S.I.C. (Beginner's All-purpose Symbolic Instruction Code) interpreters. Then on January 13, 2000, Steve Ballmer became the president and CEO of Microsoft. Microsoft is a multi-billion dollar company. The company pulled in $58.4 billion in 2009 alone. (http://www.microsoft.com/msft/reports/ar09/10k\_fh\_fin.html).

Their best product, Microsoft Windows, was first released back in May 22, 1990 with the launch of Windows 3.0.

Windows operating system retains a 91.58% share of the operating system market when compared to other popular operating systems (http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8). In 1993, Microsoft released their first server platform called Microsoft Windows NT Advanced Server 3.1 (http://www.microsoft.com/windows/WinHistorySrvrGraphic.mspx). There were many Windows Server OS developed after Windows NT Advanced Server 3.1, but none was as successful as Windows Server 2003, which was released on April 24, 2003.

Microsoft holds and is invited to many major technical keynotes and conferences around the world. They have been a driving force of keeping companies and individuals educated and well trained in both their technology and the technology of other companies. Through MSDN and TechNet, they inform, train, hold online classes and tutorials, support, and certify people from students to veteran IT administrators. Because of their success in training and development, they retain a vast majority of the customer and user base all over the world. Microsoft is a well know and trust technological brand and will be for years to come.

**Grouping Managed Devices:** Microsoft’s Windows Server 2003 uses Active Directory (AD) to facilitate the management of grouped devices. Anything that AD tracks is considered an object which can constitute a user, resource, system, or service that is managed by AD. AD structures these objects by means of a hierarchical framework. Therefore containers can also be used to group like objects together, such as a set of printers, or a set of users for a specific domain. AD also makes use of a site object, which represents a physical location that hosts networks and contain objects called subnets. Within these subnets there exists a forest, which constitutes a collection of trees and within these trees there are domains.

**Functional Coverage:**

* Architecture
* Auditing and asset management
* Remote control
* Agent procedures
* Monitoring
* Patch management
* Backup and disaster recovery
* Endpoint security
* User state management
* Help desk
* Reporting
* System/user/admin management

**Architecture**

The Windows Server 2003 solution is based on an agent-less architecture. Unlike Kaseya, workstations do not need to have any form of software installed in order to be configured to a Windows Server 2003 and there can be many advantages and disadvantages with this type of architecture. Figure 1.10 shows a simplified model of Kaseya’s architecture and what could be accomplished.



*Figure 1.10*

 With Kaseya’s architecture, a single administrator can manage many different computers onsite and offsite. This is the sole advantage with having an agent based solution. With Windows Server 2003, workstations need to be configured manually in order to be interconnected to the Domain Controller and usually the Domain Controller would be used to manage a set of workstations in one location. Kaseya has the ability to manage multiple physical locations. Kaseya’s only requirement is to have the agent installed and be connected to the internet. Windows Server 2003 requires that the workstation be added to the Domain Controller. It requires the workstation to be on the same network environment as the Domain Controller, and if not, it requires a VPN to be setup in order for the workstation to communicate with the Domain Controller.

 While Windows Server 2003 can accomplish everything Kaseya does, Windows Server 2003 has more requirements and requires more preliminary setup before IT Administrator can commence any management.

**1.2 Auditing & Asset management**

 Auditing provides a way for Windows Server 2003 to track all events, monitor system, access and ensure system security. Windows Server 2003 audits computers through a well known service called Group Policy (GP). GP is a set of rules that allows the administrator to restrict, or give, certain amount of control to users and computers on a network. The way GP audits computers is totally different from Kaseya’s hardware and software auditing. GP’s auditing can only provide the following information:

* Account Logon Events
* Account Management
* Directory Services Access
* Logon Events
* Object Access
* Policy Change
* Privilege Use
* Process Tracking
* System Events

 As shown, most of what GP can audit is based on user and system management. GP can be configured to audit these specified categories in either the “Local Policy” or “Account Policy” for greater depth as to what is audited. An event within each of the previously mentioned category can be set to be audited when it’s either “successful” or “failed”. A report is generated and sent to “Security Log” within Event Viewer.

 Unfortunately, GP cannot audit hardware changes or third-party software changes on networked computers. This makes things tedious for the administrator because it is then required to physically attend each computer and audit the computer manually. Unlike Windows Server 2003, Kaseya has the ability to remotely audit computers and set alarms when certain hardware, or software, is changed.

 Now in Windows Server 2003, there is a way to do limited advance auditing, via scripting, on all computers throughout the network; however, this requires the administrator to know how to develop the script and deploy the script to each individual computer across the network. Also, the audit script won’t be as informative as Kaseya’s auditing module. This gives the upper edge to Kaseya since the administrator can audit and view reports via Kaseya’s VSA.

**1.3 Remote Control**

 Windows Server 2003 comes with built-in remote control and remote assistance technology, but requires more configuration than Kaseya’s Remote Control module. In Kaseya, once the agent is installed and it has reported back to the Kaseya Server, everything is ready and setup to initiate a Remote Control connection with the workstation. In Windows Server 2003, certain aspects need to be covered before Remote Desktop Connection can work correctly, and both local and offsite types of connections will be covered.

By executing mstsc.exe on the run line, the Remote Desktop Connection application appears asking for the Computer Name. Upon clicking the “Options >>” button, the window expands and exposes six different tabs:

* General
* Display
* Local Resources
* Programs
* Experience
* Advanced

In the General tab, the basic logon settings can be entered as well as saving connection settings if this is a workstation that needs to be connected remotely often.

 In the Display tab, the size of the resolution that will be displayed from the remote workstation can be set as well as color quality. If the workstation is being accessed locally then resolution and colors can be maximized as bandwidth might not be an issue. However if the computer will be accessed from an offsite location, then configuring the desktop resolution to be lower than 1024x768 pixels with 16-bit color quality might be the logical choice since image quality

 In the Local Resources tab, the user can configure to receive the sound off the remote computer, use Windows key combinations (such as Alt + Tab) and configure access to local devices and resources. Figure 1.3.0 shows the types of local devices and resources that can be used remotely.



*Figure 1.3.0*

Drives can be mapped as well as any USB drives or networked mapped drives on the remote machine. Printers and clipboard data can be used seamlessly from the local machine to the remote machine.

 The Programs tab can be configured to have certain programs be executed as soon as a remote connection is made. This is equivalent to having Kaseya’s agent-procedures script be executed as a pre-script.

 The Experience tab can be configured to optimize performance based on the connection speed that the remote workstation has as well as the local machine. Certain visual elements can be omitted in order to increase response time. Figure 1.3.1 shows a list of the following properties that can be allowed from allowing desktop background to show to showing the contents of a window while it is being dragged.


*Figure 1.3.1*

 The last tab is the advanced tab and the user can configure the Server Authentication and configure settings to connect through a TS Gateway.

 In comparison with Kaseya’s Remote Control module, Kaseya provides a wider variety of tools to interact with the remote workstation. The ability to FTP and view processes remotely without having to actually ‘login’ gives Kaseya the advantage. Kaseya also provides remote connection to workstations that do not have an agent installed by means of reverse connection. This functionality is aimed towards workstations that are located offsite. Since routers and firewalls use NAT to hide the computers in the LAN, by initiating a reverse connection, this allows the admin to connect to the remote workstation without having to forward any ports, therefore giving a significant advantage over the traditional Windows Server 2003 Remote Desktop Connection application. Kaseya also gives added functionality that is outside the scope of Remote Desktop Connection, such as resetting user login passwords and being able to chat with the Users and interact with them.

**1.4 Automation**

 Windows Server 2003 can be completely automated through the use of scripts written in the Visual Basic Script (.vbs extension) language or in Windows PowerShell. VBS is based on the Active Scripting language and incorporates the Component Object Model to be able to interact with environment, while Windows PowerShell is integrated with the .NET Framework, with the ability of accessing the Component Object Model and Windows Management Interface environments. In Kaseya, they use a module called Agent Procedures. Windows Server 2003 also supports other automation scripts, however they are considered to be third party and therefore do not meet the requirements for this report.

In terms of strength and level of sophistication between VBS, Windows PowerShell and Agent Procedures, Windows PowerShell is the most sophisticated out of all three because it is built on the .NET framework. This opens new doors that Agent Procedures and VBS cannot fathom. Although VBS is sophisticated because it allows a higher degree of scripting; scripting in PowerShell would be any System Administrator’s dream. To be able to script with .NET API and to grasp some of the aspects that Unix/Linux based shells have, such as the pipeline, it makes scripting enjoyable.

Kaseya’s Agent Procedures on the other hand, does allow basic commands such as the “If-Then-Else” and the use of variables and 64-bit commands. Kaseya does not grant users the ability to use a pipeline in order to compound complex commands, and does not give any form of For, Do, While loops or any error handling. Agent Procedures however wins in overall ease of use. Somewhat like Microsoft’s IntelliSense, Agent Procedures gives you a list of possible commands that can be used and this can be proved useful if the API is not available.

 Although experienced UNIX and Windows Administrators might feel like Kaseya is lacking in the scripting department, Agent Procedures can be used to run scripts that are saved on the workstations or Domain Controllers. Therefore, Agent Procedures can interact with the .NET framework for scripting if it calls on pre-written scripts, however neither PowerShell nor VBS can call on Agent Procedures therefore limiting the automation only to its own language.

**1.5 Monitoring**

 In terms of monitoring, Windows Server 2003 contains Event Viewer (EV). Using the event logs in EV, one can gather information about hardware problems, software problems, system problems, and security events. Custom logs can be configured for certain applications or other events. An example of how EV looks can be viewed in Figure 1.5.0. EV contains the following five base categories:

* System
* Security
* Application
* Setup
* Forwarded Events



*Figure 1.5.0*

 EV has the option of remotely connecting to a computer and pulling the remote computer’s log files, making it useful for administrators. Unlike Kaseya’s Monitoring module, EV is unable to create alarms when certain thresholds are reached, either by software or hardware issues. For an administrator to check on each individual computer on the network, he would have to remotely connect to each individual EV through the Windows Server 2003’s EV. This makes things harder for the administrator in a corporate environment when the individual has to take care of hundreds and hundreds of computers.

**1.6 Patch Management**

 To administer patches and hot fixes for Windows NT environments, Windows Server 2003 utilizes Windows Server Update Service (WSUS). This service is downloaded as a separate install from the Microsoft website and not included in the default install of Windows Server 2003. Like Kaseya’s Patch Management module, WSUS cannot be used on any non-Windows system.

 WSUS allows an IT administrator to download Microsoft updates to a local server. Once on the local server, it will then push the specified updates to all the computers on the network. This helps, in the corporate model, to reduce redundant network traffic. The administrator also has the option to choose which updates get pushed to the specified network computers. This is useful so that unimportant updates and unnecessary language packs do not get installed to all the computers and save hard drive space. One of the best features of WSUS is the ability to push certain updates into a “test group” prior to sending the update to all machines on the network (Figure 1.6.0) (http://technet.microsoft.com/en-us/wsus/default.aspx). This allows the administrator to make sure the updates will not cause downtime within the work environment.



*Figure 1.6.0*

 Like Kaseya’s Patch Management, WSUS contains is the ability to maintain and update roaming clients. This greatly helps companies who use a lot of mobile users. Also, Kaseya and WSUS are capable of creating reports. The reports are used to view the status of individual updates or individual computers. The reports can be emailed or stored on the server locally. There is also an ability to email the administrator when updates are available to be viewed.

**1.7 Backup & Disaster Recovery**

In Windows Server 2003, the Backup Utility (BU) software is only limited to the local machine. Unlike Kaseya’s Backup and Disaster Recovery (BUDR) module, the Backup Utility cannot backup workstations. There is a workaround this issue; however it is not automated like Kaseya’s BUDR module. The alternative workaround will be explained, but first Windows Server 2003 Backup Utility will be explained.

 Windows Server 2003’s BU has 5 different types of backup that can be made. These types are:

* Normal Backup
* Incremental Backup
* Differential Backup
* Copy Backup
* Daily Backup

A Normal backup creates a copy of all the files that have been selected to be backed up and it flags each file as being already backed up. This is usually the preliminary method chosen by administrators when initiating the first round of backups. Backups such as Incremental and Differential usually need a baseline such in order to function correctly.

Incremental backup saves only the files that have been modified or created since the last Incremental or Normal backup. Once again, just like the Normal backup, as the Incremental backup copies each newly created or modified file, it flags each one as being backed up during this Incremental Backup. One disadvantage to this is that since the Backup utility would “need the initial Normal backup and all incremental backup files; it can be time-consuming to recover files.” (Kristofer Gafvert, ilopia.com)

A Differential backup is like the Incremental backup in which it only backs up files that have been either modified or created since the last normal backup, however it does not flag the files that have been backed up. This method is more “time-consuming” (Gafvert) in comparison to an Incremental backup, but when it comes to time to restore time-critical data, it is “faster to restore because all you need is the last normal backup and the last differential backup.”(Gafvert)

A Copy backup is a simple copy of all files that have been selected but does not flag the files once the backup has been done.

Lastly a Daily backup copies all the files that have been changed throughout the day, but does not flag the files.

In Kaseya’s BUDR module, everything mentioned above can be done. However Kaseya’s BUDR can initiate backup of workstations and have these images saved on the Kaseya server. BUDR also has embedded a fully automated scheduler, in which backups can be made automatically at any time of day without the need of any interaction from the user or administrator. While Windows Server 2003 BU does not have this aspect embedded in the utility, Windows Server 2003 along with Scheduled Tasks, another utility built in Windows Server, can be used to schedule such tasks.

One aspect that Kaseya’s BUDR module triumphs over Windows Server 2003’s BU is the ability to conduct universal restores. This feature allows any system administrator to restore systems with “dissimilar hardware or even virtual machines, eliminating the procurement and interoperability factors when trying to get the business back up and running quickly.” (http://www.kaseya.com/features/backup.aspx) Windows Server 2003 does not come with any utility that will replicate BUDR’s universal restore, unless third-party software is implemented such as Acronis Backup & Recovery 10 Advanced Server Virtual Edition.

**1.8 Endpoint Security**

 In the cyber world, security is one of the most important aspects a company looks for when trying to build their computer infrastructure along with reliability and performance. When looking into Kaseya’s Kaseya End point Security (KES) module, all the features surpass Windows Server 2003. Windows Server 2003 has no integrated Antivirus like KES. Therefore Kaseya wins by default. If your Windows Server 2003 environment requires a scheduled scan for infections; a separate third party suite would be required in order to accomplish this. However what KES strives in one aspect, Windows Server 2003 surpasses in another. In figure 1.8.0, the amount of computers infected by Trojan viruses

**

*Figure 1.8.0 (Source www.webroot.com)*

While viruses themselves are completely harmless, the harm comes when the batch of code is executed, and this is the number one reason why computers get infected in the first place. Therefore the best method to prevent infection is to refrain from executing these programs. And while end-users get educated about which programs to trust and which not to trust, there has been a rise in Trojan Antiviruses or Rouge Antiviruses. These are antivirus programs that hide their true intentions and present the user with a false statement in order to get the end-user to click ok, and upon this execution, the virus will install itself onto the system obliterating its stability. Some Trojans are such conniving programs, that any button, ranging from “Ok” or “Cancel” will automatically execute the program and infecting it. Although KES can catch these programs, if the antivirus cannot catch it in time, it creates a risk factor until it can. So how is Windows Server 2003 triumphant in this area?

 In Windows Server 2003, AD can setup users with a “limited users” account. According to Microsoft’s knowledge base, “the limited account is intended for someone who should be prohibited from changing most computer settings and deleting important files. They generally cannot install software.” (Microsoft) No antivirus can offer this level of protection. While disadvantages equate to nuisances on part of both administrator and the person trying to install a legitimate program but cannot due to this restriction, it is the best defense any computer has to avoid executing malware.

**1.9 User State Management**

 User State Management is well developed within Windows Server 2003. Through different programs within Windows Server 2003, an administrator can set up a networked printer, map network drives, and other specific desktop policies through Group Policy (GP). Also through GP, an administrator can set up desktop migration, which provides backup, restore and migration of roaming profiles. Roaming profiles are profiles that contain user settings, application settings, and system settings within a user account. Unfortunately, Windows Server 2003 does not have a native way of assigning power management policies and wake on LAN policies like Kaseya’s Desktop Policy & Migration module.

 Through the use of Print Management console (Figure 1.9.0) within Windows Server 2003, administrators can manage printers, check for errors, and allocate printer access to users. With Print Management and Group Policy, an administrator can limit printing access to only certain computers or certain users. Unlike Kaseya’s Desktop policy module, Windows Server 2003 is unable to remotely install printer drivers. This forces the administrator to physically go, or remotely connect, to each individual computer and install it. It can however provide the drivers and the network path remotely making installation of the printer easier than loading in a CD every time to install the printer.

 

*Figure 1.9.0*

 Through the use of Map Network Drive Wizard (Figure 1.9.1), an administrator can map out network drives. After creating the mapped network drive, the administrator can then use GP to allocate certain files and/or folders to different users. Through GP, configurations can be set to allow read and write access. It is also quite possible to allocate a certain quota if the administrator has given write access to the user.



*Figure 1.9.1*

 Roaming profiles can be configured within GP. Roaming user profiles are stored on the server and then they are loaded when a user logs on. This allows users to use any computer within the network and work in the same consistent environment. An administrator can set specified security settings on the user so that any computer the user would log into, they would retain the same security settings due to roaming profiles. Through folder redirection, important user folders, like My Documents, Start menu, Desktop, can be redirected.

**1.10 Help Desk**

Kaseya’s Help Desk is a module that allows service representatives to help agent-installed workstations. This includes tracking and managing incidents, problems, and service requests, as well as an integrated ticketing system and a searchable integrated Knowledge Base and Known Error database.

 Unfortunately Windows Server 2003 does not provide this type of functionality. It needs to be emphasized that Windows Server 2003 is more of an Operating System and not an IT Automation solution.

**1.11 Reporting**

By nature, Windows Server 2003 does not have any sort of native reporting system. Kaseya’s Info Center is well developed and gives a centralized location to obtain reports for all modules within Kaseya. With Windows Server 2003, an administrator needs to obtain report-like information by going to each specific console or application. Windows Server 2003 does not have a solution to provide customized reports. This feature is a big downside if the administrator needs to give detailed reports about the state of the network and all the computers on the network. A possible viable option is to use Event Viewer and monitor certain application, security, user, and system issues. However this only covers if a problem arises and it’s not as detailed as most administrators want it to be. The only option administrators have is to look at third party solutions. This gives Kaseya’s Info Center the upper edge when comparing it to Windows Server 2003.

**1.12 System/User/Admin Management**

System/User/Admin Management is a strong point within Windows Server 2003. With the power of AD (AD), System/User/Admin Management is a powerful tool for managing users within an environment. AD is known as a “network service” that allows administrators to assign policies, stores information and settings in a central database, and can administer different user accounts across networks. By using AD, one can set the state of a user’s work environment once and then rely on Windows Server 2003 to continually enforce the same settings.

With user accounts can be created, edited, and deleted within AD. At first, it’s a bit complicated to define new users because the administrator needs to plan out levels of access rights and groups during the architect stage of Windows Server 2003. Afterwards, this becomes easier by putting user accounts into groups. Groups are a collection of users, computers, and possibly other groups. Like Kaseya’s “User Roles”, AD can organize user accounts by groups. One can create users without putting them in a group; however, it’s a better practice to put users into groups for the sake of organization and easier implementation of security policies.

There are two types of user accounts within Windows Server 2003, a domain account and a local account. For the sake of discussing AD, only domain account will be mentioned since local accounts are not associated with AD. Domain accounts are the user and group accounts that are stored within AD. It’s the “key” to enter and log into the domain of a network. By managing domain accounts, an administrator can restrict access to certain computers or certain subnets within a network. Administrators can also limit access within certain time frames to improve on security or to prevent users from logging in during maintenance times.

**1.13 Usability**

 In viewing Windows Server 2003 as an operating system and the types of services it can give to workstations in a business environment, it fulfills its purpose. Unlike Kaseya’s Virtual System Administrator, Windows 2003’s utilities and programs are not web based. Therefore the only alternative to be able to access the server would be via a remote connection.

Windows Server 2003 is also not for the weak minded. In order to configure it correctly, the system administrator would need to be knowledgeable on many topics. AD is a main topic that needs to be mastered in order for the domain controller to function correctly and to have all workstations configured properly. Learning VBS or PowerShell is also another topic on the list that needs to be mastered in order to have repetitive and time-consuming administrative tasks performed automatically, giving the administrator more time to focus on other priorities.

These different utilities and programs only focus on accomplishing specific tasks, and they are integrated into a single domain. Unlike Kaseya’s VSA that allows a single administrator to control multiple locations from a single website. If a system administrator were to control multiple locations, they would need to remotely log into each domain controller, therefore there is no synergy.

**1.14 Reliability**

 Windows Server 2003 is reliable; however, it’s not the best solution. According to an article by windowsitpro.com, in which they compare multiple server operating systems, they state, “[T]he new king of downtime, was Windows 2000 Server (9.86 hours of downtime), followed in the next-to-last position by Windows Server 2003 (8.90 hours). The sole reason why Windows Server 2003 obtained a low rank was because of security issues. Of course, saying all this is not preventing administrators from using the product. According to a latest poll, Windows retains 91.58% of the market share. This poll includes all Windows OS. Windows Server 2003 is the go to product for administrators from corporate models to small business models. If Windows Server 2003 does not contain a specified functionality, it does support the ability for an administrator to install third party tools and software on the platform. The latest trend for most administrators is to use other IT Automation tools on top of Windows Server 2003 for better functionality and support. Since Windows Server 2003 also is used, in most situations, as a DNS, HDCP, File Server, Domain Controller, etc., most administrators opt to use other IT automation tools on top of the Windows Server 2003 platform.

**1.15 Performance**

The performance of Windows Server 2003 vastly on the type of edition you get. Windows Server 2003 contains four separate editions: Standard Edition, Enterprise Edition, Datacenter Edition and Web Edition. (http://media.wiley.com/product\_data/excerpt/51/07645492/0764549251.pdf) All the editions serve their specific purposes well and the performance of each vastly depends on the hardware that is used. The Standard Edition is designed for small- to medium-sized businesses. It can use a maximum of four microprocessors and no more than 4GB of memory is allowed. However, the strongest version, out of the four, is the Datacenter Edition that supports up to 32 microprocessors in a single server and up to 64GB of memory.

 All editions are responsive since Windows Server 2003 mandates that a portion of the memory and CPU is allocated towards the operating system. This prevents other applications from hogging up memory/CPU usage and keeps the operating system stable.

**1.16 Supportability**

Since Windows Server 2003 is not an IT Automation solution and there is no help desk software integrated in Windows 2003, there is no supportability at all. Workstations would only warn of an error, when it actually occurs. The system administrator can see what caused the error by viewing Event Logs and see what caused the issues. Unfortunately unless third party software is used to integrate a support desk, using Windows Server 2003 alone cannot fulfill this task.

**2. Comparison and Discussion**

**2.1 Evaluating and Discussing *Windows Server 2003***

|  |  |  |
| --- | --- | --- |
| 1 | Architecture**Rating: 3** | *Required more configuration than Kaseya per workstation and the web-less interface makes it difficult to administrate over remote locations.* |
| 2 | Audit & Asset Mgt**Rating: 3** | *Able to audit user profiles and trends; however, lacks the ability to audit hardware and third-party software.* |
| 3 | Remote Control**Rating: 3** | *Connecting to remote locations requires NAT routing to be implemented.* |
| 4 | Automation**Rating: 4** | *VBS and PowerShell scripting is sophisticated; however, unless used with another utility, it’s only limited to the local machine.* |
| 5 | Monitoring**Rating: 2** | *Inability to monitor multiple computers from the server without the use of third-party tools.*  |
| 6 | Patch Mgt**Rating: 4** | Very strong patch management utilities within WSUS and the ability to allocate updates to a test group. |
| 7 | Backup & Disaster Recovery**Rating: 3** | *Simple interface and straightforward backup capabilities, but no simple interface to configure all workstation’s backups from a single interface.* |
| 8 | Endpoint Security**Rating: 3** | *Limited Users template is the best line of defense, but needs to rely on third party antivirus software.* |
| 9 | User State Mgt**Rating: 3** | *Group Policy is a powerful tool that allows administrators to create roaming profiles and security policies on each user account.* |
| 10 | Helpdesk**Rating: 1** | *Because there is no help desk utility unless a third party program is implemented* |
| 11 | Reporting**Rating: 1** | *Universal reporting is almost nonexistent and hard to obtain reports over multiple consoles and applications.* |
| 12 | System**Rating: 4** | *AD very strong and versatile tool to manage users and system policies.* |
| 13 | Usability**Rating: 2** | *Strong learning curve and time consuming configuration required for an infrastructure to run correctly.* |
| 14 | Reliability**Rating: 3** | *Decently reliable; however, average downtime makes it somewhat unattractive.*  |
| 15 | Performance**Rating: 4** | *Strong performance, depending on the edition and hardware.*  |
| 16 | Supportability**Rating: 1** | *No help desk.* |

**2.2 Rating Results Explanation/Discussion:**

*Individual Solution Comparison Rating System Table*

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | ***Kaseya*** | ***Windows Server 2003*** |
| 1 | Architecture | 5 | 3 |
| 2 | Audit & Asset Mgt | 4 | 3 |
| 3 | Remote Control | 5 | 3 |
| 4 | Automation | 4 | 4 |
| 5 | Monitoring | 3 | 2 |
| 6 | Patch Mgt | 5 | 4 |
| 7 | Backup & Disaster Recovery | 5 | 3 |
| 8 | Endpoint Security | 5 | 3 |
| 9 | User State Mgt | 4 | 3 |
| 10 | Helpdesk | 4 | 1 |
| 11 | Reporting | 5 | 1 |
| 12 | System | 5 | 4 |
| 13 | Usability | 5 | 2 |
| 14 | Reliability | 3 | 3 |
| 15 | Performance | 3 | 4 |
| 16 | Supportability | 5 | 1 |
|  | **Total** | **70** | **44** |

 Overall Kaseya’s versatility surpasses that of Windows Server 2003 when it comes to automation. However it cannot be a stand-alone solution; it needs to be installed on top of a Windows NT based platform. Therefore they work together flawlessly but if Kaseya is missing Windows NT, it crumbles as an IT Automation solution. Windows Server 2003 however does not need Kaseya in order to operate as a stand-alone solution. This fact appeals to a greater number of companies, especially the small companies under 100 workstations that do not require the robust automation that Kaseya offers. Kaseya was designed as an IT Automation solution; whereas Windows Server 2003 was engineered as a server operating system. Kaseya’s user-friendly GUI and seamless integration of their multiple modules ranks them high as an IT Automation solution.

**3. Glossary**

**Active Directory (AD**) - Active directory is a network service that acts as a directory structure. It is used on Microsoft Windows based servers to store information and data about networks, domains and users.

**Backup Utility (BU**) - Backup Utility is Microsoft's solution for backup and recovery. It is strictly limited to the local machine and is unable to backup or recover computers remotely.

**Event Viewer (EV)** - Event Viewer is Microsoft's solution in letting administrators and users view the event logs of local or remote machines.

**Group Policy (GP)** -Group Policy is a set of rules that allows the administrator to restrict, or give, certain amount of control to users and computers on a network.

**Map Network Drive Wizard** - Map Network Drive Wizard is a utility that allows users to connect and configure hard drive access through the network.

**Microsoft Developer Network** (**MSDN**) - The Microsoft Developer Network is Microsoft's service that allows it to inform, train, and supply tools to developers on all Microsoft products.

**PowerShell** -PowerShell is an extensible command-line scripting language.

**Print Management** - Print Management is Microsoft's solution to manage and deploy network printers.

**Remote Desktop Connection (RDP)** - Remote Desktop Connection is a Windows based tool that allows users to connect to applications and date on a remote computer.

**TechNet** - TechNet is Microsoft's program and resource used to provide technical information, news, and events to IT professionals.

**Virtual Private Network (VPN**) - Virtual Private Networks are [computer network](http://en.wikipedia.org/wiki/Computer_network)s that remotely connects to another underlying computer network as if it was physically connected to it.

**Virtual System Administrator (VSA)** - Kaseya's Virtual System Administrator is their remote web-based environment that helps users to administrate, diagnose, repair, monitor, and update computers that are linked to Kaseya's agent technology.

**Visual Basic Scripting (VBS)** - Visual Basic Scripting is a Windows based scripting language. It originated as a limited variation of Microsoft's Visual Basic programming language.

**Windows Server Update Service (WSUS)** - Windows Server Update Service allows administrators to maintain and deploy Microsoft hot fixes and updates, released through Automatic Update, to computers in a corporate environment. **4. Acknowledgements**

Special thanks to Student MSDN and Kaseya for their support in providing software for this research and demo purposes.

**5. References**

Bilic, Nino. "System Event Viewer Tips." *Microsoft TechNet: Resources for IT Professionals*. Web. 26 Apr. 2010. <http://technet.microsoft.com/en-us/library/aa996105%28EXCHG.65%29.aspx>.

Bilic, Nino. "System Event Viewer Tips." *Microsoft TechNet: Resources for IT Professionals*. Web. 26 Apr. 2010. <http://technet.microsoft.com/en-us/library/aa996105%28EXCHG.65%29.aspx>.

"Chapter 1: Windows 2003 Basics." Web. <http://media.wiley.com/product\_data/excerpt/51/07645492/0764549251.pdf>.

Edwards, Mark J. "Windows Server: The New King of Downtime." *Windows IT Pro - The Leading Independent Community for IT Pros*. Web. 26 Apr. 2010. <http://www.windowsitpro.com/article/interoperability/windows-server-the-new-king-of-downtime.aspx>.

Gafvert, Kristofer. "Backup Windows Server 2003." *FAQ and Articles for Windows Server 2003, C#, SQL Server*. Web. 26 Apr. 2010. <http://www.ilopia.com/Articles/WindowsServer2003/Backup.aspx>.

Huggins, Diana. "SolutionBase: Creating a Windows Server 2003 Audit Policy." *TechRepublic Articles*. Web. 26 Apr. 2010. <http://articles.techrepublic.com.com/5100-22\_11-6028421.html>.

Microsoft. "Introduction to Group Policy in Windows Server 2003." Web. Apr. 2003. <http://download.microsoft.com/download/0/0/4/0044470e-5f3a-4569-9255-91f932e4da3b/gpintro.doc>.

Microsoft. "MSFT Annual Report 2009." *Microsoft Corporation*. Web. 26 Apr. 2010. <http://www.microsoft.com/msft/reports/ar09/10k\_fh\_fin.html>.

Microsoft. "Types of User Accounts." *Microsoft Corporation*. Web. 26 Apr. 2010. <http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua\_c\_account\_types.mspx?mfr=true>.

Microsoft. "Windows Products and Technologies History: Windows Server Timeline." *Microsoft Corporation*. Web. 26 Apr. 2010. <http://www.microsoft.com/windows/WinHistorySrvrGraphic.mspx>.

Microsoft. "Windows Server Update Services Home." *Microsoft TechNet: Resources for IT Professionals*. Web. 26 Apr. 2010. <http://technet.microsoft.com/en-us/wsus/default.aspx>.

NetMarketShare. "Operating System Market Share." *Market Share for Browsers, Operating Systems and Search Engines*. Web. 26 Apr. 2010. <http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8>.