

Centrify Infrastructure Services 19.9

Auditing & Monitoring Service 3.6.1

Release Notes

© 2007-2019 Centrify Corporation.

This software is protected by international copyright laws.

All Rights Reserved.

Contents

1.	About Centrify Auditing & Monitoring Service.....	4
2.	Feature Changes.....	5
2.1	Feature Changes in Centrify Auditing & Monitoring Service 3.6.1 (Release 19.9)	5
2.1.1	General	5
2.1.1.1	Compatibility	6
2.1.2	Security Fix.....	6
2.1.3	Centrify Audit Collector	6
2.1.4	Centrify Audit Analyzer and Session Player	6
2.1.5	Centrify Audit Manager	6
2.1.6	Centrify DirectAudit Agent for *NIX.....	7
2.1.7	Database	7
2.1.8	FindSessions Tool	7
2.1.9	Centrify Agent for Windows	7
2.1.10	Centrify Audit Module for PowerShell Centrify	7
2.1.11	Centrify Audit Management Server	7
2.1.12	Supported Platforms	7
2.2	Feature Changes in Centrify Auditing & Monitoring Service 3.6.0 (Release 19.6)	8
2.2.1	General	8

2.2.1.1	Compatibility	8
2.2.2	Centrify Audit Collector	8
2.2.3	Centrify Audit Analyzer and Session Player	9
2.2.4	Centrify Audit Manager	9
2.2.5	Centrify DirectAudit Agent for *NIX	9
2.2.6	Database	9
2.2.7	FindSessions Tool	9
2.2.8	Centrify Agent for Windows	9
2.2.9	Centrify Audit Module for PowerShell	9
2.2.10	Supported Platforms	9
2.3	Feature Changes in Centrify Auditing & Monitoring Service 3.5.2 (Release 18.11)	10
2.3.1	General	10
2.3.2	Centrify Audit Collector	10
2.3.3	Centrify Audit Analyzer and Session Player	10
2.3.4	Centrify Audit Manager	10
2.3.5	Centrify DirectAudit Agent for *NIX	10
2.3.6	Database	10
2.3.7	FindSessions Tool	11
2.3.8	Centrify Agent for Windows	11
2.3.9	Centrify Audit Module for PowerShell	11
2.3.10	Supported Platforms	11
3.	Bugs Fixed	11
3.1	Bugs Fixed in DirectAudit 3.6.1 (Release 19.9)	11
3.1.1	General	11
3.1.2	Windows Install / Upgrade / Uninstall	11
3.1.3	Centrify Audit Collector	12
3.1.4	Centrify Audit Analyzer and Session Player	12
3.1.5	Centrify Audit Manager	12

3.1.6	Centrify DirectAudit Agent for *NIX	12
3.1.7	Database	12
3.1.8	FindSessions Tool	12
3.1.9	Centrify Agent for Windows	12
3.1.10	Centrify Audit Module for PowerShell	12
3.1.11	Audit Management Server	12
3.2	Bugs Fixed in DirectAudit 3.6.0 (Release 19.6)	12
3.2.1	General	12
3.2.2	Windows Install / Upgrade / Uninstall	12
3.2.3	Centrify Audit Collector	12
3.2.4	Centrify Audit Analyzer and Session Player	13
3.2.5	Centrify Audit Manager	13
3.2.6	Centrify DirectAudit Agent for *NIX	13
3.2.7	Database	13
3.2.8	FindSessions Tool	13
3.2.9	Centrify Agent for Windows	13
3.2.10	Centrify Audit Module for PowerShell	13
3.2.11	Audit Management Server	13
3.3	Bugs Fixed in DirectAudit 3.5.2 (Release 18.11)	13
3.3.1	General	13
3.3.2	Windows Install / Upgrade / Uninstall	13
3.3.3	Centrify Audit Collector	14
3.3.4	Centrify Audit Analyzer and Session Player	14
3.3.5	Centrify Audit Manager	14
3.3.6	Centrify DirectAudit Agent for *NIX	14
3.3.7	Database	14
3.3.8	FindSessions Tool	15
3.3.9	Centrify Agent for Windows	15

3.3.10	Centrify Audit Module for PowerShell	15
4.	Known Issues.....	15
4.1	General	16
4.2	Windows Install / Upgrade / Uninstall	16
4.3	Collector	16
4.4	Audit Analyzer and Session Player	17
4.5	Audit Manager	18
4.6	Centrify DirectAudit Agent for *NIX	18
4.6.1	General.....	18
4.6.2	RedHat Linux.....	21
4.6.3	Debian Linux.....	21
4.6.4	Solaris.....	22
4.6.5	AIX.....	23
4.6.6	HPUX.....	24
4.7	Database	25
4.8	Audit Management Server	26
4.9	FindSession Tools	26
4.10	Centrify Agent for Windows	26
4.11	Centrify Audit Module for PowerShell	27
5.	Additional Information and Support.....	28

1. About Centrify Auditing & Monitoring Service

Centrify Infrastructure Services is a product category that includes the following product offerings:

- Centrify Privileged Access Service
- Centrify Authentication Service
- Centrify Privilege Elevation Service
- Centrify Auditing & Monitoring Service

The DirectControl Agent provides services for the Authentication Service and Privilege Elevation Service contained in the CentrifyDC packages. The

DirectAudit Agent provides services for Auditing & Monitoring Service contained in the CentrifyDA packages.

The **Centrify Auditing & Monitoring Service** is a key component of Centrify Infrastructure Services. It enables detailed auditing of user activity on a wide range of UNIX, Linux, and Windows computers. With this service, you can perform immediate, in-depth troubleshooting by replaying user activity that may have contributed to system failures, spot suspicious activity by monitoring current user sessions, improve regulatory compliance, and ensure accountability by capturing and storing detailed information about the applications used and the commands executed. If you enable auditing, the Centrify Agent for Windows records user activity on the Windows computer when it is installed. Centrify Auditing & Monitoring Service supports auditing of many different UNIX, Linux, and Windows operating systems. For a list of the platforms supported, see the document in www.centrify.com/platforms.

In Unix and Linux agents, Centrify DirectControl Agent is a pre-requisite for the Auditing & Monitoring service.

Starting in Release 2016, only ADMX format for group policies will be installed and ADM format will no longer be provided. (Ref: CS-6821)

Starting in Release 2016, Centrify will no longer be adding new features to the Centrify DirectManage Audit SDK component. Centrify recommends all existing users of this component to start using Centrify Audit Module for PowerShell component, which is the intended replacement of the SDK. (Ref: CS-6713)

From Release 2017.1 onward, DirectAudit no longer supports Version 1 Audit Store databases. You will no longer be able to attach Version 1 databases to an existing DirectAudit installation. To view data from version 1.x databases, please install a DirectAudit Auditor Console 1.x and attach the database. (Ref: CS-41219)

This release note updates information available in the DirectAudit Administrator's Guide and describes known issues. You can obtain information about previous releases from the Centrify Support Portal, in the Product Documentation page.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,378,391 and 9,442,962. (Ref: CS-44575)

2. Feature Changes

2.1 Feature Changes in Centrify Auditing & Monitoring Service 3.6.1 (Release 19.9)

2.1.1 General

- DirectAudit now supports auditing of Windows and Linux systems that are enrolled with the Centrify cloud platform and may not be joined to an Active Directory domain. (Ref: CS-47839)

- DirectAudit has introduced a new component named "Audit Extension for Centrify Client" which facilitates auditing of Windows systems that are enrolled with the Centrify cloud platform. (Ref: CS-47838)

2.1.1.1 Compatibility

- With the Centrify Agent for Windows version 19.6 and later, the Audit and Monitoring Service uses a different compression library to compress the video data being sent from the agent to the collector. As a result, this agent is **not** compatible with audit collector versions 18.11 or earlier. **IMPORTANT: You will lose video data if you deploy the newer agents in an environment with older collectors.** Audit trail events and indexed events lists are not affected in this situation.

Because of this incompatibility and risk of data loss, you **MUST** upgrade all of your collectors to the latest version **BEFORE** you upgrade the agents to 19.9.

As a reminder, before you upgrade the collectors you must first upgrade the database schema. So, to summarize, here's the order in which you upgrade the audit components:

1. Upgrade the database.
2. Upgrade the collectors.
3. Upgrade the agents.

2.1.2 Security Fix

- Fixed a security vulnerability in Centrify DirectAudit that allowed an attacker to perform remote code execution - related to .NET framework vulnerability detailed in CVE-2012-0161. (Ref: CS-48368)

2.1.3 Centrify Audit Collector

- DirectAudit Collector now supports auditing of both Active Directory joined systems and the systems enrolled with the Centrify cloud platform using an SSL/TLS based communication channel. (Ref: CS-47837)

2.1.4 Centrify Audit Analyzer and Session Player

- Audit Analyzer console's results pane now displays audited session's identifier (a.k.a. SessionId) for each of the returned results. (Ref: CS-48133)

2.1.5 Centrify Audit Manager

N/A

2.1.6 Centrify DirectAudit Agent for *NIX

- Centrify DirectAudit Agent for Linux now facilitates auditing of Linux systems that are not joined to an Active Directory domain. (Ref: CS-47839)
- The '/sbin/shutdown' has now been added to the list of nologin shells viz. nss.nologin.shell (Ref: CS-48180)
- The following programs have been added to the default value of nss.program.ignore: polkitd, abrt, dbus-daemon, systemd-tmpfiles, systemd-journald and crond (Ref: CS-48177)

2.1.7 Database

N/A

2.1.8 FindSessions Tool

N/A

2.1.9 Centrify Agent for Windows

N/A

2.1.10 Centrify Audit Module for PowerShell Centrify

- Centrify Audit Module for PowerShell now supports permanent deletion of audit trail events based on the specified search criteria. (Ref: CS-48167)

2.1.11 Centrify Audit Management Server

N/A

2.1.12 Supported Platforms

For the list of the supported platforms by this release, refer to the "Supported Platforms" section in the Centrify Infrastructure Services release notes.

For the platforms to be removed support in coming releases, refer to the "Notice of Termination Support" section in the Centrify Infrastructure Services release notes.

For a complete list of supported platforms in the latest releases, refer to the 'Centrify Infrastructure Services' section in the document available from www.centrify.com/platforms.

2.2 Feature Changes in Centrify Auditing & Monitoring Service 3.6.0 (Release 19.6)

2.2.1 General

2.2.1.1 Compatibility

- With the Centrify Agent for Windows version 19.6 and later, the Audit and Monitoring Service uses a different compression library to compress the video data being sent from the agent to the collector. As a result, this agent is **not** compatible with audit collector versions 18.11 or earlier. **IMPORTANT:** You will lose video data if you deploy the newer agents in an environment with older collectors. Audit trail events and indexed events lists are not affected in this situation.

Because of this incompatibility and risk of data loss, you **MUST** upgrade all of your collectors to the latest version **BEFORE** you upgrade the agents to 19.6.

As a reminder, before you upgrade the collectors you must first upgrade the database schema. So, to summarize, here's the order in which you upgrade the audit components:

4. Upgrade the database.

5. Upgrade the collectors.

6. Upgrade the agents.

- The minimum Centrify DirectControl Agent for *NIX version required by this version of the service is 5.4.0 (Release 2017) with the following exceptions:

On AIX, Linux PowerPC platforms, Centrify DirectControl Agent must be Release 2017.3 or later. (Ref: CS-44597, CS-44749, CS-44601)

On Solaris x86 and SPARC platforms, Centrify DirectControl Agent must be Release 2018 or later because the Solaris x86 packages have been changed to 64-bit in this release - The packages still provide 32-bit libraries to work with 32-bit programs. (Ref: CS-44594, CS-44084)

2.2.2 Centrify Audit Collector

- Updated encryption algorithm used in communications to Audit Collectors from 3DES to AES. (Ref: CS-47491)
- Upgrade compression library (quicklz) to the latest stable version. (Ref: CS-47546)

2.2.3 Centrify Audit Analyzer and Session Player

- Session player now generates audit trail events when user starts playing a session. (Ref: CS-47906)
- Session player now allows auditors to update the review status of the audited session. (Ref: CS-47734)

2.2.4 Centrify Audit Manager

N/A

2.2.5 Centrify DirectAudit Agent for *NIX

N/A

2.2.6 Database

N/A

2.2.7 FindSessions Tool

N/A

2.2.8 Centrify Agent for Windows

- Updated encryption algorithm used in communications to Audit Collectors from 3DES to AES. (Ref: CS-47491)
- Upgrade compression library (quicklz) to the latest stable version. (Ref: CS-47546)

2.2.9 Centrify Audit Module for PowerShell

N/A

2.2.10 Supported Platforms

For the list of the supported platforms by this release, refer to the "Supported Platforms" section in the Centrify Infrastructure Services release notes.

For the platforms to be removed support in coming releases, refer to the "Notice of Termination Support" section in the Centrify Infrastructure Services release notes.

For a complete list of supported platforms in the latest releases, refer to the 'Centrify Infrastructure Services' section in the document available from www.centrify.com/platforms.

2.3 Feature Changes in Centrify Auditing & Monitoring Service 3.5.2 (Release 18.11)

2.3.1 General

- Centrify DirectAudit now allows administrators to specify the system-type affinity when creating a new Audit Store. This can help separate and direct audited data from the Unix systems and the Windows systems to two different Audit Stores even when the systems belong to the same site or subnet. The Centrify Agent for Windows or Unix must be upgraded to the latest version in order to use this feature. (Ref: CS-43582)
- Centrify Infrastructure Services ISO now packages Microsoft SQL Server 2016 Express with Advanced Services SP2 for Centrify Auditing & Monitoring Service. (Ref: CS-46849)

2.3.2 Centrify Audit Collector

- Collector Control Panel now generates audit trail events when user starts, stops or restarts the collector service. (Ref: CS-46577)

2.3.3 Centrify Audit Analyzer and Session Player

N/A

2.3.4 Centrify Audit Manager

- Audit Management Server Control Panel now generates audit trail events when user starts, stops or restarts the audit management service. (Ref: CS-46577)

2.3.5 Centrify DirectAudit Agent for *NIX

- Compatibility

The minimum Centrify DirectControl Agent for *NIX version required by this version of the service is 5.4.0 (Release 2017) with the following exceptions:

- On AIX, Linux PowerPC platforms, Centrify DirectControl Agent must be Release 2017.3 or later. (Ref: CS-44597, CS-44749, CS-44601)
- On Solaris x86 and SPARC platforms, Centrify DirectControl Agent must be Release 2018 or later because the Solaris x86 packages have been changed to 64-bit in this release - The packages still provide 32-bit libraries to work with 32-bit programs. (Ref: CS-44594, CS-44084)

2.3.6 Database

N/A

2.3.7 FindSessions Tool

N/A

2.3.8 Centrify Agent for Windows

N/A

2.3.9 Centrify Audit Module for PowerShell

- Added new cmdlets to retrieve DirectAudit permissions (Ref: CS-46247):
 - Get-CdaInstallationRight
 - Get-CdaManagementDatabaseRight
 - Get-CdaAuditStoreRight
 - Get-AuditRoleRight
 - Get-CdaQueryRight

2.3.10 Supported Platforms

For the list of the supported platforms by this release, refer to the "Supported Platforms" section in the Centrify Infrastructure Services release notes.

For the platforms to be removed support in coming releases, refer to the "Notice of Termination Support" section in the Centrify Infrastructure Services release notes.

For a complete list of supported platforms in the latest releases, refer to the 'Centrify Infrastructure Services' section in the document available from www.centrify.com/platforms.

3. Bugs Fixed

3.1 Bugs Fixed in DirectAudit 3.6.1 (Release 19.9)

3.1.1 General

N/A

3.1.2 Windows Install / Upgrade / Uninstall

N/A

3.1.3 Centrify Audit Collector

- Fixed an issue in the DirectAudit Collector that previously resulted into a paused spool when the DirectAudit Linux/Unix agent tried to resend previously de-spoiled audited data. (Ref: CS-48234)

3.1.4 Centrify Audit Analyzer and Session Player

N/A

3.1.5 Centrify Audit Manager

N/A

3.1.6 Centrify DirectAudit Agent for *NIX

- Fixed a bug in dad that previously resulted into reuse of the same session identifier (GUID) for two or more audited sessions. (Ref: CS-48166)

3.1.7 Database

N/A

3.1.8 FindSessions Tool

N/A

3.1.9 Centrify Agent for Windows

N/A

3.1.10 Centrify Audit Module for PowerShell

N/A

3.1.11 Audit Management Server

- Fixed an issue in the DirectAudit Audit Management Server that previously resulted into failure in calculating the effective size of the audited sessions. (Ref: CS-48099)

3.2 Bugs Fixed in DirectAudit 3.6.0 (Release 19.6)

3.2.1 General

N/A

3.2.2 Windows Install / Upgrade / Uninstall

N/A

3.2.3 Centrify Audit Collector

N/A

3.2.4 Centrify Audit Analyzer and Session Player

N/A

3.2.5 Centrify Audit Manager

N/A

3.2.6 Centrify DirectAudit Agent for *NIX

- Fixed a bug such that when the NSS module is inactive and 'ssh' is enabled for command auditing, the password won't be echoed while running 'scp' and inputting user password. (Ref: CS-47527)
- Fixed a bug where DirectAudit agent 'dad' (or DirectControl agent 'adclient') process running in docker container is stopped when DirectAudit (or DirectControl) is upgraded on docker host. (Ref: CS-47406)

3.2.7 Database

N/A

3.2.8 FindSessions Tool

N/A

3.2.9 Centrify Agent for Windows

- Fixed an issue in the DirectAudit Windows daemon (dad) that sometimes resulted in auditing getting stopped if the remote host viz. the wash or the wash32 process forcibly closed the stream. (Ref: CS-47534)

3.2.10 Centrify Audit Module for PowerShell

N/A

3.2.11 Audit Management Server

- Fixed an issue in the Audit Management Server that previously resulted in service using the Windows authentication for fetching information from the Management database even when configured to use SQL Server authentication. (Ref: CS-47924)

3.3 Bugs Fixed in DirectAudit 3.5.2 (Release 18.11)

3.3.1 General

N/A

3.3.2 Windows Install / Upgrade / Uninstall

N/A

3.3.3 Centrifify Audit Collector

N/A

3.3.4 Centrifify Audit Analyzer and Session Player

N/A

3.3.5 Centrifify Audit Manager

- The database status will now be shown as Connected vs Disconnected in Audit Manager instead of Online vs Offline to be consistent with Audit Module for PowerShell. (Ref: CS-46501)

3.3.6 Centrifify DirectAudit Agent for *NIX

- Fixed an issue where 'Machine' column showed inconsistency between 'Audit sessions' of 'Audit Analyzer' and 'Audited Systems' of 'Audit Manager' if agent.send.hostname was set to true. Note that the user can use the "--hostname" parameter to specify the hostname for the container in the docker run command, and it is the hostname reported. (Ref: CS-45779)
- Fixed an issue where 'File Name' column showed incorrect filename on 'File Monitor Report' when running 'mv' to rename a file which already existed. (Ref: CS-46361)
- Sessions generated by a VNC terminal are now being audited. Do the following to enable it. (Ref: CS-46818)
 - Instead of using "vncserver :<display>" to start the VNC Server, use "SHELL=/bin/cdax/bash vncserver :<display>"
- Fixed an issue such that if Apparmor service is not running, join/leave a domain or enable/disable DirectAudit will not change the status of Apparmor service any more. (Ref: CS-46831)
- Fixed the issue where after upgrading DirectAudit on a CoreOS host, DirectAudit daemon inside the container needs to be restarted. (Ref: CS-46897)
- Fixed the issue where after uninstalling DirectAudit on a CoreOS host, DirectAudit daemon inside the container needs to be restarted. (Ref: CS-47351)
- Fixed 'dacheck' for RHEL 7.4 and up to include missing libraries in the dependency check. (Ref: CS-47276)

3.3.7 Database

N/A

3.3.8 FindSessions Tool

N/A

3.3.9 Centrify Agent for Windows

- Fixed an issue where Audit notification message window may not appear if an audited user logged in immediately after a machine was restarted and the corresponding installation turned on Audit notification. (Ref: CS-46580)
- Fixed an issue where Audit status on desktop notification message is not displayed correctly when group policy "Specify whether to keep the desktop notification message permanently visible" is enabled. (Ref: CS-46756)

3.3.10 Centrify Audit Module for PowerShell

- Fixed an issue in Set-CdaAuditStore and Set-CdaManagementDatabase that it cannot set AD site from remote forest. (Ref: CS-46718)
- Fixed an issue where specifying an account from remote forest in "Domain\Account" format as an input parameter would fail for the following cmdlets. (Ref: CS-46719)
 - New-CdaAuditRoleAssignment to create a role assignment with -Assignee parameter
 - Set-CdaManagementDatabase to set incoming users with -AllowedIncomingUsers parameter
 - Set-CdaAuditStore to set trusted agents with -TrustedAgents parameter and set trusted collectors with -TrustedCollectors parameter
 - Set-CdaAuditSessionReviewer to set reviewers with -Reviewers parameter
 - Set-CdaDatabase to set allowed collectors with -AllowedCollectors parameter and set allowed management servers with -AllowedManagementServers parameter
- Fixed an issue in the New-CdaAuditStore Powershell cmdlet to validate the specified scope of the Audit Store being created. Centrify recommends customers to not use the New-CdaAuditStore cmdlet from an older version of "Audit Module for Powershell" if they have upgraded their backend databases because doing so may result in creation of multiple Audit Stores with conflicting scopes. (Ref: CS-47161)

4. Known Issues

The following sections describe known issues, suggestions, and limitations associated with DirectAudit.

4.1 General

For the most up-to-date list of known issues, refer to the knowledge base articles in the Centrify Support Portal.

4.2 Windows Install / Upgrade / Uninstall

- On a Windows 2008/2008 R2 Core system, if user elects the option to launch the configuration wizard at the end of "Centrify Agent for Windows" installation wizard, installer will launch the older version of configuration wizard because of lack of support for Windows Presentation Foundation on these operating systems. (Ref: CS-43733)
- If a DirectManage Audit installation has been configured with multiple Audit Management Servers and some of the servers are running on an older version, the Audit Manager may not list these older servers because the new servers list supersedes the older ones. (Ref: CS-40818)
- When upgrading DirectAudit in Windows, you should use the autorun program to perform the upgrade. The autorun program automatically upgrades other Centrify components such as Centrify Licensing Report. If you upgrade DirectAudit components individually using the Microsoft Installer (msi) and then attempt to use the autorun program to uninstall all components, autorun will only be able to uninstall the Centrify Licensing Report that were upgraded to the latest version. You can remove any remaining components manually using the Add/Remove Programs and Features Control Panel. (Ref: 46293a)
- If you run setup.exe with all DirectAudit components selected for installation on a single computer, the operation is known as the "Easy Install." Although this is the default for new installations, using the "Easy Install" option requires you to have local administrator privileges.
- If you uninstall the collector component on a computer that is not joined to the domain, you will see the following messages during an uninstall operation:

The specified domain either does not exist or could not be contacted.

(Exception from HRESULT: 0x8007054B)

Despite the alert message, the collector is successfully uninstalled when you click OK.

4.3 Collector

- In the Collector Configuration wizard, if the account credentials you give for the SQL Server do not match an existing account on the SQL Server, and you have the rights to create SQL Server accounts, the credentials you give will be used to automatically create a new SQL Server account.

4.4 Audit Analyzer and Session Player

- Release 2017.3 has introduced a new version of dzdo and PAM authentication audit trail events. However, these events cannot be captured by older version of database/Collector or reported by older versions of DirectAudit Audit Analyzer console or FindSessions utility or PowerShell cmdlets. To rectify this issue, you need to upgrade the DirectAudit backend components (such as Audit Manager console, Audit Analyzer console, Collector, and Audit Store databases) to Release 2017.3 or later version. Contact Centrify support if you are unable to upgrade the DirectAudit backend components so that DirectAudit database patching scripts can be provided to you based on your current version. (Ref: CS-44654)
- When detaching and re-attaching an Audit Store database from an Audit Store, Centrify recommends refreshing the query results for all open queries in Audit Analyzer console prior to replaying a session from that database. Failure to do so may result into a database error. (Ref: CS-42125)
- If the active audit store database spans two SQL databases, the Audit Analyzer will show UNIX sessions as "Disconnected" until some data is received from those sessions. Once data has been received, the session state will change to "In Progress."
- If an audited Windows session is using multiple monitors in extended mode in DirectAudit 3.2.2 or earlier, it cannot be exported as WMV files. In DirectAudit 3.2.3 or later, it will be trimmed to 2048x2048 pixels before it is saved and can be exported as in WMV file in 2048x2048 resolution. (Ref: 27003a, 75163, CS-6450, CS-3265).
- When Centrify Agent for Windows machine's system color depth is changed during an audited session, the playback of the session may not be displayed properly. (Ref: 36818c)
- Entering specific keywords in the "Application" Event list column will not filter based on the keywords as expected. For example, entering the search term "c" will locate the string "Windows Explorer". This is because application characteristics are stored in the database as a set of related attributes as follows: "Explorer.EXE | Microsoft® Windows® Operating System | Windows Explorer | Microsoft Corporation | 6.1.7600.16385" A match with any of the Windows Explorer attributes will yield "Windows Explorer". This issue will be addressed in an upcoming release. (Ref: 39645b)
- In Audit Analyzer, you can specify double-quote enclosed strings in the query that searches for "Unix Commands and Outputs" attribute. However, if a double-quote character is inside the double-quote enclosed string, the query result is undefined. (Ref: CS-39348)
- If a DirectAudit Installation is configured to not capture video data, parameters of the UNIX command are also not captured. Therefore, the query using "Parameters of Commands and Applications" as the criteria does not

work under this configuration. This is a known issue and will be addressed in future release. (Ref: 55741b)

- If you open Audit Analyzer and right click on any child node of predefined queries such as "All, Grouped by User", "All, Grouped by Machine" or "All, Grouped by Audit Store" in the left pane, the context menu is displayed and it shows a menu item named "Properties". This context menu item, when clicked, does not open any dialog box because it is not a valid action for the selected child node. This menu item will be removed in the future release. (Ref: 48681b)
- By default, Audit Analyzer uses MSS2 codec to export audited sessions to a WMV (Windows Media Video) file. The MSS2 codec has a known issue which results in fuzzy video when an audited Windows session is exported as WMV file and opened in Windows Movie Maker 2012. From DirectAudit 3.2.0 onward, you can specify your own codec to export an audited session to a WMV file. Please refer to KB-4029 for additional information. (Ref: 56021a)

4.5 Audit Manager

- User and group criteria should not be combined in an Audit Role or it may result into inconsistent results, the workaround is for users to use two different audit roles (one for groups, another for users) if they want to mix users and groups in audit role assignment. (Ref: CS-38968)
- When creating an AuditRole with "ClientName" Audit Manager's Role Properties / Criteria will display an empty value rather than "ClientName = <IP address>" (Ref: CS-41803)
- If you assign DirectAudit permissions to a Domain Local group, which is not in the current domain in the Audit Manager Installation Property Security tab, and a user belonging to that group runs Audit Analyzer and tries to connect to the DirectAudit Installation, Audit Analyzer will display the warning "You do not have permission to connect to the SQL server." A workaround is to grant permission to a Global or Universal group instead. (Ref: 25546c)

4.6 Centrify DirectAudit Agent for *NIX

4.6.1 General

- Centrify recommends customers use the session auditing capability of DirectAudit to ensure the complete login session is audited vs. auditing individual commands. When the administrator configures Direct Audit to audit a specific command, Direct Audit moves the original command executable to a different location and replaces it by a symbolic link to the Direct Audit shell. It is possible for a user to find out the new location of the executable and runs that command directly to bypass auditing. Whereas the likelihood of this happening is very minute, Centrify recommends session auditing be turned on to avoid the chance of this happening.

- If a user is logged in to AIX and HP-UX via a GUI, for example Xmanager, a terminal opened in the GUI will not be audited. To workaroud this issue, set the centrifyda.conf parameter 'dash.allinvoked' to true. (Ref: 66330, CS-5876)
- Obfuscation of session data has the following limitation: If the information is sent to stdout not as a whole, but piece by piece, the information will not be obfuscated. Example: A user wants to obfuscate a pattern "1234-5678". However, "1234-" is shown first and "5678" is shown 1 second later, this pattern will not be obfuscated. Since the stdout buffer in the audit shell is 4KB, the obfuscation string is at most 4KB long. Note: this applies to stdout only. (80462a)
- Auditing init during startup on UNIX is not possible. The init command used during the boot process should not be audited using per-command auditing. If you attempt to audit init, your operating system will not reboot properly.
- You cannot start a GUI session if you are logged in via an interactive session. Running startx or starting a GUI session from an interactive session results in the following message:

X: user not authorized to run the X server, aborting.

Workaround:

- Run "sudo dpkg-reconfigure x11-common"
- When you are prompted for users allowed to start the X server, choose "anybody" (the default is "console users only").

The GUI session or X server should start normally. (Ref: 25036a)

- To audit the GUI terminal emulators, GUI login managers have to be fully reinitialized after auditing is enabled. On Linux, "init 3 && init 5" will start the reinitialization. (Stopping the X server only, or pressing ctrl+alt+backspace in Gnome, will not start the reinitialization.)
- When a local user and an Active Directory user use the same UNIX user name, the user name will default to the name of the Active Directory user. If the local user name is intended, setting the pam.allow.override parameter in /etc/centrifydc/centrifydc.conf will help. After this setting, the user name implies the Active Directory user; and <username>@localhost will imply the local user.

DirectAudit 3.0 or later understands the "@localhost" syntax. DirectControl Agent will respond to <username>@localhost if the user name is set in pam.allow.override.

If you upgrade from DirectAudit 2.0, disable DirectAudit so that the new DirectAudit mechanism for hooking shells can be installed: Run 'dacontrol -d -a' to disable auditing, then restart the upgrade.

DirectAudit maintains a cache of user information for performance reasons. This cache interferes with Unix commands that manipulate the local user database (passwd file). These commands include useradd, userdel and usermod. From DirectAudit 3.2.0 onwards, DirectAudit will not access its local cache to fully support the following commands: useradd, userdel, adduser, usermod, mkuser, rmuser, chuser

Please contact support if your operating system platform has other programs that directly access the local passwd file. (Ref: 56259a)

- If session auditing is enabled, all local user logins are processed by DirectAudit to determine whether the session should be audited. This may block login if domain controllers are not responsive and/or DirectControl Agent is not running. Two new parameters are introduced in /etc/centrifyda/centrifyda.conf:
 - user.ignore: specifies a list of local users that DirectAudit does not use Active Directory to determine audit level. By default, the list is /etc/centrifydc/user.ignore (the same one that DirectControl uses), which includes some important accounts like root, bin, daemon, etc.
 - user.ignore.audit.level - specifies the audit level for the local users specified in the user.ignore list. The supported values are 0 (audit if possible) and 1 (audit not requested/required). Default is 0 (audit if possible). Note that "audit required" is not a reasonable choice, as this user needs to login all the time; and "audit required" may block login if DirectAudit does not function correctly. (Ref: 55599a, 57946a, 56935a, 58251a)
- The /usr/share/centrifydc/bin/centrifyda script should be used to start/stop DirectAudit service in all *nix platforms. However, systemd is not fully supported in /usr/share/centrifydc/bin/centrifyda. For platforms that use systemd by default (such as SUSE Linux Enterprise 12/SUSE Linux Desktop 12), users need to set the environment variable SYSTEMD_NO_WRAP to 1 before calling the /usr/share/centrifydc/bin/centrifyda. Operations such as killing a daemon, running dad (DirectAudit daemon) directly, or running dastop command, could lead to issues in daemon managers in some *nix platforms. For example, SMF of Solaris, SRC of AIX and systemd of Fedora 20, may record incorrect running status of the daemon; and may fail to start daemon. (Ref: 57653a, 71211a)
- Disable auditing before upgrade

If you upgrade from DirectAudit 2.0, please run "dacontrol -d -a" to disable DirectAudit before upgrade. Both the installer shell script, install-da.sh, and the native package manager will detect if auditing is enabled and abort if so.

If you are using the native package manager to upgrade and you attempt to upgrade while auditing is enabled, you may find that, after the package manager aborts, the DirectAudit installation is shown as broken. This may be

ignored. Simply disable auditing, upgrade and then re-enable auditing and the package will be shown as committed.

4.6.2 RedHat Linux

- Due to a limitation of some implementations of audispd (audit dispatcher daemon provided by the operating system), DirectAudit advanced monitoring feature may not work if "dacontrol -n/-m" was run multiple times and over the limit specified in the parameter max_restarts in /etc/audisp/audispd.conf (default 10). If you enable the DirectAudit Advanced monitoring feature and it does not generate the audit trail events as expected, you can run dainfo to check on the status of advanced monitoring feature. If the program /usr/share/centrifydc/bin/dadispatcher is not running, dainfo will show "DirectAudit advanced monitoring status" as "not running". In this case, you need to restart the system audit daemon using the command "service auditd restart". This will re-activate the advanced monitoring feature. (Ref: CS-41267)
- The characters ('%', '#', '>' and '\$') are used by DirectAudit to recognize UNIX commands. They should not be used in role names and as part of trouble-tickets; otherwise they will be recognized as part of a UNIX command. (Ref: 51687a)
- DirectAudit advanced monitoring features may not work with early versions of RedHat 5 due to different system configurations. The earliest version that Centrify tested is RedHat 5.6. Please contact Centrify Support if you need support in versions earlier than RedHat 5.6. (Ref: CS-43042)
- The advanced monitoring feature in RedHat 5 version only supports selinux mode set to 'disabled' or 'permissive', 'enforcing' is not supported due to incompatible selinux policies. Moreover, advanced monitoring feature may not work with earlier versions of RedHat 5 releases due to different system configurations. Please contact Centrify support if you need support in versions earlier than RedHat 5.6. (Ref: CS-43024)

4.6.3 Debian Linux

- To install the Centrify DirectAudit package on a computer with the Debian operating environment, you must use the dpkg --install or dpkg -i option. You cannot use the dpkg --update or dpkg -u options to install or update the Centrify DirectAudit package. If you need to update the Centrify DirectAudit package, you need to first delete the old package using the dpkg --purge or dpkg -P option then install the new package with the dpkg --install or dpkg -i option.

Note: Do not use the `dpkg --remove` or `dpkg -r` command to remove Centrify DirectAudit. Using the `--remove` option prevents the Centrify DirectAudit configuration file, `/etc/centrifyda/centrifyda.conf`, from being created properly when you reinstall the package.

4.6.4 Solaris

- Centrify recommends that you install the appropriate recommended patch bundles for the version of Sun Solaris you are using before installing Centrify DirectAudit.

The patch installation will skip any individual patches that don't apply to your system, and you can use Sun's patch management system to ensure your computers get the latest security fixes.

To help you identify any required patches for your environment, Centrify supplies the `pca` patch checker in all Solaris Centrify Infrastructure Services packages. `Install.sh` will prompt you to check the patch level of your environment during installation.

To check for Sun recommended patches with the `pca` patch checker you should have the `wget` package installed. This package may be obtained from:

http://ftp.wayne.edu/sun_freeware/

And source code may be obtained from:

<http://www.gnu.org/software/wget/>

For more information about downloading and installing patches, see the Sun Web site.

The minimum patches required for Centrify DirectAudit are provided below for reference purposes. In some cases these patches may be obsoleted or incorporated into other patches, so the patch numbers on your Solaris machines may be different. The authoritative source on patch compatibility is Sun; their Web site will allow you to follow patch histories to ensure any later patches you are using are compatible with the ones required by DirectAudit.

For Solaris 10: 119254-65 120011-14 127127-11 138263-03

- Please contact technical support if you are using sparse zone(s) and like to do one of the following:
 - Change session auditing status from disabled to enabled during upgrade.

- o Enable session auditing in a global zone and want to disable session auditing in sparse zone(s) when using the same global zone. (Ref: 76572, 80616b)
- The following commands, located in /usr/bin, might be implemented as ksh programs or scripts:

```
alias    bg        cd
command fc         fg
getopts hash       jobs
kill     read      test
type     ulimit    umask

unalias wait
```

To identify commands implemented as ksh scripts, run the following script:

```
#!/bin/ksh -p

cmd=`basename $0`

$cmd "$@"
```

The commands that are implemented internally by ksh should not be audited.

- On a system using SMF (Service Management Facility), such as Solaris 10, the DirectAudit daemon might not start up after an upgrade from DirectAudit 1.x. This does not affect a fresh installation. To bring the daemon up, run these commands:
 - o `svcadm disable centrifyda`
 - o `svcadm enable centrifyda`
 - o Run 'svcs' and find 'centrifyda' to confirm the daemon is online.

4.6.5 AIX

- Some versions of AIX sshd do not function reliably with Centrify products. When possible, Centrify recommends using sshd included in Centrify openSSH on AIX platforms. (Ref: CS-7098)

- Local AIX users cannot be audited when they log in via built-in ssh, due to a change in AIX 7.0 ML1. Customers are advised to install Centrify OpenSSH if auditing of ssh login by local users is required (Ref: 33299a).
- Change in AIX root user behavior: By default, all releases starting with Release 2014 (DirectAudit 3.2.0) DO NOT modify the root stanza in AIX for new installations. One side effect is that root user login WILL NOT be audited. If your environment requires session auditing of root user login, you need to do the followings:
 - a. Set up a DirectAuthorize role that has the audit level of "audit required" or "audit if possible"; and assign this role to root.
 - b. Set the parameter adclient.autoedit.user.root to TRUE in /etc/centrifydc/centrifydc.conf.
 - c. If DirectAudit session auditing is not enabled, enable DirectAudit session auditing using the command "dacontrol -e".
 - d. Restart adclient (Ref: 56239a, 56604a)
- For AIX customers who upgrade from prior versions of Release 2014 (DirectAudit 3.2.0), there is NO change in behavior. The parameter adclient.autoedit.user.root is set to true in /etc/centrifydc/centrifydc.conf. The root user will still be audited. (Ref: 56235)

4.6.6 HPUX

You can install this package by copying it to a HP-UX computer and running install.sh, the installer, or by running the following commands, where <release> is the version of the Centrify DirectAudit package you are installing:

```
gzip -d centrifyda-<release>-hp11.31-ia64.depot.gz
swinstall -s /path/centrifyda-<release>-hp11.31-ia64.depot \
    -x allow_incompatible=true
```

- You must specify the full path to the Centrify DirectAudit depot file and set the allow_incompatible option to true to install successfully.
- The installation script checks your environment for the minimum patch levels required. If you have more recent patches installed, however, you may see an error message. To install, re-run the installation command with the following additional command line option:


```
-x enforce_scripts=false
```


4.7 Database

- When adding an Audit Store database to a SQL Server Availability Group with the multi subnet failover feature, the SQL Server that hosts the management database must be SQL Server 2012 or above. In addition, when upgrading an existing DirectAudit installation to use the SQL Server Availability Group feature, Centrify recommends upgrading Collectors, Audit Management Server service, Audit Manager consoles and Audit Analyzer consoles to the latest version to benefit from this feature. (Ref: CS-39872)
- In previous versions of DirectAudit, it was possible to specify the location of the database file. In DirectAudit 2.0.0 and later this capability is not provided in the Audit Store Database Wizard. However, you can still specify the full text file location, database file location, or transaction log file location by choosing "View SQL Scripts" and modifying the relevant database location manually in the script.
- If the default memory setting for SQL Server is more than the actual memory in the system a memory error may occur. For more information see:

<http://social.msdn.microsoft.com/Forums/en-US/sqldatabaseengine/thread/74a94f06-adf5-4059-bb92-57a99def37bd/>

SQL Server 2008 R2 full text search categorizes certain words as stop words by default and ignores them for searches. Some stop words are common UNIX commands such as like, which, do, and while. For more details about stop words and how to configure, please refer to <http://technet.microsoft.com/en-us/library/ms142551.aspx>

- The collector monitors the active Audit Store database to check if it is running low on disk space. If an active Audit Store the database is on a disk with volume mount point, the collector may give a false alarm. In such cases, it is recommended to disable the detection by setting the following registry key with the type of DWORD to 0 on all your collector machines. (Ref: 53389a)

HKLM\Software\Centrify\DirectAudit\Collector\AuditStoreDiskSpaceLowThreshold

- Collector only detects AuditStore disk space low against a configurable threshold if the SQL Server version is 2008 R2 SP1 (10.50.2500.0) and above. The threshold can be configured at Collector machine Registry:
HKLM\Software\Centrify\DirectAudit\Collector\AuditStoreDiskSpaceLowThreshold
DWORD in MB, not configured, default to 1024 MB. If free disk space is less than the threshold, Collector state is changed to "AuditStore database disk space is low", and stops accepting audit data from Agent(s).

4.8 Audit Management Server

- To configure the audit management server to point to an installation, the user who is running the Audit Management Server Configuration Wizard must have the "Manage SQL Logins" permission on the management database of the installation. For example, if you are configuring an audit management server in an external forest with a one-way trust, be sure that the installation supports Windows and SQL Server authentication and the account you are using is from the internal forest and has the "Manage SQL Logins" permission on the management database. (Ref: 46989a)

4.9 FindSession Tools

- For per-command auditing of dzdo command, when a ticket is entered, the role and ticket are associated with the audited session. For such sessions, the FindSessions tool's export of type UnixCommand, UnixInput, or UnixInputOutput based on the role and/or ticket criteria will have the exported command, STDIN, or STDIN and STDOUT marked with role and ticket. When per session auditing is enabled, the exported data will not have role and ticket information. (Ref: 53936a)
- When per-command auditing is enabled for dzdo command, and role and trouble ticket capturing is also configured, FindSessions.exe run with /export=UnixCommand option will not show the role and trouble ticket information in the exported file for the dzdo command itself, if the dzdo command executed is "dzdo su -" or "dzdo -i". However, all the command executed within that dzdo session will have correct role and trouble ticket information. (Ref: 51787a)

4.10 Centrify Agent for Windows

- When a user disconnects and then later reconnects to an existing user session from a switch user operation, a successful logon audit trail message will not be logged after the user has reconnected to the session though authentication. This does not apply when the user is performing lock and unlock operations or the logon method is different from the previous login (remote vs. console logon). (Ref: CS-41453)
- There will be no audit trail event generated when a user fails to login and unlock a computer on Windows Server 2008 R2 and Windows 7. (Ref: CS-41455)
- In the DirectAudit Agent for Windows control panel, the setting "Maximum size of the offline data file" indicates the minimum amount of disk space (in percentage) that must be available/free in the spool volume in order to continue auditing users (especially when the DirectAudit Agent cannot send audit data to collector). The DirectAudit Agent makes its best attempt to pause auditing when the specified amount of disk space is no longer available and in certain cases may continue to write to spool volume for a

few minutes before eventually pausing the auditing activity. (78072, CS-6718)

- The optional video capture feature requires both the Collector and the DirectAudit Agent to use 2013.2 or later. If any of collectors or agents are running an older version, video data may still be recorded even though you have turned it off in Release 2013 Update 2 Audit Manager. (Ref: 44064a)
- If Centrify Agent for Windows is auditing a Windows 8 or Windows 2012 system, the Indexed Event List of the corresponding audited session will not show any events for the applications that are using the Metro User Interface. The Metro UI is not supported. (Ref: 56556b)
- Upon making changes to Group Policy "Centrify Audit Trail Setting" > "Centrify Common Setting" > "Send audit trail to log file", it would require reboot of the client computer (agent) for this setting to be effective despite the Group Policy has already been refreshed on the client computer. (Ref: 73368b)
- The offline data location (and subdirectories below it) is expected to be a location dedicated to spooling, for example c:\spool. If the offline data location is changed, all files in the old location (including subdirectories and their contents) are moved to the new location. This may cause problems if the old location was not exclusively for spooling use. For example, choosing c:\ as the original spool location and d:\spool as the new location would cause all files on the c:\ drive to be copied to d:\spool. (Ref: 26592a)
- Some events related to the login script are not listed in the indexed events list. The login script cannot be audited for an initial few seconds because the DirectAudit software has not completed its setup. (Ref: 26286a)
- Some events related to the login script are not listed in the indexed events list. The login script cannot be audited for an initial few seconds because the Centrify Agent for Windows software has not completed its setup. (Ref: 26286a)

4.11 Centrify Audit Module for PowerShell

- Audit Module for PowerShell may take a long time to start because of the publisher's certificate verification. To resolve the problem, disable the "Check for publisher's certificate revocation" option in System Control Panel\Internet Options\Advanced\Security. (Ref: 72499)
- After installing Audit Module for PowerShell in a RDP session, PowerShell complains module "Centrify.DirectAudit.PowerShell" cannot be loaded. This is because the installation package needs to modify system environment variables to let PowerShell know where to load the module. This operation needed to be done in a "Console Session" if installation is done via

RDP. To resolve this problem, logout and re-login or run RDP with the "admin" option as "mstsc /admin" or "mstsc /console". (Ref: 72500a)

5. Additional Information and Support

In addition to following instructions in the documentation provided with this package, you can find the answers to common questions and information about any general or platform-specific known limitations, as well as tips and suggestions, from the Centrify Knowledge Base on the Centrify Support Portal.

The Centrify Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Centrify products. For more information, see the Centrify Resources web site:

www.centrify.com/resources

You can also contact Centrify Support directly with your questions through the Centrify web site, by email, or by telephone. To contact Centrify Support or to get help with installing or using this version of Centrify DirectAudit, send email to [Support](mailto:support@centrify.com) or call 1-669-444-5200, option 2.

For information about purchasing or evaluating Centrify products, send email to [info](mailto:info@centrify.com).