Who, What, When, Where and Why:

Tracking the 5 Ws of Change in Active Directory, SharePoint, SQL Server, Exchange and VMware

A key strategist of our time said that his biggest concern was he didn’t know he didn’t know. And that fits the threat scape facing today’s information systems. Without visibility into your key infrastructure technologies and applications, you have no idea the following might be happening:

- When a disabled user account is suddenly re-enabled for no apparent reason
- That Alice is spending hours perusing the CEO’s mailbox
- When an entire server virtual machine is downloaded to a USB drive
- That someone just downloaded hundreds of files from a confidential SharePoint site
- That a non-application account is directly accessing a sensitive SQL Server database

A Randy Franklin Smith white paper commissioned by

DELL Software

The technologies covered in this white paper form the core of most organization networks today, and each one provides native audit capabilities. For each one we will explore

- What activity can you audit?
- How do you enable auditing?
- Where can you find audit data?
- What are your gaps, caveats and weaknesses?

Randy Franklin Smith's ULTIMATE WINDOWS SECURITY.COM™

SECURITY IN CONTEXT

Events like those above may be innocuous, legitimate activity or may indicate major security incidents. You won't know which without putting them into context. This highlights the need for *security in context*. How can you know more about the resources and actors involved when you cannot get the context you need from a single event with native auditing? For example:

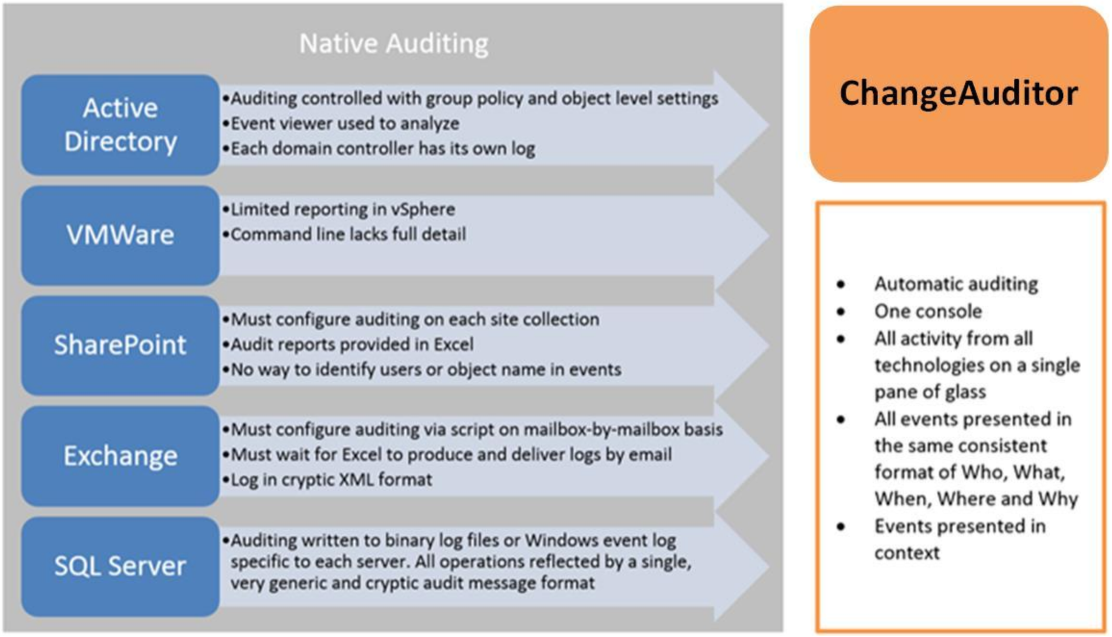
- How do you know individual actions taken independently may or may not be suspicious?
- How do you know what other change(s) occurred around this event and if they are critical?
- Is the actor trustworthy, and should he or she be accessing this resource?
- Does this resource contain sensitive data?

Security requirements cannot be met unless you understand the importance of events in relation to other things happening in your environment. Having related data helps you get insights and answers more quickly, make better decisions on whether suspicious events are really security issues and resolve problems faster.

Even though each technology discussed in this paper provides some level of native audit capability it becomes clear that event logging and change reporting for enterprise applications and services are cumbersome, time-consuming and, in some cases, impossible using native IT auditing tools. Moreover the security context of events is very difficult to establish. Certainly you can rely on your own brain to put pieces together and delve further, chasing down various "rabbit holes" with native audit tools – but having it all connected for you in a single tool is what security analysts really need.

Fortunately there's ChangeAuditor from Dell Software, which takes you beyond each technology's audit data silo and provides a comprehensive view of your entire environment's activities. ChangeAuditor normalizes event data into a simple Who, What, When, Where and Why structure that provides true security in context. The latest version of ChangeAuditor was designed to provide you with the context around events to help you get the big picture and draw accurate decisions, without having to go through the mental gymnastics and time involved in learning each technology's native audit function, accessing them through different interfaces and manually correlating audit data from such vastly different sources and formats.

After exploring each technology's native audit capabilities we will compare and contrast them with the simplicity and security in context made possible by ChangeAuditor.


Native Auditing
Active Directory
•Auditing controlled with group policy and object level settings
•Event viewer used to analyze
•Each domain controller has its own log
VMWare
•Limited reporting in vSphere
•Command line lacks full detail
SharePoint
•Must configure auditing on each site collection
•Audit reports provided in Excel
•No way to identify users or object name in events
Exchange
•Must configure auditing via script on mailbox-by-mailbox basis
•Must wait for Excel to produce and deliver logs by email
•Log in cryptic XML format
SQL Server
•Auditing written to binary log files or Windows event log specific to each server. All operations reflected by a single, very generic and cryptic audit message format
ChangeAuditor
• Automatic auditing
• One console
• All activity from all technologies on a single pane of glass
• All events presented in the same consistent format of Who, What, When, Where and Why
• Events presented in context

CONTENTS

FOUNDATION AWARENESS

VMware, and to an even greater degree, Active Directory, are cornerstones of IT infrastructure at organizations around the world. Both technologies individually have a tremendous impact on security, but when they are combined, it becomes even more crucial to have deep visibility into what's happening within.

On its own, VMware is critical to security because virtual machines are only as secure as the ESX hosts and vCenter environment in which they run. But with VMware's integrated authentication with Active Directory, the VMware environment is only as secure as Active Directory.

Likewise, as the core identity and access management repository for most organizations, Active Directory is the "kernel" of security for the entire network. But if Active Directory domain controllers run as virtual machines, it implicitly follows that Active Directory is only as secure as the VMware environment.

Let's explore the native audit capabilities of both technologies.

ACTIVE DIRECTORY

Active Directory provides auditing through the Windows security event log and audit policies in Group Policy that define what types of activity are audited. Since Active Directory is a set of services hosted on domain controllers, all Windows audit policies are potentially relevant to Active Directory security, since AD itself is only as secure as the Windows system upon which it runs. But in this paper we will cover several audit policies specific to Active Directory for tracking authentication activity, policy changes and modifications to AD objects.

WHAT ACTIVITIES CAN YOU AUDIT?

- Authentication for any system integrating with Active Directory
- High-level changes to users, groups and computers
- Low-level changes to all AD objects, including organizational units and Group Policy Objects

HOW DO YOU ENABLE AUDITING?

Enable appropriate audit policies in a Group Policy Object applied to domain controllers. Audit policies are found under Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration.

To Audit	Enable	
Authentication	*Audit Credential Validation*	Tracks NTLM events
	Audit Kerberos Authentication Service	Shows initial Kerberos logons
	Audit Kerberos Service Ticket Operations	Logs computers accessed during logon session
Changes to Users, Groups and Computer objects	*Audit Computer Account Management* *Audit User Account Management*	

	Audit Security Group Management	
Changes to Organizational Units and Group Policy Objects	*Audit Directory Service Changes* Auditing changes to OUs is important for detecting delegations of privileged authority. OUs also have attributes that control which GPOs are linked to the OU and if GPOs from parent OUs are blocked. Inadvertent or unauthorized changes to these attributes can impact the security posture of thousands of computers within an OU. Auditing changes to GPOs is critical because Group Policy controls the security configuration of all computers in the domain, including servers, workstations and event domain controllers. In addition to enabling the above audit category, object-level audit policy must be defined in Active Directory Users and Computers for the specific object types, operations and users desired for auditing. This should be configured in the Audit tab of the Advanced Security Settings dialog on the root of each domain in the organization.	
Domain policy changes	*Audit Policy Change*	Tracks changes to the audit policy itself
	Audit Authentication Policy Change	Changes to account lockout, password policies and Kerberos ticket parameters
	Audit Authorization Policy Change	Changes to rights and privileges

WHERE CAN YOU FIND THE AUDIT DATA?

Each domain controller has its own security log reflecting the activity handled by that system. There is no centralized audit trail for the entire domain; you must somehow aggregate the activity from all your domain controllers. You can view the Security Log using the Windows Event Viewer. To see the events produced by the categories above, visit www.ultimatewindowssecurity.com/securitylog/encyclopedia and filter by audit policy.

WHAT ARE THE GAPS, CAVEATS AND WEAKNESSES?

Each domain controller has its own security log as noted above. There is no alerting capability or support for secure long-term archival. Aside from those facts, the quality and understandability of events varies greatly from one category to the next.

	Massive quantity of events Extremely cryptic messages Limited ability to correlate events and no way to reconstruct logon sessions
Changes to Users, Groups and Computer objects	These audit policies produce the best quality events found in the Windows security log. Distinct event IDs are logged for each type of object and operation on that object. However, most events show only the after values of changes, not the field values before the change. There are also a number of false positives such as bogus “password change” and “account enabled” events logged when a new account is created. Some events are logged multiple times.
Changes to organizational units and Group Policy Objects	The biggest challenges with auditing organizational units and Group Policy Objects is to: • **Properly configure object-level audit policy** in Active Directory Users and Computers. In addition, the root of the domain needs the same type of auditing as organizational units, but it is a different object type and therefore requires its own audit policy entries. Administrators must be careful to limit object-level audit policy settings so that massive audit loads are not created, especially avoiding the auditing of Read access in Active Directory. • **Correctly interpret audit events.** Directory Service Change events are rather cryptic. You must understand the class names of the objects involved and the names of the properties being changed. This requires knowledge of the literal class and attribute names in the Active Directory schema. For instance, Group Policy Objects are listed as groupPolicyContainer and domain roots as domainDNS. Group policy attributes on OUs are gpOptions and gpLink.
Domain policy changes	The events generated by this category are fairly straightforward, although privilege names can be cryptic, and some trust relationship changes tend to be logged in duplicate. Trust relationship changes may also be mislabeled in terms of trust direction.

CHANGEAUDTOR FOR ACTIVE DIRECTORY

Contrast native AD auditing with ChangeAuditor for Active Directory. ChangeAuditor for Active Directory is a powerful Windows auditing tool that proactively tracks, reports and alerts users to vital configuration changes – in real time and without the overhead of native auditing.

This Active Directory reporting tool enhances security by telling you instantly who made what change when, where and from which workstation – eliminating the risks associated with day-to-day modifications. Plus, you can compare the original and current values for fast troubleshooting and remediation.

For compliance, ChangeAuditor for AD generates intelligent, in-depth forensics for auditors and management. You'll have confidence knowing that your organization can pass its next internal security or regulatory compliance audit. Here are some of robust capabilities of ChangeAuditor:

- **At-a-Glance Display:** Tracks user and administrator activity with detailed information including who, what, when, where and from which workstation for change events, plus original and current values for all changes.
- **Real-time Alerts on the move:** Sends critical change and pattern alerts to email and mobile devices to prompt immediate action, enabling you to respond faster to threats even while you're not on site.
- **Account Lockout:** Captures the originating IP address/workstation name for account lockout events to simplify troubleshooting.
- **Object Protection:** Provides protection against changes to the most critical AD objects, such as accidentally deleted OU and modified GPO settings.
- **High-performance Auditing Engine:** Removes auditing limitations and captures change information without the need for native audit logs, resulting in faster results and significant savings of storage resources.
- **Auditor-ready Reporting:** Generates comprehensive reports for best practices and regulatory compliance mandates for SOX, PCI-DSS, HIPPA, FISMA, GLBA and more.
- **Role-based Access:** Configures access so auditors can run searches and reports without making any configuration changes to the application, and without requiring the assistance and time of the administrator.
- **Event Timeline:** Enables the viewing, highlighting and filtering of change events and the relation of other events over the course of time in chronological order across your Windows environment for better understanding and forensic analysis of those events and trends.
- **Related Searches:** Like the World Wide Web, with just one click you instantly get all information on the change you're viewing and all related events such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.
- **AD Change Rollback:** Restores previous values on unauthorized, mistaken or improper changes with the click of a button, directly in the CA console, honoring the rights and privileges of the user requesting the rollback.
- **Web-based access with Dashboard Reporting:** Searches from anywhere using a web browser and creates targeted dashboard reports to provide upper management and auditors with access to the information they need without having to understand architecture or administration.

VMWARE

VMware produces primarily two different audit trails. First, ESXi hosts each log event occurring on the local host. These events can be collected via syslog. Second, vCenter is widely used to provide centralized management of ESXi hosts. vCenter is a Windows application that uses SQL Server for data storage. The text logs produced by vCenter are not very useful. However, there is a detailed audit trail captured by several related tables in SQL Server. Both ESXi syslog and vCenter audit events are important since important security events can happen at either level. Without both log sources, you have a blind spot.

WHAT ACTIVITY CAN YOU AUDIT?

ESXi syslog	ESXi hosts log the same kinds of events you expect to see from a lean Linux system like secure shell (SSH) sessions and logon events. If you are managing ESXiwith vCenter, most activity should be

	attributed to vpxuser, which is the local account used by vCenter. Be on the lookout for logins and subsequent actions by other users that indicate vCenter is being bypassed. There are some operations that cannot be executed through vCenter, but direct connections to ESXI are an effective way to bypass the centralized authentication, authorization and monitoring provided by vCenter. Besides normal Linux-type system events, ESXi logs a number of security events specific to ESXi such as: • Attempts to log on to a host in lockdown mode. Lockdown mode prevents direct connections to ESXi that bypass vCenter and its security controls. • Lockdown mode disabled • Tech support mode started • Secure Shell service starting • File copies and deletes • Firewall rules and service configuration changes
vCenter	Best practice security as defined by VMware is to manage ESXi hosts exclusively through vCenter to take advantage of the centralized authentication, authorization and monitoring provided by vCenter. vCenter records all operational actions and events to several tables within its SQL Server database. Important vCenter events include: • Role changes • Permissions added or changed • VM copied/cloned • Virtual disk files downloaded or copied • Login attempts • vCenter settings changed • Host setting or profile changes • Host profiles applied/unapplied • Network settings changed

HOW DO YOU ENABLE AUDITING?

ESXi	In the vSphere Client, select the host, select the Configuration tab and open Advanced Settings. Select Syslog. At that point you can configure where and how local logs are managed as well as specify a remote host to receive syslog messages.
vCenter	Auditing is automatic in vCenter

WHERE CAN YOU FIND THE AUDIT DATA?

vCenter	File system location varies for vCenter logs depending on operating system hosting vCenter. See VMware knowledge base. The primary vCenter log with security value is vpxd.log, which records all vSphere Client and web services connections, internal tasks and events and communication with the vCenter Server Agent (vpxa) on managed ESX/ESXi hosts. But this data tends to be very low level and is missing the higher level security events listed above.

The real source of valuable audit activity are the event tables in vCenters database, which can be accessed several ways:

- The vSphere client under Home\Management\Events
- The PowerCLI (VMware PowerShell) Get-VIEvent

ESXi

Selected ESXilogs with the following security values:

Component	Location	Purpose
VMkernel	/var/log/vmkernel.log /var/log/vmkwarning.log	Activities related to virtual machines and ESXi
ESXi host agent log	/var/log/hostd.log	Contains information about the agent that manages and configures the ESXi host and its virtual machines.
Shell log	/var/log/vpxa.log	All commands typed into the ESXi Shell and other shell events
Authentication	/var/log/auth.log	Local authentication events
System messages	/var/log/syslog.log	General log messages
Virtual machines	The same directory as the affected virtual machine's configuration files, named VMware.log and VMware*.log. For example, /vmfs/volumes/*datastore*/*virtual machine*/vwmare.log	Virtual machine power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, machine clones, etc

WHAT ARE THE GAPS, CAVEATS AND WEAKNESSES?

ESXi

None

vCenter

None of the actual log files produced by vCenter provide the audit trail needed to fulfill compliance and security requirements. vCenter does capture this activity but stores it in several tables in the SQL Server where it is accessible only within the vSphere client with limited reporting and analysis capabilities or through the VMware PowerShell interface – PowerCLI using the Get-VIEvent command. Unfortunately, though, Get-VIEvent does not report the full details of the events stored in the database. Omitted details include:

- Critical event arguments
- Name/ID of the event itself

CHANGEAUDITOR FOR VMWARE VCENTER

ChangeAuditor for VMware vCenter helps you ensure the security, compliance and control of event activity and security of VMware vCenter Server by managing, auditing, reporting and providing alerts on all changes to the platform in real time.

With ChangeAuditor, administrators can report on, analyze and manage events and changes without the complexity and time required by native auditing or concerns over system performance. You'll be confident knowing that your data is safe and that you've met the compliance demands necessary to satisfy the scrutiny of any auditor.

ChangeAuditor for VMware vCenter is freeware and is included with other ChangeAuditor modules, including all trial versions.

- **At-a-glance display:** Tracks user and administrator activity with detailed information including who, what, when, where, which workstation and why for change events, plus original and current values for all changes.
- **Real-time alerts on the move:** Sends critical change and pattern alerts to email and mobile devices to prompt immediate action, enabling you to respond faster to threats even while you're not on site.
- **Event timeline:** Enables the viewing, highlighting and filtering of change events and the relation of other events over the course of time in chronological order across your Windows environment for better understanding and forensic analysis of those events and trends.
- **Related searches:** Provides instant, one-click access to all information on the change you're viewing and all related events, such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.
- **Role-based access:** Configures access so auditors can run searches and reports without making any configuration changes to the application, and without requiring the assistance and time of the administrator.
- **Centralized auditing:** Provides the ability to manage, monitor and audit all file server changes from a single location, which streamlines management of multiple servers and locations to a single, easy-to-use console.
- **Server configuration change auditing:** Tracks changes to vCenter configuration and security, which protects against system performance issues and unwanted security gaps.
- **Event filter:** Narrows searches by event type, server, users and more, enabling administrators to quickly pinpoint the source of problems by eliminating the "noise" from safe, routine events.
- **Rapid reporting:** Provides preconfigured and customizable reports that satisfy auditor requests so that administrators can get back to their regular jobs quickly.
- **Web-based access with dashboard reporting:** Searches from anywhere using a web browser and creates targeted dashboard reports to provide upper management and auditors with access to the information they need without having to understand architecture or administration.

CORE APPLICATIONS: WHERE THE DATA IS

While you have to protect your infrastructure, at the end of the day, attackers don't care about your operating system, directory service or virtualization infrastructure. They want the information in your applications. Likewise, compliance is about protecting information – the information in your applications. To achieve compliance and to stop attackers, your security analysts need to see what's happening in your applications. Three applications that arguably store more of an organization's information than any others are SharePoint, Exchange and SQL server.

SHAREPOINT

SharePoint is an ever-growing repository of confidential documents and sensitive workflows. Yet do you know who is accessing those documents, what privileged users are doing or when security controls are changed?

WHAT ACTIVITY CAN YOU AUDIT?

SharePoint has a built-in audit logging capability that allows you to track site-collection users and administrative activity. You can also track end-user activity like the viewing and updating of documents and lists as well as audit administration such as permission changes, changes to groups and other security settings.

HOW DO YOU ENABLE AUDITING?

In SharePoint, auditing is controlled at the site collection level. From the Site Settings page, look under Site Collection Administration for "Site collection audit settings." Here you can configure which *audit flags* are enabled.

Audit Flags	As exposed on "Site collection audit settings" page
CheckOut CheckIn	Checking out or checking in items
View	Opening or downloading documents, viewing items in lists, or viewing item properties
Delete Undelete	Deleting or restoring items
Update	Editing items
SchemaChange ProfileChange	Editing content types and columns
SecurityChange	Editing users and permissions
Copy Move	Moving or copying items to another location in the site
Search	Searching site content

WHERE CAN YOU FIND THE AUDIT DATA?

The SharePoint audit log is completely internal to SharePoint; in fact, it is stored in the SharePoint content database. The SharePoint audit log is accessible through the "View Auditing Reports" page in Site Collection Administration. These reports allow you to select a category of activity and date range and gives you the option of choosing a specific user or object (e.g., list or library) for further filtering. The report is produced as an Excel spreadsheet and is stored in a specified document library. From the document library, you can view the report.

WHAT ARE THE GAPS, CAVEATS AND WEAKNESSES?

- **No way to manage audit policy at the farm level.** Each site collection has its own audit policy. There is no way to ensure consistent audit policy across all site collections. When a new site collection is created, administrators must remember to enable auditing on the site collection. This problem is exacerbated by environments with self-service site collection enabled.
- **SharePoint's audit log does not provide the names of users or objects.** Although events are audited, SharePoint captures only the ID codes and GUIDs of various objects. Without the actual object names, you have no idea what object or user to which a given event refers.
- **There is no alerting capability or support for secure long-term archival.**

CHANGEAUDITOR FOR SHAREPOINT

ChangeAuditor for SharePoint enables you to audit SharePoint faster, easier and more securely. It tracks, audits, reports and alerts on changes to SharePoint farms, servers, sites, users, permissions and more in real time. It also translates events into simple terms, stores data in one centralized and secure database and generates intelligent, in-depth reports to protect against policy violations, delivering the SharePoint tracking and governance organizations need today. With ChangeAuditor for SharePoint, you'll have confidence knowing that your organization can pass its next audit.

- **At-a-glance display:** Tracks user and administrator activity with detailed information including who, what, when, where, which workstation–and why for change events, plus original and current values for all changes.
- **Real-time alerts on the move:** Sends critical change and pattern alerts to email and mobile devices to prompt immediate action, enabling you to respond faster to threats even while you're not on site.
- **Event timeline:** Enables the viewing, highlighting and filtering of change events and the relation of other events over the course of time in chronological order across your Windows environment for better understanding and forensic analysis of those events and trends.
- **Related searches:** Provides instant, one-click access to all information on the change you're viewing and all related events, such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.
- **Server configuration change auditing:** Tracks changes to SharePoint server configurations and security changes that involve SharePoint users, permissions, farms, servers, site collections, lists and documents, which protects against system performance issues and unwanted security gaps.
- **Event filter:** Narrows searches from multiple SharePoint farms, servers and sites by event type, data range, user account and objects, enabling administrators to quickly pinpoint the source of the problem while eliminating the "noise" from safe, routine events.
- **Centralized auditing:** Stores audit data in one centralized and secure database, providing the necessary separation of duties (SoD) between SharePoint administrators and security staff tasked with monitoring.
- **Rapid reporting:** Provides preconfigured and customizable reports that satisfy auditor requests so that administrators can get back to their regular jobs quickly.
- **Role-based access:** Configures access so auditors can run searches and reports without making any configuration changes to the application, and without requiring the assistance and time of the administrator.
- **Web-based access with dashboard reporting:** Searches from anywhere using a web browser and creates targeted dashboard reports to provide upper management and auditors with access to the information they need without having to understand architecture or administration.

EXCHANGE

Exchange email carries an organization's greatest secrets: decisions, marketing plans, customer data, et al. You need to know if Alice is spending hours perusing the CEO's mailbox or whether a privileged user exports an entire mailbox database.

WHAT ACTIVITY CAN YOU AUDIT?

Exchange generates numerous logs, two of which are specifically audit trails.

Administrator Audit Log	Detailed record of all administrative activity in the Exchange environment. In Exchange, all administrative operations are resolved to PowerShell commands. These commands, their parameters and meta data such as date, time and user comprise the admin audit log, which includes: • Exports of mailboxes • Copies of entire mailbox databases • Security configuration changes to Exchange • Access control changes to groups, roles and permissions • Modifications to Exchange policies
Mailbox Audit Log	Primarily for tracking non-owner access to mailboxes for protecting confidential mailbox data and sender integrity. Types of activity that can be audited include: • Users viewing folders in another user's mailbox • Email sent on behalf of another user • Deletion of emails

HOW DO YOU ENABLE AUDITING?

Administrator Audit Log	Admin audit specifications are configured with the Set-AdminAuditLogConfigcmdlet. You can audit all commands (except read-only commands that have no impact), or you can specify subsets of commands and parameters to be audited using wild cards.
Mailbox Audit Log	Audit policy is defined on a mailbox-by-mailbox basis using the Set-Mailbox cmdlet.

WHERE CAN YOU FIND THE AUDIT DATA?

Exchange audit logs are not stored in normal text files or the Windows event log. Instead, Exchange stores the admin audit log in a special audit mailbox and stores audit events for each mailbox within a hidden folder in the same mailbox.

To view audit logs you must use the web-based Exchange Control Panel or the newer Exchange Administration Center. You can also use the Search-AdminAuditLog and Search-MailboxAuditLog cmdlets in PowerShell.

WHAT ARE THE GAPS, CAVEATS AND WEAKNESSES?

Exchange audit log reporting has limited flexibility and power. For full audit detail, it is often necessary to submit audit report requests and wait for Exchange to email you the results in a cryptic XM format.

CHANGEAUDITOR FOR EXCHANGE

ChangeAuditor for Exchange is the watchful eye that proactively tracks, audits, reports and alerts on Exchange configuration and permission changes. It will automatically generate intelligent, in-depth reports to protect against policy violations and avoid the risks and errors associated with day-to-day modifications. Plus, you always get the original and current values for fast troubleshooting.

ChangeAuditor for Exchange audits all critical changes to Exchange, including administrative groups, mailbox policies and public and private information-store auditing. It will keep you advised of all organizational changes such as Active Sync mailbox policy changes, distribution list changes and more. Simply put, real-time auditing helps enforce your organization’s security policies and prevents the triple whammy of compliance violations, system downtime and massive productivity losses

- **At-a-glance display:** Tracks user and administrator activity with detailed information including who, what, when, where, which workstation and why for change events, plus original and current values for all changes.
- **Non-owner mailbox-access auditing:** Provides a detailed view of any changes made to mailboxes that have been accessed by a non-owner, which enhances security and compliance.
- **Real-time alerts on the move:** Sends critical change and pattern alerts to email and mobile devices to prompt immediate action, enabling you to respond faster to threats even while you're not on site.
- **Object protection:** Prevents anyone but the mailbox owner from accessing sensitive or critical mailboxes.
- **Event timeline:** Enables the viewing, highlighting and filtering of change events and the relation of other events over the course of time in chronological order across your Windows environment for better understanding and forensic analysis of those events and trends.
- **Related searches:** Provides instant, one-click access to all information on the change you're viewing and all related events, such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.
- **Server configuration change auditing:** Tracks changes to Microsoft® Exchange Server configuration parameters such as policy changes, (message size, mailbox size), which protects against system performance issues and unwanted security gaps.
- **Public Folders support:** Tracks changes made to Exchange Public Folders, which speeds troubleshooting and ensures compliance.
- **High-performance auditing engine:** Removes auditing limitations and captures change information without the need for native audit logs, resulting in faster results and significant savings of storage resources.
- **Auditor-ready reporting:** Generates comprehensive reports for best practices and regulatory compliance mandates for SOX, PCI-DSS, HIPAA, FISMA, GLBA and more.
- **Role-based access:** Configures access so auditors can run searches and reports without making any configuration changes to the application, and without requiring the assistance and time of the administrator.
- **Web-based access with dashboard reporting:** Searches from anywhere using a web browser and creates targeted dashboard reports to provide upper management and auditors with access to the information they need without having to understand architecture or administration.

SQL SERVER

WHAT ACTIVITIES CAN YOU AUDIT?

SQL Server 2008 and later versions provide a comprehensive audit capability that allows you to track administrator, application and user-level activity across all types of objects and operations. SQL audit specifications afford granular capability for defining exactly which actions, users and objects are audited. You can track things like:

- Security operations involving logins, roles and permissions
- Maintenance of tables, stored procedures and any other object
- Database operations like backup and restore
- Transact SQL table commands like insert, delete, update and select

HOW DO YOU ENABLE AUDITING?

To control auditing you create *audit specification* objects at the server or database level using either SQL Server Management Studio or commands like

- CREATE SERVER AUDIT SPECIFICATION
- ALTER SERVER AUDIT SPECIFICATION
- DROP SERVER AUDIT SPECIFICATION

Different types of activity are divided into *audit action groups* that are added to the audit specification along with your choice of users or roles to be included in the auditing. For a complete list of action groups, see this page at UltimateWindowsSecurity.com.

WHERE CAN YOU FIND THE AUDIT DATA?

SQL Server can output events to the Windows event log or to a binary log file format that is readable via SQL Server using a built-in stored procedure: sys.fn.get_audit_file().

WHAT ARE THE GAPS, CAVEATS AND WEAKNESSES?

SQL auditing is comprehensive in terms of coverage and granular in terms of policy, but typical of many audit logs, the data is cryptic. Despite hundreds of different operations that can be audited, SQL Server uses a single set of fields to describe every possible action. This leads to a generic, cryptic audit message that requires significant knowledge and translation to interpret.

CHANGEAUDITOR FOR SQL SERVER

ChangeAuditor for SQL Server tracks, audits, reports and alerts on changes in real time, translating events into simple terms and eliminating the time and complexity required for auditing. You will instantly know who made what change, when it was made, where it occurred and the originating workstation. You can then automatically generate intelligent, in-depth forensics for auditors and management—and reduce the risks associated with day-to-day modifications. Capabilities include:

- **At-a-glance display:** Tracks user and administrator activity with detailed information including who, what, when, where, which workstation and why for change events, plus original and current values for all changes.
- **Real-time alerts on the move:** Sends critical change and pattern alerts to email and mobile devices to prompt immediate action, enabling you to respond faster to threats even while you're not on site.
- **High-performance auditing engine:** Removes auditing limitations and captures change information without the need for native audit logs, resulting in faster results and significant savings of storage resources.

- **Centralized Auditing:** Provides the ability to manage, monitor and audit all Microsoft® SQL Server® changes from a single location, which streamlines management of multiple servers and locations to a single, easy-to-use console.
- **Auditor-ready reporting:** Generates comprehensive reports for best practices and regulatory compliance mandates for SOX, PCI-DSS, HIPAA, FISMA, GLBA and more.
- **Role-based access:** Configures access so auditors can run searches and reports without making any configuration changes to the application, and without requiring the assistance and time of the administrator.
- **Event timeline:** Enables the viewing, highlighting and filtering of change events and the relation of other events over the course of time in chronological order across your Windows environment for better understanding and forensic analysis of those events and trends.
- **Related searches:** Provides instant, one-click access to all information on the change you're viewing and all related events, such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.
- **Web-based access with dashboard reporting:** Searches from anywhere using a web browser and creates targeted dashboard reports to provide upper management and auditors with access to the information they need without having to understand architecture or administration.

THE PROBLEM WITH NATIVE AUDITING

As seen in this paper, each of these five technologies provide some level of native audit capability. But event logging and change reporting for enterprise applications and services are cumbersome, time-consuming and, in some cases, impossible using native IT auditing tools. In addition, it's very difficult to establish the context surrounding individual events in order to determine if they are legitimate, innocent activity or part of a security violation or even an attack.

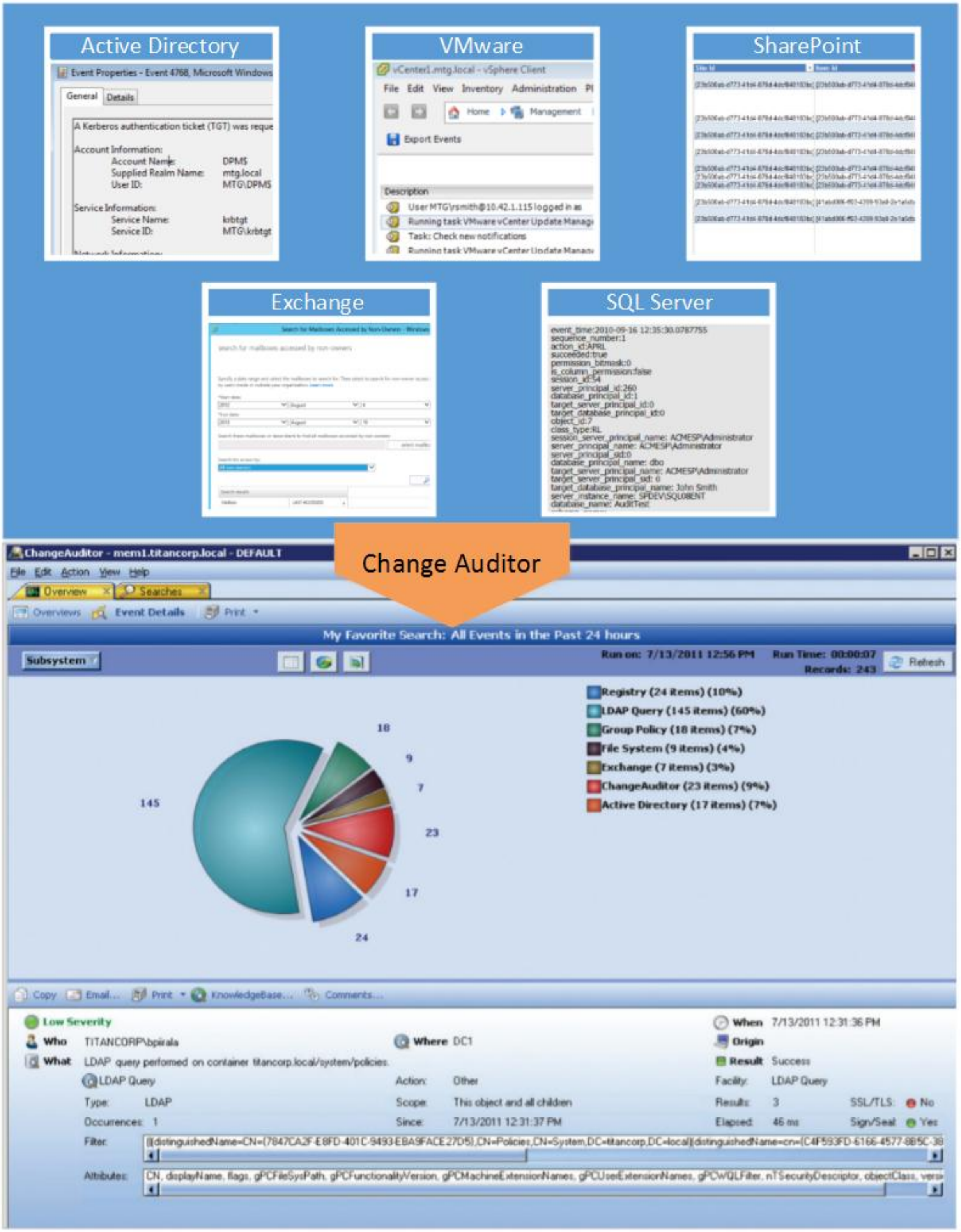
To understand what's happening in your environment you must:

1. Master the five very different ways that auditing works in each of these technologies
2. Maintain audit policy settings across each technology
3. Use five different interfaces for accessing audit events
4. Mentally correlate events from five different disparate report sources and formats

Even after that effort you still fail to see events in context with related events from other technologies. Moreover there is a "penalty" of sorts for organizations that either upgrade to new versions or manage multiple versions in the same enterprise: even within one technology you have to learn and use different versions of tools. Exchange is a great example. Even if you're just using Exchange 2010 and 2013 – you have two different tools, the Exchange Control Panel and the new Exchange Administration Console.

CHANGEAUDITOR: SECURITY IN CONTEXT

The ChangeAuditor solution family audits, alerts and reports on all changes and deletions made to: Active Directory, Exchange, SharePoint, VMware, EMC, NetApp, SQL Server, Windows file servers and even LDAP queries against Active Directory — all in real time and without enabling native auditing. A central console eliminates the need and complexity for multiple IT audit solutions.



Event Properties - Event 4768, Microsoft Windows

General | Details

A Kerberos authentication ticket (TGT) was reque

```
Account Information:
        Account Name:           DPMS
        Supplied Realm Name:    mtg.local
        User ID:                MTG\DPMS

Service Information:
        Service Name:           krbtgt
        Service ID:             MTG\krbtgt
```

vCenter1.mtg.local - vSphere Client

File Edit View Inventory Administration Pl

Home ▸ Management

Export Events

Description

```
User MTG\ysmith@10.42.1.115 logged in as
Running task VMware vCenter Update Manag
Task: Check new notifications
Running task VMware vCenter Update Manag
```

```
event_time:2010-09-16 12:35:30.0787755
sequence_number:1
action_id:APRL
succeeded:true
permission_bitmask:0
is_column_permission:false
session_id:54
server_principal_id:260
database_principal_id:1
target_server_principal_id:0
target_database_principal_id:0
object_id:7
class_type:RL
session_server_principal_name: ACMESP\Administrator
server_principal_name: ACMESP\Administrator
server_principal_sid:0
database_principal_name: dbo
target_server_principal_name: ACMESP\Administrator
target_server_principal_sid: 0
target_database_principal_name: John Smith
server_instance_name: SPDEV\SQL08ENT
database_name: AuditTest
```

ChangeAuditor - mem1.titancorp.local - DEFAULT

File Edit Action View Help

Overview | Searches

Overviews | Event Details | Print

My Favorite Search: All Events in the Past 24 hours

Subsystem

Run on: 7/13/2011 12:56 PM Run Time: 00:00:07 Records: 243 Refresh

- Registry (24 items) (10%)
- LDAP Query (145 items) (60%)
- Group Policy (18 items) (7%)
- File System (9 items) (4%)
- Exchange (7 items) (3%)
- ChangeAuditor (23 items) (9%)
- Active Directory (17 items) (7%)

Copy | Email... | Print | KnowledgeBase... | Comments...

Low Severity

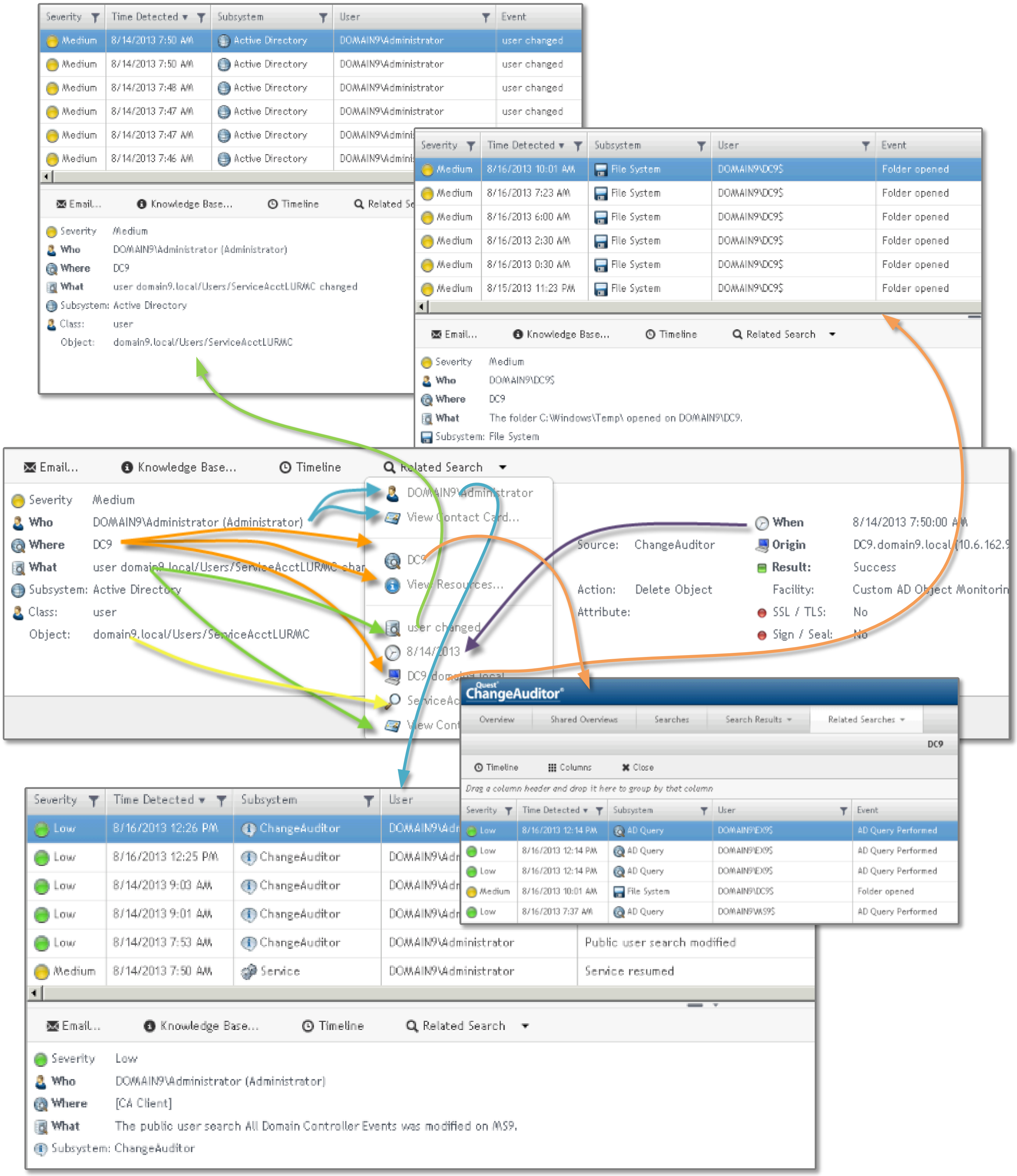
Who	TITANCORP\bpirala	Where	DC1	Origin			
What	LDAP query perfomed on container titancorp.local/system/policies.			Result	Success		
LDAP Query		Action:	Other	Facility:	LDAP Query		
Type:	LDAP	Scope:	This object and all children	Results:	3	SSL/TLS:	● No
Occurences:	1	Since:	7/13/2011 12:31:37 PM	Elapsed:	46 ms	Sign/Seal:	● Yes

When 7/13/2011 12:31:36 PM

Filter: (|(distinguishedName=CN={7847CA2F-E8FD-401C-9493-EBA9FACE27D5},CN=Policies,CN=System,DC=titancorp,DC=local)(distinguishedName=cn={C4F593FD-6166-4577-8B5C-38

Attributes: CN, displayName, flags, gPCFileSysPath, gPCFunctionalityVersion, gPCMachineExtensionNames, gPCUserExtensionNames, gPCWQLFilter, nTSecurityDescriptor, objectClass, versi

But the latest version of ChangeAuditor does more than just bring audit events from different technologies together and present them on a single pane of glass. ChangeAuditor 6 provides true security in context by allowing you to look at context from different angles. Each event allows you to branch off into related searches to answer questions like: What else has that user been doing? What else has been happening on that system? What happened before and after this event?



Severity	Time Detected	Subsystem	User	Event
Medium	8/14/2013 7:50 AM	Active Directory	DOMAIN9\Administrator	user changed
Medium	8/14/2013 7:50 AM	Active Directory	DOMAIN9\Administrator	user changed
Medium	8/14/2013 7:48 AM	Active Directory	DOMAIN9\Administrator	user changed
Medium	8/14/2013 7:47 AM	Active Directory	DOMAIN9\Administrator	user changed
Medium	8/14/2013 7:47 AM	Active Directory	DOMAIN9\Admini	
Medium	8/14/2013 7:46 AM	Active Directory	DOMAIN9\Admini	

Severity Medium
Who DOMAIN9\Administrator (Administrator)
Where DC9
What user domain9.local/Users/ServiceAcctLURMC changed
Subsystem: Active Directory
Class: user
Object: domain9.local/Users/ServiceAcctLURMC

Severity	Time Detected	Subsystem	User	Event
Medium	8/16/2013 10:01 AM	File System	DOMAIN9\DC9$	Folder opened
Medium	8/16/2013 7:23 AM	File System	DOMAIN9\DC9$	Folder opened
Medium	8/16/2013 6:00 AM	File System	DOMAIN9\DC9$	Folder opened
Medium	8/16/2013 2:30 AM	File System	DOMAIN9\DC9$	Folder opened
Medium	8/16/2013 0:30 AM	File System	DOMAIN9\DC9$	Folder opened
Medium	8/15/2013 11:23 PM	File System	DOMAIN9\DC9$	Folder opened

Severity Medium
Who DOMAIN9\DC9$
Where DC9
What The folder C:\Windows\Temp\ opened on DOMAIN9\DC9.
Subsystem: File System

Severity Medium
Who DOMAIN9\Administrator (Administrator)
Where DC9
What user domain9.local/Users/ServiceAcctLURMC char
Subsystem: Active Directory
Class: user
Object: domain9.local/Users/ServiceAcctLURMC

Source: ChangeAuditor
Action: Delete Object
Attribute:

When 8/14/2013 7:50:00 AM
Origin DC9.domain9.local (10.6.162.9
Result: Success
Facility: Custom AD Object Monitorin
SSL / TLS: No
Sign / Seal: No

Severity	Time Detected	Subsystem	User	Event
Low	8/16/2013 12:14 PM	AD Query	DOMAIN9\EX9$	AD Query Performed
Low	8/16/2013 12:14 PM	AD Query	DOMAIN9\EX9$	AD Query Performed
Low	8/16/2013 12:14 PM	AD Query	DOMAIN9\EX9$	AD Query Performed
Medium	8/16/2013 10:01 AM	File System	DOMAIN9\DC9$	Folder opened
Low	8/16/2013 7:37 AM	AD Query	DOMAIN9\MS9$	AD Query Performed

Severity	Time Detected	Subsystem	User	
Low	8/16/2013 12:26 PM	ChangeAuditor	DOMAIN9\Adr	
Low	8/16/2013 12:25 PM	ChangeAuditor	DOMAIN9\Adr	
Low	8/14/2013 9:03 AM	ChangeAuditor	DOMAIN9\Adr	
Low	8/14/2013 9:01 AM	ChangeAuditor	DOMAIN9\Adr	
Low	8/14/2013 7:53 AM	ChangeAuditor	DOMAIN9\Administrator	Public user search modified
Medium	8/14/2013 7:50 AM	Service	DOMAIN9\Administrator	Service resumed

Severity Low
Who DOMAIN9\Administrator (Administrator)
Where [CA Client]
What The public user search All Domain Controller Events was modified on MS9.
Subsystem: ChangeAuditor

ChangeAuditor’s security in context relieves you from the exhausting work of mentally correlating different information sources and dissimilar formats and from the time-consuming work of constantly switching between each technology’s arcane, audit-search interface. With ChangeAuditor you can focus on the investigation instead of the tools.

Auditing & Compliance	ChangeAuditor provides easy-to-understand and meaningful security and compliance reports on the fly. Built-in compliance library reports and the ability to customize reports make it easy to prove compliance for standards such as SOX, HIPAA, PCI, FISMA and SAS 70.
Real-time Alerting	ChangeAuditor tracks critical configuration changes to your Windows infrastructure and applications, and then translates raw data into meaningful, searchable, intelligent data to help safeguard the security and compliance of your infrastructure. This comprehensive solution offers real-time alerts and “Smart Alert” technology for intelligent alerting and in-depth reports on the activities taking place in your environment.
Change Management	ChangeAuditor helps tighten enterprise-wide change-control policies by tracking user and administrator activity for account lockouts and access to critical settings. Guard your Windows environment from exposure to suspicious behavior or unauthorized access, and maintain compliance with corporate and government standards.
Performance Optimization	Native tools make it next to impossible to report on and analyze what is happening on your network. Active Directory queries and native auditing put a strain on the most efficient and best-architected networks, and IT professionals need to consider these factors daily. Ignoring these factors makes it difficult to provide first-class service to your users, plan for migrations or disaster recoveries, and perform directory consolidations. **New Feature in ChangeAuditor 6.0: High Performance Auditing Engine**. Removes auditing limitations and captures change information without the need for native audit logs, resulting in faster results and significant savings of storage resources.
Analysis	Analyzes critical configuration changes to your Windows environment, and then translates raw data into meaningful intelligent data to help safeguard the security and compliance of your infrastructure. New Features in Change Auditor 6.0: • **Event Timeline**: View, highlight and filter on change events and the relation of other events over the course of time in chronological order across your Windows environment for better understanding and forensic analysis of those events and trends. • **Related Searches**: Like the World Wide Web, with just one click you instantly get all information on the change you're viewing and all related events such as what other changes came from specific users and workstations, eliminating additional guesswork and unknown security concerns.

Learn more about ChangeAuditor and try it for free at www.software.dell.com/changeauditor.

ABOUT DELL SOFTWARE

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

Visit www.software.dell.com/changeauditor for more information.

ABOUT RANDY FRANKLIN SMITH

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and Active Directory security. Randy publishes www.UltimateWindowsSecurity.com and wrote *The Windows Server 2008 Security Log Revealed*—the only book devoted to the Windows security log. Randy is the creator of LOGbinder software, which makes cryptic application logs understandable and available to log-management and SIEM solutions. As a Certified Information Systems Auditor, Randy performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations. Randy is also a Microsoft Security Most Valuable Professional.

DISCLAIMER

Monterey Technology Group, Inc. and Dell Software make no claim that use of this white paper will assure a successful outcome. Readers use all information within this document at their own risk.