

Security Auditing and Alerting for eDirectory, NDS and NetWare File Systems

Facilitating Regulatory Compliance

Written by:
John T. McCann
Product Architect
Visual Click Software, Inc.

<http://www.visualclick.com>

Corporate Background

Visual Click Software was founded in May of 1999 by John T. McCann and Steve Garms. Visual Click's first product, DSRAZOR® for eDirectory, NDS and NetWare file systems, was initially released in November 1999. In November 2000, Visual Click released its second product, DSMETER® for eDirectory, NDS and NetWare file systems. At the end of 2003 Visual Click released its third product, DSRAZOR for GroupWise.

As a leader in automated security auditing, alerting and control technology, Visual Click Software serves over 600 customers worldwide across a wide range of industries including financial services, medical and healthcare, education, legal, insurance and government.

Our strength is providing your organization with security access management solutions that are powerful yet cost-effective.

Visual Click's objective is to reduce network security risks within your organization while decreasing the time, complexity and costs of managing network security.

Copyright © 2004 Visual Click Software, Inc. All rights reserved.

This document is for informational purposes only. Visual Click Software makes no warranties, express or implied in this document.

DSRAZOR, DSMETER and Visual Click are registered trademarks of Visual Click Software, Inc.

Novell, NDS, eDirectory and NetWare are either registered trademarks or trademarks of Novell, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.

Introduction

Fact: Many governmental security regulations demand monitoring and auditing of access to secure systems. Satisfying today's government and industry regulatory demands requires a multifaceted approach.

Directory Services METER or DSMETER® and DSRAZOR® benefit your organization by facilitating your compliance with regulatory and industrial needs such as GLBA, HIPAA, Sarbanes-Oxley, ISO 17799 and others.

Fact: Current research indicates that authorized users commit a majority of security breaches.

When you use DSMETER and DSRAZOR, your organization gains an effective security auditing, change tracking and alerting solution for eDirectory, NDS and NetWare file systems.

This document has been prepared to clearly show the benefits of using DSMETER and DSRAZOR throughout your NetWare-based enterprise to provide security auditing, change tracking and alerting.

Rapid Deployment and Implementation

Leading the benefits of using DSMETER is its simple and quick installation. Its automated, server-only technology requires no client agents. Architected to be simple and intuitive to use, you will be productive with DSMETER in the first few hours of use. This benefits your organization by *eliminating* the need to spend weeks or months in preparation for installation. There is also no need to hire costly consultants to assist with its implementation.

Leading the benefits of using DSRAZOR is its simple and quick installation. Installation of DSRAZOR upon a single administrator workstation is all that is required to perform vulnerability assessments. Once installed, it can be immediately used to perform many vulnerability assessments without requiring any additional supporting software. You will be productive within minutes of installing DSRAZOR. The compelling benefit here is that you will be productive with DSRAZOR without the need to spend time preparing for its installation and by eliminating the need to hire costly consultants.

BENEFIT:

Simplicity of the architecture and design of DSMETER and DSRAZOR accelerates your return on investment.

Disabling Hidden Objects

Quick, can you account for all objects within your eDirectory/NDS Tree? Have you included all hidden objects that may exist? Whether introduced intentionally or accidentally, hidden objects represent a serious security concern. If your administrators do not know they exist, it is possible that these hidden objects are being used with impunity to access your network and sensitive data. With DSMETER you will receive a complete report of all hidden objects in your eDirectory/NDS Tree. And, if DSMETER finds any hidden objects you can direct it to automatically disable them so they can no longer be used to access your network.

BENEFIT:

Your organization benefits immediately with increased peace of mind that hidden objects are not being used to abuse your network.

Tracking Logins and Logouts

Many eDirectory/NDS administrators are required to provide management with reports detailing login and logout actions. Addressing the need to audit access, DSMETER provides reports that include the user name, event time, network address used and server where the login/logout event occurred. Complementing the login/logout reports is DSMETER's ability to detect failed login activity. Failed logins include those attempts made with an incorrect login name, invalid password as well as the use of old-style bindery logins.

BENEFIT:

Your organization gains valuable insight when all login and logout attempts are tracked.

Auditing Supervisor Privileges

Achieving regulatory compliance requires the detection of security assignments. The highest security assignment within eDirectory/NDS and NetWare file systems is the Supervisor privilege. Where granted, this privilege allows it users to perform any possible action. It is therefore critical to know when Supervisor privileges are assigned. By detecting changes in security level of both eDirectory/NDS and NetWare file system as they occur, DSMETER provides you with reports detailing who requested the new security level, network address used, what object received the new security assignment, what security was bestowed and other details as appropriate. These reports are essential to securing access of your network.

BENEFIT:

Your organization benefits when it becomes aware of changes in security assignments, particularly those resulting in the conveyance of Supervisor privileges.

Assessing and Correcting Vulnerabilities

Fulfillment of regulatory compliance requires assessing the configuration of security-related access parameters. Parameters such as file system access assignments, password configurations, and eDirectory/NDS security privileges must be carefully assessed to determine vulnerability. Without a vulnerability assessment you may be unaware that low-ranking individuals have read access to classified or otherwise privileged file system folders and files. If user accounts are allowed to exist without a password or are never required to reset their password, this represents a vulnerability that could result in a serious breach of security. The improper assignment of security within eDirectory/NDS

can result in granting individuals the ability to hide their user account which can be later used as a “backdoor” to gain unauthorized access to your network.

DSRAZOR includes many reports to help you assess the configuration of security-related access parameters of your eDirectory/NDS and NetWare file systems. All reports provided by DSRAZOR are interactive and can be directly used to quickly correct all vulnerabilities found.

BENEFIT:

Your organization benefits when it can quickly assess and correct vulnerabilities of security-related access parameters.

Controlling Media File Usage

Connectivity to the internet opens your network to the receipt of data of all types. Data types include those that are useful, distracting and others that contain the risk of copyright infringement. DSMETER provides the capability to block unwanted files, monitor users for their frequency of selected file use and produce real-time alerts for selected activities occurring within your NetWare file systems. DSMETER’s server-only technology can be configured to block, monitor and alert on the following NetWare file system actions:

- File Open
- File Create
- File Read
- File Write
- File Delete
- File Salvage
- File Purge
- File Rename

DSMETER allows these actions to be implemented by file extension, filename, file path, server volume and server name. Wildcards can be used in any portion of the filename and/or path.

File activity reports will identify who used specific files including the actions performed, when the files were used and even who deleted files.

BENEFIT:

Your organization gains control when you use DSMETER to automate the blocking and monitoring of file access and use within your NetWare file systems.

Alerting of Intruder Detection

Included in the implementation of eDirectory/NDS is the option to detect intruders. Intruder detection is accomplished by enumerating failed login attempts. Once the failed login threshold has been reached, eDirectory/NDS automatically locks the account and disables further logins. After the lockout-

reset interval expires, which defaults to 15 minutes, the account will be available for another login attempt and data regarding the intruder will be removed. Although an alert message is displayed on the server screen where the lockout occurred, all but the most attentive administrators will entirely “miss” the intruder lockout event.

DSMETER completes the intruder detection process by including the ability to present administrative users with an alert the moment an account is intruder locked. Configuration of the DSMETER-generated alert includes delivery via NetWare popup message and via email. Email delivery includes presentation to the administrator’s mobile/cell phone. Almost all mobile/cell phones are able to receive short text-based emails. The alert generated provides the administrators with actionable information that can be used to track down the intruder. Information provided includes: the full name of eDirectory/NDS account being locked and the IPX or TCP/IP address where the intruder last attempted login.

BENEFIT:

Strength of your eDirectory/NDS security improves when intruder detections are immediately acted upon.

Conclusion

This document has been prepared to clearly show the benefits of using DSMETER and DSRAZOR throughout your NetWare-based enterprise to provide security auditing, change tracking and alerting. DSMETER provides many additional features and benefits not included here. And DSRAZOR provides many additional beneficial features to help your organization maintain its regulatory compliance.

To learn more about DSMETER and DSRAZOR, please visit:

<http://www.visualclick.com>