Delinea

Server Suite

Audit Events Guide

Version: 2024.x

Publication Date: 7/14/2025

Server Suite Audit Events Guide

Version: 2024.x, Publication Date: 7/14/2025

Table of Contents

About this Guide

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 Audit Analyzer. Audit events are organized into categories in the Audit Analyzer and these categories are identified in this document.

Depending on your environment and role as an administrator or auditor, you may want to read portions of this guide selectively.

Overview of Server Suite 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 Server Suite audit event data.

- Windows and UNIX/Linux Audit Events
- How to Read Audit Event Data
- Configuring the Audit Event Log Location
- Which Events Only in Delinea Audit & Monitoring Service

About Server Suite Auditing & Monitoring Service

DelineaServer Suite is a product category that includes the following product offerings:

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

The DirectControl Agent provides services for the Authentication Service and Privilege Elevation Service contained in the DelineaDC packages. The DirectAudit Agent provides services for Auditing & Monitoring Service contained in the DelineaDA packages.

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

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

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

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

Which Events are Only in Delinea Audit & Monitoring Service

Audit events may come from Delinea Authentication Service, Delinea Privilege Elevation Service, or Delinea Audit & Monitoring Service. If you are using only authentication and privilege elevation, the following events will not be available to you as they are from audit and monitoring service:

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

Configuring the Audit Event Log Location

You can configure audit event logs to go to DirectAudit or your system's default logging system (Windows event log or UNIX syslog). You configure the log location either manually for each computer or by way of group policy.

You can also configure a global audit event logging behavior or specify different settings for different feature areas.

Configuring the Audit Event Logging Location by Group Policy

Audit trail group policies are located in category-specific subfolders (such as **Audit Analyzer Settings**, **Audit Manager Settings**, and so on.

Additionally, a **Centrify Global Settings** subfolder contains group policies that you can set at a global level.

Any category-specific audit trail targets that you set (for example, **Audit Manager Settings** > **Send audit trail to log file**) override global audit trail targets (for example, **Centrify Global Settings** > **Send audit trail to log file**). Each subfolder in **Centrify Audit Trail Settings** contains the same set of group policies.

Note: To send audit trail events to both the database and the local logging facility, enable both of these group policies.

Send Audit Trail to Audit Database

Enable this group policy to specify that audit events for this component **Audit Analyzer**, **Audit Manager**, and so on are sent to the active audit store database.

See the **Explain** tab in the group policy for details about which parameter each group policy sets in the agent configuration file.

Send Audit Trail to Log File

Enable this group policy to specify that audit events for this component such as **Audit Analyzer**, **Audit Manager**, and so on are sent to the local logging facility (syslog on UNIX systems, Windows event log on Windows systems).

See the **Explain** tab in the group policy for details about which parameter each group policy sets in the agent configuration file.

Set Global Audit Trail Targets

Specify the target for audit trail information.

If you set this group policy to **Not configured** or **Disabled**, the destination of audit trail information depends on which version of DirectAudit is installed. If DirectAudit 3.2 or later is installed, audit trail information is sent to the local logging facility and DirectAudit. If a DirectAudit version earlier than 3.2 is installed, audit trail information is only sent to the local logging facility.

If you set this group policy to **Enabled**, you can specify the target for audit trail information. Possible settings are:

- 0 (Audit information is not sent.)
- 1 (Audit information is sent to Delinea Audit & Monitoring Service. This capability is supported by DirectAudit version 3.2 and later.)
- 2 (Audit information is sent to the local logging facility, either syslog on UNIX systems or Windows event log on Windows systems.)
- 3 (Audit information is sent to both DirectAudit and the local logging facility.)

This group policy modifies the audittrail.targets setting in the agent configuration file.

How to Read Audit Event Data

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

Event ID/DelineaEventID

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 DelineaEventID in the common fields identifies the unique ID among all Delinea audit event types.

Windows Example

Delinea audit event header fields	Category	Privilege Elevation Service - Windows	
	Product Version	1.0	
	Event ID	3	
	Event Name	Remote login success	5
Delinea audit event common fields	user	administrator@member.acme.vms	
	userSid	S-1-5-21-3789923312-3040275127-1160560412-500	
	DAInst	AuditingInstallation	
	DASessID	c72252aa-e616-44ff-a5f6-d3f53f09bb67	
	sessionId	6	
	Delinea EventID	6003	

UNIX/Linux Example

Delinea 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
Delinea audit event common fields	user	dwirth(type:ad,dwirth@acme.vms)
	pid	7456
	utc	1459784055479
	Delinea EventID	27100

Delinea audit event header fields	Event Type	AUDIT_TRAIL
	DAInst	
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. Delinea 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.

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 audit event data to understand the similarities and differences.

Windows Audit Event Log Line Example

The following is an example of a Delinea audit event recorded in the Windows application event log. Standard Windows audit event fields (in black) contain information about the Delinea event. Delinea 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.acme.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.acme.vms dzagent[1496]: INFO AUDIT_TRAIL|Centrify
Suite|DirectAuthorize - Windows|1.0|3|Remote login success|5|user=
administrator@member.acme.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.

Windows Audit Event Log Line Information

Field Type	Field Name	Sample Field Value
Syslog header fields	Timestamp	Apr 05, 2016 02:15:37 PM
	Host Name	member.acme.vms
	Process Name	dzagent
	Process ID	1496
	Log Level	INFO
Delinea audit event header fields	Event Type	AUDIT_TRAIL
	Product	Centrify Suite
	Category	privilege elevation service - Windows
	Product Version	1.0
	Event ID	3
	Event Name	Remote login success
	Severity	5
Delinea audit event common fields for Windows	user	administrator@member.acme.vms
	userSid	S-1-5-21-3789923312-3040275127-1160560412-500
	DAInst	AuditingInstallation
	DASessID	c72252aa-e616-44ff-a5f6-d3f53f09bb67
	sessionId	6

Field Type	Field Name	Sample Field Value
	Delinea EventID	6003
Delinea 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. Delinea 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@acme.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)
```

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.

UNIX/Linux Audit Event Log Information

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
Delinea 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

Field Type	Field Name	Sample Field Value
	Severity	5
Delinea audit event common fields	user	dwirth(type:ad,dwirth@acme.vms)
	pid	7456
	utc	1459784055479
	DelineaEventID	27100
	DAInst	AuditingInstallation
	DASessID	c72252aa-e616-44ff-a5f
	service	ssh-connection
Delinea audit event-specific fields	tty	/dev/pts/0
	authMechanism	keyboard-interactive
	client	192.168.81.11
	sshRights	shell
	command	(none)

Server Suite Audit Events

This section includes the following topics:

- Delinea Authentication Service UNIX Agent
- dzdo
- dzinfo
- dzsh
- License Management
- Kerberos
- Local Account Management
- Multi-factor Authentication
- PAM
- Trusted Path

Audit Analyzer

The Audit Analyzer console is a graphical user interface that administrators can use to query and review captured user sessions. The Audit Analyzer is available with the Delinea Audit & Monitoring Service. The Audit Analyzer events focus on session modification.

Audit Analyzer Audit Event Log Sample

The following is a sample of an audit event log for Delinea Audit Event ID 3001. This log sample documents a session being deleted. The change was made by user=administrator@acme.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.acme.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.acme.vms mmc[4064]: INFO
 AUDIT_TRAIL|Centrify Suite|Audit Analyzer|1.0|1|Delete
 session|5|user=administrator@acme.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

Audit Analyzer Audit Events

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
3007	Update session review status succeeded added in release 18.8	Installation: Name of the installation Session Id: Unique identifier of the session Review Status: Name of the review status
3008	Update session review status failed added in release 18.8	Installation: Name of the installation Session Id: Unique identifier of the session Review Status: Name of the review status Reason: Error message
3009	Replay session succeeded Added in release 19.6	Installation: Name of the installation Session Id: Unique identifier of the session User: User of the session Machine: Machine of the session
3010	Replay session failed Added in release 19.6	Installation: Name of the installation Session Id: Unique identifier of the session Reason: Error message
3011	Delete audit trail events succeeded Added in release 19.9	SearchFilter: Search Filter
3012	Delete audit trail events failed Added in release 19.9	SearchFilter: Search Filter Reason: Error Message
3013	Delete session succeeded Added in release 2020.1	Session Id: Unique identifier of the session Username: Name of the user whose session was recorded Machinename: Name of the machine where the session was recorded

3014	Delete session failed Added in release 2020.1	Session Id: Unique identifier of the session Username: Name of the user whose session was recorded Machinename: Name of the machine where the session was recorded 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 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 Analyzer Audit Event Log Sample

The following is a sample of an audit event log for Delinea Audit Event ID 3001. This log sample documents a session being deleted. The change was made by user=administrator@acme.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.acme.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.acme.vms mmc[4064]: INFO
AUDIT_TRAIL|Centrify Suite|Audit Analyzer|1.0|1|Delete
session|5|user=administrator@acme.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 Manager Audit Events

Audit Manager Audit Events

Event Id	Description	Parameters
12200	Video capture status updatedv	installation: audit and monitoring service Installation VideoCaptureStatus: video capture status
12201	Create new installation succeededv	installation: Name of the installation

12202	Create new installation failedv	installation: Name of the installation reason: Error message
12203	Installation update succeededv	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 failedv	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 succeededv	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
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: audit and monitoring service 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)
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
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
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 audit and monitoring service Version 1 Database succeeded	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the audit and monitoring service Version 1 Database

12230	Attach audit and monitoring service Version 1 Database failed	installation: Name of the installation Audit Store: Name of the Audit Store Audit Store Database: Name of the audit and monitoring service Version 1 Database reason: Error message
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
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)
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
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

Delinea Audit & Monitoring Service Advanced Monitoring

If you have enabled Delinea Audit & Monitoring Service 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 Delinea 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.acme.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.
acme.com processid=32393 ppid=32392 gid=root
euid=root@al_rhel6_2.altest.acme.com cwd=/ accessType=2
command=/usr/bin/python argc=-1 args=/etc/pki/nssdb/
/etc/pki/nssdb/cert9.db-journal
```

Delinea Audit & Monitoring Service Advanced Monitoring Audit Events

Audit and Monitoring Service Advanced Monitoring Audit Events

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

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
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

Delinea Audit & Monitoring Service System Management

The auditing module'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. Delinea Audit & Monitoring Service System Management is available with Delinea Audit & Monitoring Service. The audit and monitoring service audit events focus on collector service, collector settings, and agent settings.

Delinea Audit & Monitoring Service System Management audit event log sample

The following is a sample of an audit event log for Delinea 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.acme.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.acme.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
```

Delinea Audit & Monitoring Service System Management audit events

Audit and Monitoring Service System Management Audit Events

Delinea 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
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

42263	Start audit management service succeeded added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer
42264	Start audit management service failed added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer reason: Error message
42265	Stop audit management service succeeded added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer
42266	Stop audit management service failed added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer reason: Error message
42267	Started the collector service added in release 18.11	installation: Name of the installation Collector: Name of the collector computer User: User name
42268	Failed to start the collector service added in release 18.11	installation: Name of the installation Collector: Name of the collector computer User: User name reason: Error message
42269	Stopped the collector service added in release 18.11	installation: Name of the installation Collector: Name of the collector computer User: User name
42270	Failed to stop the collector service added in release 18.11	installation: Name of the installation Collector: Name of the collector computer User: User name reason: Error message
42271	Restarted the collector service added in release 18.11	installation: Name of the installation Collector: Name of the collector computer User: User name

42272	Failed to restart the collector service added in release 18.11	installation: Name of the installation Collector: Name of the collector computer User: User name reason: Error message
42273	Started the audit management service added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer User: User name
42274	Failed to start the audit management service added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer User: User name reason: Error message
42275	Stopped the audit management service added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer User: User name
42276	Failed to stop the audit management service added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer User: User name reason: Error message
42277	Restarted the audit management service added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer User: User name
42278 Good	Failed to restart the audit management service added in release 18.11	installation: Name of the installation Audit Management: Name of the audit management computer User: User name reason: Error message

Delinea Authentication Service UNIX Agent

The Delinea Authentication Service UNIX Agent audit events are focused on the success or failure of starting and stopping the Delinea Agent: **adclient**.

Delinea Authentication Service UNIX Agent Audit Event Log Sample

The following is a sample of an audit event log for Delinea Audit Event ID 17000. This log sample documents the successful start of the Delinea 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
```

Delinea Authentication Service UNIX Agent Audit Events

Authentication Service UNIX Agent Audit Events

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

Delinea Audit & Monitoring Service – Windows

Delinea Audit & Monitoring Service collects login success audit data from Windows computers. The Delinea Audit & Monitoring Service audit event focuses on login success.

Delinea Audit & Monitoring Service – Windows Audit Event Log Sample

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

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

Delinea Audit & Monitoring Service - Windows Audit Events

Audit and Monitoring Service - Windows Audit Events

Event Id	Description	Parameters
9001	login success	
9002	logoff success	
9003	Enable Delinea Auditing and Monitoring Service succeeded added in release 2017.3	InstallationName: Installation Name

9004	Disable Delinea Auditing and Monitoring Service succeeded added in release 2017.3	InstallationName: Installation Name
9005	Enable Delinea Auditing and Monitoring Service failed added in release 2017.3	InstallationName: Installation Name Reason: Reason for failure
9006	Disable Delinea Auditing and Monitoring Service failed added in release 2017.3	InstallationName: Installation Name Reason: Reason for failure
9007	Session auditing started added in Release 2020	
9008	Session auditing started added in Release 2020	

Delinea Authentication Service UNIX Agent

The Delinea Authentication Service UNIX Agent audit events are focused on the success or failure of starting and stopping the Delinea Agent: **adclient**.

Delinea Authentication Service UNIX Agent Audit Event Log Sample

The following is a sample of an audit event log for Delinea Audit Event ID 17000. This log sample documents the successful start of the Delinea 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
```

Delinea Authentication Service UNIX Agent Audit Events

Authentication Service UNIX Agent Audit Events

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

Command (Audited and Successfully Executed Commands)

Command audit events are recorded when Delinea UNIX command-line programs are used on Delinea-managed computers. Delinea 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=
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

Event Source Category: Command

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

Delinea Commands (UNIX Commands)

Audit events in the Delinea 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.

Delinea Command Audit Event Log Sample

The following is a sample of an audit event log for Delinea 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
```

Delinea Commands Audit Events

Delinea Commands Audit Events

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
18300	Desktop auditing enabled Added in Release 2020	
18301	Desktop auditing not enabled Added in Release 2020	reason: error message
18400	Desktop auditing disabled Added in Release 2020	
18401	Desktop auditing not disabled Added in Release 2020	reason: error message
18500	Session auditing started Added in Release 2020	
18501	Session auditing ended Added in Release 2020	
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
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 (Centrify.conf) reloaded	parameters: parameters
20501	Configuration settings (Centrify.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
20910	Advanced monitoring disabled	service: service
20911	Advanced monitoring not disabled	service: service reason: error message
21100	Changing web proxy configuration succeeded added in release 18.8	parameters: parameters
21101	Changing web proxy configuration failed added in release 18.8	parameters: parameters reason: error message
21200	Editing Kerberos keytab file succeeded	parameters: parameters
21201	Editing Kerberos keytab file failed	parameters: parameters reason: error message

Delinea Configuration

Delinea hierarchical zones are used to 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.

Delinea Configuration Audit Event Log Sample

The following is a sample of an audit event log for Delinea Audit Event ID 36101. This log sample documents a user giving zone administrative tasks to another user. The change was made by user=dwirth@acme.vms on April 19, 2016 at 03:01:04.

```
04/19/2016 03:01:04 PM LogName=Application
SourceName=CentrifyAuditTrail V2 EventCode=36101
EventType=4 Type=Information
ComputerName=member.acme.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@acme.vms" (running as "dwirth@acme")
delegated "acmepankaj" to perform "Change zone
properties" on "acme.vms/acmese/Zones/zone-14".
Apr 19 15:01:04 member mmc[5792]: INFO AUDIT_TRAIL|Centrify
Suite|CentrifyvConfiguration|1.0|101|Zone
tasks delegated|5|user=dwirth@acme.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@acme.vms runas=dwirth@acme type=AD
status=SUCCESS trustee=acmepankaj task=Change zone
properties zone=acme.vms/acmese/Zones/zone-14
```

Delinea Configuration Audit Events

Delinea Configuration Audit Events

Event Id	Description	Parameters
36101	Zone administrative tasks delegated	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 trustee: username@domain task: delegation task name zone: zone name computer: computer name

36104	Delegation of computer administrative tasks failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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: 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: failed trustee: username@domain task: delegation task name zone: zone name computerRole: computer role name reason: error message
36201	Zone created	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded zone: zone name
36202	Zone creation failed	PID: process id user: username@domain RunAs: username@domain type: user type status: failed zone: zone name reason: error message
36203	Zone deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded zone: zone name
36204	Zone deletion failed	status: 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 zone: zone name
36206	Zone update failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 ZoneUser: unixname zone: zone name
36304	Delete user from a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 : unixname computer: computer hostname zone: zone name
36308	Add user to a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 ZoneUser: unixname computer: computer hostname zone: zone name
36312	Modify user on a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 group: group name zone: zone name
36404	Delete group from a zone failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 group: group name computer: computer hostname zone: zone name
36408	Add group to a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 group: group name computer: computer hostname zone: zone name
36412	Modify group for a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 computer: hostname zone: zone name
36502	Add computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 computer: hostname zone: zone name
36504	Delete computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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: computer: hostname zone: zone name
36506	Modify computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 pam: pam name zone: zone name
36602	Add PAM right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 pam: pam name zone: zone name
36604	Delete PAM right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: 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 pam: pam name zone: zone name
36606	Modify PAM right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 desktop: desktop right name zone: zone name
37204	Delete desktop right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: 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 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: 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 network: network right name zone: zone name
37302	Add network right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 network: network right name zone: zone name
37306	Modify network right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 application: application right name zone: zone name
37404	Delete application right failed	PID: process id user: username@domain RunAS: username@domain type: user type status: 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 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: 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 dzcmd: dzcmd zone: zone name
36702	Add command right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 dzcmd: dzcmd zone: zone name
36704	Delete command right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 dzcmd: dzcmd zone: zone name
36706	Modify command right failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 role: role name zone: zone name
36802	Add role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 role: role name zone: zone name
36804	Delete role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 role: role name zone: zone name
36806	Modify role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 right: right name role: role name
36808	Add right to role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 zone: zone name role: role name trustee: username@domain
36902	Role assignment failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: 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 zone: zone name role: role name trustee: username@domain
36906	Modify role assignment failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: failed computer: computer hostname zone: zone name role: role name trustee: username@domain reason: error message

36909	Role assignment deleted from a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: 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: 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 computer: computer hostname zone: zone canonical role: role name trustee: username@domain
36912	Modify role assignment for a computer failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: failed computerRole: computer role name zone: zone name role: role name trustee: username@domain reason: error message
36915	Role assignment deleted from a computer role	PID: process id user: username@domain RunAs: username@domain type: user type status: 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: 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 computerRole: computer role name zone: zone canonical role: role name trustee: username@domain
36918	Modify role assignment in a computer role failed	PID: process id user: username@domain RunAs: username@domain type: user type status: 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 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: failed computerRole: computer role name zone: zone name reason: error message
37003	Computer role deleted	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: failed computerRole: computer role name zone: zone name reason: error
37005	Computer role modified	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: failed computerRole: computer role zone: zone name reason: error message
37101	User added to a group	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 account: username
37104	Reset password failed	PID: process id user: username@domain RunAs: username@domain type: user type status: failed account: username reason: error message
37501	user added to a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 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: failed ZoneUser: unixname zone: zone name reason: error message
37505	Local user profile modified in a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 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: failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message
37513	Local user deleted from computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 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: failed ZoneUser: unixname computer: computer hostname zone: zone name reason: error message
37521	Local group added to a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 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: failed group: group name zone: zone name reason: error message
37525	Local group profile modified in a zone	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 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: failed group: group name computer: computer hostname zone: zone name reason: error message
37533	Local group deleted from a computer	PID: process id user: username@domain RunAs: username@domain type: user type status: succeeded 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: 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 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: failed group: group name computer: computer hostname zone: zone name reason: error message
37601	Local Windows user added to a zone added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name zone: zone name
37602	Add local Windows user to a zone failed added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name zone: zone name reason: error message

37603	Local Windows user deleted from a zone added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name zone: zone name
37604	Delete local Windows user from a zone failed added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name zone: zone name reason: error message
37605	Local Windows user modified in a zone added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name zone: zone name
37606	Modify local Windows user in a zone failed added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name zone: zone name reason: error message
37611	Local Windows user added to a computer added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name computer: computer hostname zone: zone name
37612	Add local Windows user to a computer failed added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name computer: computer hostname zone: zone name reason: error message
37613	Local Windows user deleted from computer added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name computer: computer hostname zone: zone name
37614	Delete local Windows user from a computer failed added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name computer: computer hostname zone: zone name reason: error message
37615	Local Windows user modified on a computer added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name computer: computer hostname zone: zone name

37616	Modify local Windows user on a computer failed added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed ZoneUser: local Windows user name computer: computer hostname zone: zone name reason: error message
37621	Local Windows group added to a zone added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
37622	Add local Windows group to a zone failed added in Release 2020	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
37623	Local Windows group deleted from a zone added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
37624	Local Windows group modified in a zone added in Release 2020	PID: process ID user: username@domain RunAs: username@domain type: user type status: succeeded or failed group: group name zone: zone name
37626	Modify local Windows group in a zone failed added in Release 2020	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
37631	Local Windows group added to a computer added in Release 2020	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
37632	Add local Windows group to a computer failed added in Release 2020	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
37633	Local Windows group deleted from a computer added in Release 2020	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

37634	Delete local Windows group from a computer failed added in Release 2020	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
37635	Local Windows group modified on a computer added in Release 2020	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
37636	Modify local Windows group for a computer failed added in Release	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

dzdo

For Linux and UNIX computers, 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 Delinea Audit Event ID 30004. This log sample documents that the dzdo service has been granted authorization.The change was made by user=dwirth (type:ad,dwirth@acme.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@acme.vms)
pid=32224 utc=1460010012602 Centrify EventID=30004
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

dzdo Audit Events

Event Id	Description	Parameters
30000-Deprecated	dzdo granted This event has been deprecated. Use Delinea Event Id 30004 introduced in release 2017.3 instead.	command: command runas: username@domain role: role name env: environment variables

30001-Deprecated	dzdo denied This event has been deprecated. Use Delinea Event Id 30005 introduced in release 2017.3 instead. If the command is valid and requires authentication, Delinea Event Id 30005 is generated in release 2017.3 (and later versions) to show whether MFA is required or not.	command: command runas: username@domain reason: error message
30002	Trouble ticket entered	ticket: ticket
30004	dzdo granted added in release 2017.3	command: command runas: username@domain role: role name env: environment variables MfaRequired: whether user was required to do MFA EntityName: Entity Name
30005	dzdo denied added in release 2017.3	command: command runas: username@domain reason: error message MfaRequired: whether user was required to do MFA EntityName: Entity Name
30100	dzdo command execution starts added in release 18.11	command: command runas: username@domain role: role name env: environment variables MfaRequired: whether user was required to do MFA EntityName: Entity Name
30101	dzdo command execution ends added in release 18.11	command: command exitcode: exit code

dzsh

For Linux and UNIX computers, 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 Delinea 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@acme.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

dzsh Audit Events

Event Id	Description	Parameters
33000-Deprecated	dzsh command execution granted This event has been deprecated. Use Delinea Event Id 33002 instead, which was introduced in release 2017.3.	command: command runas: username@domain role: role name env: environment variables
33001-Deprecated	dzsh command execution denied This event has been deprecated. Use Delinea Event Id 33003 instead, which was introduced in release 2017.3.	command: command reason: error message
33002	dzsh command execution granted added in release 2017.3	command: command runas: username@domain role: role name env: environment variables MfaRequired: whether user was required to do MFA EntityName: Entity Name
33003	dzsh command execution denied added in release 2017.3	command: command reason: error message MfaRequired: whether user was required to do MFA EntityName: Entity Name
34000	dzsh role change granted	fromRole: fromRole toRole: toRole
34001	dzsh role change denied	

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 Delinea 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

dzinfo Audit Events

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

Kerberos

Audit events in the Kerberos category are focused on the success or failure of kerberos credential access. Audit events are recorded when programs access the KCM (Kerberos Cache Manager) credential cache.

Kerberos Audit Event Log Sample

```
Sep 29 11:27:22 AbelRedhat5 adclient[8002]: INFO
AUDIT_TRAIL|Centrify Suite|Kerberos|1.0|200|Initializing
KCM credential cache succeeded|5|user=root pid=8584
utc=1538191642025 CentrifyEventID=63200 DASessID=N/A
DAInst=N/A status=SUCCESS service=kcm process=adclient
pid=8002 ccache=1001 principal=user1@ABEL.TEST
```

Kerberos Audit Events

Kerberos Audit Events

Event ID	Description	Parameters
63100	Generating new KCM credential cache name succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name
63101	Generating new KCM credential cache name failed	process: process name pid: process id reason: error message
63200	Initializing KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name principal: principal name
63201	Initializing KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name principal: principal name reason: error message

63300	Destroying KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name
63301	Destroying KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
63400	Updating KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name principal: user principal services: service principal
63401	Updating KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
63500	Retrieving credential in the given KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: ccache name
63501	Retrieving credential in the given KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
63600	Reading principal in the given KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name principal: principal name
63601	Reading principal in the given KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
63700	Iterating credentials in the given KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name
63701	Iterating credentials in the given KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
63800	Reading credentials in the given KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name
63801	Reading credentials in the given KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message

63900	Removing credentials from KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name principal: user principal services: service principal
63901	Removing credentials from KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
64000	Iterating KCM credential caches succeeded added in release 18.11	
64100	Reading KCM credential caches succeeded	process: process name pid: process id
64101	Reading KCM credential caches failed added in release 18.11	process: process name pid: process id reason: error message
64200	Changing the ownership for the given credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name uid: uid gid: gid
64201	Changing the ownership for the given credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name reason: error message
64300	Reading status for the given KCM credential cache succeeded added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name
64301	Reading status for the given KCM credential cache failed added in release 18.11	process: process name pid: process id ccache: Kerberos credential cache name 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 Delinea 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 Delinea 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 27 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

License Management Audit Events

Event ID	Description	Parameters
60100	authentication service license key added	PID: process id user: username@domain RunAs: username@domain type: user type key: license key container: license container
60101	Add authentication service 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	authentication service license key removed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key container: license container
60103	Remove authentication service 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	authentication service license container added	PID: process id user: username@domain RunAs: username@domain type: user type container: license container
60105	Add authentication service license container failed	PID: process id user: username@domain RunAs: username@domain type: user type container: license container reason: Error message
60106	authentication service license container removed	PID: process id user: username@domain RunAs: username@domain type: user type container: license container
60107	Remove authentication service license container failed	PID: process id user: username@domain RunAs: username@domain type: user type container: license container reason: Error message
60200	Add audit and monitoring service license key failed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key installation: installation reason: Error

60202	audit and monitoring service license key removed	PID: process id user: username@domain RunAs: username@domain type: user type key: license key installation: installation
60203	Remove audit and monitoring service 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

Delinea 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 Delinea 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

Event Source Category: Local Account Management

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
53000	Managing local accounts succeeded	parameters: parameters
53001	Managing local accounts failed	parameters: parameters reason: error message
53100	Added enabled local user added in Release 2020	localuser: user name
53101	Added disabled local user added in Release 2020	localuser: user name
53102	Failed to add local user added in Release 2020	localuser: user name reason: error message
53103	Removed local user added in Release 2020	localuser: user name
53104	Failed to remove local user added in Release 2020	localuser: name reason: error message
53105	Enabled local user added in Release 2020	localuser: user name
53106	Failed to enable local user added in Release 2020	localuser: user name reason: error message
53107	Disabled local user added in Release 2020	localuser: user name
53108	Failed to disable local user added in Release 2020	localuser: user name reason: error message
53109	Modified local user added in Release 2020	localuser: user name
53110	Failed to modify local user added in Release 2020	localuser: user name reason: error message
53111	Added local group added in Release 2020	localgroup: group name
53112	Failed to add local group added in Release 2020	localgroup: group name reason: error message
53113	Removed local group added in Release 2020	localgroup: group name
53114	Failed to remove local group added in Release 2020	localgroup: group name reason: error message
53115	Modified local group added in Release 2020	localgroup: group name

53116	Failed to modify local group added in Release 2020	localgroup: group name reason: error message
53117	Managed local users and groups added in Release 2020	
53118	Failed to manage local users and groups added in Release 2020	reason: Reason for failure
53119	Invoked notification command added in Release 2020	command: notification command
53120	Failed to invoke notification command added in Release 2020	reason: Reason for failure

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.

Multi-Factor Authentication Audit Event Log Sample

The following is a sample of an audit event log for Delinea 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
CentryifyEventID=54100 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67
status=SUCCEED service=sshd tty=ssh client=::1
challenge=EMAIL
```

Multi-Factor Audit Events

MFA Audit Events

Event Id	Description	Parameters
54100-Deprecated	MFA challenge succeeded This event has been deprecated. Use Delinea Event Id 54102 introduced in release 2017.3 instead.	service: service tty: tty client: client challenge: challenge

54101-Deprecated	MFA challenge failed This event has been deprecated. Use Delinea Event Id 54103 introduced in release 2017.3 instead.	service: service tty: tty client: client challenge: challenge reason: error message
54102	MFA challenge succeeded added in release 2017.3	service: service tty: tty authmethod: Reserved. factorcount: Number of MFA challenges factors: MFA challenges used. mfaresult: MFA challenge status. sourcehost: Remote host username: Username entityname: local system name devicetype: host operating system type initiatortype: MFA event type entitytype: event type description rolename: DirectAuthorize role used command: command used
54103	MFA challenge failed added in release 2017.3	service: service tty: tty authmethod: Reserved. factorcount: Number of MFA challenges factors: MFA challenges used. mfaresult: MFA challenge status. sourcehost: Remote host username: Username entityname: local system name devicetype: host operating system type initiatortype: MFA event type entitytype: event type description rolename: DirectAuthorize role used command: command used 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
54203	MFA is skipped	service: service reason: message
54204	MFA challenge succeeded added in release 2017.3 This event has been deprecated. Use Delinea Event ID 54206 instead, which was introduced in release 2018.	service: service authmethod: authmethod factorcount: factorcount factors: factors mfaresult: mfaresult sourcehost: sourcehost username: username entityname: entityname entitytype: entitytype devicetype: devicetype rolename: rolename command: command

54205	MFA challenge failed added in release 2017.3 This event has been deprecated. Use Delinea Event ID 54207 instead, which was introduced in release 2018.	service: service reason: error message authmethod: authmethod factorcount: factorcount factors: factors mfaresult: mfaresult sourcehost: sourcehost username: username entityname: entityname entitytype: entitytype devicetype: devicetype rolename: rolename command: command
54206	MFA challenge succeeded Added in release 2018	service: service authmethod: authmethod factorcount: factorcount factors: factors mfaresult: mfaresult sourcehost: sourcehost username: username entityname: entityname entitytype: entitytype initiatortype: initiatortype devicetype: devicetype rolename: rolename command: command
54207	MFA challenge failed Added in release 2018	service: service reason: error message authmethod: authmethod factorcount: factorcount factors: factors mfaresult: mfaresult sourcehost: sourcehost username: username entityname: entityname entitytype: entitytype initiatortype: initiatortype devicetype: devicetype rolename: rolename command: command
54208	Setup MFA offline profile succeeded added in release 18.11	Username: The name of user configurationType: The MFA offline confguration type deviceType: The MFA offline device type
54209	Setup MFA offline profile failed added in release 18.11	Reason: The reason why it is failed Username: The name of user configurationType: The MFA offline confguration type deviceType: The MFA offline device type
54210	MFA challenge succeeded added in release 19.6	service: service authentication: authentication challenge: challenge
54211	MFA challenge failed added in release 19.6	

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 Delinea Audit Event ID 24100. This log sample documents PAM authentication being granted. The change was made by user=dwirth(type:ad,dwirth@acme.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@acme.vms) pid=7458
utc=1459784054942 CentrifyEventID=24100
DAInst=AuditingInstallation DASessID=c72252aa-e616
-44ff-a5f6-d3f53f09bb67 status=GRANTED
service=sshd tty=ssh client=dc.acme.vms
```

PAM Audit Events

PAM Audit Events

Event Id	Description	Parameters
24100-Deprecated	PAM authentication granted This event has been deprecated. Use Delinea Event Id 24102 introduced in release 2017.3 instead.	service: service tty: tty client: client
24101-Deprecated	PAM authentication denied This event has been deprecated. Use Delinea Event Id 24103 introduced in release 2017.3 instead.	service: service tty: tty client: client reason: error message
24102	PAM authentication granted added in release 2017.3	service: service tty: tty client: client MfaRequired: whether user was required to do MFA EntityName: Entity Name
24103	PAM authentication denied added in release 2017.3	service: service tty: tty client: client reason: error message MfaRequired: whether user was required to do MFA EntityName: Entity Name
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
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	
24700	The user logins to the system in rescue mode added in release 18.11	service: service tty: tty client: client	
24800	The dzo user authenticates to the system in rescue mode, added in Release 2023.1	service: service tty: tty client: client	

Delinea Privilege Elevation Service – Windows

Delinea Privilege Elevation Service for Windows provides role-based access control for Windows desktops and applications, and to remote Windows servers. Delinea Privilege Elevation Service 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.

Delinea Privilege Elevation Service Windows Audit Event Log Sample

The following is a sample of an audit event log for Delinea Audit Event ID 6029. This log sample documents a user with local and network role privileges launching a .msc file.

```
Log Name: Application
Source: Centrify AuditTrail V2
Date: 9/19/2019 2:05:17 PM
Event ID: 6029
Task Category: None
Level: Information
Keywords: Classic
User: bob@acme.vms
Computer: member.acme.vms
Description:
Product: Centrify Suite
Category: DirectAuthorize - Windows
Event name: Run with privilege success
Message: User launched 'C:Program FilesCentrifyAccess
ManagerCentrifyDC.msc' on
desktop 'Default' using local role 'ROLE_SYSTEM_Archt/Global'
and network roles 'ROLE_SYSTEM_Archt/Global'.
Sep 19 14:05:17 member.acme.vms dzagent[1348]:
INFO AUDIT_TRAIL|Centrify Suite|DirectAuthorize - Windows|1.0|29|Run with
privilege
success|5|bob@acme.vms
userSid=S-1-5-21-569763308-1211465464-1224152175-3219
sessionId=3 CentrifyEventID=6029
DAInst=AuditingInstallation DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67
role=ROLE_SYSTEM_Archt/Global
```

```
effectivesid=S-1-5-21-569763308-1211465464-1224152175-3219
effectivegroupsids=S-1-5-32-544
logonguid=ad7b6538-e2a4-4304-ab6e-86c5b0dabfaf
desktopguid=1e09a3dd-276f-4629-bb27-e215dfe0a0c8
command=C:Program FilesCentrifyAccessManagerCentrifyDC.msc
passwordprompted=False desktopname=Default
networkroles=ROLE_SYSTEM_Archt/Global
entityname=acme.vms mfarequired=False
```

Delinea Privilege Elevation Service - Windows Audit Events

Privilege elevation service - Windows Audit Events

Event ID	Description	Parameters
6001-Deprecated	Console login success This event has been deprecated. Use Delinea Event Id 6031 introduced in release 2017.2 instead.	Role: role DesktopGuid: desktop GUID
6002-Deprecated	Console login failure This event has been deprecated. Use Delinea Event Id 6032 introduced in release 2017.2 instead.	
6003-Deprecated	Remote login success This event has been deprecated. Use Delinea Event Id 6033 introduced in release 2017.2 instead.	Role: role DesktopGuid: desktop GUID

6004-Deprecated	Remote login failure This event has been deprecated. Use Delinea Event Id 6034 introduced in release 2017.2 instead.	
6005-Deprecated	Run with privilege success This event has been deprecated. Use Delinea Event Id 6029 introduced in release 2017.2 instead.	Role: local role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID DesktopGuid: desktop GUID Command: command
6006-Deprecated	Run with privilege failure This event has been deprecated. Use Delinea Event Id 6030 introduced in release 2017.2 instead.	Role: local role DesktopGuid: desktop GUID Command: command
6007-Deprecated	Create desktop success This event has been deprecated. Use Delinea Event Id 6035 introduced in release 2017.2 instead.	Role: local role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID DesktopGuid: desktop GUID
6008-Deprecated	Create desktop failure This event has been deprecated. Use Delinea Event Id 6036 introduced in release 2017.2 instead.	Role: local role

6009-Deprecated	Network access success This event has been deprecated. Use Delinea Event Id 6039 introduced in release 2017.2 instead.	Role: role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID
6010-Deprecated	Console logon failure This event has been deprecated. Use Delinea Event Id 6032 introduced in release 2017.3 instead.	Reason: reason
6011-Deprecated	Remote login failure This event has been deprecated. Use Delinea Event Id 6034 introduced in release 2017.2 instead.	Reason: reason
6012-Deprecated	Run with privilege success This event has been deprecated. Use Delinea Event Id 6029 introduced in release 2017.2 instead.	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-Deprecated	Run with privilege failure This event has been deprecated. Use Delinea Event Id 6030 introduced in release 2017.2 instead.	Role: local role DesktopGuid: desktop GUID Command: command Reason: reason DesktopName: desktop name NetworkRoles: network roles

6014-Deprecated	Create desktop success This event has been deprecated. Use Delinea Event Id 6035 introduced in release 2017.2 instead.	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
6018-Deprecated	Run with privilege failure This event has been deprecated. Use Delinea Event Id 6030 introduced in release 2017.2 instead.	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
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
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
6029	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 EntityName: Entity Name MFARequired: whether user was required to do MFA
6030	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 EntityName: Entity Name MFARequired: whether user was required to do MFA

6031	Console login success	Role: role DesktopGuid: desktop GUID EntityName: Entity Name MFARequired: whether user was required to do MFA
6032	Console logon failure	Reason: reason EntityName: Entity Name MFARequired: whether user was required to do MFA
6033	Remote login success	Role: role DesktopGuid: desktop GUID EntityName: Entity Name MFARequired: whether user was required to do MFA
6034	Remote login failure	Reason: reason EntityName: Entity Name MFARequired: whether user was required to do MFA
6035	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 EntityName: Entity Name MFARequired: whether user was required to do MFA
6036	Create desktop failure	Role: local role Reason: reason NetworkRoles: network roles PasswordPrompted: whether user was required to re-enter their password EntityName: Entity Name MFARequired: whether user was required to do MFA
6037	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 EntityName: Entity Name MFARequired: whether user was required to do MFA
6038	Switch desktop failure	DesktopName: desktop name Reason: reason PasswordPrompted: whether user was required to re-enter their password EntityName: Entity Name MFARequired: whether user was required to do MFA
6039	Network access success	Role: role EffectiveSid: effective user SID EffectiveGroupSids: effective group SID's LogonGuid: logon GUID EntityName: Entity Name MFARequired: whether user was required to do MFA
6040	Self-service password reset success added in release 2017.3	Username: username
6041	Self-service password reset failure added in release 2017.3	Username: username Reason: failure reason

6042	Self-service account unlock success added in release 2017.3	Username: username
6043	Self-service account unlock failure added in release 2017.3	Username: username Reason: failure reason
6044	Enable Delinea Identity Services Platform succeeded added in release 2017.3	PlatformInstance: Platform Instance
6045	Disable Delinea Identity Services Platform succeeded added in release 2017.3	PlatformInstance: Platform Instance
6046	Enable Delinea Identity Services Platform failed added in release 2017.3	PlatformInstance: Platform Instance Reason: Reason for failure
6047	Disable Delinea Identity Services Platform failed added in release 2017.3	PlatformInstance: Platform Instance Reason: Reason for failure
6048	PowerShell remote connection success added in release 18.8	User: user Role: role
6049	PowerShell remote connection failure added in release 18.8	User: user Reason: reason

6050	Trouble ticket entered added in release 18.11	ticket: ticket reason: reason for privilege elevation comment: additional comment
6051	Run with privilege as an alternate user success added in release 18.11	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 EntityName: Entity Name MfaRequired: whether user was required to do MFA AlternateUsername: An alternate username AlternateUserSid: An alternate user's SID
6052	Run with privilege as an alternate user failure added in release 18.11	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 EntityName: Entity Name MfaRequired: whether user was required to do MFA AlternateUsername: An alternate username AlternateUserSid: An alternate user's SID
6053	Windows authentication is skipped added in release 18.11	service: service reason: Reason message for skip
6054	Run with alternate account success added in Release 2020	Command: command AlternateUsername: alternate username tenant: tenant URL PasswordPrompted: whether user was required to re-enter their password
6055	Run with alternate account failure added in Release 2020	Command: command AlternateUsername: alternate username tenant: tenant URL Reason: reason PasswordPrompted: whether user was required to re-enter their password
6300	Add roles and features success added in release 2018	PID: process id user: username@domain status: succeeded feature: feature name computer: computer name
6301	Add roles and features failure added in release 2018	PID: process id user: username@domain status: failed feature: feature name computer: computer name reason: reason for failure

6302	Remove roles and features success added in release 2018	PID: process id user: username@domain status: succeeded feature: feature name computer: computer name
6303	Remove roles and features failure added in release 2018	PID: process id user: username@domain status: failed feature: feature name computer: computer name reason: reason for failure
6350	Uninstall program success added in release 2018	PID: process id user: username@domain status: program: program name computer: computer name
6351	Uninstall program failure added in release 2018	PID: process id user: username@domain status: failed program: program name computer: computer name reason: reason for failure
6352	Change program success added in release 2018	PID: process id user: username@domain status: program: program name computer: computer name
6353	Change program failure added in release 2018	PID: process id user: username@domain status: failed program: program name computer: computer name reason: reason for failure
6354	Repair program success added in release 2018	PID: process id user: username@domain status: succeeded program: program name computer: computer name
6355	Repair program failure added in release 2018	PID: process id user: username@domain status: program: program name computer: computer name reason: reason for failure
6400	Enable network adapter success added in release 2018	PID: process id user: username@domain status: succeeded adapter: adapter name computer: computer name
6401	Enable network adapter failure added in release 2018	PID: process id user: username@domain status: failed adapter: adapter name computer: computer name reason: reason for failure

6402	Disable network adapter success added in release 2018	PID: process id user: username@domain status: succeeded adapter: adapter name computer: computer name
6403	Disable network adapter failure added in release 2018	PID: process id user: username@domain status: failed adapter: adapter name computer: computer name reason: reason for failure
6404	Rename network adapter success added in release 2018	PID: process id user: username@domain status: succeeded adapter: adapter name computer: computer name
6405	Rename network adapter failure added in release 2018	PID: process id user: username@status: failed adapter: adapter name computer: computer name reason: reason for failure
6406	Update IPv4 settings success added in release 2018	PID: process id user: username@domain status: succeeded adapter: adapter name computer: computer name
6407	Update IPv4 settings failure added in release 2018	PID: process id user: username@domain status: failed adapter: adapter name computer: computer name reason: reason for failure
6408	Update IPv6 settings success added in release 2018	PID: process id user: username@domain status: succeeded adapter: adapter name computer: computer name
6409	Update IPv6 settings failure added in release 2018	PID: process id user: username@domain status: failed adapter: adapter name computer: computer name reason: reason for failure
6500	Auto-enroll as corporate owned device success added in release 2018	computer: computer name tenant: tenant URL

6501	Auto-enroll as corporate owned device failure added in release 2018	computer: computer name tenant: tenant URL reason: reason for failure
6502	Unenroll device success added in release 2018	user: user name computer: computer name
6503	Unenroll device failure added in release 2018	user: user name computer: computer name reason: reason for failure
6504	Enroll as corporate owned device success added in release 2018	user: user name computer: computer name tenant: tenant URL
6505	Enroll as corporate owned device failure added in release 2018	user: user name computer: computer name tenant: tenant URL reason: reason for failure
6506	Enroll device success added in release 2018	user: user name computer: computer name tenant: tenant URL
6507	Enroll device failure added in release 2018	user: user name computer: computer name tenant: tenant URL reason: reason for failure
6508	Auto-unenroll success added in release 18.8	computer: computer name
6509	Auto-unenroll failure added in release 18.8	computer: computer name reason: reason for failure
6510	PowerShell remote command execution added in release 2020.1	userSid: User SID userName: User name authMechanism: Authentication mechanism url: HTTP URL of inbound request command: PowerShell remote command isScript: Command is a remote script

Delinea sshd

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

Delinea sshd Audit Event Log Sample

The following is a sample of an audit event log for Delinea 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@acme.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@acme.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
```

Delinea sshd Audit Events

Delinea sshd Audit Events

Note: Starting in the Server Suite 2023.1 release, the scp command's default protocol is now the sftp protocol.

When scp uses the sftp protocol (the default configuration):

- Audit events 27000 and 27001 list the service as `dzssh-sftp`.
- Success or failure events are listed as 27300 (success) or 27301 (failure) instead of 27200 (success) and 27201 (failure).

When scp uses the scp protocol (specified by the option `-o`):

- Audit events 27000 and 27001 list the service as `dzssh-scp`.
- Success or failure events are listed as 27200 (success) and 27201 (failure).

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-Deprecated	SSHD granted This event has been deprecated. Use Delinea Event Id 27104 introduced in release 2017.3 instead.	service: service tty: tty authMechanism: authentication type client: client sshRights: ssh rights command: command

27101-Deprecated	SSHD denied This event has been deprecated. Use Delinea Event Id 27105 introduced in release 2017.3 instead.	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
27104	SSHD granted added in release 2017.3	service: service tty: tty authMechanism: authentication type client: client sshRights: ssh rights command: command MfaRequired: whether user was required to do MFA EntityName: Entity Name
27105	SSHD denied added in release 2017.3	service: service tty: tty authMechanism: authentication type client: client reason: error message MfaRequired: whether user was required to do MFA EntityName: Entity Name
27200	SCP succeeded added in release 18.8	dataFlowType: send a file/directory to remote machine or receive a file/directory from remote machine fileType: file or directory path name: the full path name of file or directory
27201	SCP failed added in release 18.8	dataFlowType: send a file/directory to remote machine or receive a file/directory from remote machine fileType: file or directory pathname: the full path name of file or directory reason: Error message
27300	SFTP command execution succeeded added in release 18.8	operation: SFTP command arguments: the arguments of SFTP command
27301	SFTP command execution failed added in release 18.8	

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$@acme.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$@acme.vms pid=1395
utc=1459783929161 CentrifyEventID=23700 DAInst=AuditingInstallation
DASessID=c72252aa-e616-44ff-a5f6-d3f53f09bb67
status=GRANTED server=ldap/dc.acme.vms@acme.vms
```

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

Trusted Path Audit Events

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