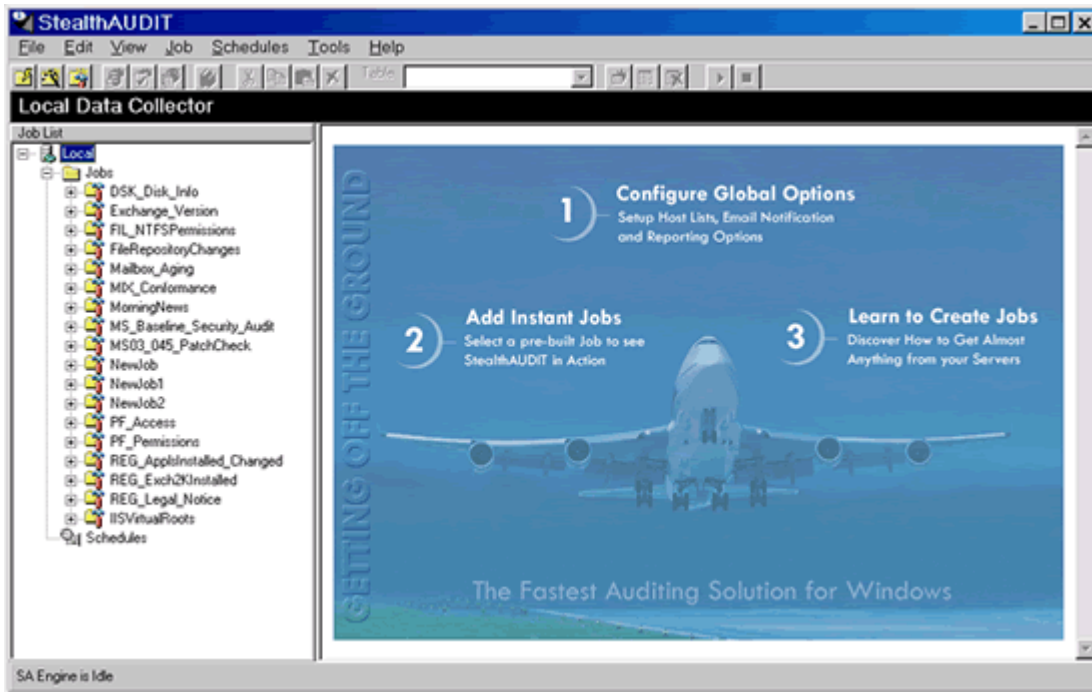


StealthAUDIT

Adaptive Real-Time Windows Auditing



Customers are discovering the many benefits of using StealthAUDIT. StealthAUDIT has been described as the “Swiss Army Knife” of Windows Auditing tools.



STEALTHbits Technologies has engineered a number of “snap-in” data collectors capable of retrieving data from almost every Windows data repository. Data collectors are included for the File System, Disk, Active Directory, Patch Checking, Performance Monitor, Registry, Event Logs, INI Files, Users & Groups, among others. An optional data collector for

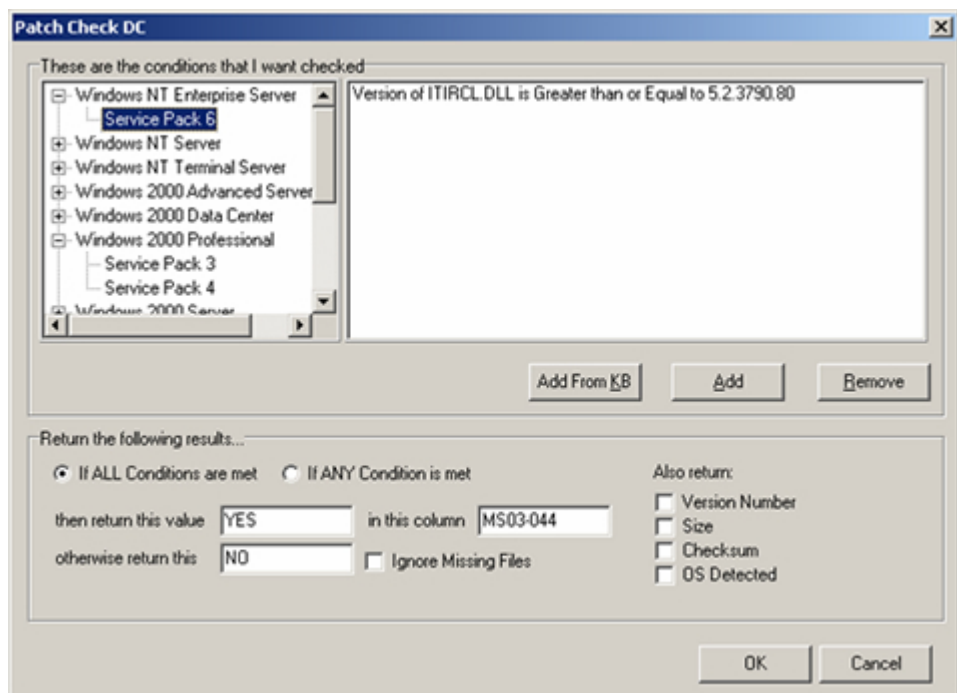
querying the Exchange Store is also available.

By combining these data collectors with a fast real-time retrieval engine and a single user interface, you have a powerful tool that can replace numerous Windows utilities, Resource Kit tools, freeware tools, and custom scripts. One customer observed “the most powerful thing about StealthAUDIT is that it helped solve problems I didn’t know I had!”

Here are a few examples of how some Fortune 1000 customers are using StealthAUDIT today;

"Patch and Hot Fix Verification"

One company recently had to deploy the Microsoft MS03-039 security patch across 9,700 Windows Hosts. They use Microsoft's SMS tool for deployment. They had assumed a patch success rate of 95%. They used StealthAUDIT for patch verification and found they had attained a success rate of 72%. In less than four hours,



StealthAUDIT

Adaptive Real-Time Windows Auditing



StealthAUDIT was able to determine which hosts were missed, shutdown, or did not have SMS clients. The customer received a list indicating which hosts were left un-patched, allowing them to rapidly follow-up with a second patch run.

"Server Consolidation"

StealthAUDIT was recently used by a customer to assist with merger of two IS environments into one. StealthAUDIT was able to quickly provide all the information required to merge Active Directory domains and a very complex Exchange 2000 environment. The information provided by StealthAUDIT enabled administrators to better plan, and budget for the exercise and to help identify which servers could be consolidated in the new environment.

"Exchange Management"

Many customers use StealthAUDIT's Exchange Store Data Collector to better manage very large email environments. StealthAUDIT can rapidly inventory both a Private and Public Folder information store providing detailed information including structure, contents, usage statistics, and permissions.

"Proactive Management"

STEALTHbits created an "Exchange Morning News" job at a customer's request. This job scans all Exchange Server event logs for all errors and warnings, reports on the status of MBCLEAN processes, checks and reports on the Backup status, AntiVirus messages, and the service status for each Exchange Server. This job is scheduled to run daily at 5:00am posting the results to an Intranet site, and emailing reports to the Exchange Administration team. The work automated into this job has saved one administrator 4hrs of daily effort that has been redirected to other tasks. The "Morning News" report can easily be adapted to any critical server that needs to be regularly monitored.

Mailbox Size Report
AUTHOR: StealthAUDIT
DESCRIPTION: Reports size of mailboxes by message count and total size

Mailbox Sizes (by Server)

DisplayName	MessageSize	MessageCount	StorageWarning
HOST : MAIL (COUNT=5)			
Administrator	0.01	15	No check
bruces	0	0	No check
chris	0	1	No check
darlenes	0	1	No check
System Attendant (eval)			

Data accurate as of: 9/18/2003 11:35:58 AM

Produced by StealthAUDIT. Copyright STEALTHbits Technologies, 2001 - 2003

"Security Policy Adherence"

StealthAUDIT is being used by security groups in a number of organizations for vulnerability assessment and security policy adherence. StealthAUDIT is user adaptable and real-time, unlike most security assessment tools. This permits security groups to build organizational specific security audit jobs rather than having to use pre-canned scripts that are inflexible. StealthAUDIT is able to automatically email reports directly to the security group once the job is run.

"Incident Management"

Machines vulnerable to Blaster Worm
AUTHOR: StealthAudit
DESCRIPTION: Machines that do not have Bulletin MS03-026 installed

Vulnerable Hosts

HOST	MS03_026
ZEUS	NO

(NOT (MS03_026 = 'YES'))
Data accurate as of: 10/24/2003 11:40:12 AM

Produced by StealthAUDIT. Copyright STEALTHbits Technologies, 2001 - 2003

StealthAUDIT was recently used by a customer during the Blaster worm crisis. STEALTHbits created a job that would identify each host vulnerability, as well as checking for the latest AntiVirus DAT file, and whether or not the host contained the worm's signature. The Job was scheduled to run every 4hrs across 4,700 Windows Hosts. This allowed StealthAUDIT to perform change audits providing the customer with detailed information on the progress of the Blaster worm in their environment. This information

StealthAUDIT

Adaptive Real-Time Windows Auditing



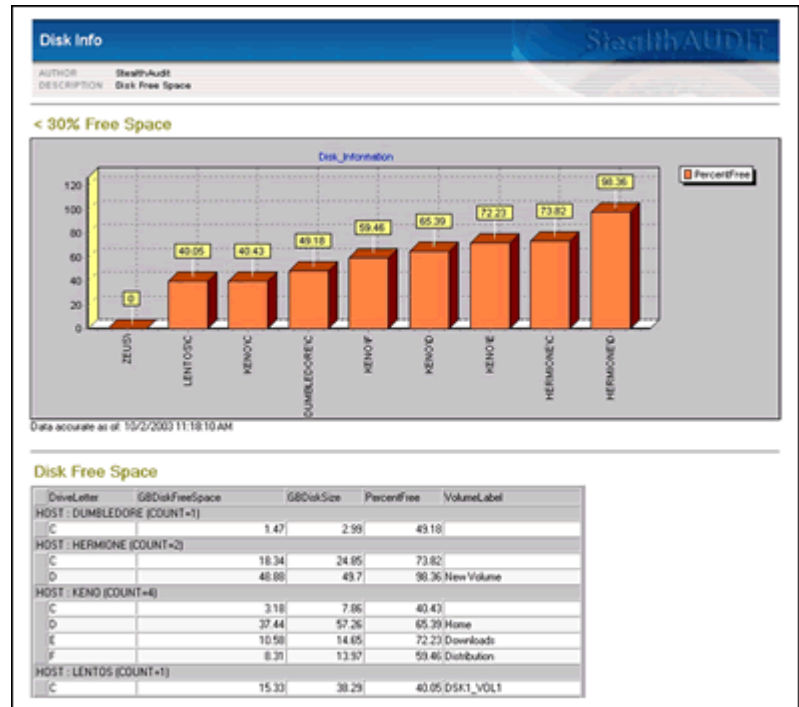
was used by the customer to determine what actions needed to be taken to perform containment and control. The information provided by StealthAUDIT was information the customer would not have otherwise had. As the customer so aptly stated “ You need to see the fire in order to fight it. StealthAUDIT let us see the fire.”

“Storage Management”

StealthAUDIT is being used by many customers to automate the process of disk space monitoring. By creating jobs and scheduling them, StealthAUDIT is able to proactively report on disk space consumption empowering administrators to identify dangerous trends and take action.

“Workstation Image Verification”

StealthAUDIT’s conformance feature permits customers to verify that new workstations created from an image are conforming to standard. By creating a “reference” host to be used by StealthAUDIT as the baseline, jobs can be created that will automatically compare all new imaged hosts against the reference host. The resulting differences are then output to a report detailing any differences. This job could be scheduled to run on a regular basis to assure end-users are not making “unauthorized” changes to the environment.



“Change Management”

Application Change Report
AUTHOR: StealthAUDIT
DESCRIPTION: Reports application changes for the last 24hrs

Change Deltas

CHG_ID	SOURCE	InstalDate	DisplayName	DisplayVersion
HOST : CHRISTOPHER (COUNT=86)				
1	BEFORE	8/12/2003 9:46:03 PM	Command & Conquer Generals	
1	AFTER	8/12/2003 9:46:29 PM	Command & Conquer Generals	
15	BEFORE	8/12/2003 8:03:01 PM	Windows Media Encoder 9 Series	
15	AFTER	8/12/2003 8:02:28 PM	Windows Media Encoder 9 Series	
16	BEFORE	8/12/2003 9:46:03 PM	Command & Conquer Generals	
16	AFTER	8/12/2003 9:46:29 PM	Command & Conquer Generals	
17	BEFORE	8/12/2003 8:01:49 PM	DA0	
17	AFTER	8/12/2003 8:01:50 PM	DA0	
19	BEFORE	8/7/2003 6:22:12 PM	Windows XP Hottix (SP2) Q328210	
2	BEFORE	8/12/2003 8:02:28 PM	Windows Media Encoder 9 Series	
2	AFTER	8/12/2003 8:03:01 PM	Windows Media Encoder 9 Series	
20	BEFORE	8/7/2003 6:27:58 PM	Windows XP Hottix (SP2) [See Q329048 for more information]	
21	BEFORE	8/7/2003 6:21:28 PM	Windows XP Hottix (SP2) [See Q329115 for more information]	
22	BEFORE	8/7/2003 7:52:37 PM	Windows XP Hottix (SP2) Q327979	
23	BEFORE	8/13/2003 12:52:41 AM	Operation Flashpoint uninstall	
24	BEFORE	8/20/2003 3:26:32 PM	Risk 2	
25	BEFORE	8/7/2003 7:50:13 PM	Windows XP Hottix (SP2) Q322011	
26	BEFORE	8/7/2003 6:30:02 PM	Windows XP Hottix (SP2) Q331953	
27	BEFORE	8/7/2003 6:23:05 PM	Windows XP Hottix (SP2) Q810965	
28	BEFORE	8/7/2003 6:24:35 PM	Windows XP Hottix (SP2) Q810577	
29	BEFORE	8/7/2003 6:21:06 PM	Windows XP Hottix (SP2) [See Q329834 for more information]	
3	BEFORE	8/12/2003 8:01:50 PM	DA0	
3	AFTER	8/12/2003 8:01:49 PM	DA0	

StealthAUDIT is providing change control for a number of customers. One of STEALTHbits customers is using StealthAUDIT’s change control feature to report changes between their development and certification environments. During the development cycle of their “in-house” applications, they often found the development and certification environments “out of sync”. They would find themselves having to perform time consuming analysis, or complete restores to synchronize the environments. StealthAUDIT is able to produce a difference report in minutes indicating the specific differences between the two environments.

“Ad hoc Queries”

StealthAUDIT empowers administrators to retrieve virtually any type of information that might be needed from a Windows host. Administrators rely on accurate real-time information to perform their

duties, especially when responding to a crisis situation. StealthAUDIT empowers them to retrieve the real-time information they need, and quickly present it in a meaningful user presentable report.

StealthAUDIT

Adaptive Real-Time Windows Auditing



“Instant Jobs”

StealthAUDIT currently contains over 90 “Instant Jobs” that have been created to automate many of the routine administrative queries regularly made by administrators. Most customers will run an instant job, and then adapt it to their specific requirements. Many customers have found Instant Jobs to retrieve information they didn’t know was previously available to them. The following table is a list of some of the “Instant Jobs” bundled with StealthAUDIT.

Instant Job Name	Description
AD_Fragmentation	AD Size, Freespace and Frag reporting enabled
AD_Size_Location	Disk Space consumed and location of ntds.dit file
E2K_E2K3_Quota_Size	Exchange Priv and Pub size limits
E2K_Queue_Size	Reports Exchange 2000 Messages/minute, send and receive Queue Sizes.
E2K_Service_Status	Indicates the service status for all Exchange 2000 related services.
MorningNews	Exchange Server App & Sys Logs, checks MBClean and Veritas Backup Exec events
Exchange_55_Health	CPU Util, Message Traffic, Service Status, Store Disk Space, Store Frag, Store Size, Trans logs
Exchange-Mailbox_Warning_Limits	Mailbox Sizes, Storage Limits
Mailbox_Security	Mailboxes with potential Security problems
Message_Store_Properties	Displays General properties for Exchange 2000 Private and public message stores.
BIOS_Information	Retrieves System BIOS information through WMI
CD_Drive_Information	Enumerates CD Drive Information through WMI
Compaq_NIC_Settings	Returns the NIC settings for a Compaq Netflex network adapter
NIC_Information	Name, IP, DHCP, Name Server, and NIC ID
Number_of_CPUs	Number installed cpus from registry
Printers	Enumerates installed printers including Driver, and share name
Processor_Information	CPU information from registry
Serial_Number	Returns system serial number via WMI
Sound_Card_Information	Retrieves Sound Card Information through WMI
Video_BIOS_Information	Retrieves Video BIOS Information through WMI
IIS_Lockdown	Provides an IIS Lockdown report, and URLSCAN version and INI settings
IISServices	Checks state of IISADMIN, MSFTPSVC, and W3SVC
IISVersions	Returns version of INETINFO
IISVirtualRoots	W3 and FTP virtual roots from registry
IIS_Log_File_Sizes	FTP and W3 Service Log File details
Installed_Hotfixes	Enumerates Installed Hotfixes from the registry
MS03_039_PatchCheck	Verifies the patch state for Microsoft Security Patch MS03-039
MS03_040_PatchCheck	Verifies the patch state for Microsoft Security Patch MS03-040
W32SobigF_Scan	Checks for Trayx in registry, and winppr32.exe in System32\drivers
W32_Blast_Worm_Scan	Patchcheck on MS03_26, Search for msblast.exe and if its running
W32_Swen_Worm_Scan	Identifies hosts infected or vulnerable to the Swen Worm Virus.
SQLVersions	Returns SQL version from registry
Disabled_Accounts	Reports all disabled accounts
Group_Accounts	Local and Global Group Account Information
Monitor_DomainAdmin_Group_Change	Displays members of DomainAdmin group, and subsequent changes

StealthAUDIT

Adaptive Real-Time Windows Auditing



User_Accounts	User Account List.
User_Group_Security_Policy	Lists Security Policy settings for Users and Groups.
User_Profiles	Reports on saved profiles and disk consumption
Applications_Last_Used	Returns a list of installed apps and the date last accessed
Applications_Installed	Returns list of installed apps from registry
Auto_Update_Settings	Returns state of auto-update service and settings
BootINI_Settings	Parses the contents of the Boot.ini file
Browser_Settings	Returns browser service settings from registry
DiskReports	Reports disk usage and low disk
Disk_Info	Reports free disk space
Domain_Membership	Displays the Domain name for each Host.
Environment_Settings	OS Environment settings from the Registry
Logical_Drive_Mappings	Enumerates logical drive mappings
MDAC_Versions	MDAC version from registry
Memory_Status	Memory installed and available
PageFile_Settings	Reports the Pagefile settings
SNMP_Community_Names	Retrieves the configured SNMP community Name(s)
ServerInfo	Collection of items: CPUINFO, Crash Recovery settings, Disk Info, NIC Info, OS Info, Windows Misc info
Service_Driver_Listing	Lists all service drivers and their run state through WMI
Service_Packs_Installed	Displays both Windows service packed and non-service packed hosts.
System_Failure_Information	Displays the OS Settings in the event of a system failure
Terminal_Services_Installed	Retrieves the Version information of Terminal Services.
Time_Zones	Retrieves the time zone information for each host.
Uptime	Generates uptime from PerfMON
All-Server_Morning_News	This Job is designed to be run every night as a scheduled Job. The Job reports on Errors and Warnings from your eventlogs, including Veritas and Norton Anti-virus messages. You can customize this for your backup and Anti-Virus solutions.
HealthStats	Reports on Memory, Disk, Processor Queue length, and time
Reboot_History	Reports the Reboot events from the Event Viewer.
Windows_Log_File_Sizes	Reports on Eventlog and all log files located under %systemroot% folder
AutoAdminLogon_Settings	Retrieves the settings for AutoAdminLogon value from the Registry
High_Risk_Disks	Reports all non-NTFS disks
High_Risk_Services	Reports the status of high risk services
KeyVolumesSecurity	Reports permissions on key system folders
Last_User_Logon	Returns last user logged on from registry
Locked_Accounts	Returns any locked-out user accounts
LogonSettings	Returns the standard server security settings from registry
SecurityFailureEvents	Reports on any failed events from the audit log

Getting StealthAUDIT

If you would like to learn more about how StealthAUDIT can help you with your security requirements, please feel free to contact us for an interactive web demonstration. You can contact STEALTHbits Technologies at (613)822-2661, or send an email to sales@stealthbits.com.