Centrify®

CENTRIFY WHITE PAPER. SEPTEMBER 2011

Privileged User Activity Auditing: The Missing Link for Enterprise Compliance and Security

User activity auditing is the missing element that enterprises require to improve security and speed compliance by quickly establishing who performed which actions on Windows, UNIX and Linux servers with a clear context for each event or change to a system, file or database.

Abstract

Capturing the detailed actions of privileged users is even more critical in today's business environment that is driving cost efficiencies through IT outsourcing, off-shoring and supplementing IT staff with contractors. Security and compliance issues also exist with third-parties including Cloud Providers, Service Providers and ISVs. And every major compliance regulation requires organizations to document what users actually do with the privileges and rights granted to them and how their actions impact the IT environment. Traditional approaches, such as log files, cannot fully meet these requirements. Log files are well suited to aggregating and correlating events and management data for alerting and reporting purposes. But for a full accounting of what specific actions were taken on a specific system, at a specific time, by a specific user, there is no substitute for a high-fidelity recording of individual user sessions. By recording all privileged user activity (screen actions, events and metadata) a complete picture of intentions and impacts can be achieved. Organizations need to ensure that every privileged session can be audited across their extended enterprise creating a high level of visibility on UNIX, Linux and Windows systems whether in the data center or in cloud computing environments. Additionally, the auditing approach should scale up to meet organizations growing needs without interruptions and with minimal administrative resources. The solution should be realized with a proven architectural approach that is fault tolerant, reliable and highly scalable across thousands of systems and users. Centrify DirectAudit solves these critical business and technical challenges with an auditing solution that makes the capture and collection, and search and replay of user session activity simple. DirectAudit can also be deployed on all modern Windows releases as well as all major distributions of UNIX and Linux providing a complete solution for real-time and historical privileged user activity auditing across the broad set platforms in the heterogeneous enterprise.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Centrify Corporation.

Centrify may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Centrify, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2004-2011 Centrify Corporation. All rights reserved. WP-025-2011-09-20

Centrify, DirectControl and DirectAudit are registered trademarks and Centrify Suite, DirectAuthorize, DirectSecure and DirectManage are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Introduction 4
Traditional Approaches Alone Fail to Address Requirements 4
User Activity Auditing Addresses Critical Challenges 5
  Compliance Demands 5
  Mitigating Insider Attacks 6
  Third-Party Access, Troubleshooting and Training 6
Key Requirements for User Activity Auditing 6
  Capture and Collection Requirements 7
  Search and Replay Requirements 7
  Enterprise Ready and Integrated Requirements 7
  Security Management Requirements 7
Centrify DirectAudit Solution 7
  Capture and Collect 10
  Search and Replay 11
  Enterprise Ready and Integrated 12
  Security Management 12
Summary 13

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Introduction

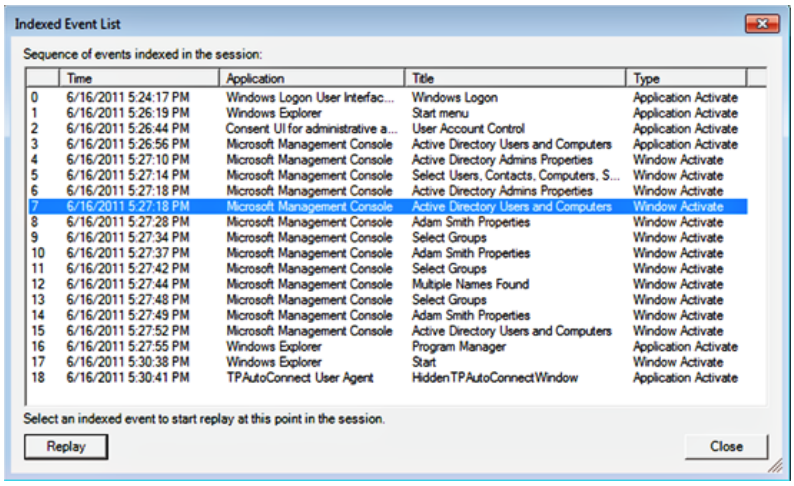
Organizations are facing escalating complexity in every aspect of their IT operations including the datacenter, identity and access management infrastructure, cross-platform systems and staffing. Establishing and maintaining a security and compliance posture, in what is often a disparate and dynamically changing environment, is regularly cited as the top concern of IT leaders who are responsible for mitigating risk and protecting the information assets of their enterprises. And enterprises of all sizes are lowering costs through outsourcing, off-shoring and contractor staffing and increasingly rely on cloud service providers and independent software vendors to manage critical parts of their information systems. How do diligent IT leaders create accountability, audit this complex environment and guard against unintentional and malicious actions of privileged users that may lead to a system failure or data breach?

This white paper describes how Centrify DirectAudit solves the security, compliance and third-party access challenges organizations face when auditing and monitoring UNIX, Linux and Windows systems and why traditional approaches, like log rollup tools, alone do not meet the requirements of today's demanding IT environments. A compelling case will be made that DirectAudit's capture of high-fidelity video and associated events and metadata give organizations the missing user-centric context they require to demonstrate compliance, guard against insider threats and monitor third-party access by a variety of privileged users.

Traditional Approaches Alone Fail to Address Requirements

Log files generated by systems and applications provide an incomplete picture because they contain large amounts of inconsequential event and management data and are often not detailed enough to determine which user performed specific actions on a system that resulted in a system failure or attack. In addition, interpreting log files is time consuming and requires specialized skills held by only a very small subset of people in the organization. Log data is useful for top-level alerting and notification of potential problems but logged events are not tied to the actions of a specific user so troubleshooting and root-cause analysis cannot provide the accountability that security best practices and compliance regulations demand.

Another critical factor organizations must consider is lack of visibility because some applications have little or no internal auditing. This can be the case with custom-built applications where auditing capabilities may not be the highest priority and developers may not understand the organizations audit needs including the level of detail required and importance of securing access to log data itself. Also, many enterprise applications that are highly customized may not be logging critical events.



	Time	Application	Title	Type
0	6/16/2011 5:24:17 PM	Windows Logon User Interfac...	Windows Logon	Application Activate
1	6/16/2011 5:26:19 PM	Windows Explorer	Start menu	Application Activate
2	6/16/2011 5:26:44 PM	Consent UI for administrative a...	User Account Control	Application Activate
3	6/16/2011 5:26:56 PM	Microsoft Management Console	Active Directory Users and Computers	Application Activate
4	6/16/2011 5:27:10 PM	Microsoft Management Console	Active Directory Admins Properties	Window Activate
5	6/16/2011 5:27:14 PM	Microsoft Management Console	Select Users, Contacts, Computers, S...	Window Activate
6	6/16/2011 5:27:18 PM	Microsoft Management Console	Active Directory Admins Properties	Window Activate
7	6/16/2011 5:27:18 PM	Microsoft Management Console	Active Directory Users and Computers	Window Activate
8	6/16/2011 5:27:28 PM	Microsoft Management Console	Adam Smith Properties	Window Activate
9	6/16/2011 5:27:34 PM	Microsoft Management Console	Select Groups	Window Activate
10	6/16/2011 5:27:37 PM	Microsoft Management Console	Adam Smith Properties	Window Activate
11	6/16/2011 5:27:42 PM	Microsoft Management Console	Select Groups	Window Activate
12	6/16/2011 5:27:44 PM	Microsoft Management Console	Multiple Names Found	Window Activate
13	6/16/2011 5:27:48 PM	Microsoft Management Console	Select Groups	Window Activate
14	6/16/2011 5:27:49 PM	Microsoft Management Console	Adam Smith Properties	Window Activate
15	6/16/2011 5:27:52 PM	Microsoft Management Console	Active Directory Users and Computers	Window Activate
16	6/16/2011 5:27:55 PM	Windows Explorer	Program Manager	Application Activate
17	6/16/2011 5:30:38 PM	Windows Explorer	Start	Window Activate
18	6/16/2011 5:30:41 PM	TPAutoConnect User Agent	HiddenTPAutoConnectWindow	Application Activate

DirectAudit metadata example: User was displaying the Active Directory Users and Computers panel, an indication the user was attempting to make unauthorized configuration changes.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

To increase visibility and gain a clear understanding of the intentions, actions and results of privileged user activity on systems higher-level alerts should point to more detailed data on the actions, events and commands that the user actually performed on the system that lead up to the alert. This metadata can only be collected by capturing the critical user-centric data (events and screen video) and cannot be reconstructed from log data generated by systems and applications.

This new, user-centric approach to auditing privileged systems can address the security, compliance and third-party challenges organizations face.

User Activity Auditing Addresses Critical Challenges

Compliance Demands

The myriad of compliance regulations create ongoing challenges for enterprises in every industry and many companies must meet multiple requirements for internal controls (SOX), payments data security (PCI DSS), patient health information (HIPAA) and other industry specific requirements (GBLA, NERC/FERC and FISMA/NIST SP 800-53). Common to every major compliance regulation and industry mandate are requirements to ensure users authenticate with a unique identity, privileges are limited to only ones needed to perform job functions and user activity is audited with enough detail to determine what events occurred, who performed them and the outcome.

Table: Sample of major user activity auditing compliance requirements

Compliance Rule	Description
Sarbanes-Oxley Section 404 (2)	…contain an assessment … of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
PCI DSS Section 10.2.1-2	10.2 Implement automated audit trails to reconstruct the [user activity], for all system components 1. Verify all individual access to cardholder data. 2. Verify actions taken by any individual with root or administrative privileges.
HIPPA 164.312(b) Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
NIST SP 800-53 (AU-14)	The information system provides the capability to: a. Capture/record and log all content related to a user session; and b. Remotely view all content related to an established user session in real time.
NERC CIP-005-1 R3 (Monitoring Electronic Access)	Implement and document an electronic or manual process(es) for monitoring and logging access

Compliance specifications often refer to "logging" or "log" when describing a specific audit control. In order to fully address the compliance rule and satisfy auditors it often requires organizations to provide more detail than application and system log files provide — this has created an audit gap. Privileged user activity auditing provides the detailed metadata and visual record of actions that meet the strictest interpretation of the regulation.

The lack of effective and detailed user activity auditing can result in increased costs due to slower compliance reporting, increased staff time and ultimately fines for non-compliance. System logs track when users sign-in and sign-out but don't capture user activity with sufficient granularity to address compliance requirements.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Mitigating Insider Attacks

Mitigating the risk of insider attacks that can lead to a data breach or system outage remains a key concern for security managers. Several factors have led to an increase in insider incidents including the sharing account credentials, privileged users with too many credentials across systems and assignment of privileges that are too broad with respect to the job responsibilities of the user. Because many organizations have privileged users that are geographically dispersed organizations must be have visibility into the activities of local and remote administrators and users.

User activity auditing can create the accountability required for security and compliance including:

- Capture and search historical user activity so that suspicious actions can be examined to determine if an attack is occurring — before the damage is done.
- Change privileged user behavior through deterrents ensuring that trustworthy employees are not taking shortcuts and disgruntled employees know any malicious actions will be recorded.
- Establish a clear, unambiguous record for evidence in legal proceedings and dispute resolution.

And insider threats are not going away, one report from US-CERT (with cooperation from the U.S. Secret Service) estimated that 86% of internal computer sabotage incidents are perpetrated by a company's own technology workers and 33% of participants in the 2011 CyberSecurity Watch Survey responded that insider attacks are more costly than external ones.

Third-Party Access, Troubleshooting and Training

Today's business environment is driving enterprises to find cost efficiencies at every level of their operations. Outsourcing, off-shoring and cloud computing are giving organizations agility, flexibility and the cost control they require to remain competitive but, organizations are still responsible for the security and compliance of their IT systems. This is made clearer in newly revised compliance requirements that specifically call out the enterprise's responsibility when contracting Independent Software Vendors, Service Providers and outsourcing firms. In fact, the HITECH act enhancements to HIPAA closed one of the last loopholes related to third-party liability.

Third-party user access creates even more impetus to deploy detailed user activity auditing. In addition to the insider attacks and compliance demands already mentioned third-party access increases the pressure to quickly troubleshoot ailing systems, auto-document critical processes and create training procedures for personnel hand-offs, which occur more frequently with contractors and service providers.

Key Requirements for User Activity Auditing

In order for enterprises to take full advantage of the benefits that user activity auditing can provide they should consider the requirements that are essential to the easy and efficient capture and collection of user activity; and thorough search with detailed replay of user sessions. In addition, any solution for privileged user activity auditing should fit into the enterprise environment integrating with existing infrastructure and ensuring that audit data is secure and can only be replayed by auditors, security managers and other authorized staff. Below is a list of requirements enterprise should consider when deploying a user activity auditing solution.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Capture and Collection Requirements

- Capture both remotely as well as locally initiated user sessions across Windows, UNIX and Linux systems.
- Ensure the solution can scale up from a single system deployment to the demands of auditing user sessions on thousands of cross-platform systems.
- Supports the ability to selectively capture sessions based on Active Directory users and groups.
- High-fidelity capture of session video with detailed capture of events and metadata.
- Encryption and compression of all audit data in transit and at rest.

Search and Replay Requirements

- Ease to use interface supporting granular queries across multiple user sessions and systems.
- Support for ad-hoc, distributed searches for commands, applications and text independent of operating system.
- Intuitive and fast session navigation, preview and replay.

Enterprise Ready and Integrated Requirements

- Automated discovery and (re)configuration of audit system components for reliability and fault tolerance with minimal administrative personnel involvement.
- Ensure only trusted components can participate in the auditing system.
- Built-in integration support for existing SIEM, event and monitoring tools.

Security Management Requirements

- Role-based control to user session replay so only authorized users can access audit data and replay sessions.
- Delegated administration and management of all auditing system components.

Centrify DirectAudit Solution

Centrify DirectAudit enables detailed, real-time auditing of privileged user sessions on Windows, UNIX and Linux systems, providing a full accounting of user activity and system access. DirectAudit's detailed capture of historical user activity establishes accountability and advances compliance reporting by recording which users accessed which systems, what commands they executed, with what privilege, and the exact changes they made to key files and configurations. With DirectAudit, enterprises can report on historical user activity, pinpoint suspicious activity through real-time monitoring, and troubleshoot system failures by replaying actions for root-cause analysis.

DirectAudit is a comprehensive solution for user activity and session auditing that supports an array of popular protocols used to access privileged systems, provides easy search and replay for auditors and managers and integration into established tools and processes used by personnel in security and network operations centers, helpdesk staff and teams monitoring service levels of third-party vendors.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

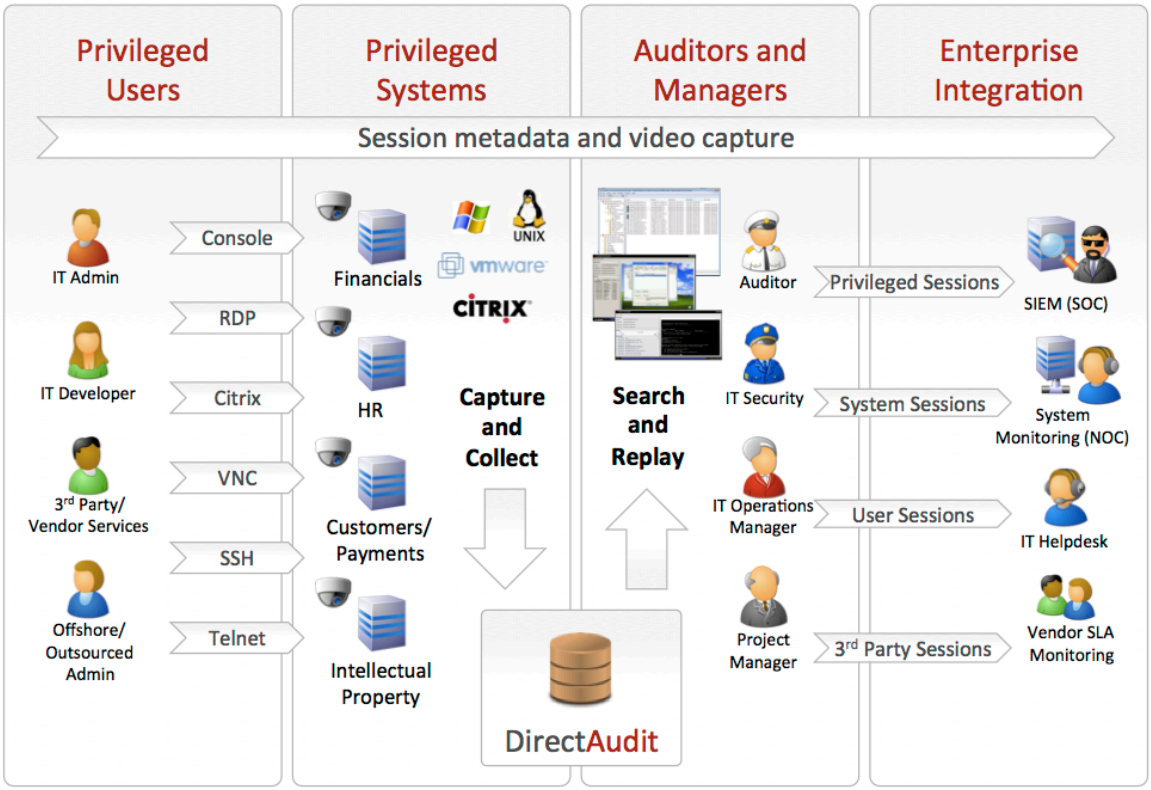
DirectAudit captures session video and metadata encompassing:

- **Privileged Users** — DirectAudit supports all the commonly used remote protocols (Citrix, RDP, VNC, SSH, Telnet) ensuring the capture of privileged sessions of IT administrators and developers, third-party vendors and outsourced and off-shored staff.

- **Privileged Systems** — DirectAudit is the only solution that supports session capture on Windows, UNIX and Linux systems so enterprises can examine user activity across sensitive areas of their operations such as Financials, Human Resources, Payment Systems and access to Intellectual Property.

- **Auditors and Managers** — Through granular audit roles DirectAudit allows enterprises to limited visibility and replay of user sessions based on the roles in the organization such as Auditor, Security Manager, Operations Manager and Project Managers.

- **Enterprise Integration** — DirectAudit has built-in integration for popular SIEM, event and monitoring tools empowering security and network operations personnel, helpdesk staff and teams monitoring vendor service levels to quickly drilldown on relevant sessions.



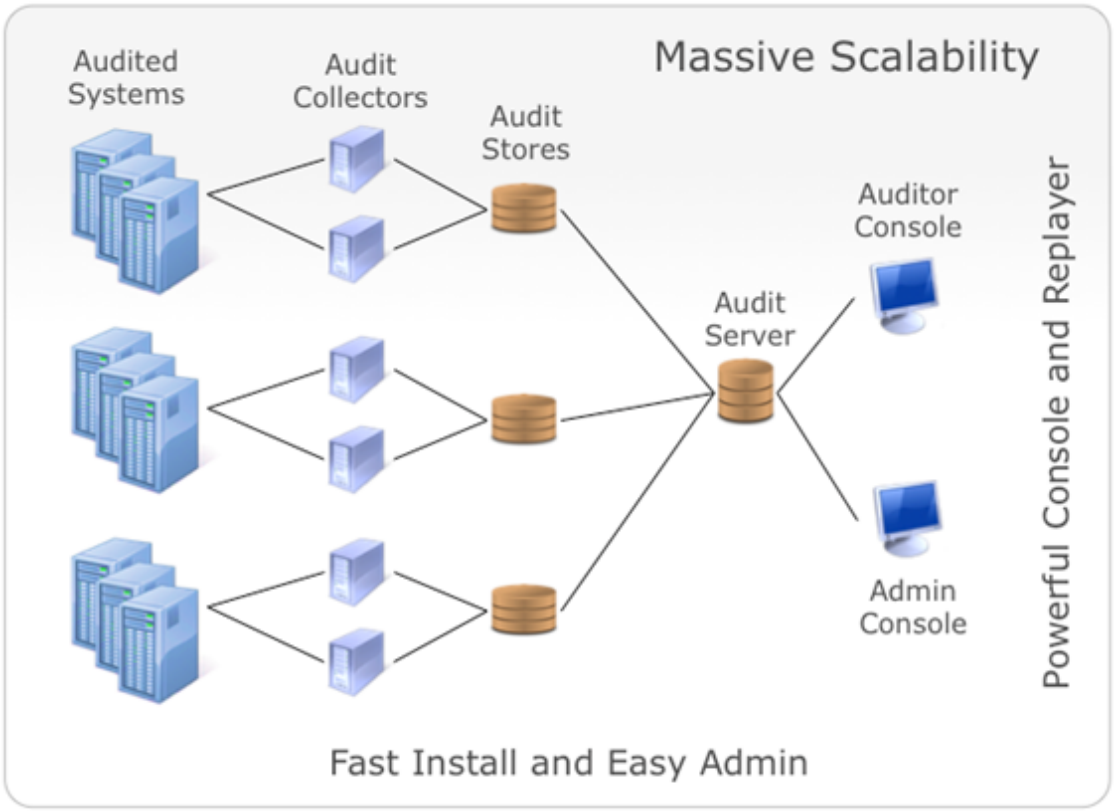
DirectAudit watches over user activity and system access, enabling auditors, security and operations staff to mitigate security violations, report on compliance and monitor privileged sessions in real-time.

Centrify DirectAudit consists of five major components:

- DirectAudit **Agent** — A system agent that runs on wide range of Windows, UNIX and Linux systems and efficiently captures user activity, session output. This captured data is securely streamed to a DirectAudit Collector for processing. The DirectAudit Agent requires minimal system resources and supports offline capture spooling for unparalleled reliability.

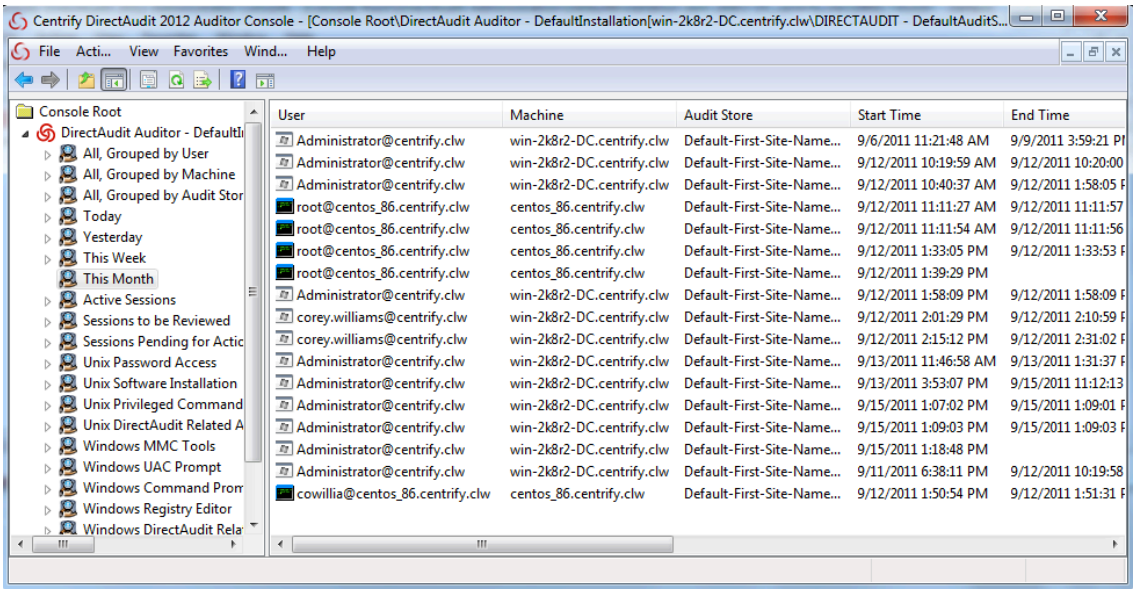
© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

- DirectAudit **Collector** — Executing as a Windows service to collect, compress and save to Audit Store, the Collector can handle dozens of users and hundreds of servers. Multiple Collectors can be deployed to provide load balancing and failover. New Collectors can be added on the fly with automatic configuration and discovery and no downtime.
- **Audit Store** — Built on Microsoft SQL Server and designed to help provide massive scalability and efficient use of network resources, Audit Stores help scale session databases to multiple instances on separate hosts. Audit Stores also provide automated or manual archiving and deleting of sessions with push button simplicity.
- **Audit Server** — Audit Servers provide central management and enforcement of Audit Roles and execution of distributed queries across the Audit Stores. Audit Servers also centrally control, monitor and report on Audit Stores, Smart Collectors and audited systems.
- Auditor and Administrator **Consoles** — Easy to learn and use, Windows-based consoles to provide search and replay of user activity and sessions as well as a central management console. The Auditor console seamlessly executes distributed auditor queries through a powerful query search or via ad-hoc Google style text queries. The Auditor also launches an elegant combination session replayer with support for session playback, navigation and export. The Administrative console provides central control and status of agents, collectors and stores. Additionally, the Administrative Console allows a manager to define and assign granular audit roles for limiting visibility and access to user session search and replay.



DirectAudit scales to thousands of systems through a reliable and fault-tolerant architecture that ensures high-availability and performance.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.



DirectAudit Console: View who is currently logged into an audited system their user name, the system they're logged into, and start time and drill down to watch sessions in real-time.

DirectAudit meets and exceeds the key requirements that every enterprise should consider when selecting a user activity auditing solution. And because Centrify Suite centralizes identities and privileges detailed reports of assigned rights, permissions and policies can be generated to complete compliance documentation such as the PCI DSS Report on Compliance (ROC).

Below is a mapping of Centrify's value-added features and benefits to the key capabilities enterprises require to deploy secure and effective privileged user activity auditing.

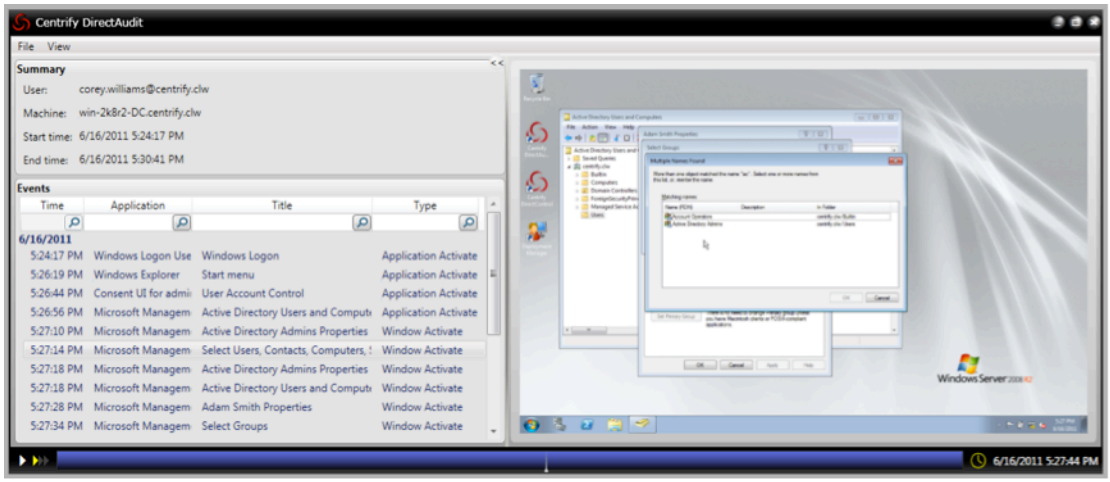
Capture and Collect

Below are the value-added features in Centrify DirectAudit for capturing and collecting cross-platform user sessions.

Category	Feature	Description
Capture	**Windows session auditing**	DirectAudit supports the capture of Windows sessions, in addition to UNIXand sessions.
	Multiple attached databases	A single Audit Store can support multiple attached databases for querying (with one of them the active — or receiving — database for new sessions).
	Massively scalable deployments	DirectAudit is designed to handle the added demand of Windows GUI sessions and many tens of thousands of audited systems of any platform.
	Selective auditing	Selectively capture user sessions based on Active Directory users or groups, to reduce the amount of collected data or limit auditing to those with privileged access.
Collect	**Audit Servers**	Audit Servers provide central management and enforcement of Audit Roles and execution of distributed queries across the Audit Stores. Audit Servers also centrally control, monitor and report on Audit Stores, Smart Collectors and audited systems.
	Audit Stores	Designed to help provide massive scalability and efficient use of network resources, Audit Stores help scale session databases to multiple instances on separate hosts.
	Smart Collectors	Support for automatic collector discover and service for network subnets in addition to Active Directory sites.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Search and Replay



DirectAudit's Replayer acts like a real-time camera and DVR supervising activity against privileged systems and recording all sessions to playback for suspicious activity and system troubleshooting.

Below are the value-added features in Centrify DirectAudit that make search and replay of relevant user sessions quick and easy.

Category	Feature	Description
Search	**Distributed auditor queries**	Queries and reports on sessions across multiple Audit Stores from a single Audit Server.
	Powerful query search	Wizard-driven, granular queries across distributed sets of sessions (distributed Audit Stores).
	Ad-hoc queries improved	Free-form search for commands, applications or text across distributed sets of sessions regardless of operating system.
Replay	**Combo session replayer**	Single session replayer supports both Window and UNIX session playback.
	Session scrubbing with preview	Visually examine a lengthy session through a scrub bar with quick preview window.
	Session magnify and zoom	Easily magnify the area under the cursor with the built-in magnifying glass; zoom in on session playback for easier reading or zoom out for a birds-eye view.
Share	**Export .wmv movies**	Both Windows and UNIX sessions an be exported to a standard movie format
	Export .txt transcript	UNIX sessions can further be exported as a text transcript and text can be selected and copied directly from the replay area
	Copy URI to clipboard	A shareable URI link can be copied to the clipboard for sharing a direct link to the current session with other auditors that have the replay tool installed

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Enterprise Ready and Integrated

Centrify DirectAudit is designed and built to deploy in enterprise environments large and small.

Category	Feature	Description
Enterprise Ready	**Auto-discover and configuration**	Audited system agents automatically find the correct collector; collectors automatically find the correct audit store; audit stores automatically find the right audit server. The administrative console provides information on the status of all agents and collectors in the installation.
	Dynamic reconfiguration	Many of the changes to DirectAudit system agents, collectors and audit stores can be applied without restarting the service or system.
	Fast & secure install	A single install for fast installation of all components on a single system (useful for pilots and demonstration systems). Ensures that only trusted components with trusted credentials are used with auto-discovery and configuration.
	SQL database	SQL database store provides maximum flexibility for query, backup and archiving.
Integrated	**Replayer CLI**	Enables integration with SIEM and third-party monitoring tools.
	Integration with MS SCOM	Drill down from an alert, then to the relevant session, and then to the specific user actions and commands.

Security Management

Centrify DirectAudit provides delegated administration for ease of management and to secure who has permissions audit servers across the data center and in cloud computing environments.

Feature	Description
Easy-to-add auditors	By basing access control on Audit Roles, auditor user permissions are assigned based on Active Directory group membership. Adding or removing auditors from an Audit Role is as easy as adding or removing group membership.
Audit security roles	You can now control or limit access to specific types of sessions using Audit Roles, which are defined as a query assigned to a named role.
Administrative delegation	Delegation of DirectAudit administration and management tasks based on Active Directory users or groups.

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Summary

Centrify DirectAudit is a powerful user-centric solution for supervising privileged activity so that enterprise's can a keep a close watch on privileged systems that contain sensitive data, are mission critical to business operations and require detailed auditing for compliance. These capabilities allow auditors, security and operations staff to quickly troubleshoot system failures and spot suspicious activity by replaying which users accessed which systems, what commands they executed, with what privilege, and the exact changes they made to key files and configurations. Centrify DirectAudit answers critical business and technical challenges enterprises face including compliance demands, mitigating insider attacks and third-party risks. By supervising activity against privileged systems DirectAudit enables a full accounting of a user's activity and system access. And DirectAudit is unique in supporting these auditing capabilities on Windows and major distributions of UNIX and Linux providing a complete solution for real-time and historical user activity auditing across a broad set of platforms deployed on-premise and in cloud computing environments.

Learn more:

View a 5-Minute DirectAudit Demo

http://www.centrify.com/directaudit/directaudit_demo.asp

Download a 30-day trial of DirectAudit for Windows

http://www.centrify.com/windowsaudit

Request a Free Evaluation of DirectAudit for UNIX, part of the Centrify Suite Enterprise Edition.

http://info.centrify.com/Centrify-DirectAudit-evaluation.html

© 2011 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.