

## Detailed, real-time auditing of user sessions on UNIX and Linux systems and hypervisors

Centrify DirectAudit addresses regulatory compliance requirements for auditing, logging and reporting on user activity within your UNIX/Linux environment. It also helps you detect suspicious activity, conduct in-depth troubleshooting, and perform real-time monitoring of your UNIX/Linux systems.

DirectAudit's easy-to-install, low-overhead Agent silently gathers all user session activity on a system — all user input as well as all system responses. The Agent forwards this data in a compressed, encrypted format to a DirectAudit Collector Service, which in turn stores the data in a central SQL Server database.

Using the DirectAudit Console, you can play back any user session on 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, a integrated set of solutions that also include secure Active Directory-based authentication and single sign-on, role-based access control, privileged identity management, user-level auditing, server isolation and encryption of data-in-motion..

### DirectAudit's Key Benefits

#### Meet stringent auditing requirements

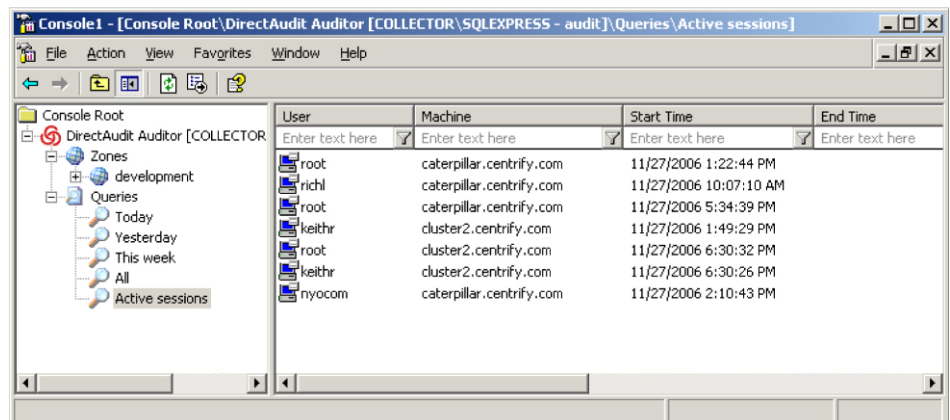
DirectAudit enables you to comply with stringent government and industry regulations that require you to log and track user activity: who accessed what systems, what commands they executed, and what files and data they changed. This detailed auditing also enables you to strengthen security in general by tracking suspicious activity and to enforce user accountability. With DirectAudit you can answer questions such as:

- Who logged onto our UNIX servers running our ERP apps over the last month, and what did they do?
- What was that recently fired systems admin doing on our systems last week?
- Has anyone edited these key system files, or typed suspicious commands?

#### Conduct in-depth diagnostics

DirectAudit lets you replay and report on user activity that may have contributed to a system outage and to identify changes made by users. Data capture and replay includes all keystrokes as well as responses that appeared during the session. With DirectAudit you can find out the answer to questions such as:

- Did anybody do anything to the Oracle config file on sol-ora-4 yesterday?



The screenshot shows the DirectAudit Console interface. On the left is a tree view with 'Active sessions' selected. The main area displays a table with columns: User, Machine, Start Time, and End Time. The table contains several rows of session data.

User	Machine	Start Time	End Time
root	caterpillar.centrify.com	11/27/2006 1:22:44 PM	
richl	caterpillar.centrify.com	11/27/2006 10:07:10 AM	
root	caterpillar.centrify.com	11/27/2006 5:34:39 PM	
keithr	cluster2.centrify.com	11/27/2006 1:49:29 PM	
root	cluster2.centrify.com	11/27/2006 6:30:32 PM	
keithr	cluster2.centrify.com	11/27/2006 6:30:26 PM	
nyocom	caterpillar.centrify.com	11/27/2006 2:10:43 PM	

The DirectAudit Console provides a real-time view of who is logged in to specific systems.

- Did Operations actually apply that required patch on all 10 of our web servers over the weekend?
- Why is this system misbehaving? Did anyone touch it over the last few days?

#### Perform real-time monitoring

DirectAudit provides you with a central view into who is currently accessing all of your distributed UNIX/Linux systems and what activities they are performing. With it you can answer questions such as:

- Is anyone logged onto those development systems that we need to restart?
- What is the consultant who is logged on that ailing Linux server actually doing to fix the problem?

## DirectAudit's Unique Features

### Detailed logging of user input and system responses

Most auditing tools simply capture who logged on and when. DirectAudit captures all keystrokes as well as the system responses during the user's session. This level of detail is essential to comply with regulatory requirements and provides indispensable insight for troubleshooting.

### Ability to replay entire user sessions

DirectAudit lets you play back any user session on any monitored system. You can 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 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 DirectAudit Collector Service when the network is back up.

### Enterprise-class scalability

DirectAudit supports multiple load-balanced Collector Services

gathering data from large numbers of monitored systems across your enterprise. It stores data in a central SQL Server database that can act as a large-scale data warehouse.

### Open SQL data storage format

Unlike other solutions that store data in proprietary formats, DirectAudit uses a SQL Server database. This makes reporting and searching on all the session data easy via either the DirectAudit Console or third-party reporting tools. Archiving or purging data is likewise easy as well.

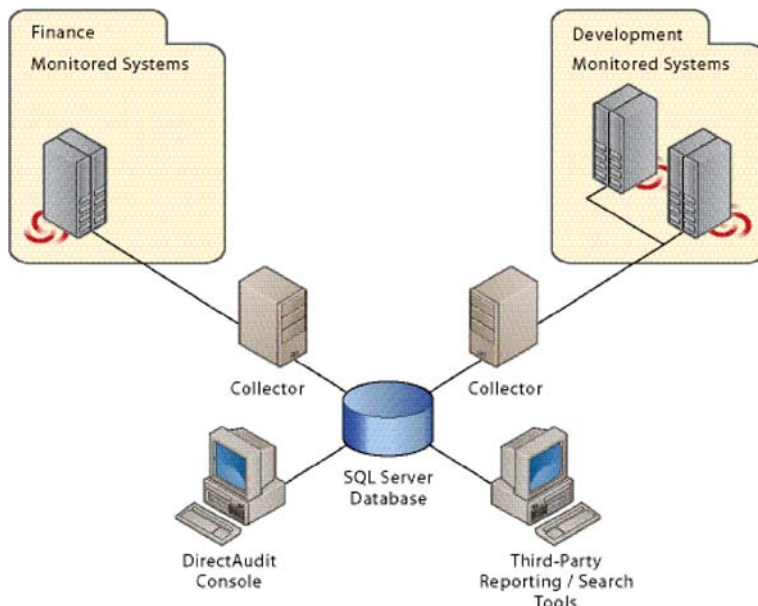
### Robust ad hoc querying and reporting

Other solutions that use proprietary data formats severely limit your ability to perform ad hoc queries. DirectAudit not only provides summary reporting but also the ability to perform full-text searches to pinpoint specific keywords. Mining key audit and system availability is as easy as searching the Internet.

### Real-time monitoring

Other auditing solutions provide only a historical view of what occurred. From its central console, DirectAudit 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



The DirectAudit Agent records user sessions on monitored systems and forwards these logs to the DirectAudit Collector Service. For scalability in large environments, Centrifry supports load balancing across multiple DirectAudit Collector Services. The DirectAudit Collection Service forwards logs to a central SQL database for consolidated reporting and auditing. You can use the DirectAudit Console to replay user sessions, run reports, perform queries, and do real-time monitoring. You can also use third-party tools to create your own customized reports and queries.

### About Centrifry

Centrifry is the leading provider of security and compliance solutions that centrally control, secure and audit cross-platform systems and applications using Active Directory.

To contact us at:

PHONE: +1 (408) 542-7500

EMEA: +44 (0) 1344 317950

EMAIL: [info@centrifry.com](mailto:info@centrifry.com)

WEB: [www.centrifry.com](http://www.centrifry.com)

To get started, try our free version:

[www.centrifry.com/express](http://www.centrifry.com/express)

Copyright © 2005-2011 Centrifry Corporation. All rights reserved. Centrifry, DirectAudit and DirectControl are trademarks of Centrifry Corporation. DS-011-2011-02-15