

What's New in Centrify DirectAudit 2.0

Introduction

Centrify DirectAudit's detailed, real-time auditing of privileged user sessions on Windows, UNIX and Linux systems provides a full accounting of user activity and system access. DirectAudit's detailed logging of historical user activity establishes accountability and strengthens your compliance reporting by showing which users accessed what systems, what commands they executed, with what privilege, and what changes they made to key files and data. With DirectAudit you can also spot suspicious activity through real-time monitoring of current user sessions, and perform in-depth troubleshooting by replaying user activity that may have contributed to system failures.

Business Benefits

- Quickly address and dramatically lower your cost of compliance to mandates and regulations (including PCI, SOX, HITECH/HIPAA, SAS-70 type II, FISMA and many others).
- Lower business risk through raising visibility of elevated privilege use across your enterprise.
- Mitigate visibility risks associated with outsourcing and offshore service levels.
- Improve security and modify user behavior through real-time surveillance of privileged systems.
- Automatically document vendor procedures and mitigate personnel transitions and hand-offs.

Highlighted Features for DirectAudit 2.0

- **Windows Support.** DirectAudit 2.0 now supports the capture of Windows sessions, in addition to UNIX and Linux sessions, providing complete visibility across your IT environment.
- **Robust Architecture.** Scales to thousands of systems with high-availability and performance without sacrificing easy deployment and management of the entire solution.
- **Combo Session Replayer.** Rewritten from the ground up, the new version of the DirectAudit session replayer supports both Windows and UNIX sessions.

Key Capabilities of DirectAudit

Capture and Collect

- High resolution and efficient capture of session video and metadata.
- Encryption and compression of session and metadata both in motion and at rest.

Search and Replay

- Easy-to-use console for session search with rich visual replay and export of user sessions.
- Summarized activity and command log of each session for easy navigation.

Enterprise Ready and Integrated

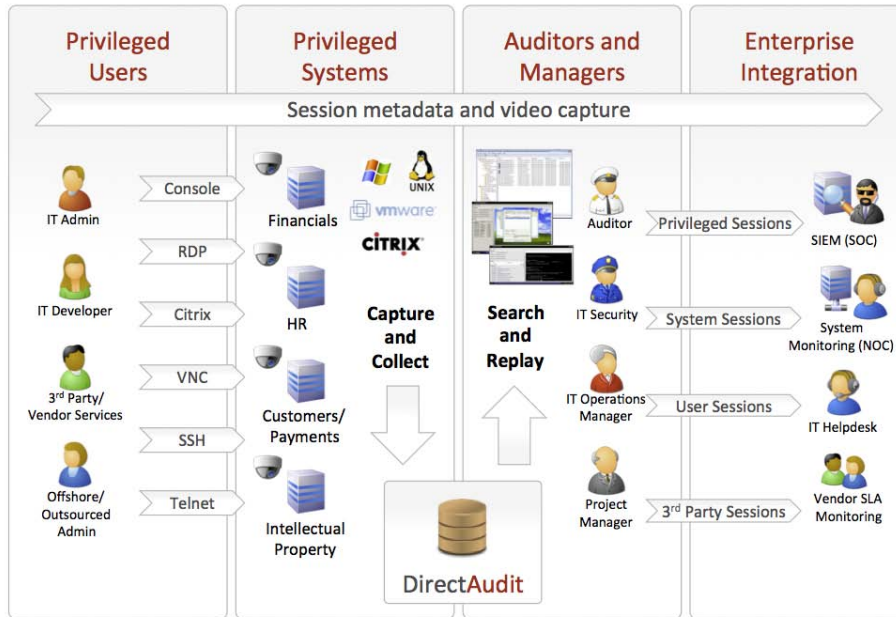
- Distributed scalable session stores with automated rolling databases for easy archive and backup.
- Command-line interface for replayer integration into leading monitoring and SIEM products.

Security Management

- Highly scalable and distributable solution with automated deployment and configuration.
- Flexible role-based access to session replay and platform administration.

New Feature and Enhancement Detail

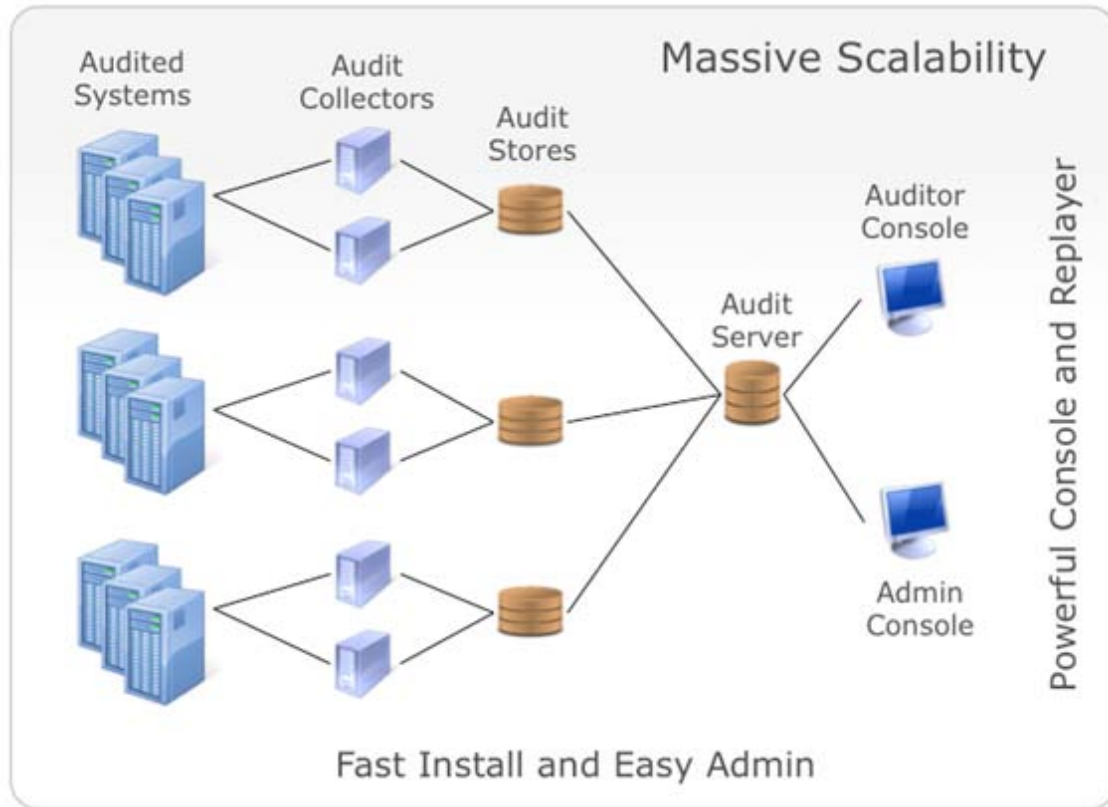
DirectAudit 2.0 is an integrated component of Centrify Suite 2012 Enterprise Edition, the leading solution for controlling, securing and auditing access to cross-platform systems and applications using Active Directory. Below is a detailed depiction of just some of the over 75 new features of DirectAudit 2.0. DirectAudit capabilities include session capture and collection, search and replay, enterprise readiness and integration, and security management.



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.

Capture and Collect

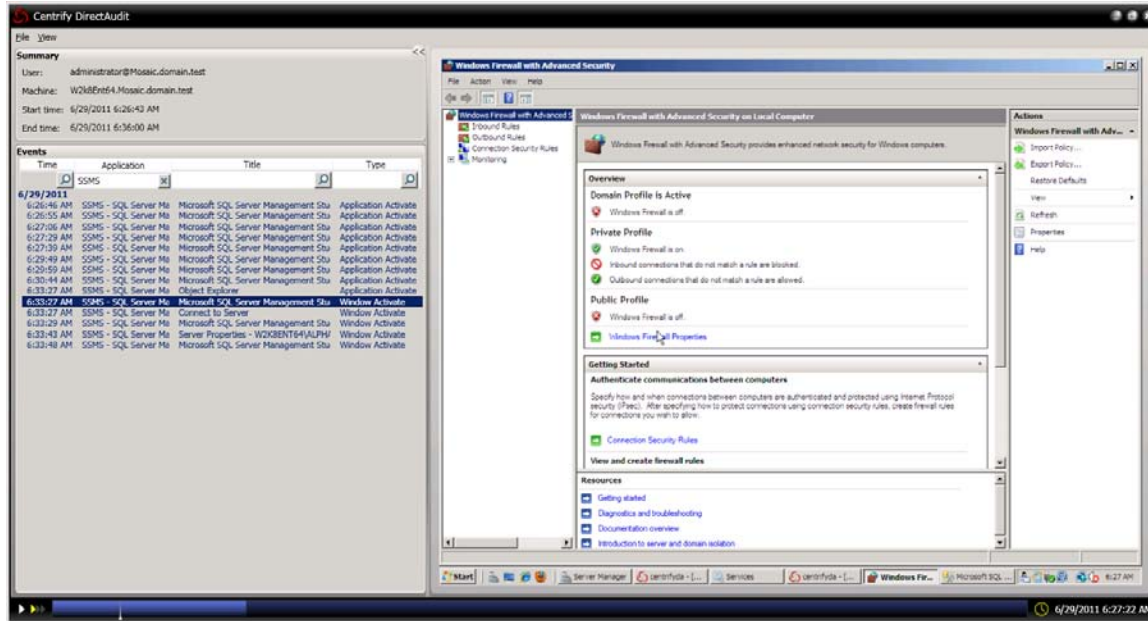
Category	Feature	Description
Capture	Windows session auditing	DirectAudit 2.0 now supports the capture of Windows sessions, in addition to UNIX sessions.
	Multiple attached databases	A single Audit Store can support multiple attached databases for querying (with one of them the active – or receiving – database for new sessions). An attached database can also include DirectAudit 1.x databases.
	Massively scalable deployments	DirectAudit 2.0 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.



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

Search and Replay

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.



The DirectAudit Replayer acts like a user helmet camera, supervising activity against privileged systems and recording all sessions to playback for suspicious activity and system troubleshooting.

Enterprise Ready and Integrated

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.
Integrated	SQL database	SQL database store provides maximum flexibility for query, backup and archiving.
	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

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.

Centrify DirectAudit 2.0 Technical Specifications

New Operating Systems Support

- Microsoft Windows 2003, 2008, 2008 R2 (all editions, both 32- and 64-bit)
- Fedora 15 (32- and 64-bit)
- Ubuntu Server 11.04 (32- and 64-bit)
- Oracle Enterprise Linux 6 (32- and 64-bit)
- Plus dozens of existing platform releases:
<http://www.centrify.com/products/all-supported-platforms.asp#directaudit>

Minimum Hardware Requirements

Collector Machines

- Processor speed \geq 2.4GHz
- Recommended free disk space: 500 GB
- Basic OS memory usage: 30 GB+
- Additional memory usage per agent served: 128KB – 400KB
 - agent sending steady stream of large amounts of data

SQL Server Machines

- Processor speed \geq 2.4GHz, multicore
- Dedicated to the SQL Server system

Additional DirectAudit Enhancements

- Generate DBA scripts for DB actions
- DirectAudit agent status in console
- Collector status in console
- Audit Store status in console
- dadebug CLI utility
- dadiag enhanced to report low disk space
- Support for multiple installations
- Session events shown in replayer
- Session events clickable in replayer
- Session events filterable in replayer
- Session events sortable in replayer
- Session events for *NIX and Windows
- Session summary in replayer
- Toggle real-time and linear playback
- Preview in session scrub bar
- Easier speed control in replayer
- Export of diagnostics format in replayer
- Improved look and feel in replayer
- Partial buffering in replayer
- Improved performance in replayer
- MSI packaging for all components
- Improved quick install
- Support for concurrent active agents licensing
- Unlimited use of auditor console licensing
- Support for multiple versions of DA on same server