Global Information Assurance Certification Paper

Host Based IDS Research Paper

By Robert Grill, GCIA, CISSP, CISA, CNA, MBA

Title: Windows NT and Novell Host Based Intrusion Detection Using Native Logging and 3rd Party Log Reporting Tools.

Outline of Paper

- Introduction
- NW and NT Auditing from an Auditors Point of View
- Log Monitoring Without Consuming Bandwidth During Peak Network Usage
- Event Log Scenarios for NT
- How to Use the Auditing Information in a NW environment
- Appendix A: Signature Development
- Appendix B: NT Event ID Codes for Security

Introduction

Auditing is defined for this paper as the process of examining operating system (OS) logs to assure information stored on computers is properly protected, and managed and meets corporate security policies. This paper will cover the Novell NetWare 4.11 (NW) and Windows NT 4.0 (NT) operating systems. NW is capable of auditing Novell Directory Services (NDS) and file system actions, and NT for domain and file systems actions, performed on a company's WAN. Auditing tracks the following types of information:

- User Actions
- Resource Usage
- File System Security and Access Control
- Login and Logoff Activity

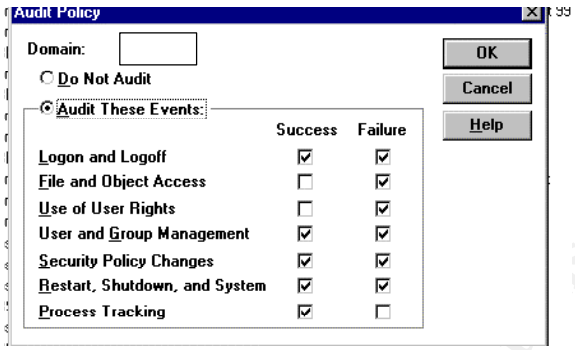
NT and NW include auditing features to collect information about how a system is being used. These features monitor events related to system security, to identify any security breaches, and to determine the extent and location of any damage. The level of audited events is adjustable to suit the needs of an organization. This paper illustrates the usage of NT and NW security monitoring separately; however, the concepts apply to both platforms.

The chart below illustrates security goals and what to audit:[1]

Goal	What to Audit
Justify Resources	Writes to an application file Use of print queues
Diagnose Performance Problems	File opens related to an application that is slow
Determine holes in security	Changes to access control list (ACL) (NDS, or NT Shares and Trust Relationships) File opens of sensitive files
Determine if a user has accessed unauthorized areas	File opens in the audited areas File writes in the audited areas File opens by an audited user
Determine NW and NT server security	Login Security (NDS, PDC or NT member server login) Volume Mounts and Dismounts NW or NT Server Events
Audit File Security	File reads and writes File creations and deletions

Source: Novell Application Notes, April 1994, Volume 5, Number 4, page 152

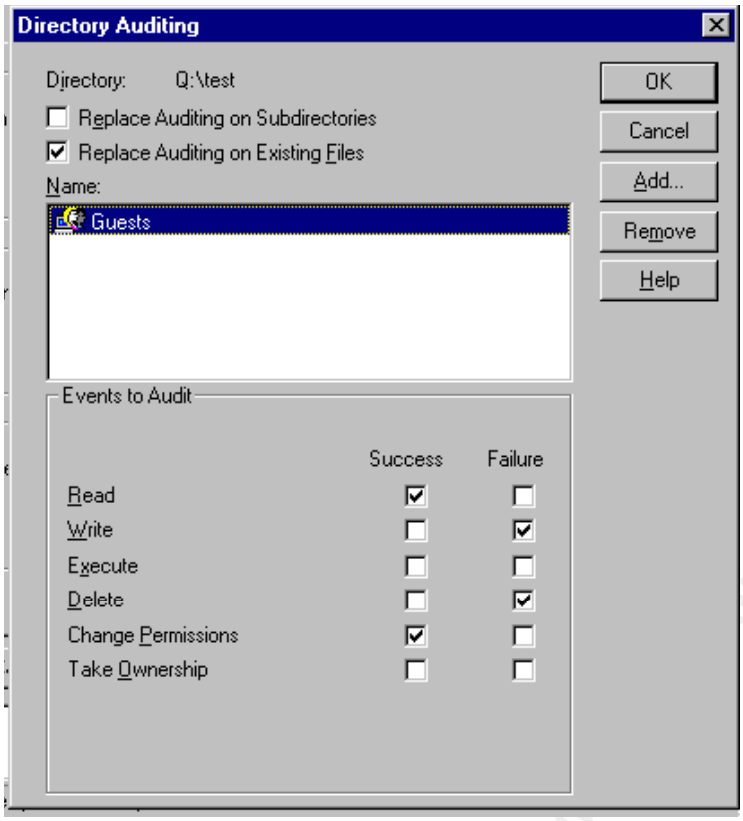
A picture of what NT auditing looks like and audit options are as follows:



The definitions of what the event categories mean are as follows:[2]

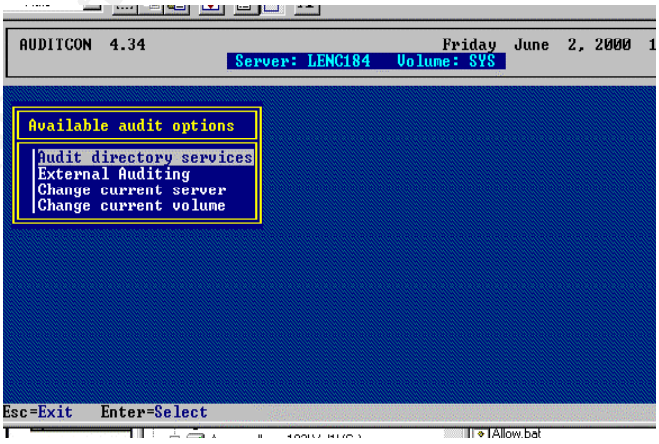
Type of event	Description
Logon and Logoff	A user logged on or off or made a network connection.
File and Object Access	A user opened a directory or a file that is set for auditing in File Manager, or a user sent a print job to a printer that is set for auditing in Print Manager.
Use of User Rights	A user used a user right (except those rights related to logon and logoff).
User and Group Management	A user account or group was created, changed, or deleted. A user account was renamed, disabled, or enabled; or a password was set or changed.
Security Policy Changes	A change was made to the User Rights, Audit, or Trust Relationships policies.
Restart, Shutdown, and System	A user restarted or shut down the computer, or an event has occurred that affects system security or the security log.
Process Tracking	These events provided detailed tracking information for things like program activation, some forms of handle duplication, indirect object accesses, and process exit.

Below is a picture of what file system auditing looks like for NT. Of course, as with most NT file system features, you have to partition the drive as NTFS.

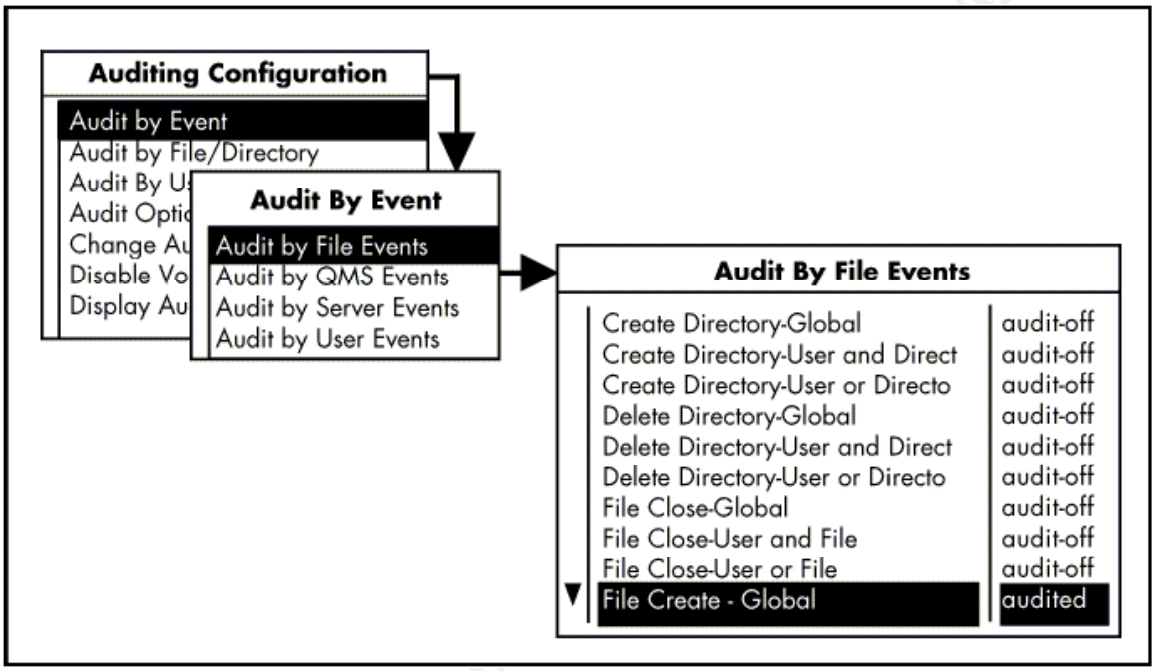


If a directory has a list of users whose access to the directory is to be audited, a new file added to the directory will inherit the auditing list from the directory.

The Auditcon.exe utility for NW is below. It can be accessed by a windows client or other OS attached to a NW network. The picture below is a dos window on a Windows 95 client. The Auditcon.exe file is installed by default in the SYS/PUBLIC directory on the network drive.



The picture below illustrates how a sample of the menus work:[1]



After running the EXE file, numerous pull down menus provide a customizable solution for auditing any object on the NW landscape.

Some examples of the events NW tracks are listed in the following table.[1]

File Events	User Events	Server Events	Queue Management Services (QMS) Events
Opens	Logins	Changing date/time Rconsole Usage	Queue creations
Closes	Logouts	Accessing NDS	Job creations
Reads	Password changes	Downing the Server	Job edits
Writes	Modifications of trustee rights	• Adding NLM • Changing NDS	Job service start-up
Salvages	Grantings of trustee rights		Job service removal
Rename/moves		Renaming NDS objects	Setting job priority
Deletes		Deleting NDS objects	
Modifications of directory entries			

NW and NT auditing from an Auditors Point of View

NW auditing is a true audit tool because it provides independence to the auditor. Once NW auditing is set up only the auditor can access or reconfigure the audit logs, without dependence on operations. NW auditing functionality is provided by the AUDITCON utility, which is protected by a confidential password. The auditing feature records specific NW, NDS and file system actions, called events, performed on the network.

It is important to note that in NW 4.01 AUDITCON is a public utility, found in the SYS: PUBLIC directory of each NW server. Starting with NW 4.1 the actual audit files are encrypted and are stored in a non-public directory.

NW auditing adds accountability to networks by serving as a check and balance system. As a network grows and more users are added, many factors can cause security to deteriorate and allow unauthorized access to the network or to sensitive information such as:[2]

- Control becomes decentralized as core users are given specific security responsibilities.
- Users create new files without setting the appropriate level of security.
- New users are granted access to the system, increasing the complexity of the security structure.
- File ownership is changed without corresponding changes being made to trustee rights.

Conversely, a disadvantage to NT auditing, from the auditors point of view, is the lack of independence. In the NT environment, the administrator may reconfigure audit settings or alter the audit logs. NT auditing cannot be configured or read without being a member of the administrators group. This makes the logs

vulnerable to sabotage by an administrator and puts the auditor in a position where he can be accused of an abuse of privilege.

NT can track events related to the operating system itself and to individual applications. Each application can define its own auditable events, this is not true for NW. Definitions of these events are added to the Registry when the application is installed on NT.

The security log in the NT Event Viewer can list events by category and by event ID. The following categories of events are listed in the security log. (Those in parentheses are configured by the Audit Policy dialog box in NT User Manager.)

NT Security Events Categories[2]	
Category	**Meaning**
Account Management (User and Group Management)	These events describe high-level changes to the user-accounts database, such as User Created or Group Membership Change. Potentially, a more detailed, object-level audit can also be performed. (See the "Object Access" category, below).
Detailed Tracking (Process Tracking)	These events provide detailed subject-tracking information, such as program activation, handle duplication, and indirect object access.
Logon/Logoff	These events describe a single logon or logoff attempt, whether successful or unsuccessful. Included in each logon description is an indication of what type of logon (that is, interactive, network, or service)was requested or performed.
Object Access (File and Object Access)	These events describe both successful and unsuccessful accesses to protected objects.
Policy Change (Security Policy Changes)	These events describe high-level changes to the security policy database, such as assignment of privileges or logon capabilities. Potentially, a more detailed, object-level audit is also performed. (See the "Object Access" category, above).
Privilege Use (Use of User Rights)	These events describe both successful and unsuccessful attempts to use privileges. The category also includes information about when some special privileges are assigned. These special privileges are audited only at assignment time, not at the time of use.
System Event (System)	These events indicate something occurred that affects the security of the entire system or audit log

Event logging starts automatically each time NW or NT is started. NT and NW logs can be archived in various file formats.

Because the security log is limited in size, and because a large number of routine audit records can make it difficult to find records that suggest a security problem, carefully plan how to audit object access. Use of object-access auditing can help identify areas where security policy should be tightened or even where a security breach has been attempted successfully or unsuccessfully.

NT and NW can audit successful and failed attempts of the following types of directory and file access:[3]

Types of directory access	Types of file access
Displaying names of files in the directory	Displaying the file's data
Displaying directory attributes	Displaying file attributes
Changing directory attributes	Displaying the file's owner and permissions
Creating subdirectories and files	Changing the file
Going to the directory's subdirectories	Changing file attributes
Displaying the directory's owner and permissions	Running the file
Deleting the directory	Deleting the file
Changing directory permissions	Changing the file's permissions
Changing directory ownership	Changing the file's ownership

Band Width and Performance Issues

When auditing, there is a small performance overhead for each audit check the system performs. Measuring the performance overhead of a security strategy is not as simple as monitoring a separate process. NW and NT server security services are integrated into several different operating system services. Security features cannot be monitored separately from other aspects of the services.

The best method of measuring security overhead is to run tests comparing the server performance with and without the security feature. The tests should be run with fixed workloads and a fixed server configuration so that the security feature is the only variable. During the tests measure the items in the following list:

- Processor activity and the processor queue. Increased processor activity, and an increase in the rate of context switches and interrupts. If the processors in the server are not sufficient to handle the increased load, queues develop.
- Physical memory used. Security requires that the system store and retrieve more user information.
- Network activity and latency. Latency is a measure of the time required to complete a task.

Log Monitoring Without Consuming Bandwidth During Peak Network Usage

(Example shown using a tool named Bindview EMS, for NW and NT http://www.bindview.com)

The following scenario to monitor audit logs used the audit of failed login attempts as an example.

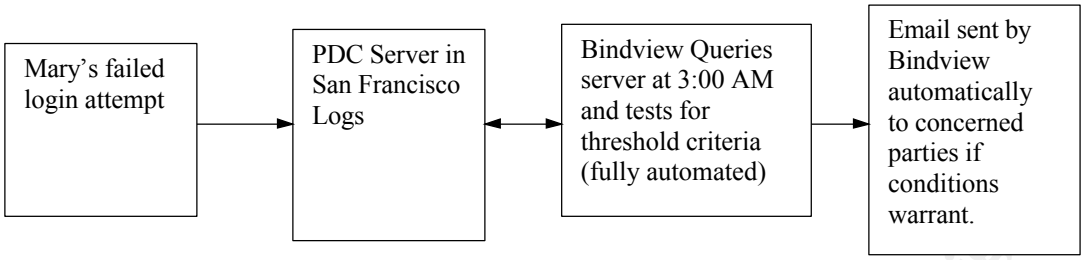
Step 1: Auditing turned on at local server

Step 2: Only auditing for failed login attempts activated

Step 3: Log starts to fill set to overwrite at 4 MB

Step 4: Once a night a log query tool (such as Bindview EMS) queries the logs

Step 5: Bindview sends an E-Mail to designated parties if an attack signature is discovered



Other Tools that can be used to query and report on audit logs are in the following table:

NW	NT
Auditcon (comes with NW)	Event Viewer (comes with NT)
Auditware (purchase from Novell)	LT Auditor+ http://www.bluelance.com/freestuff/default.html
LT Auditor + http://www.bluelance.com/freestuff/default.html	NT Last http://www. ntobjectives.com/
	Dumpel (Utility comes with NT)
	Crystal Reports (comes with the Windows NT resource kit)

Try this one for Unix http://www.psionic.com/download/.

Event Log Scenarios for NT [2]

When reading NT logs the event header contains the following information:

Information	Meaning
Date	The date the event occurred.
Time	The (local) time the event occurred.
User	The username of the user on whose behalf the event occurred. This name is the client ID if the event was actually caused by a server process, or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs. (Impersonation occurs when NT allows one process to take on the security attributes of another.)
Computer	The name of the computer where the event occurred. The computer name is usually your own, unless you are viewing an event log on another NT computer.
Event ID	A number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is "The Event log service was started. " The Event ID and the Source can be used by product support representatives to troubleshoot system problems.
Source	The software that logged the event, which can be either an application name, such as "SQL Server," or a component of the system or of a large application, such as a driver name. For example, "Elnkii" indicates the EtherLink II driver.
Type	A classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log. In Event Viewer's normal list view, these are represented by a symbol.
Category	A classification of the event by the event source. This information is primarily used in the security log. For example, for security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in the NT User Manager Audit Policy dialog box. (See the table on the next page for a description of the NT categories)

For NT all event-log records, regardless of type, consist of a header containing standard information, a description that varies depending on the event type, and (optionally) additional data. Most security log entries consist of the header and a description.

The security log identifies the user account that caused each recorded event to happen. In some cases, more than one account is actually involved because of the client-server design of NT. This design makes it possible for one process to perform actions on behalf of another process.

When the server process is acting on behalf of the client, NT security treats it as though it were the client process. The server process is not allowed to access objects that are off limits to the client.

Audit event records include header information that is present in all event records. The following list describes this common information:[1]

Category	Description
System Event	Events in this category indicate that something affecting the security of the entire system or of the audit log has occurred.
Logon/Logoff	Events in this category describe a single successful or unsuccessful logon or logoff. Included in each logon description is an indication of what type of logon was requested/performed (for example, interactive, network, or service).
Object Access	Events in this category describe both successful and unsuccessful accesses to protected objects.
Privilege Use	Events in this category describe both successful and unsuccessful attempts to use privileges. The Privilege Use category also covers a special case of informing when some special privileges are assigned. These special privileges are only audited when they are assigned, not when they are used.
Account Management	Events in this category describe high-level changes to the security account database, such as the creation of a user account or a change in group membership. There can also be a finer granularity of auditing performed at the object level under the Object Access category.
Policy Change	Events in this category describe high-level changes in security policy, such as the assignment of privileges or changes in the audit policy. There can also be a finer granularity of auditing performed at the object level under the Object Access category.
Detailed Tracking	Events in this category provide detailed subject tracking information, such as program activation, some forms of handle duplication and indirect object accesses, and process exit.

The following is an example of the NT security events for file access:[2]

Event ID and Description	Analysis
Event 560:	Object Open
Event 561:	Handle Allocated
Event 562:	Handle Closed - In this sequence of events, NT is doing some internal checks, such as checking to see if the file exists and checking to see that there is no sharing violation.
Event 592:	A New Process Has Been Created
Event 560:	Object Open
Event 561:	Handle Allocated
Event 562:	Handle Closed - In this series of events, a new process is created for Notepad.exe. This process opens the .txt file for reading. Next, the process allocates, then closes, a handle to the file. Note that from the security log it is clear that Notepad does not keep an open handle to the file; it simply keeps a copy of the file in memory.
Event 560:	Object Open
Event 561:	Handle Allocated
Event 562:	Handle Closed - The process opens the file for reading and writing, and since the event is a successful audit, new data is written to the file. Next, the handle is allocated for the open file, then closed.
Event 593:	A Process Has Exited - This event indicates that the process, whose process ID relates to Notepad.exe, has ended.

Example 2: Security Events for System Startup

Event ID and description	Analysis
Event 512:	NT is starting up identifies the date and time the system started.
Event 514:	Authentication package loaded. The description of this event says An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts. Authentication Package Name: msv 1_0. This is the standard authentication package shipped with NT.
Events 515:	Trusted logon process. The description for each of these events says , A trusted logon process has registered with the Local Security Authority. This logon process will be trusted to submit logon requests. The logon process name is listed for each of these events, as follows: Winlogon Service Control Manager LAN Manager Workstation Service LAN Manager Server LAN Manager Redirector

This is a successful audit in the category of system event. The event indicates that the respective logon processes have registered with the Local Security Authority and are now trusted to submit logon requests.

Auditing can identify actions that could pose a security risk and also identify the user accounts that performed the audited actions. It should be noted that auditing only tells you what user accounts were used for the audited events. If users passwords are adequately protected, this in turn indicates which user attempted the audited events. However, if a users password has been stolen or if actions were taken while a user was logged on but away from the computer, the action could have been initiated by someone other than the person to whom the user account is assigned.

At a minimum failed logon attempts, attempts to access sensitive data, and changes to security settings should be audited. Below are common security threats and the type of auditing that can track them:2

Threat	Action
Hacker-type break-in using random passwords	Enable failure auditing for logon and logoff events.
Break-in using stolen password	Enable success auditing for logon and logoff events. The log entries will not distinguish between the real users and the phony ones. What you are looking for here is unusual activity on user accounts, such as logons at odd hours or on days when you would not expect any activity.
Misuse of administrative privileges by authorized users	Enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown, and system events.
Virus outbreak	Enable success and failure write access auditing for program files such as files with .exe, .nlm, and .dll extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. Note that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log.
Improper access to sensitive files	Enable success and failure auditing for file- and object-access events, and then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files.
Improper access to printers	Enable success and failure auditing for file- and object-access events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.

How to Use the Auditing Information in a NW environment[1]

The following cases illustrate situations where auditing is helpful. These cases also illustrate how to:

- Justify the purchase of another word processor license.
- Locate a potential security breach.
- Locate and correct a trustee rights problem.
- Monitor volumes being dismounted or mounted.
- Determine if a workgroup manager is abusing his or her rights.
- Monitor changes in partitions and replicas.

Case 1:

The network administrator is told to justify the purchase of another word processor license.
The auditor flags the word processor file for OPEN by all users and counts the number of accesses to that file. The resulting information gives the network administrator an idea of how many people use the word processor program and how often. The persons responsible for purchasing can then decide whether the need is great enough to buy another license based on number and frequency of accesses.

Case 2:
The auditor helps the network administrator find a potential security breach.
The network administrator finds that some of the console parameters have changed in the past few days. The auditor may be asked to check the server events and RCONSOLE accesses within the past week to determine who has gained access to the server console.

Case 3:
The auditor helps the network administrator find and correct a trustee rights problem.
A user says that he cannot access a database program that he used to have rights to. The auditor searches the auditing records, determines that the rights to the database directory have been changed, and tells the network administrator that the rights were changed on a certain date and by whom.

Case 4:
The network administrator wants reports on volume mounts and dismounts.
The administrator has the auditor flag the Volume mount and Volume Dismount under Audit by Event server events. Each time the volumes are mounted or dismounted for that server, auditing records the event.

Case 5:
The network administrator suspects a workgroup manager of abusing power and changing users' rights.
The administrator has the auditor flag the User object in the container with the Change in ACL flag under the Audit by NDS Events menu. When the user makes any change to trustee assignments or ACLs, the auditing file reflects the change.

Case 6:
The network administrator wants to monitor changes in NDS partitions and replicas.
The auditor goes to the Audit by DS Events menu and flags the following:

- Add Partition
- Change Replica Type
- Join Partitions
- Remove Partitions
- Remove Replicas
- Split Partitions

Conclusion

It is only access that is auditable, not intent. In other words, the audit log records will show that a particular user opened an object; it will not tell you what the user's intent was. Regular review of the security event logs is a critical, and often overlooked, security requirement. Government systems which process classified information are required to review these logs, and it's a good idea for any sensitive system. A review should be looking for security-related failures, as well as any other occurrence that strikes you as unusual based on knowledge of users and their activity patterns. Third-party event log management tools can help you automate the gathering and analysis process.

APPENDIX A: Signature Development

1. Failed Login Attempts over a threshold, over one day or for many days, this analysis should be correlated to every machine in the network.
2. Audit Log Cleared This event record indicates that the audit log has been cleared. This event is always recorded, regardless of the audit policy. It is recorded even if auditing is turned off.
3. Creation or Deletion of Container objects
4. Passwords changed between the hours of 5 P.M. and 5 A.M.
5. Failed or Successful logins between the hours of 5 P.M. and 5 A.M.
6. Tracking specific the actions of specific users, such as super users
7. File system and NDS Tree change control
8. NDS events to be audited:
   - 8.1. Addition of any container object
   - 8.2. Deletion of any container object
   - 8.3. Addition / Deletion of any server object
   - 8.4. Any Container or Leaf Object added between 7 P.M and 5 A.M
   - 8.5. Trustee Assignment changes between 7 P.M and 5 A.M
9. Down Server Events
10. Additions of Servers
11. Rconsole Usage
12. Abuse of Privileges
13. Server Restarts
14. ACL Events
15. Security and Auditing Configuration changes
16. Accounts Enabled/Disabled
17. Change in Trust Relationships
18. Password Change Failures

Correlation (Requiring the use of logs from multiple systems and / or over a period of time.)

19. The same person logging into different physical locations of the network at the same time.
20. Different people signing into the same machine
21. All paired events (such as logon/logoff or open/close). A missing event may indicate an issue.

Recommended Reports[4]

General

1. After Hours Report
2. Creation/Deletion of Objects Reports
3. Failed File Access Report
4. File Attribute Changes Report
5. Intruder Detection Report
6. Trustee Assignments Changes Report
7. Users Given Supervisor Equivalence Report

NW Reports

1. Bindery Password Changes Report
2. NDS Password Changes Report
3. NDS/Bindery Changes Report
4. NLM Modules Loaded/Unloaded Report
5. Volumes Mounted/Dismounted Report
6. Security Equivalence Changes Report
7. Bindery Users Made Supvsr. Equivalent
8. Trustee Assignments Changes Report
9. Volumes Mounted/Dismounted Report

NT Reports

1. NT Groups Created/Deleted Report
2. NT Group Mbrs. Added/Deleted Report
3. NT Password Changes Report
4. NT Policy Changes Report
5. NT Rights Assigned/Removed Report
6. NT Security Changes Report
7. Trusted Domain Added/Deleted Report

Bibliography

1. Author Unknown. "Novell Application Notes." April 1994. URL: http://developer.novell.com/research/appnotes/1994/april/ (May 30, 2000)

2. Microsoft Press. "auditcat.hlp" November 1996. File, part of the Windows NT Resource Kit - must be purchased from Microsoft. URL: http://www.microsoft.com/ (Not Applicable)

3. Glaser, JD. "Intrusion Auditing with NTLast." Document Date Unknown. Link to file not valid anymore, downloaded from URL http://www. ntobjectives.com/ (May 15, 2000)

4. Author Unknown, "LT Auditor+ User Manual", (Published date unknown), URL: http://www.bluelance.com/freestuff/default.html. (May 31, 2000)

Appendix B: Windows NT Server Security Event Codes[2]

Event Log	Event Type	Event ID	Event Source	Message
Security	Success Audit	512	Security	Windows NT is starting up.
Security	Success Audit	513	Security	Windows NT is shutting down. All logon sessions will be terminated by this shutdown.
Security	Success Audit	514	Security	An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts. Authentication Package Name:
Security	Success Audit	515	Security	A trusted logon process has registered with the Local Security Authority This logon process will be trusted to submit logon requests. Logon Process Name:
Security	Success Audit	516	Security	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. Number of audit messages discarded:
Security	Success Audit	517	Security	The audit log was cleared Primary User Name: Primary Domain Primary Logon ID : Client User Name Client Domain: Client Logon ID:
Security	Success Audit	518	Security	An notification package has been loaded by the Security Account Manager. This package will be notified of any account or password changes. Notification Package Name:
Security	Success Audit	528	Security	Successful Logon: User Name: Domain Logon ID: Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	529	Security	Logon Failure: Reason: Unknown user name or bad password User Name: Domain: Logon Type: Logon Process: Authentication Package: Workstation Name:

Security	Failure Audit	530	Security	Logon Failure: Reason: Account logon time restriction violation User Name: Domain: Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	531	Security	Logon Failure: Reason: Account currently disabled User Name: Domain Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	532	Security	Logon Failure Reason The specified user account has expired User Name: Domain Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	533	Security	Logon Failure: Reason: User not allowed to logon at this computer User Name: Domain: Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	534	Security	Logon Failure: Reason The user has not be granted the requested logon type at this machine User Name: Domain Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	535	Security	Logon Failure Reason The specified account's password has expired User Name: Domain: Logon Type: Logon Process: Authentication Package: Workstation Name:

Security	Failure Audit	536	Security	Logon Failure Reason The NetLogon component is not active User Name: Domain Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Failure Audit	537	Security	Logon Failure Reason: An unexpected error occurred during logon User Name: Domain Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Success Audit	538	Security	User Logoff User Name: Domain Logon ID Logon Type:
Security	Failure Audit	539	Security	Logon Failure Reason Account locked out User Name: Domain: Logon Type: Logon Process: Authentication Package: Workstation Name:
Security	Success Audit	560	Security	Object Open: Object Server: Object Type: Object Name: New Handle ID: Operation ID {5,6} Process ID: Primary User Name: Primary Domain: Primary Logon ID: Client User Name: Client Domain: Client Logon ID: Accesses Privileges
Security	Success Audit	561	Security	Handle Allocated Handle ID: Operation ID: {2,3} Process ID
Security	Success Audit	562	Security	Handle Closed: Object Server: Handle ID: Process ID

Security	Success Audit	563	Security	Object Open for Delete: Object Server: Object Type: Object Name: New Handle ID: Operation ID: {5,6} Process ID: Primary User Name: Primary Domain: Primary Logon ID: 0ntClient User Name: Client Domain: Client Logon ID: Accesses Privileges
Security	Success Audit	564	Security	Object Deleted: Object Server: Handle ID: Process ID:
Security	Success Audit	576	Security	Special privileges assigned to new logon: User Name: Domain Logon ID Assigned:
Security	Success Audit	577	Security	Privileged Service Called: Server: Service Primary User Name: Primary Domain: Primary Logon ID: Client User Name: Client Domain: Client Logon ID: Privileges:
Security	Success Audit	578	Security	Privileged object operation: Object Server: Object Handle: Process ID: Primary User Name: Primary Domain: Primary Logon ID: Client User Name: Client Domain: Client Logon ID: Privileges:
Security	Success Audit	592	Security	A new process has been created: New Process ID: Image File Name: Creator Process ID: User Name: Domain: Logon ID:

Security	Success Audit	593	Security	A process has exited: Process ID: User Name: Domain: Logon ID:
Security	Success Audit	594	Security	A handle to an object has been duplicated: Source Handle ID: Source Process ID: Target Handle ID: Target Process ID:
Security	Success Audit	595	Security	Indirect access to an object has been obtained: Object Type: Object Name: Process ID: Primary User Name: Primary Domain: Primary Logon ID: Client User Name: Client Domain: Client Logon ID: Accesses:
Security	Success Audit	608	Security	User Right Assigned: User Right: Assigned To: Assigned By: User Name: Domain Logon ID:
Security	Success Audit	609	Security	User Right Removed: User Right: Removed From: Removed By: User Name: Domain Logon ID:
Security	Success Audit	610	Security	New Trusted Domain: Domain Name: Domain ID: Established By: User Name: Domain Logon ID:
Security	Success Audit	611	Security	Removing Trusted Domain Domain Name: Domain ID: Removed By: User Name: Domain Logon ID:

Security	Success Audit	612	Security	Audit Policy Change New Policy: Success Failure 1t System Logon/Logoff Object Access Privilege Use Detailed Tracking Policy Change Account Management Changed By: User Name: Domain Name: Logon ID
Security	Success Audit	624	Security	User Account Created: New Account Name: New Domain: New Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges
Security	Success Audit	625	Security	User Account Type Change: Target Account Name: Target Domain: Target Account ID: New Type: Caller User Name: Caller Domain: Caller Logon ID:
Security	Success Audit	626	Security	User Account Enabled: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID:
Security	Success Audit	627	Security	Change Password Attempt: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	628	Security	User Account password set: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID:

Security	Success Audit	629	Security	User Account Disabled: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID
Security	Success Audit	630	Security	User Account Deleted: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	631	Security	Global Group Created: New Account Name: New Domain: New Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	632	Security	Global Group Member Added: Member: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	633	Security	Global Group Member Removed: Member: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	634	Security	Global Group Deleted: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:

Security	Success Audit	635	Security	Local Group Created: New Account Name: New Domain: New Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	636	Security	Local Group Member Added: Member: Target Account Name: Target Domain Target Account ID Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	637	Security	Local Group Member Removed: Member: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	638	Security	Local Group Deleted: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	639	Security	Local Group Changed: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	640	Security	General Account Database Change: Type of change: Object Type: Object Name: Object ID: Caller User Name: Caller Domain: Caller Logon ID:

Security	Success Audit	641	Security	Global Group Changed: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	642	Security	User Account Changed: Target Account Name: Target Domain: Target Account ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:
Security	Success Audit	643	Security	Domain Policy Changed: Domain: Domain ID: Caller User Name: Caller Domain: Caller Logon ID: Privileges:

Last Updated: May 29th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event