Ⓢ Centrify®

Detailed Auditing and Playback of User Sessions on Windows, UNIX and Linux Servers

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 strengthens compliance reporting by recording user access to systems, specific commands and privileges used and the exact modifications to key files and configurations that were made. With DirectAudit enterprises can closely monitor IT contractors and offshore workers, pinpoint suspicious activity through real-time monitoring and troubleshoot system failures by replaying actions for root-cause analysis.

well as all system responses. The Agent forwards this data in an encrypted format to a DirectAudit Collector Service, which in turn compresses and stores the data in a central SQL Server database called an Audit Store.

Using the DirectAudit Console, you can play back any user session from any monitored system, run reports, perform searches and ad hoc queries, or conduct real-time monitoring of user sessions. Using third-party tools, you can run customized reports and queries as well.

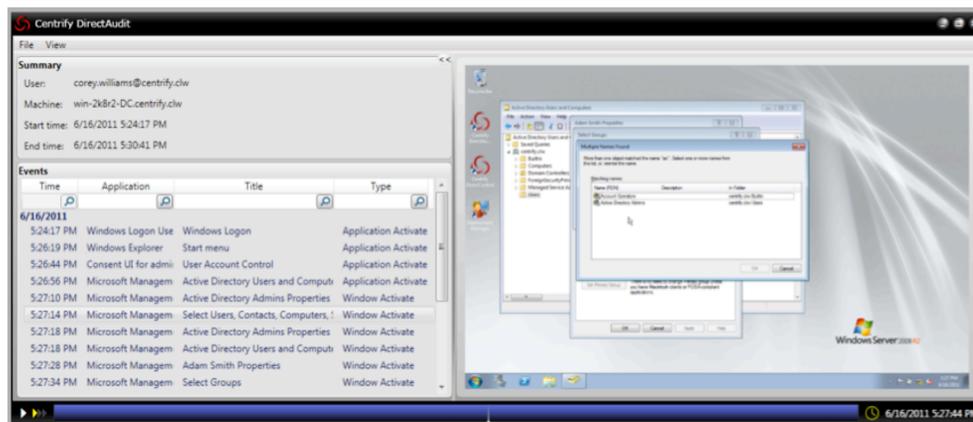Centrify DirectAudit is part of the Centrify Suite, an integrated set of solutions that also includes secure Active Directory-based authentication and single sign-on, role-based access control, privileged identity management, server isolation and encryption of data-in-motion.

DirectAudit delivers a high-fidelity user session playback with detailed summary events.

DirectAudit's easy-to-install, low-overhead Agent securely gathers all user session activity on a system — all user input as

DirectAudit's Key Benefits

Meet stringent auditing requirements
DirectAudit enables you to comply with stringent government and industry regulations that require you to audit and monitor privileged user activity: who accessed what systems, what commands they executed, and what files and data they changed. This detailed auditing also enables you to strengthen security by tracking suspicious activity and to enforce user accountability.

Strengthen security
DirectAudit strengthens security by mitigating the risk of internal threats through real-time monitoring which accelerates the identification of objectionable actions and ensures a complete context for user actions on systems implicated in a security incident.

Mitigate third party risk and promote best practices
DirectAudit mitigates the risks associated with driving cost efficiencies through outsourcing, off-shoring, contractors, managed service providers, cloud providers and ISVs by creating an environment that promotes proper user behavior and encourages self-regulation of corporate policies.

Reduce operational costs while increasing efficiency
DirectAudit permits in-depth troubleshooting and recording enabling automated documentation of vendor procedures, training processes and personnel hand-offs.

DirectAudit's Unique Features

Capture and collect privileged user sessions

Detailed, nonintrusive capture of user sessions on Windows, UNIX and Linux systems provides high fidelity, yet efficient capture of the user session video stream and detailed session metadata including applications ran, actions taken, commands executed as well as the complete system responses.

Search and replay entire user sessions

DirectAudit lets you play back any user session from any monitored system with a rich visual replay tool. It allows management to inspect user sessions to see what commands were executed, what changes were made to key files and data, and exactly what system responses appeared during the user's session.

Reliable, "always on" monitoring

Most auditing tools are not designed to work in large or complex enterprise environments. For example, some solutions stop collecting audit data if the network goes down. DirectAudit is designed to be highly reliable. If a network link goes down, it will continue to collect critical audit data and will subsequently forward that data to the Collector when the network is back up.

Enterprise-class scalability

DirectAudit supports multiple load-balanced Collectors gathering sessions from large numbers of monitored systems across your enterprise and storing sessions in one or more Audit Stores using a SQL Server database that can scale to support large data sets.
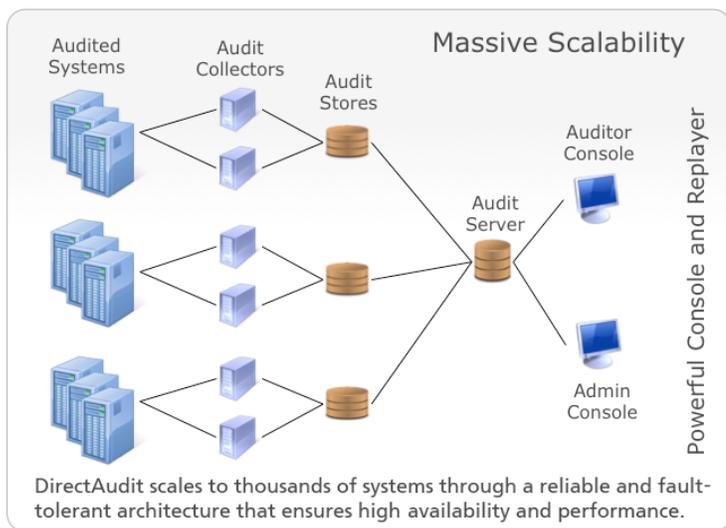
Automatic discovery and configuration

DirectAudit deployment, management and scaling are enterprise-class. Audited system agents automatically find the correct collector; collectors automatically find the correct audit store; audit stores automatically find the right audit server. Additional agents, collectors and stores can be added as necessary. The administrative console provides information on the status of all agents and collectors in the installation. Archiving or purging data is also easy and can be automated.

Real-time monitoring

Other auditing solutions provide only a historical view of what occurred. From its central console, DirectAudit also provides you with a real-time view of which users are currently logged on all systems. You can then drill down to see what an individual user is currently doing. This is key to not only spotting suspicious activity but to also quickly troubleshooting system issues.

How DirectAudit Works

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

Minimum hardware requirements

Collector machines
- Processor speed $\geq$ 2.4GHz multicore
- Recommended free disk space: 500 GB
- Basic OS memory usage: 30 GB+
- Additional memory per audited system served: 128KB – 400KB, based on level of streaming activity

About Centrify

Centrify is the leading provider of security and compliance solutions that centrally control, secure and audit access to cross-platform systems and applications using Active Directory.
Contact us at:

PHONE: +1 (408) 542-7500
EMEA: +44 (0) 1344 317950
EMAIL: info@centrify.com
WEB: www.centrify.com

To get started, try our 30-day trial version:
www.centrify.com/windowsaudit