Centrify Server Suite 2017

Audit Events Administrator's Guide

June 2017

Centrify Corporation

Legal notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrify Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrify Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify User Suite, and Centrify Server Suite are registered trademarks and Centrify for Mobile, Centrify for SaaS, Centrify for Mac, DirectManage, Centrify Express, DirectManage Express, Centrify Identity Platform, Centrify Identity Service, and Centrify Privilege Service are trademarks of Centrify Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103 B2; 9,112,846; 9,197,670; and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

About this guide

Centrify Server Suite (CSS) is a multi-tier software solution that enables administrators to centrally manage access to on-premise servers and workstations, mobile devices, and applications across a broad range of platforms. CSS audit events record login and privilege activity on Windows, UNIX, and Linux computers. The formatting of these audit events logs are similar to a common event format (CEF).

Intended audience

This guide is for individuals who need to extract audit event information from UNIX and Linux syslogs and Windows application event logs. Additionally, this information is available in the Centrify Audit Analyzer. Audit events are organized into categories in the Audit Analyzer and these categories are identified in this document.

Using this guide

Depending on your environment and role as an administrator or auditor, you may want to read portions of this guide selectively. This guide provides the following information:

- Chapter 1, "Overview of CSS audit events," provides an overview of how to read audit events.
- Chapter 2, "Centrify Server Suite audit events," identifies the different audit event categories. Each audit event includes a sample log with an explanation of how to read the log as well as a list of the available audit events.

Conventions used in this guide

The following conventions are used in this guide:

- `Fixed-width` font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *`italicized`*, this font indicates variables. In addition, Square brackets ([ ]) indicate optional command-line arguments.
- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.
- *Italics* are used for book titles and to emphasize specific words or terms.
- Standalone software packages include version and architecture information in the file name. For example, the standalone software package with the file name centrify-suite-2016-deb5-i386.tgz contains Centrify software that supports Debian Linux on a computer with 32-bit architecture. Full file names are not documented in this guide. For complete file names for the software package you want to install, see the distribution media.

Finding more information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and features, start by visiting the Centrify website. From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

For access to documentation for all Centrify products and services, visit the Centrify documentation portal. From the Centrify documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

To get to the documentation portal, go to docs.centrify.com or https://www.centrify.com/support/documentation.

Contacting Centrify

You can contact Centrify by visiting our website, www.centrify.com. On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the Centrify Customer Support Portal. From the support portal, you can to search knowledge base articles, open and view support cases, connect with other Centrify users on customer forums, and access additional resources—such as online training, how-to videos, and diagnostic tools.

Overview of CSS audit events

To familiarize yourself with the elements of audit event logs, read the explanations of Windows and UNIX/Linux audit events, and then review how to read Centrify audit event data.

Windows and UNIX/Linux Audit Events

Review the following examples to understand the Windows and UNIX/Linux audit event logs, and then review "How to read Centrify audit event data" on page 13 to understand the similarities and differences.

Windows Audit Event Log Line Example

The following is an example of a Centrify audit event recorded in the Windows application event log. Standard Windows audit event fields (in black) contain information about the Centrify event. Centrify augments these standard fields with additional data (in red) to help you to track logon and privilege activity data.

```
04/05/2016 02:15:37 PM LogName=Application SourceName=Centrify
AuditTrail V2 EventCode=6003 EventType=4 Type=Information
ComputerName=member.centrify.vms User=NOT_TRANSLATED Sid=S-1-
5-21-3789923312-3040275127-1160560412-500 SidType=0
TaskCategory=%1 OpCode=Info RecordNumber=51645
Keywords=Classic Message=Product: Centrify Suite Category:
DirectAuthorize - Windows Event name: Remote login success Message:
User successfully logged on remotely using role
'ROLE_Windows_Local_Accounts/Global'. Apr 05 14:15:37
member.centrify.vms dzagent[1496]: INFO AUDIT_TRAIL|Centrify
Suite|DirectAuthorize - Windows|1.0|3|Remote login
success|5|user=administrator@member.centrify.vms userSid=S-1-5-21-
3789923312-3040275127-1160560412-500 sessionId=6
centrifyEventID=6003 DAInst=AuditingInstallation DASessID=c72252aa-
e616-44ff-a5f6-d3f53f09bb67 role=ROLE_Windows_Local_Accounts/
Global desktopguid=a16f50d8-179b-4d47-93ed-14c10ca76d63
```

Windows Audit Event Log Line Information

The following table provides definitions for each field type and name with their associated field value for the previous example.

Field Type	Field Name	Sample Field Value
Syslog header fields	Timestamp	Apr 05, 2016 02:15:37 PM
	Host Name	member.centrify.vms
	Process Name	dzagent
	Process ID	1496
	Log Level	INFO
Centrify audit event header fields	Event Type	AUDIT_TRAIL
	Product	Centrify Suite
	Category	DirectAuthorize - Windows
	Product Version	1.0
	Event ID	3
	Event Name	Remote login success
	Severity	5

Field Type	Field Name	Sample Field Value
Centrify audit event common fields for Windows	user	administrator@member.centrify.vms
	userSid	S-1-5-21-3789923312-3040275127-1160560412-500
	DAInst	AuditingInstallation
	DASessID	c72252aa-e616-44ff-a5f6-d3f53f09bb67
	sessionId	6
	centrifyEventID	6003
Centrify audit event-specific fields	role	ROLE_Windows_Local_Accounts/Global
	desktopguid	a16f50d8-179b-4d47-93ed-14c10ca76d63

UNIX/Linux Audit Event Log Line Example

The following is an example of a UNIX/Linux audit event. Centrify audit event information is highlighted in red.

```
Apr 4 21:04:15 engcen6 adclient[1749]: INFO AUDIT_TRAIL|Centrify Suite|Centrify sshd|1.0|100|SSHD granted|5|user=dwirth(type:ad,dwirth@CENTRIFY.VMS) pid=7456 utc=1459784055479 centrifyEventID=27100DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=GRANTED service=ssh-connection tty=/dev/pts/0 authMechanism=keyboard-interactive client=192.168.81.11 sshRights=shell command=(none)
```

Centrify UNIX/Linux Audit Event Log Information

The following table provides definitions for each field type and name with their associated field value for the previous example.

Field Type	Field Name	Sample Field Value
Syslog header fields	Timestamp	Apr 4 21:04:15
	Host Name	engcen6
	Process Name	adclient
	Process ID	1749
	Log Level	INFO
Centrify audit event header fields	Event Type	AUDIT_TRAIL
	Product	Centrify Suite
	Category	Centrify sshd
	Product Version	1.0
	Event ID	100
	Event Name	SSHD granted
	Severity	5

Field Type	Field Name	Sample Field Value
Centrify audit event common fields	user	dwirth(type:ad,dwirth@CENTRIFY.VMS)
	pid	7456
	utc	1459784055479
	centrifyEventID	27100
	DAInst	AuditingInstallation
	DASessID	c72252aa-e616-44ff-a5f6-d3f53f09bb67
	status	GRANTED
	service	ssh-connection
Centrify audit event-specific fields	tty	/dev/pts/0
	authMechanism	keyboard-interactive
	client	192.168.81.11
	sshRights	shell
	command	(none)

How to read Centrify audit event data

The following information can help you understand how to read Centrify audit events.

Event ID / CentrifyEventID

Every Windows and UNIX/Linux audit event includes two numeric IDs that describe the event. The `Event ID` in the header fields identifies the unique ID of the event within a particular event category, whereas the `centrifyEventID` in the common fields identifies the unique ID among all Centrify audit event types.

Windows example

Centrify audit event header fields	Category	DirectAuthorize - Windows
	Product Version	1.0
	Event ID	3
	Event Name	Remote login success
	Severity	5

Centrify audit event common fields	user	administrator@member.centrify.vms
	userSid	S-1-5-21-3789923312-3040275127-1160560412-500
	DAInst	AuditingInstallation
	DASessID	c72252aa-e616-44ff-a5f6-d3f53f09bb67
	sessionId	6
	centrifyEventID	6003

UNIX/Linux example

Centrify audit event header fields	Event Type	AUDIT_TRAIL
	Product	Centrify Suite
	Category	Centrify sshd
	Product Version	1.0
	Event ID	100
	Event Name	SSHD granted
	Severity	5
Centrify audit event common fields	user	dwirth(type:ad,dwirth@CENTRIFY.VMS)
	pid	7456
	utc	1459784055479
	centrifyEventID	27100
	DAInst	AuditingInstallation
	DASessID	c72252aa-e616-44ff-a5f6-d3f53f09bb67
	status	GRANTED
	service	ssh-connection

Severity

Severity is defined by an integer from 0 - 10, with 10 being the most important level. Centrify events are typically a Severity 5.

Spacing

A field name is one word (no spaces) in the audit event file. When the file is processed into a readable format, spaces are added to field names. For example, if you need to search for Management Database Property, you should search on the following term: managementdatabaseproperty.

Case-insensitive field names

Use case-insensitive field names in all search filters.

Which events are only in Centrify Server Suite Enterprise Edition

Audit events may come from either Standard or Enterprise editions of Centrify Server Suite. If you are using only Standard Edition, the following events will not be available to you as they are from Enterprise Edition:

- All the audit events from the following categories:
  - Audit Analyzer
  - Audit Manager
  - Command
  - DirectAudit - Windows
  - DirectAudit System Management
  - DirectAudit UNIX Agent
  - DirectAudit advanced monitoring
- The following audit events from the category Centrify Commands
  - Auditing enabled (Centrify Event Id 18000)
  - Auditing not enabled (Centrify Event Id 18001)
  - Auditing disabled (Centrify Event Id 18100)
  - Auditing not disabled (Centrify Event Id 18101)

Centrify Server Suite audit events

For each category of Centrify Server Suite audit events, this chapter provides the following:

- An overview
- A log sample
- An explanation of the sample for all CSS audit events for log in and privilege activity on Windows, UNIX, and Linux computers
- A listing of all Centrify audit event IDs in the specified category

If you are using the Audit Analyzer console to view audit events, you cannot individually access the audit events documented in this chapter. The audit events are grouped into Audit Analyzer categories.

Tip: Instead of querying audit event categories, you can query a day's worth of audit events in the Audit Analyzer console to review all audit events for the day.

Audit Analyzer

The Audit Analyzer console is a graphical user interface, which administrators can use to configure and manage the deployment of audit components, such as agents and collectors, or to query and review captured user sessions. The Audit Analyzer is available with the Enterprise Centrify Server Suite.The Audit Analyzer events focus on collector service, collector settings, and agent settings.

Audit Analyzer audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 3001. This log sample documents a session being deleted. The

change was made by user=administrator@centrify.vms on April 20, 2016 at 05:51:01.

```
04/20/2016 05:51:01 PM LogName=Application SourceName=Centrify
AuditTrail V2 EventCode=3001 EventType=4 Type=Information
ComputerName=member.centrify.vms User=NOT_TRANSLATED Sid=S-1-
5-21-3883016548-1611565816-1967702834-500 SidType=0
TaskCategory=%1 OpCode=Info RecordNumber=60622
Keywords=Classic Message=Product: Centrify Suite Category: Audit
Analyzer Event name: Delete session Message: 1 out of 1 selected
sessions are successfully deleted. Apr 20 17:51:00 member.centrify.vms
mmc[4064]: INFO AUDIT_TRAIL|Centrify Suite|Audit
Analyzer|1.0|1|Delete session|5|user=administrator@centrify.vms
userSid=S-1-5-21-3883016548-1611565816-1967702834-500
sessionId=11 centrifyEventID=3001 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 sessions_deleted=1
sessions_selected=1
```

Audit Analyzer audit events

Table 1. Audit Analyzer audit events

Centrify Event ID	Description	Parameters
3001	Delete session	Sessions_Deleted: Sessions_deleted Sessions_Selected: Sessions_selected
3002	Delete session by criteria	Delete_criteria: Delete session selection criteria Sessions_Deleted: Sessions_deleted Sessions_Selected: Sessions_selected
3003	Set session reviewers succeeded	Installation: Name of the installation Session Id: Unique identifier of the session Reviewers: List of reviewers of the session
3004	Set session reviewers failed	Installation: Name of the installation Session Id: Unique identifier of the session Reviewers: List of reviewers of the session Reason: Error message
3005	Remove session reviewers succeeded	Installation: Name of the installation Session Id: Unique identifier of the session
3006	Remove session reviewers failed	Installation: Name of the installation Session Id: Unique identifier of the session Reason: Error message

Audit Manager

Audit Manager is a Microsoft management console (MMC) that you can use to configure and manage the deployment of audit components, such as audit stores and audit store databases, audit roles, collectors, and agents. Audit Manager is available with the Enterprise Centrify Server Suite. Audit events generated by Audit Manager primarily involve the installation and configuration of auditing components such

as management databases, audit stores, and audit store databases, and changes to audit role and user permissions.

Audit Manager audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 12200. This log sample documents enabling video capture in a DirectAudit installation. The change was made by user=dwirth@centrify.vms on April 21, 2016 at 11:17:35.

```
04/21/2016 11:17:35 AM LogName=Application SourceName=Centrify
AuditTrail V2 EventCode=12200 EventType=4 Type=Information
ComputerName=member.centrify.vms User=NOT_TRANSLATED Sid=S-1-
5-21-3883016548-1611565816-1967702834-1107 SidType=0
TaskCategory=%1 OpCode=Info RecordNumber=60975
Keywords=Classic Message=Product: Centrify Suite Category: Audit
Manager Event name: Video capture status updated Message: Video
capture in DirectAudit Installation DefaultInstallation is enabled Apr 21
11:17:35 member.centrify.vms mmc[7592]: INFO AUDIT_TRAIL|Centrify
Suite|Audit Manager|1.0|200|Video capture status
updated|5|user=dwirth@centrify.vms userSid=S-1-5-21-3883016548-
1611565816-1967702834-1107 sessionId=7 centrifyEventID=12200
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-
d3f53f09bb67 installation=DefaultInstallation
videocapturestatus=enabled
```

Audit Manager audit events

Table 2. Audit Manager audit events (Sheet 1 of 9)

Centrify Event Id	Description	Parameters
12200	Video capture status updated	installation: DirectAudit Installation VideoCaptureStatus: video capture status
12201	Create new installation succeeded	installation: Name of the installation
12202	Create new installation failed	installation: Name of the installation reason: Error message
12203	Installation update succeeded	installation: Name of the installation Installation Property: Name of the updated installation property Installation Property Value: Value of the updated installation property Operation: Type of operation (Set or Add or Remove)
12204	Installation update failed	installation: Name of the installation Installation Property: Name of the updated installation property Installation Property Value: Value of the updated installation property Operation: Type of operation (Set or Add or Remove) reason: Error message
12205	Installation permissions update succeeded	installation: Name of the installation User/Group: Name of the user or group Permissions: Permissions assigned to the user or group
12206	Installation permissions update failed	installation: Name of the installation User/Group: Name of the user or group Permissions: Permissions assigned to the user or group reason: Error message

Table 2. Audit Manager audit events (Sheet 2 of 9)

Centrify Event Id	Description	Parameters
12207	Remove installation succeeded	installation: Name of the installation
12208	Remove installation failed	installation: Name of the installation reason: Error message
12251	Audit options updated	installation: DirectAudit Installation DisableSelfReview: Disable reviewing own sessions DisableSelfDelete: Disable deleting own sessions
12209	Add Management Database succeeded	installation: Name of the installation Management Database: Name of the Management Database
12210	Add Management Database failed	installation: Name of the installation Management Database: Name of the Management Database reason: Error message
12211	Management Database update succeeded	installation: Name of the installation Management Database: Name of the Management Database Management Database Property: Name of the updated Management Database property Management Database Property Value: Value of the updated Management Database property Operation: Type of operation (Set or Add or Remove)

Table 2. Audit Manager audit events (Sheet 3 of 9)

Centrify Event Id	Description	Parameters
12212	Management Database update failed	installation: Name of the installation Management Database: Name of the Management Database Management Database Property: Name of the updated Management Database property Management Database Property Value: Value of the updated Management Database property Operation: Type of operation (Set or Add or Remove) reason: Error message
12213	Management Database permissions update succeeded	installation: Name of the installation Management Database: Name of the Management Database User/Group: Name of the user or group Permissions: Permissions assigned to the user or group
12214	Management Database permissions update failed	installation: Name of the installation Management Database: Name of the Management Database User/Group: Name of the user or group Permissions: Permissions assigned to the user or group reason: Error message
12215	Remove Management Database succeeded	installation: Name of the installation Management Database: Name of the Management Database
12216	Remove Management Database failed	installation: Name of the installation Management Database: Name of the Management Database reason: Error message
12217	Add Audit Store succeeded	installation: Name of the installation Audit Store: Name of the Audit Store

Table 2. Audit Manager audit events (Sheet 4 of 9)

Centrify Event Id	Description	Parameters
12218	Add Audit Store failed	installation: Name of the installation Audit Store: Name of the Audit Store reason: Error message
12219	Audit Store update succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Property: Name of the updated Audit Store property Audit Store Property Value: Value of the updated Audit Store property Operation: Type of operation (Set or Add or Remove)
12220	Audit Store update failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Property: Name of the updated Audit Store property Audit Store Property Value: Value of the updated Audit Store property Operation: Type of operation (Set or Add or Remove) reason: Error message
12221	Audit Store permissions update succeeded	installation: Name of the installation Audit Store: Name of the Audit Store User/Group: Name of the user or group Permissions: Permissions assigned to the user or group
12222	Audit Store permissions update failed	installation: Name of the installation Audit Store: Name of the Audit Store User/Group: Name of the user or group Permissions: Permissions assigned to the user or group reason: Error message
12223	Remove Audit Store succeeded	installation: Name of the installation Audit Store: Name of the Audit Store

Table 2. Audit Manager audit events (Sheet 5 of 9)

Centrify Event Id	Description	Parameters
12224	Remove Audit Store failed	installation: Name of the installation Audit Store: Name of the Audit Store reason: Error message
12225	Add Audit Store Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database
12226	Add Audit Store Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database reason: Error message
12227	Attach Audit Store Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database
12228	Attach Audit Store Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database reason: Error message
12229	Attach DirectAudit Version 1 Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the DirectAudit Version 1 Database
12230	Attach DirectAudit Version 1 Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the DirectAudit Version 1 Database reason: Error message

Table 2. Audit Manager audit events (Sheet 6 of 9)

Centrify Event Id	Description	Parameters
12231	Set Active Audit Store Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database
12232	Set Active Audit Store Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database reason: Error message
12233	Audit Store Database update succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database Audit Store Database Property: Name of the updated Audit Store Database property Audit Store Database Property Value: Value of the updated Audit Store Database property Operation: Type of operation (Set or Add or Remove)
12234	Audit Store Database update failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database Audit Store Database Property: Name of the updated Audit Store Database property Audit Store Database Property Value: Value of the updated Audit Store Database property Operation: Type of operation (Set or Add or Remove) reason: Error message

Table 2. Audit Manager audit events (Sheet 7 of 9)

Centrify Event Id	Description	Parameters
12235	Detach Audit Store Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database
12236	Detach Audit Store Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database reason: Error message
12237	Delete Audit Store Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database
12238	Delete Audit Store Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the Audit Store Database reason: Error message
12239	Add Audit Role succeeded	installation: Name of the installation Audit Role: Name of the Audit Role
12240	Add Audit Role failed	installation: Name of the installation Audit Role: Name of the Audit Role reason: Error message
12241	Audit Role update succeeded	installation: Name of the installation Audit Role: Name of the Audit Role Audit Role Property: Name of the updated Audit Role property Audit Role Property Value: Value of the updated Audit Role property Operation: Type of operation (Set or Add or Remove)

Table 2. Audit Manager audit events (Sheet 8 of 9)

Centrify Event Id	Description	Parameters
12242	Audit Role update failed	installation: Name of the installation Audit Role: Name of the Audit Role Audit Role Property: Name of the updated Audit Role property Audit Role Property Value: Value of the updated Audit Role property Operation: Type of operation (Set or Add or Remove) reason: Error message
12243	Audit Role permissions update succeeded	installation: Name of the installation Audit Role: Name of the Audit Role User/Group: Name of the user or group Permissions: Permissions assigned to the user or group
12244	Audit Role permissions update failed	installation: Name of the installation Audit Role: Name of the Audit Role User/Group: Name of the user or group Permissions: Permissions assigned to the user or group reason: Error message
12245	Audit Role assign member succeeded	installation: Name of the installation Audit Role: Name of the Audit Role User/Group: Name of the user or group
12246	Audit Role assign member failed	installation: Name of the installation Audit Role: Name of the Audit Role User/Group: Name of the user or group reason: Error message
12247	Audit Role remove member succeeded	installation: Name of the installation Audit Role: Name of the Audit Role User/Group: Name of the user or group

Table 2. Audit Manager audit events (Sheet 9 of 9)

Centrify Event Id	Description	Parameters
12248	Audit Role remove member failed	installation: Name of the installation Audit Role: Name of the Audit Role User/Group: Name of the user or group reason: Error message
12249	Delete Audit Role succeeded	installation: Name of the installation Audit Role: Name of the Audit Role
12250	Delete Audit Role failed	installation: Name of the installation Audit Role: Name of the Audit Role reason: Error message

Centrify Commands (UNIX commands)

Audit events in the Centrify Commands category are focused on capturing command line activity. Audit events are recorded when users or administrators run command line programs to enable or disable auditing, join or leave a domain, query Active Directory for user or group information, change their password configuration settings or license mode, or perform other operations.

Centrify Command audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 18000. This log sample documents auditing being enabled. The change was made by user=root on April 5 at 11:37:28.

```
Apr 5 11:37:28 engcen6 adclient[1749]: INFO AUDIT_TRAIL|Centrify
Suite|Centrify Commands|1.0|0|Auditing enabled|5|user=root
pid=14874 utc=1459836448489 centrifyEventID=18000
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-
d3f53f09bb67 status=GRANTED service=NSS
```

Centrify Commands audit events

Table 3. Centrify commands audit events (Sheet 1 of 3)

Centrify Event Id	Description	Parameters
18000	Auditing enabled	service: service
18001	Auditing not enabled	service: service reason: error message
18100	Auditing disabled	service: service
18101	Auditing not disabled	service: service reason: error message
18200	The user login to the system successfully	service: service tty: tty
20100	Joined domain	parameters: parameters zone: zone name domain: domain computer: computer name runas: username@domain
20101	Join failed	parameters: parameters zone: zone name domain: domain computer: computer name runas: username@domain reason: error message
20200	Left domain	parameters: parameters
20201	Leaving domain failed	parameters: parameters reason: error message
20300	Query as root was successful	parameters: parameters
20301	Query was successful	parameters: parameters

Table 3. Centrify commands audit events (Sheet 2 of 3)

Centrify Event Id	Description	Parameters
20302	Query request failed	parameters: parameters reason: error message
20400	Password changed	parameters: parameters unixUser: user name
20401	Password change failed	parameters: parameters unixUser: user name reason: error message
20500	Configuration settings (centrifydc.conf) reloaded	parameters: parameters
20501	Configuration settings (centrifydc.conf) failed to reload	parameters: parameters reason: error message
20600	Local cache flushed	parameters: parameters
20601	Cache flush failed	parameters: parameters reason: error message
20650	Object refreshed	parameters: parameters
20651	Object refresh failed	parameters: parameters reason: error message
20800	License modes changed	parameters: parameters
20801	License modes change failed	parameters: parameters reason: error message
20900	Advanced monitoring enabled	service: service
20901	Advanced monitoring not enabled	service: service reason: error message

Table 3. Centrify commands audit events (Sheet 3 of 3)

Centrify Event Id	Description	Parameters
20910	Advanced monitoring disabled	service: service
20911	Advanced monitoring not disabled	service: service reason: error message

Centrify Configuration

Centrify hierarchical zones are enable information about non-Windows computers, user profiles, access rights, and roles to be stored in Active Directory. Hierarchical zones can be used to segregate and perform privilege management on both UNIX/Linux and Windows systems. These configuration audit events focus on zones, computers, groups, users, rights, and roles.

Centrify Configuration audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 36101. This log sample documents a user giving zone administrative

tasks to another user. The change was made by user=dwirth@centrify.vms on April 19, 2016 at 03:01:04.

```
04/19/2016 03:01:04 PM LogName=Application SourceName=Centrify AuditTrail V2 EventCode=36101 EventType=4 Type=Information ComputerName=member.centrify.vms User=NOT_TRANSLATED Sid=S-1-5-21-3883016548-1611565816-1967702834-1107 SidType=0 TaskCategory=%1 OpCode=Info RecordNumber=59436 Keywords=Classic Message=Product: Centrify Suite Category: Centrify Configuration Event name: Zone administrative tasks delegated Message: "dwirth@centrify.vms" (running as "dwirth@CENTRIFY") delegated "CENTRIFY\pankaj" to perform "Change zone properties" on "centrify.vms/centrifyse/Zones/zone-14". Apr 19 15:01:04 member mmc[5792]: INFO AUDIT_TRAIL|Centrify Suite|Centrify Configuration|1.0|101|Zone administrative tasks delegated|5|user=dwirth@centrify.vms userSid=S-1-5-21-3883016548-1611565816-1967702834-1107 sessionId=3 centrifyEventID=36101 DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 pid=5792 user=dwirth@centrify.vms runas=dwirth@CENTRIFY type=AD status=SUCCESS trustee=CENTRIFY\\pankaj task=Change zone properties zone=centrify.vms/centrifyse/Zones/zone-14
```

Centrify Configuration audit events

Table 4. Centrify Configuration audit events (Sheet 1 of 35)

Centrify Event Id	Description	Parameters
36101	Zone administrative tasks delegated	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed trustee: username@domain task: delegation task name zone: zone name
36102	Delegation of zone administrative tasks failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed trustee: username@domain task: delegation task name zone: zone name reason: failure reason
36103	Computer administrative tasks delegated	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed trustee: username@domain task: delegation task name zone: zone name computer: computer name

Table 4. Centrify Configuration audit events (Sheet 2 of 35)

Centrify Event Id	Description	Parameters
36104	Delegation of computer administrative tasks failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed trustee: username@domain task: delegation task name zone: zone name computer: computer name reason: error message
36105	Computer role administrative tasks delegated	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed trustee: username@domain task: delegation task name zone: zone name computerRole: computer role name
36106	Delegation of computer role administrative tasks failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed trustee: username@domain task: delegation task name zone: zone name computerRole: computer role name reason: error message

Table 4. Centrify Configuration audit events (Sheet 3 of 35)

Centrify Event Id	Description	Parameters
36201	Zone created	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name
36202	Zone creation failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name reason: error message
36203	Zone deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name
36204	Zone deletion failed	status: succeeded or failed PID: process id user: username@domain RunAs: username@domain type: user type zone: zone name reason: error message
36205	Zone modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name

Table 4. Centrify Configuration audit events (Sheet 4 of 35)

Centrify Event Id	Description	Parameters
36206	Zone update failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name reason: error message
36301	User added to a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name
36302	Add user to a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name reason: error message
36303	User deleted from a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name

Table 4. Centrify Configuration audit events (Sheet 5 of 35)

Centrify Event Id	Description	Parameters
36304	Delete user from a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name reason: error message
36305	User profile modified in a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name
36306	Modify user in a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name reason: error message
36307	User added to a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name

Table 4. Centrify Configuration audit events (Sheet 6 of 35)

Centrify Event Id	Description	Parameters
36308	Add user to a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message
36309	User deleted from computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name
36310	Delete user from a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message
36311	User profile modified on a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name

Table 4. Centrify Configuration audit events (Sheet 7 of 35)

Centrify Event Id	Description	Parameters
36312	Modify user on a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message
36401	Group added to a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
36402	Add group to a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name reason: error message
36403	Group deleted from a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 8 of 35)

Centrify Event Id	Description	Parameters
36404	Delete group from a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name reason: error message
36405	Group profile modified in a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
36406	Modify group in a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name reason: error message
36407	Group added to a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name

Table 4. Centrify Configuration audit events (Sheet 9 of 35)

Centrify Event Id	Description	Parameters
36408	Add group to a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name reason: error message
36409	Group deleted from a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name
36410	Delete group from a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name reason: error message
36411	Group profile modified on a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name

Table 4. Centrify Configuration audit events (Sheet 10 of 35)

Centrify Event Id	Description	Parameters
36412	Modify group for a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name reason: error message
36501	Computer added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: hostname zone: zone name
36502	Add computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: hostname zone: zone name reason: error message
36503	Computer deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: hostname zone: zone name

Table 4. Centrify Configuration audit events (Sheet 11 of 35)

Centrify Event Id	Description	Parameters
36504	Delete computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: hostname zone: zone name reason: error message
36505	Computer modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: hostname zone: zone name
36506	Modify computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: hostname zone: zone name reason: error message
36601	PAM access right added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed pam: pam name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 12 of 35)

Centrify Event Id	Description	Parameters
36602	Add PAM right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed pam: pam name zone: zone name reason: error message
36603	PAM right deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed pam: pam name zone: zone name
36604	Delete PAM right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: succeeded or failed pam: pam name zone: zone name reason: error message
36605	PAM right modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed pam: pam name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 13 of 35)

Centrify Event Id	Description	Parameters
36606	Modify PAM right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed pam: pam name zone: zone name reason: error message
37201	Desktop right added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed desktop: desktop right name zone: zone name
37202	Add Desktop Right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed desktop: desktop right name zone: zone name reason: error message
37203	Desktop right deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed desktop: desktop right name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 14 of 35)

Centrify Event Id	Description	Parameters
37204	Delete desktop right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: succeeded or failed desktop: desktop right name zone: zone name reason: error message
37205	desktop right modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed desktop: desktop right name zone: zone name
37206	Modify desktop right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed desktop: desktop right name zone: zone name reason: error message
37301	Network right added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed network: network right name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 15 of 35)

Centrify Event Id	Description	Parameters
37302	Add network right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed network: network right name zone: zone name reason: error message
37303	network right deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed network: network right name zone: zone name
37304	Delete network right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: succeeded or failed network: network right name zone: zone name reason: error message
37305	Network right modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed network: network right name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 16 of 35)

Centrify Event Id	Description	Parameters
37306	Modify network right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed network: network right name zone: zone name reason: error message
37401	Application right added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed application: application right name zone: zone name
37402	Add application right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed application: application right name zone: zone name reason: error message
37403	Application right deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed application: application right name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 17 of 35)

Centrify Event Id	Description	Parameters
37404	Delete application right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: succeeded or failed application: application right name zone: zone name reason: error message
37405	Application right modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed application: application right name zone: zone name
37406	Modify application right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed application: application right name zone: zone name reason: error message
36701	UNIX command right added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed dzcmd: dzcmd zone: zone name

Table 4. Centrify Configuration audit events (Sheet 18 of 35)

Centrify Event Id	Description	Parameters
36702	Add command right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed dzcmd: dzcmd zone: zone name reason: error message
36703	UNIX command right deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed dzcmd: dzcmd zone: zone name
36704	Delete command right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed dzcmd: dzcmd zone: zone name reason: error message
36705	UNIX command right modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed dzcmd: dzcmd zone: zone name

Table 4. Centrify Configuration audit events (Sheet 19 of 35)

Centrify Event Id	Description	Parameters
36706	Modify command right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed dzcmd: dzcmd zone: zone name reason: error message
36801	Role added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed role: role name zone: zone name
36802	Add role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed role: role name zone: zone name reason: error message
36803	Role deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed role: role name zone: zone name

Table 4. Centrify Configuration audit events (Sheet 20 of 35)

Centrify Event Id	Description	Parameters
36804	Delete role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed role: role name zone: zone name reason: error message
36805	Role modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed role: role name zone: zone name
36806	Modify role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed role: role name zone: zone name reason: error message
36807	Add right to role was successful	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed right: right name role: role name

Table 4. Centrify Configuration audit events (Sheet 21 of 35)

Centrify Event Id	Description	Parameters
36808	Add right to role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed right: right name role: role name reason: error message
36809	Delete right from role was successful	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed right: right name role: role name
36810	Delete right from role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed right: right name role: role name reason: error message
36901	Role assignment added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name role: role name trustee: username@domain

Table 4. Centrify Configuration audit events (Sheet 22 of 35)

Centrify Event Id	Description	Parameters
36902	Role assignment failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name role: role name trustee: username@domain reason: error message
36903	Role assignment removed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name role: role name trustee: username@domain
36904	Delete role assignment failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name role: role name trustee: username@domain reason: error message
36905	Role assignment modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name role: role name trustee: username@domain

Table 4. Centrify Configuration audit events (Sheet 23 of 35)

Centrify Event Id	Description	Parameters
36906	Modify role assignment failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed zone: zone name role: role name trustee: username@domain reason: error message
36907	Role assignment added to a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: computer zone: zone name role: role name trustee: username@domain
36908	Add role assignment to computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: computer hostname zone: zone name role: role name trustee: username@domain reason: error message

Table 4. Centrify Configuration audit events (Sheet 24 of 35)

Centrify Event Id	Description	Parameters
36909	Role assignment deleted from a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: computer hostname zone: zone name role: role name trustee: username@domain
36910	Delete role assignment from computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: computer hostname zone: zone canonical role: role name trustee: username@domain reason: error message
36911	Role assignment modified for a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: computer hostname zone: zone canonical role: role name trustee: username@domain

Table 4. Centrify Configuration audit events (Sheet 25 of 35)

Centrify Event Id	Description	Parameters
36912	Modify role assignment for a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computer: computer hostname zone: zone canonical role: role name trustee: username@domain reason: error message
36913	Role assignment added to a computer role	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role zone: zone name role: role name trustee: username@domain
36914	Role assignment for a computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name role: role name trustee: username@domain reason: error message

Table 4. Centrify Configuration audit events (Sheet 26 of 35)

Centrify Event Id	Description	Parameters
36915	Role assignment deleted from a computer role	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name role: role name trustee: username@domain
36916	Delete role assignment from a computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone canonical role: role name trustee: username@domain reason: error message
36917	Role assignment modified for a computer role	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone canonical role: role name trustee: username@domain

Table 4. Centrify Configuration audit events (Sheet 27 of 35)

Centrify Event Id	Description	Parameters
36918	Modify role assignment in a computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone canonical role: role name trustee: username@domain reason: error message
37001	Computer role added	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name
37002	Add computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 28 of 35)

Centrify Event Id	Description	Parameters
37003	Computer role deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name
37004	Delete computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name reason: error message
37005	Computer role modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role name zone: zone name
37006	Modify computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed computerRole: computer role zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 29 of 35)

Centrify Event Id	Description	Parameters
37101	User added to a group	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed member: username group: group name
37102	Add user to a group failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed member: username group: group name reason: error message
37103	Password reset	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed account: username
37104	Reset password failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed account: username reason: error message

Table 4. Centrify Configuration audit events (Sheet 30 of 35)

Centrify Event Id	Description	Parameters
37501	Local user added to a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name
37502	Add local user to a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name reason: error message
37503	Local user deleted from a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name
37504	Delete local user from a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 31 of 35)

Centrify Event Id	Description	Parameters
37505	Local user profile modified in a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name
37506	Modify local user in a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname zone: zone name reason: error message
37511	Local user added to a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name
37512	Add local user to a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 32 of 35)

Centrify Event Id	Description	Parameters
37513	Local user deleted from computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name
37514	Delete local user from a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message
37515	Local user profile modified on a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name
37516	Modify local user on a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 33 of 35)

Centrify Event Id	Description	Parameters
37521	Local group added to a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
37522	Add local group to a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name reason: error message
37523	Local group deleted from a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
37524	Delete local group from a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 34 of 35)

Centrify Event Id	Description	Parameters
37525	Local group profile modified in a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
37526	Modify local group in a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name reason: error message
37531	Local group added to a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name
37532	Add local group to a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name reason: error message

Table 4. Centrify Configuration audit events (Sheet 35 of 35)

Centrify Event Id	Description	Parameters
37533	Local group deleted from a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name
37534	Delete local group from a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name reason: error message
37535	Local group profile modified on a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name
37536	Modify local group for a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name computer: computer hostname zone: zone name reason: error message

Centrify sshd

Centrify sshd is Centrify's enhanced version of OpenSSH. This software program uses the secure shell protocol to connect to a remote computer. Centrify sshd audit events identify DZ SSH rights and SSHD activities.

Centrify sshd audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 27000. This log sample documents the rights granted to the DZ SSH shell client. The change was made by user=dwirth(type:ad,dwirth@CENTRIFY.VMS) on April 4 at 01:04:15.

```
Apr 4 21:04:15 engcen6 adclient[1749]: INFO AUDIT_TRAIL|Centrify
Suite|Centrify sshd|1.0|0|DZ SSH right
granted|5|user=dwirth(type:ad,dwirth@CENTRIFY.VMS) pid=7461
utc=1459784055474 centrifyEventID=27000 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=GRANTED
service=dzssh-shell client=192.168.81.11
```

Centrify sshd audit events

Table 5. Centrify sshd audit events

Centrify Event Id	Description	Parameters
27000	DZ SSH right granted	service: service client: client
27001	DZ SSH right denied	service: service client: client reason: error message
27100	SSHD granted	service: service tty: tty authMechanism: authentication type client: client sshRights: ssh rights command: command
27101	SSHD denied	service: service tty: tty authMechanism: authentication type client: client reason: error message
27102	SSHD connection close successfully	service: service tty: tty authMechanism: authentication type client: client reason: error message

Command (Audited and successfully executed commands)

Command audit events are recorded when Centrify UNIX command-line programs are used on Centrify-managed computers. Centrify UNIX command audit events focus on the execution success or failure of the audited command.

Command audit event log sample

```
Nov 26 00:32:01 Eason adclient[31118]: INFO AUDIT_TRAIL|Centrify
Suite|Command|1.0|100|Audited command is executed|5|user=root
pid=31937 utc=1416979921469 centrifyEventID=48100
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-
d3f53f09bb67 status=SUCCESS command=/bin/ls -l data.txt
```

Command audit events

Table 6. Event Source Category: Command

Centrify Event Id	Description	Parameters
48100	Audited command is executed	command: command
48101	Audited command fails to be executed	command: command reason: error message

DirectAudit advanced monitoring

If you have enabled DirectAudit for advanced monitoring, you can generate data for three additional auditing reports, as follows:

- Monitored execution report: This report shows the monitored commands being executed on the audited machines—including information on commands that are run individually or as part of scripts.
- Detailed execution report: This report shows all of the commands being executed on the audited machines—including commands that are run as part of scripts or other commands.
- File monitor report: This report shows the sensitive files being modified by users on the audited machines.

Advanced monitoring audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 57300. This log sample documents a session where a user attempted to modify a monitored file. The change was made by root@al_rhel6_2.altest.centrify.com on November 2, 2016 at 06:09:01.

```
Nov  2 06:09:01 al_rhel6_2 adclient[27002]: INFO  AUDIT_TRAIL|Centrify
Suite|DirectAudit Advanced Monitoring|1.0|300|Monitored file
modification attempted|5|user=<no_login_user> pid=32393
utc=1478092141432 centrifyEventID=57300 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=SUCCESS
syscall=unlink status=0 timestamp=1478092141.432000
auid=<no_login_user> uid=root@al_rhel6_2.altest.centrify.com
processid=32393 ppid=32392 gid=root
euid=root@al_rhel6_2.altest.centrify.com cwd=/ accessType=2
command=/usr/bin/python argc=-1 args=/etc/pki/nssdb/ /etc/pki/nssdb/
cert9.db-journal
```

DirectAudit advanced monitoring audit events

Table 7. DirectAudit advanced monitoring audit events (Sheet 1 of 3)

Centrify Event ID	Description	Parameters
57200	Monitored program is executed	syscall: system call exitcode: exit code timestamp: timestamp auid: login user uid: user procid: process id ppid: parent process id gid: group euid: effective user cwd: current working directory cmd: command argc: no of arguments args: arguments
57201	Monitored program failed to execute	syscall: system call exitcode: exit code timestamp: timestamp auid: login user uid: user procid: process id ppid: parent process id gid: group euid: effective user cwd: current working directory cmd: command argc: no of arguments args: arguments

Table 7. DirectAudit advanced monitoring audit events (Sheet 2 of 3)

Centrify Event ID	Description	Parameters
57300	Monitored file modification attempted	syscall: system call exitcode: exit code timestamp: timestamp auid: login user uid: user procid: process id ppid: parent process id gid: group euid: effective user cwd: current working directory accType: access Type cmd: command argc: no of arguments args: arguments
57301	Monitored file modification attempt failed	syscall: system call exitcode: exit code timestamp: timestamp auid: login user uid: user procid: process id ppid: parent process id gid: group euid: effective user cwd: current working directory accType: access Type cmd: command argc: no of arguments args: arguments

Table 7. DirectAudit advanced monitoring audit events (Sheet 3 of 3)

Centrify Event ID	Description	Parameters
57400	Command execution is started	syscall: syscall exitcode: exit code timestamp: timestamp auid: auid uid: uid pid: pid ppid: ppid gid: gid euid: euid cwd: current working directory command: command argc: no of arguments args: arguments
57401	Command execution fails to start	syscall: syscall exitcode: exit code timestamp: timestamp auid: auid uid: uid pid: pid ppid: ppid gid: gid euid: euid cwd: current working directory command: command argc: no of arguments args: arguments

DirectAudit System Management

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 System Management is available with the Enterprise Centrify Server Suite. The DirectAudit audit events focus on collector service, collector settings, and agent settings.

DirectAudit System Management audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 42251. This log sample documents the successful start of the collector service on computer ‘MEMBER’. The change was made by user=system@nt authority on April 05, 2016 at 14:59:56.

```
04/05/2016 03:00:01 PM LogName=Application SourceName=Centrify AuditTrail V2 EventCode=42251 EventType=4 Type=Information ComputerName=member.centrify.vms User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 TaskCategory=%1 OpCode=Info RecordNumber=51722 Keywords=Classic Message=Product: Centrify Suite Category: DirectAudit System Management Event name: Start collector service succeeded Message: Collector service was started successfully on computer 'MEMBER'. Apr 05 14:59:56 member.centrify.vms collector[1344]: INFO AUDIT_TRAIL|Centrify Suite|DirectAudit System Management|1.0|251|Start collector service succeeded|5|user=system@nt authority userSid=S-1-5-18 sessionId=0 centrifyEventID=42251 DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 installation=DefaultInstallation collector=MEMBER
```

DirectAudit System Management audit events

Table 8. DirectAudit System Management audit events (Sheet 1 of 2)

Centrify Event Id	Description	Parameters
42251	Start collector service succeeded	installation: Name of the installation Collector: Name of the collector computer
42252	Start collector service failed	installation: Name of the installation Collector: Name of the collector computer reason: Error message
42253	Stop collector service succeeded	installation: Name of the installation Collector: Name of the collector computer
42254	Stop collector service failed	installation: Name of the installation Collector: Name of the collector computer reason: Error message
42255	Collector settings update succeeded	installation: Name of the installation Collector: Name of the collector computer Collector setting: Name of the updated collector setting Collector setting value: Value of the updated collector setting
42256	Collector settings update failed	installation: Name of the installation Collector: Name of the collector computer Collector setting: Name of the updated collector setting Collector setting value: Value of the updated collector setting reason: Error message
42257	Start agent service succeeded	installation: Name of the installation Audited system: Name of the audited system

Table 8. DirectAudit System Management audit events (Sheet 2 of 2)

Centrify Event Id	Description	Parameters
42258	Start agent service failed	installation: Name of the installation Audited System: Name of the audited system reason: Error message
42259	Stop agent service succeeded	installation: Name of the installation Audited system: Name of the audited system
42260	Stop agent service failed	installation: Name of the installation Audited system: Name of the audited system reason: Error message
42261	Agent settings update succeeded	installation: Name of the installation Audited system: Name of the audited system Agent setting: Name of the updated agent setting Agent setting value: Value of the updated agent setting
42262	Agent settings update failed	installation: Name of the installation Audited system: Name of the audited system Agent setting: Name of the updated agent setting Agent setting value: Value of the updated agent setting reason: Error message

DirectAudit UNIX Agent

The DirectAudit UNIX Agent audit events are focused on the success or failure of starting and stopping the Centrify agent: **dad**.

DirectAudit UNIX Agent audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 45000. This log sample documents the successful start of the Centrify agent: dad. The change was made by user=root on April 15 at 01:35:11.

```
Apr 15 01:35:11 engcen6 adclient[101241]: INFO AUDIT_TRAIL|Centrify
Suite|DirectAudit UNIX Agent|1.0|0|DirectAudit agent (dad)
started|5|user=root pid=101574 utc=1460702111116
centrifyEventID=45000 DAInst=AuditingInstallation DASessID=c72252aa-
e616-44ff-a5f6-d3f53f09bb67 status=SUCCESS service=dad
```

DirectAudit UNIX Agent audit events

Table 9. DirectAudit UNIX Agent audit events audit events

Centrify Event Id	Description	Parameters
45000	DirectAudit agent (dad) started	
45001	DirectAudit agent (dad) failed to start	reason: error message
45100	DirectAudit agent (dad) stopped	
45101	DirectAudit agent (dad) failed to stop	reason: error message

DirectAudit – Windows

Centrify DirectAudit collects login success audit data from Windows computers. DirectAudit – Windows is available with the Enterprise Centrify Server Suite. The DirectAudit audit event focuses on login success.

DirectAudit – Windows audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 9001. This log sample documents a successful login. The change was made by user=administrator@p3f1r2.test on January 06 at 15:53:10..

```
Jan 06 15:53:10 s2k8r2p1v1.p3f1r2.test wdad[1128]: INFO
AUDIT_TRAIL|Centrify Suite|DirectAudit - Windows|1.0|1|login
success|5|user=administrator@p3f1r2.test userSid=S-1-5-21-
1986235188-3370598863-2160698129-500 sessionId=1
centrifyEventID=9001 DAInst=AuditingInstallation DASessID=c72252aa-
e616-44ff-a5f6-d3f53f09bb67
```

DirectAudit - Windows audit events

Table 10. DirectAudit - Windows audit events

Centrify Event Id	Description	Parameters
9001	login success	
9002	logoff success	

DirectAuthorize – Windows

DirectAuthorize for Windows provides role-based access control for Windows desktops and applications, and to remote Windows servers. DirectAuthorize for Windows audit events focus on successful and failed local console and remote log in attempts, administrative activity using desktop or application privileges, network access to remote servers, changes to the zone information for Windows computers and changes to role information for Windows users.

DirectAuthorize Windows audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 6012. This log sample documents a user with local and network role

privileges launching a `.msc` file. The change was made by user=dwirth@centrify.vms on April 05, 2016 at 03:43:33.

```
04/05/2016 03:43:33 PM LogName=Application SourceName=Centrify
AuditTrail V2 EventCode=6012 EventType=4 Type=Information
ComputerName=member.centrify.vms User=NOT_TRANSLATED Sid=S-1-
5-21-3883016548-1611565816-1967702834-1107 SidType=0
TaskCategory=%1 OpCode=Info RecordNumber=51931
Keywords=Classic Message=Product: Centrify Suite Category:
DirectAuthorize - Windows Event name: Run as role success Message:
User launched 'C:\Program Files\Centrify\DirectManage Access
Manager\Centrifydc.msc' on desktop 'Default' using local role
'ROLE_SYSTEM_Archt/Global' and network roles 'ROLE_SYSTEM_Archt/
Global'. Apr 05 15:43:33 member.centrify.vms dzagent[1400]: INFO
AUDIT_TRAIL|Centrify Suite|DirectAuthorize - Windows|1.0|12|Run as
role success|5|user=dwirth@centrify.vms userSid=S-1-5-21-
3883016548-1611565816-1967702834-1107 sessionId=4
centrifyEventID=6012 DAInst=AuditingInstallation DASessID=c72252aa-
e616-44ff-a5f6-d3f53f09bb67 role=ROLE_SYSTEM_Archt/Global
effectivesid=S-1-5-21-3883016548-1611565816-1967702834-500
effectivegroupsids= logonguid=f26eb789-50da-41c7-a7e3-8e913cc9c4ae
desktopguid=3c2ef049-6e26-4dc9-8428-100ad4484e66
command=C:\\Program Files\\Centrify\\DirectManage Access
Manager\\Centrifydc.msc passwordprompted=True
desktopname=Default networkroles=ROLE_SYSTEM_Archt/Global
```

DirectAuthorize - Windows audit events

Table 11. DirectAuthorize - Windows audit events (Sheet 1 of 5)

Centrify Event ID	Description	Parameters
6001	Console login success	Role: role DesktopGuid: desktop GUID
6002	Console login failure	
6003	Remote login success	Role: role DesktopGuid: desktop GUID
6004	Remote login failure	
6005	Run with privilege success	Role: local role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID DesktopGuid: desktop GUID Command: command
6006	Run with privilege failure	Role: local role DesktopGuid: desktop GUID Command: command
6007	Create desktop success	Role: local role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID DesktopGuid: desktop GUID
6008	Create desktop failure	Role: local role
6009	Network access success	Role: role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID

Table 11. DirectAuthorize - Windows audit events (Sheet 2 of 5)

Centrify Event ID	Description	Parameters
6010	Console logon failure	Reason: reason
6011	Remote login failure	Reason: reason
6012	Run with privilege success	Role: local role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID DesktopGuid: desktop GUID Command: command PasswordPrompted: whether user was required to re-enter their password DesktopName: desktop name NetworkRoles: network roles
6013	Run with privilege failure	Role: local role DesktopGuid: desktop GUID Command: command Reason: reason DesktopName: desktop name NetworkRoles: network roles
6014	Create desktop success	Role: local role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID DesktopGuid: desktop GUID PasswordPrompted: whether user was required to re-enter their password DesktopName: desktop name NetworkRoles: network roles
6015	Create desktop failure	Role: local role Reason: reason NetworkRoles: network roles

Table 11. DirectAuthorize - Windows audit events (Sheet 3 of 5)

Centrify Event ID	Description	Parameters
6016	Switch desktop success	DesktopName: desktop name DesktopGuid: desktop GUID PasswordPrompted: whether user was required to re-enter their password Role: local role NetworkRoles: network roles
6017	Switch desktop failure	DesktopName: desktop name Reason: reason
6018	Run with privilege failure	Role: local role DesktopGuid: desktop GUID Command: command Reason: reason DesktopName: desktop name NetworkRoles: network roles PasswordPrompted: whether user was required to re-enter their password
6019	Create desktop failure	Role: local role Reason: reason NetworkRoles: network roles PasswordPrompted: whether user was required to re-enter their password
6020	Switch desktop failure	DesktopName: desktop name Reason: reason PasswordPrompted: whether user was required to re-enter their password
6021	Join to zone success	zone: zone name ZoneDomainName: zone domain name ComputerName: computer name ComputerDomainName: computer domain name LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation

Table 11. DirectAuthorize - Windows audit events (Sheet 4 of 5)

Centrify Event ID	Description	Parameters
6022	Join to zone failure	zone: zone name ZoneDomainName: zone domain name ComputerName: computer name ComputerDomainName: computer domain name Reason: reason LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation
6023	Leave from zone success	zone: zone name ZoneDomainName: zone domain name ComputerName: computer name ComputerDomainName: computer domain name LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation
6024	Leave from zone failure	zone: zone name ZoneDomainName: zone domain name ComputerName: computer name ComputerDomainName: computer domain name Reason: reason LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation

Table 11. DirectAuthorize - Windows audit events (Sheet 5 of 5)

Centrify Event ID	Description	Parameters
6025	Add role success	zone: zone name ZoneDomainName: zone domain name RoleName: role name LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation
6026	Add role failure	zone: zone name ZoneDomainName: zone domain name RoleName: role name Reason: reason LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation
6027	Add role assignment success	zone: zone name ZoneDomainName: zone domain name RoleName: role name Assignee: assignee LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation
6028	Add role assignment failure	zone: zone name ZoneDomainName: zone domain name RoleName: role name Assignee: assignee Reason: reason LogonUser: logon user LogonUserSid: logon user SID AlternateUser: whether alternate user is used to perform the operation

DirectControl UNIX Agent

The DirectControl UNIX Agent audit events are focused on the success or failure of starting and stopping the Centrify agent: **adclient**.

DirectControl UNIX Agent audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 17000. This log sample documents the successful start of the Centrify agent: adclient. The change was made by user=root on April 05 at 06:46:43.

```
Apr 5 06:46:43 newcentos adclient[1837]: INFO AUDIT_TRAIL|Centrify Suite|DirectControl UNIX Agent|1.0|2000|Centrify agent (adclient) started|5|user=root pid=1837 utc=1459856803582 centrifyEventID=17000 DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=SUCCESS service=adclient
```

DirectControl UNIX Agent audit events

Table 12. DirectControl UNIX Agent audit events

Centrify Event Id	Description	Parameters
17000	Centrify agent (adclient) started	
17001	Centrify agent (adclient) failed to start	reason: error message
17002	Centrify agent (adclient) stopped	
17003	Centrify agent (adclient) failed to stop	reason: error message

dzdo

For Linux and UNIX computers, Centrify Server Suite includes authorization services that enable users to run with elevated privileges using the `dzdo` command line program. The `dzdo` program is similar to `sudo` except that, instead of using a `sudoers` configuration file, the program uses the role-based access rights for zones stored in Active Directory.

dzdo audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 30000. This log sample documents that the `dzdo` service has been

granted authorization.The change was made by user=dwirth(type:ad,dwirth@CENTRIFY.VMS) on April 7 at 01:20:12.

```
Apr 7 01:20:12 engcen6 adclient[2191]: INFO AUDIT_TRAIL|Centrify
Suite|dzdo|1.0|0|dzdo
granted|5|user=dwirth(type:ad,dwirth@CENTRIFY.VMS) pid=32224
utc=1460010012602 centrifyEventID=30000 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=GRANTED
service=dzdo command=/bin/vi runas=root role=ROLE_SYSTEM_Archt/
Global env=(none)
```

dzdo audit events

Table 13. dzdo audit events

Centrify Event Id	Description	Parameters
30000	dzdo granted	command: command runas: username@domain role: role name env: environment variables
30001	dzdo denied	command: command runas: username@domain reason: error message
30002	Trouble ticket entered	ticket: ticket

dzinfo

The `dzinfo` command displays rights, roles, and role assignments events. The `dzinfo` audit events focus on the success and failure of the `dzinfo` command.

dzinfo audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 42001. This log sample documents that a user failed run `dzinfo` to view another user's settings; only the user=root can view other user's

settings. The change was made by user=eugene.user(type:ad,eugene.user@CENTSPLUNK.COM) on April 28 at 10:35:47.

```
Apr 28 10:35:47 sspl1-n2 adclient[1835]: INFO  AUDIT_TRAIL|Centrify
Suite|dzinfo|1.0|3001|Dzinfo
failed|5|user=eugene.user(type:ad,eugene.user@CENTSPLUNK.COM)
pid=59947 utc=1461864947244 centrifyEventID=42001
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-
d3f53f09bb67 status=FAILURE service=dzinfo parameters=-c
aaron.admin reason=Only root may view other user's settings
```

dzinfo audit events

Table 14. dzinfo audit events

Centrify Event Id	Description	Parameters
42000	Dzinfo successful	parameters: parameters
42001	Dzinfo failed	parameters: parameters reason: error message

dzsh

For Linux and UNIX computers, Centrify Server Suite includes authorization services that enable users to run with elevated privileges in a restricted shell environment using the `dzsh` program.

dzsh audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 33001. This log sample documents a user being denied `dzsh`

command execution.The change was made by user=dwirth(type:ad,dwirth@CENTRIFY.VMS) on April 7 at 01:20:12.

```
Apr 28 10:26:41 sspl1-n2 adclient[1835]: INFO  AUDIT_TRAIL|Centrify
Suite|dzsh|1.0|1|dzsh command execution denied|5|user=root
pid=59860 utc=1461864401103 centrifyEventID=33001
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-
d3f53f09bb67 status=DENIED service=dzsh command=/usr/share/
centrifydc/bin/dzinfo reason=sam checking returned false, user is not
allowed to use this command or runas
```

dzsh audit events

Table 15. dzsh audit events

Centrify Event Id	Description	Parameters
33000	dzsh command execution granted	command: command runas: username@domain role: role name env: environment variables
33001	dzsh command execution denied	command: command reason: error message
34000	dzsh role change granted	fromRole: fromRole toRole: toRole
34001	dzsh role change denied	fromRole: fromRole toRole: toRole reason: error message

License Management

Auditing licenses are issued for each computer that will be connected to an auditing collector, and are managed by the Centrify Licensing Service. You can use the Licensing Service control panel as described in the License Management Administrator's Guide to add and remove licenses, monitor license usage, and configure license usage notification.

License management audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 20101. This log sample documents a user being denied an `adjoin` command execution due to missing license information. The change was made by user=root on October 277 at 17:24:25.

```
Oct 27 17:24:25 Eason5 adjoin[9886]: INFO AUDIT_TRAIL|Centrify
Suite|Centrify Commands|1.0|2101|Join failed|5|user=root pid=9886
utc=1477560265956 centrifyEventID=20101 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=FAILURE
service=adjoin parameters=-z developer -p * eason.test zone=developer
domain=eason.test computer=eason5 runas=Administrator
reason=Valid Centrify license information was not found.
```

License management audit events

Table 16. License Management audit events (Sheet 1 of 3)

Centrify Event ID	Description	Parameters
60100	DirectControl license key added	PID: process id user: username@domain RunAs: username@domain type: user type key: license key container: license container
60101	Add DirectControl license key failed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key container: license container reason: Error message
60102	DirectControl license key removed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key container: license container
60103	Remove DirectControl license key failed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key container: license container reason: Error message
60104	DirectControl license container added	PID: process id user: username@domain RunAs: username@domain type: user type container: license container

Table 16. License Management audit events (Sheet 2 of 3)

Centrify Event ID	Description	Parameters
60105	Add DirectControl license container failed	PID: process id user: username@domain RunAs: username@domain type: user type container: license container reason: Error message
60106	DirectControl license container removed	PID: process id user: username@domain RunAs: username@domain type: user type container: license container
60107	Remove DirectControl license container failed	PID: process id user: username@domain RunAs: username@domain type: user type container: license container reason: Error message
60200	DirectAudit license key added	PID: process id user: username@domain RunAs: username@domain type: user type key: license key installation: installation
60201	Add DirectAudit license key failed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key installation: installation reason: Error message

Table 16. License Management audit events (Sheet 3 of 3)

Centrify Event ID	Description	Parameters
60202	DirectAudit license key removed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key installation: installation
60203	Remove DirectAudit license key failed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key installation: installation reason: Error message

Local Account Management

Centrify administrators use the Local Account Management feature to create, manage, lock, and delete local UNIX and Linux user and group accounts. The Local Account Management audit events focus on local users, groups, and accounts.

Local Account Management audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 51300. This log sample documents the removal of a local user from a local password file. The change was made by user=root on November 25 at 16:51:20.

```
Nov 25 16:51:20 rhed57x64v3 adclient[4423]: INFO
AUDIT_TRAIL|Centrify Suite|Local Account
Management|1.0|300|Removing local user from local passwd
file|5|user=root pid=4423 utc=1448441900487 centrifyEventID=51300
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-
d3f53f09bb67 status=SUCCESS removedUser=locud01
```

Local Account Management audit events

Table 17. Event Source Cateogry: Local Account Management

Centrify Event Id	Description	Parameters
51100	Adding enabled local user to local passwd file	enabledUser: enabled local user
51200	Adding disabled local user to local passwd file	disabledUser: disabled local user
51300	Removing local user from local passwd file	removedUser: removed local user
51400	Local user is marked as disabled	localUser: local user
51500	Local user is marked as enabled	localUser: local user
51101	Local passwd file update failed	reason: error message
51600	Invoking notification cli succeeded	parameters: parameters
51601	Invoking notification cli failed	reason: error message
52000	Adding enabled local group to local group file	enabledGroup: enabled local group
52100	Removing local group from local group file	removedGroup: removed local group
52001	Local group file update failed	reason: error message

Table 17. Event Source Cateogry: Local Account Management

Centrify Event Id	Description	Parameters
53000	Managing local accounts succeeded	parameters: parameters
53001	Managing local accounts failed	parameters: parameters reason: error message

Multi-factor Authentication

Multi-factor authentication (MFA) strengthens security by requiring users to provide more than one form of identification to authenticate their identity when they attempt to access servers or applications. Multi-factor authentication challenges might require users to type a password, respond to an email message or phone call, enter a passcode, or answer a security question. Audit events in the MFA category focus on the success and failure of MFA challenges.

MFA audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 54100. This log sample documents the success of an MFA challenge. The change was made by user=laniu1(type:ad,laniu1@SINGLE01.CDC) on April 20 at 14:51:18.

```
Apr 20 14:51:18 sol112x64v3 adclient[5640]: [ID 702911 auth.info] INFO
AUDIT_TRAIL|Centrify Suite|MFA|1.0|100|MFA challenge
succeeded|5|user=laniu1(type:ad,laniu1@SINGLE01.CDC) pid=6160
utc=1461135078139 centrifyEventID=54100 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=SUCCEED
service=sshd tty=ssh client=::1 challenge=EMAIL
```

MFA audit events

Table 18. MFA audit events

Centrify Event Id	Description	Parameters
54100	MFA challenge succeeded	service: service tty: tty client: client challenge: challenge
54101	MFA challenge failed	service: service tty: tty client: client challenge: challenge reason: error message
54200	MFA challenge succeeded	service: service challenge: challenge
54201	MFA challenge failed	service: service challenge: challenge reason: error message
54202	MFA is offline	service: service reason: error message

PAM

A pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API). The PAM audit events include authorization, credentials, account management, password changes, open session, and multi-factor authentication.

PAM audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 24100. This log sample documents PAM authentication being

granted. The change was made by user=dwirth(type:ad,dwirth@CENTRIFY.VMS) on April 4 at 21:04:14.

```
Apr 4 21:04:14 engcen6 adclient[1749]: INFO AUDIT_TRAIL|Centrify
Suite|PAM|1.0|100|PAM authentication
granted|5|user=dwirth(type:ad,dwirth@CENTRIFY.VMS) pid=7458
utc=1459784054942 centrifyEventID=24100 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=GRANTED
service=sshd tty=ssh client=dc.centrify.vms
```

PAM audit events

Table 19. PAM audit events (Sheet 1 of 2)

Centrify Event Id	Description	Parameters
24100	PAM authentication granted	service: service tty: tty client: client
24101	PAM authentication denied	service: service tty: tty client: client reason: error message
24200	PAM set credentials granted	service: service tty: tty client: client
24201	PAM set credentials denied	service: service tty: tty client: client reason: error message
24300	PAM account management granted	service: service tty: tty client: client
24301	PAM account management denied	service: service tty: tty client: client reason: error message
24400	PAM change password granted	service: service tty: tty client: client
24401	PAM change password denied	service: service tty: tty client: client reason: error message

Table 19. PAM audit events (Sheet 2 of 2)

Centrify Event Id	Description	Parameters
24500	PAM open session granted	service: service tty: tty client: client
24501	PAM open session denied	service: service tty: tty client: client reason: error message
24600	PAM close session granted	service: service tty: tty client: client
24601	PAM close session denied	service: service tty: tty client: client reason: error message

Trusted Path

The trusted path configuration parameter (audittrail.Centrify_Suite.Trusted_Path.machinecred.skipda) specifies whether trusted path audit trail events are sent to the audit installation database in situations where the user is using a computer credential. The audit events identify a granted and denied Trusted Path.

Trusted Path audit event log sample

The following is a sample of an audit event log for Centrify Audit Event ID 23700. This log sample documents a Trusted Path being granted.

The change was made by user=newcentos$@CENTRIFY.VMS on April 04 at 21:02:09.

```
Apr 4 21:02:09 newcentos adclient[1395]: INFO AUDIT_TRAIL|Centrify
Suite|Trusted Path|1.0|2700|Trusted path
granted|5|user=newcentos$@CENTRIFY.VMS pid=1395
utc=1459783929161 centrifyEventID=23700 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67 status=GRANTED
server=ldap/dc.centrify.vms@CENTRIFY.VMS
```

Note The Trusted path audit event log sample identifies a server field type instead of the usual service field type found in UNIX/Linux audit events.

Trusted Path audit events

Table 20. Trusted Path audit events

Centrify Event Id	Description	Parameters
23700	Trusted path granted	server: server
23701	Trusted path denied	server: server reason: error message