

# Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service

## *Auditing Administrator's Guide*

January 2020 (release 19.9)

Centrify Corporation



## Legal Notice

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

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

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

© 2004-2020 Centrifry Corporation. All rights reserved. Portions of Centrifry software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

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

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

Centrifry 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; 9,442,962 and 9,378,391.

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

# Contents

<b>About this guide .....</b>	<b>8</b>
Intended audience .....	8
Using this guide .....	8
Documentation conventions .....	9
Finding more information about Centrify products .....	10
Product names .....	10
Contacting Centrify .....	12
Getting additional support .....	13
 <b>Overview of the auditing infrastructure .....</b>	 <b>14</b>
Deciding whether to audit user activity .....	14
Capturing detailed and summary information for user sessions .....	15
Reviewing recorded activity .....	16
Auditing requires a scalable architecture .....	17
How audited sessions are collected and stored .....	18
Auditing architecture and data flow .....	18
Deploying auditing components in an audit installation .....	20
Agent components on audited UNIX computers .....	22
Agent components on audited Windows computers .....	23
 <b>Planning an audit installation .....</b>	 <b>24</b>
Decide on the scope of the installation .....	24
Decide where to install the management database .....	25
Decide where to install collectors and audit stores .....	26
Decide where to install agents .....	31
Decide where to install consoles .....	31
Make sure you have a supported edition of SQL Server .....	32
Check SQL Server logins for auditing .....	32

Determining storage requirements for auditing .....	34
What's involved in the deployment process .....	36

## Installing Centrify Audit & Monitoring Service ..... 40

Installation preview .....	41
Installing and configuring Microsoft SQL Server for auditing .....	43
Installing the Audit Manager and Audit Analyzer consoles .....	48
Creating a setup user account for installation .....	50
Creating a new installation .....	50
Installing the audit collectors .....	61
Installing the Centrify Agent for Windows .....	64
Installing the Audit Management Server .....	82
Enabling or disabling auditing on Windows computers .....	83
Installing an Centrify Agent for *NIX .....	84
Installing additional Audit Manager or Audit Analyzer consoles .....	86
Checklist for auditing systems outside of Active Directory .....	87
Auditing systems that are inside a DMZ .....	89

## Managing an installation ..... 92

Securing an installation .....	93
Configuring selective auditing .....	98
Configuring agents to prefer collectors .....	100
Audit license enforcement .....	101
Enabling audit notification .....	102
Enabling or disabling video capture auditing .....	103
Preventing users from reviewing or deleting sessions .....	104
Adding an installation .....	105
Publishing installation information .....	106
Removing or deleting an installation .....	108

Managing audit store databases .....	108
Managing audit stores .....	119
Managing the audit management database .....	122
Maintaining database indexes .....	125
Managing collectors .....	126
Managing audited computers and agents .....	128
Delegating administrative permissions .....	130
Managing audit roles .....	131

## Querying and reviewing audited activity .....135

Accessing audited sessions .....	136
Predefined queries for audit sessions .....	136
Predefined queries for audit events .....	138
Predefined queries for reports .....	138
Creating new session queries .....	143
Creating queries for audit events .....	149
Organizing queries in custom folders .....	151
Exporting and importing query definitions .....	152
Displaying session information .....	153
Adding session reviewers without designating auditing roles .....	153
Changing the review status for audited sessions .....	154
Playing back a session .....	156
Exporting sessions .....	160
Deleting sessions .....	162
Viewing sessions outside of Audit Analyzer .....	163

## Advanced monitoring .....166

Set up advanced monitoring .....	167
Using the advanced monitoring reports .....	169

## Troubleshooting and common questions .....171

Checking the status of the UNIX agent .....	171
Viewing and changing log file settings .....	174
Tracing database operations .....	179
Stopping auditing on a computer .....	182
Determining collector status and connectivity .....	183
Managing Microsoft SQL Server databases .....	187
Publishing installation information in Active Directory .....	189
Monitoring file system disk space usage .....	189

## Command line programs for managing audited sessions ..... 191

How to use command line programs .....	191
Displaying usage information and man pages .....	192
Using commands for administrative tasks .....	192

## Installing the UNIX agent on remote computers .....196

Installing the agent silently using a configuration file .....	196
Using other programs to install the UNIX agent .....	197

## Permissions required to perform administrative and auditing tasks .....199

Setting and synchronizing audit-related permissions .....	199
Installation permissions .....	200
Management database permissions .....	202
Audit store and audit store database permissions .....	204
Audit role permissions .....	205
Auditor permissions .....	205

Sizing recommendations for audit installations .....	207
Planning an audit and monitoring service deployment .....	208
Best practices for an audit installation .....	212
Creating an initial estimate of your database storage needs .....	216
Guidelines for determining hardware configuration .....	216
Identifying typical deployment issues .....	220
Settings to adjust for performance improvement .....	222
Conclusion .....	225
Glossary .....	226

# About this guide

The *Auditing Administrator's Guide* provides complete information for installing and configuring the auditing infrastructure, including guidelines for planning your deployment, managing audited activity, and how to use Audit Analyzer to find and replay captured user sessions. Centrify software helps you comply with regulatory requirements and improve accountability by collecting detailed information about user activity on Linux, UNIX, and Windows computers. The Centrify auditing features enable you to monitor user activity for immediate analysis or specific incidents, such as application failures or security breaches.

## Intended audience

This guide is intended for administrators responsible for installing and maintaining auditing-related software and the databases that store audit-related data, including the roles and permissions assigned to the users and groups who are responsible for monitoring and reviewing user activity on audited computers. In addition, some of the information in this guide is intended for security personnel and auditors who are responsible for identifying audit requirements, querying the audit store databases, examining user activity, and managing the status of sessions they have reviewed.

## Using this guide

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

- **Overview of the auditing infrastructure** provides an overview of what you can audit and how auditing works.
- **Planning an audit installation** explains how to prepare for the deployment of auditing components.





- **Installing Centrify Audit & Monitoring Service** explains how to install and configure auditing components in a production environment.
- **Managing an installation** explains how to secure, change, reconfigure, add, and remove audit and monitoring service components.
- **Querying and reviewing audited activity** explains how to use Audit Analyzer to find and review the audited sessions and audit trail events in which you are interested.
- **Advanced monitoring** explains how to use the advanced monitoring features to gather additional information about which users and what programs are accessing or modifying production systems.
- **Troubleshooting and common questions** describes how to view log files and diagnostics for components of the auditing infrastructure and how to identify and resolve common issues.
- **Command line programs for managing audited sessions** provides a summary of the command line programs and Windows utilities.
- **Installing the UNIX agent on remote computers** describes how to install the agent package using non-interactive scripts and native installers.
- **Permissions required to perform administrative and auditing tasks** discusses the permissions required to perform actions in the Audit Manager and Audit Analyzer consoles.

In addition, an index is provided for your reference.

## Documentation conventions

The following conventions are used in Centrify documentation:

- Fixed-width font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *italicized*, this font indicates variables. Square brackets ([ ]) indicate optional command-line arguments.
- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.
- *Italics* are used for book titles and to emphasize specific words or terms. In fixed-width font, italics indicate variable values.
- Standalone software packages include version and architecture information in the file name. Full file names are not documented in this



guide. For complete file names for the software packages you want to install, see the distribution media.

- For simplicity, UNIX is used to refer to all supported versions of the UNIX and Linux operating systems. Some parameters can also be used on Mac OS X computers.

## Finding more information about Centrify products

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

For access to documentation for all Centrify products and services, visit the [Centrify documentation portal](#) at [docs.centrixy.com](https://docs.centrixy.com). From the Centrify documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

For details about supported platforms, please consult the release notes.

For the most up to date list of known issues, please login to the Customer Support Portal at <http://www.centrixy.com/support> and refer to Knowledge Base articles for any known issues with the release.

## Product names

Over the years we've made some changes to some of our product offerings and features and some of these previous product names still exist in some areas. Our current product offerings include the following services:

Current Overall Product Name	Current Services Available
Centrify Zero Trust Privilege Services	Privileged Access Service
	Gateway Session Audit and Monitoring
	Authentication Service
	Privilege Elevation Service
	Audit and Monitoring Service
	Privilege Threat Analytics Service

Whether you're a long-time or new customer, here are some quick summaries of which features belong to which current product offerings:

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	Centrify Privileged Service (CPS)		Privileged Access Service
DirectControl (DC)			Authentication Service
DirectAuthorize (DZ or DZwin)			Privilege Elevation Service
DirectAudit (DA)			Audit and Monitoring Service
	Infrastructure Services		Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service, and Privilege Threat Analytics Service
DirectManage (DM)	Management Services	Consoles that are used by all 3 services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	
DirectSecure (DS)	Isolation and Encryption Service		Still supported but no longer being developed or updated
	User Analytics Service		Privilege Threat Analytics Service



Depending on when you purchased a Centrify product offering, you may have purchased one of the following product bundles:

Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
		Centrify Zero Trust Privilege Services Core Edition	Privileged Access Service and Gateway Session Audit and Monitoring	
Centrify Server Suite Standard Edition	Centrify Infrastructure Services Standard Edition	Centrify Zero Trust Privilege Services Standard Edition	Privileged Access Service, Authentication Service, and Privilege Elevation Service	
Centrify Server Suite Enterprise Edition	Centrify Infrastructure Services Enterprise Edition	Centrify Zero Trust Privilege Services Enterprise Edition	Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service (includes Gateway Session Audit and Monitoring)	
Centrify Server Suite Platinum Edition				Discontinued bundle that included DirectControl, DirectAuthorize, DirectManage, DirectAudit, and DirectSecure

## Contacting Centrify

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



## Getting additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the [Centrify Technical Support Portal](#). From the support portal, you can search knowledge base articles, open and view support cases, download software, and access other resources.

To connect with other Centrify users, ask questions, or share information, visit the [Centrify Community](#) website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.

# Overview of the auditing infrastructure

Auditing is a key feature of Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service. If you choose to enable auditing in your organization, you can capture detailed information about user activity on Linux, UNIX, and Windows computers and store that activity to improve regulatory compliance and accountability and mitigate security risks. This section provides an overview of the auditing infrastructure, including key components and terminology.

The following topics are covered:

Deciding whether to audit user activity .....	14
Capturing detailed and summary information for user sessions .....	15
Reviewing recorded activity .....	16
Auditing requires a scalable architecture .....	17
How audited sessions are collected and stored .....	18
Auditing architecture and data flow .....	18
Deploying auditing components in an audit installation .....	20
Agent components on audited UNIX computers .....	22
Agent components on audited Windows computers .....	23

## Deciding whether to audit user activity

Just as it is important to protect assets and resources from unauthorized access, it is equally important to track what users who have permission to access those resources are doing or have done in the past. For users who have



privileged access to computers and applications with sensitive information, auditing their actions helps ensure accountability and improve regulatory compliance.

There are many reasons for organizations to establish auditing policies and enable auditing of user activity. For example, you might want to audit activity for any of the following reasons:

- To prove certain computers or applications are secure in order to comply with government or industry regulatory requirements.
- To report on actions taken by users with elevated privileges.
- To prevent the use of shared passwords when more than one person needs administrative access to a computer or an application.
- To improve accountability when users with elevated permissions have access to privileged resources.
- To detect suspicious activity and mitigate the threat posed by malicious insiders or third parties who have access to sensitive systems.
- To pinpoint actions that may have caused failures and simplify troubleshooting procedures.
- To capture information, such as the steps that resolved an open case, that can be used to help your organization improve its helpdesk operations or security procedures.

## Capturing detailed and summary information for user sessions

After you deploy the auditing infrastructure, you can capture detailed information about user activity and the events that occurred on the computers you choose to audit. On those computers, an agent starts recording user activity when a user selects an audited role or starts a login shell locally, using a remote shell, or through a virtual network connection such as Citrix or VNC.

Each record of continuous user activity is called a **session**. A session ends when the user logs out, disconnects, or is inactive long enough to lock the desktop. If the user reconnects or unlocks the desktop, the agent resumes recording the user's activity as a new session. When users start a new session on an audited computer, they can be notified that their session is being audited but they



cannot turn off auditing except by logging off, so you have a complete record of what happened, includes an audit trail of the actions a user has taken.

You can choose whether to record only summaries of user activity or a full visual record of user activity. When auditing Windows computers, each session is a video capture of everything that takes place on the desktop, including the applications opened, text that was entered, and the results that were displayed. When auditing Linux and UNIX computers, the agent records shell activity, such as the commands a user runs or the changes made to key files and data. On Linux and UNIX computers, actions performed using a display manager, such as GNOME or KDE, are not recorded.

In addition to capturing detailed information about user activity, sessions provide a summary of actions taken so that you can scan the applications opened or commands executed for potentially interesting or damaging actions without playing back a complete session. After you select a session of interest in the Audit Analyzer, the console displays an indexed list of actions taken in the order in which they occurred. You can then select any entry in the list to start viewing the session beginning with that action. For example, if a user opened an application that stores credit card information, you can scan the list of actions for that event and begin reviewing what happened in the session from the time the user opened that particular application.

If users change their account permissions to take any action with elevated privileges, the change is recorded as an audit trail event. You can also search for these events to find sessions of interest.

## Reviewing recorded activity

The information recorded in each session is transferred to a Microsoft SQL Server database so that it is available for querying and playback. Because the information is collected as it happens, you can monitor computers for suspicious activity or troubleshoot problems immediately after they occur.

You can also search for and play back sessions to locate past events that occurred on specific computers or that affected particular users. For example, you might be interested in activity that occurred immediately before a security breach or want to investigate the cause of an application failure. Similarly, a security expert might want to see who had access to computers with sensitive data, such as payroll information or medical records, during a particular period of time, such as the last 72 hours.



## Auditing requires a scalable architecture

To ensure scalability for large organizations and provide fault tolerance, the auditing infrastructure has a multi-tier architecture that consists of the following layers:

- **Audited computers** are the computers on which you want to monitor activity. To be audited, the computer must have an agent installed, audit features enabled, and be joined to an Active Directory domain.
- **Collectors** are intermediate services that receive and compress the captured activity from the agents on audited computers as the activity occurs. You should establish at least two collectors to ensure that auditing is not interrupted. You can add collectors to your installation at any time and it is common to have multiple collectors to provide load balancing and redundancy.
- **Audit stores** define a scope for auditing and include the audit store databases that receive captured activity and audit trail records from the collectors and store it for querying and playback. Audit store databases also keep track of all the agents and collectors you deploy. For scalability and network efficiency, you can have multiple audit stores each with multiple databases.
- A **management database server** is a computer that hosts the Microsoft SQL Server instance with the audit management database. The management database stores information about the overall installation, such as the scope of each audit store, which audit store database is active and where there are attached databases, the audit roles you create, and the permissions you define. The management database enables centralized monitoring and reporting across all audit stores, collectors, and audited computers.
- The **Audit Manager** and **Audit Analyzer consoles** are the graphical user interfaces which administrators can use to configure and manage the deployment of audit components, such as agents and collectors, or to query and review captured user sessions.

To ensure that audit data transferred over the network is secure, communication between components is authenticated and encrypted.

In addition to these core components of the auditing infrastructure, there is a separate Windows service that collects audit trail events when there are audit store databases that are not accessible, for example, because of network issues or the database server is shut down. This audit management server runs



as a Windows service and spools the events on the management database, then sends them to the audit store database when the inaccessible database comes back online.

In addition to spooling audit trail events, the audit management server automatically calculates the approximate disk space used by audited sessions on the database server. The audit management server will calculate the session size for all completed audited sessions. The session size is not calculated for in-progress or disconnected sessions. You can view the session size for all completed sessions in the Audit Analyzer console's query results.

## How audited sessions are collected and stored

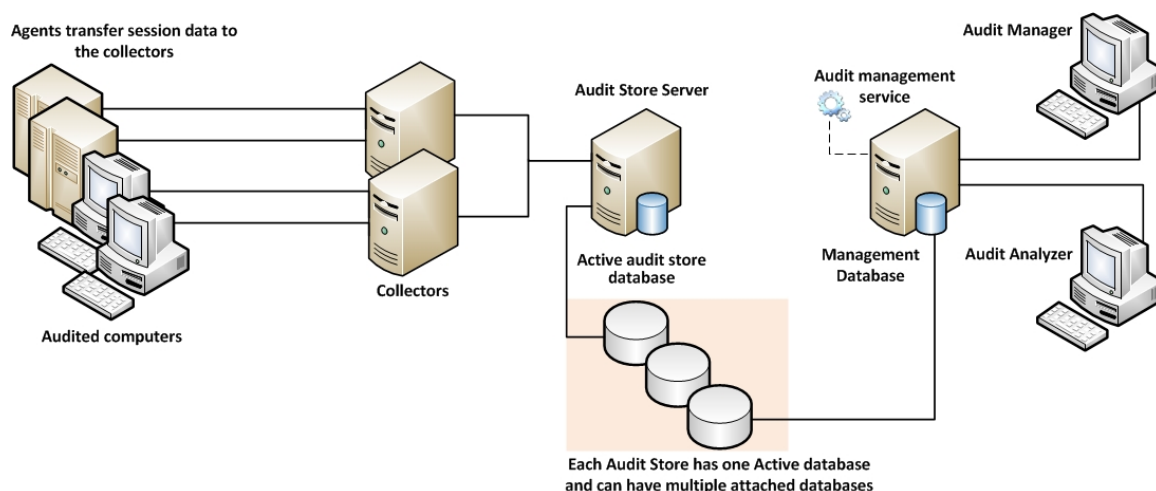
The agent on each audited computer captures user activity and forwards it to a collector on a Windows computer. If the agent cannot connect to a collector—for example, because all of the computers hosting the collector service for the agent are shut down for maintenance—the agent spools the session data locally and transfers it to a collector later.

The collector sends the data to an audit store server, where the audit data is stored in the Microsoft SQL Server database that you have designated as the **active audit store database**. As you accumulate data, you can add more SQL Server databases to the audit store to hold historical information or to change the database designated as the active audit store database.

After the audit data is transferred to the audit store database, you can use the Audit Analyzer console to request session data. The audit management database, which stores information about all of the components that make up the auditing infrastructure, retrieves the session data from the appropriate audit store database.

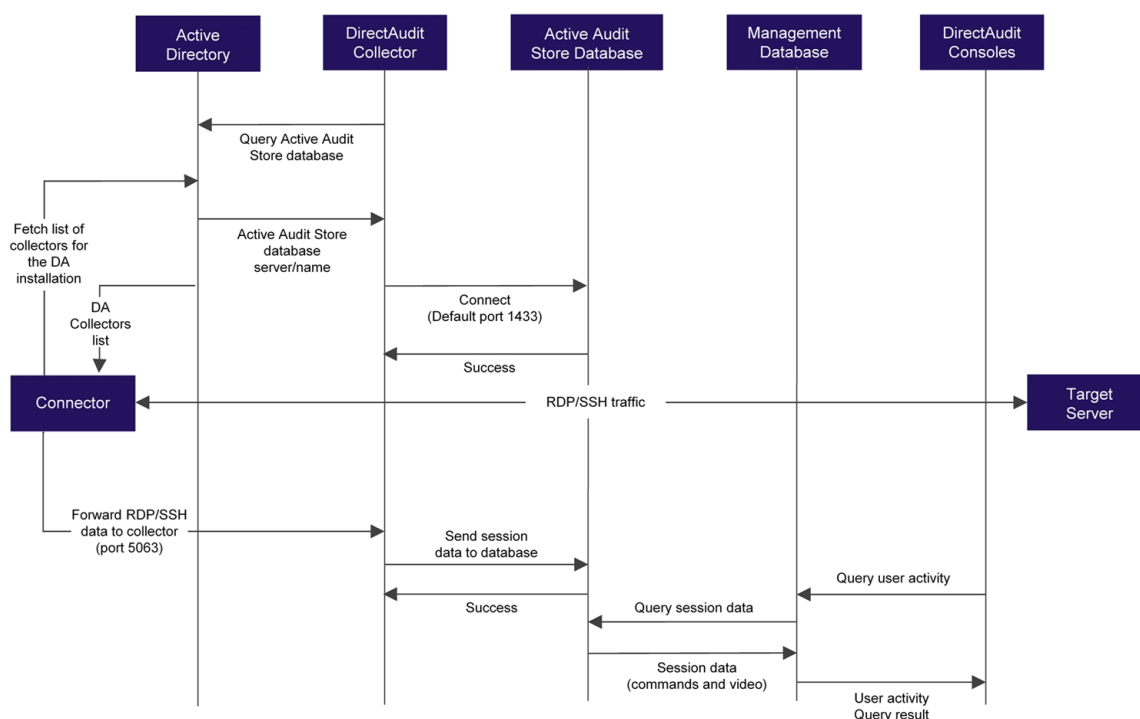
## Auditing architecture and data flow

The following figure illustrates the basic architecture and flow of data with a minimum number of auditing components installed.



In the illustration, each agent connects to one collector. In a production environment, you can configure agents to allow connections to additional collectors for redundancy and load balancing or to prevent connections between specific agents and collectors. You can also add audit stores and configure which connections are allowed or restricted. The size and complexity of the auditing infrastructure depends on how you want to optimize your network topology, how many computers you are auditing, how much audit data you want to collect and store, and how long you plan to retain audit records.

The following figure illustrates the data flow details. You can see which components communicate to other components and in what order. The diagram also includes some port details.



## Deploying auditing components in an audit installation

The multi-tiered architecture of the auditing infrastructure is referred to collectively as a **DirectAudit installation**. The DirectAudit installation represents a logical object similar to an Active Directory forest or site. It encompasses all of the auditing components you deploy—agents, collectors, audit stores, management database, and consoles—regardless of how they are distributed on your network. The installation also defines the scope of audit data available. All queries and reports are against the audit data contained within the installation boundary.

The most common deployment scenario is to have a single audit installation for an entire organization so that all audit data and management of the audit data is centralized. Within a single installation, you can have components wherever they are needed, as long as you have the appropriate network connections that allow them to communicate with each other. The audit data for the entire installation is available to users who have permission to query and view it using a console. For most organizations, having a single installation is a scalable solution that allows a “separation of duties” security model through the use of audit roles. If you establish a single installation, there will be one Master Auditor role for the entire organization, and that Master Auditor can control the audit data that other users and groups can see or respond to by defining roles that limit access rights and privileges.

However, if you have different lines of business with different audit policies—in different geographic locations, or with different administrative groups—you can configure them as separate audit installations. For example, if you have offices in North America and Hong Kong managed by two different IT teams—IT-US and IT-HK—you might want to create two DirectAudit installations to maintain your existing separation of duties for the IT-US and IT-HK teams.

## Planning where to install auditing components

Before you install Centrify Audit & Monitoring Service, you should develop a basic deployment plan for how you will distribute and manage the components that make up an installation. For example, you should decide how many collectors and audit stores to create and where to put them. You should also consider the network connections required and how many computers you plan to audit. For example, you can have multiple agents using the same set of



collectors, but you should keep the collectors within one hop of the agents they serve and within one hop of the audit stores to which they transfer data.

By planning where to install components initially, you can determine the number of collectors you should have for load balancing or redundancy. After the initial deployment, you can add collectors and audit stores whenever and wherever they are needed.

## Using multiple databases in an audit store

Each audit store uses Microsoft SQL Server to provide database services to the audit installation. When you install the first audit store, you configure the database instance you want to use and that database becomes the active database for storing incoming audit data. A single audit store, however, can have several databases attached to it. Attached databases store historical information and respond to queries from the management database. You can use the Audit Manager console to control the databases that are attached to the audit store and to designate which database is active. Only one database can be active in an audit store at any given time.

Although the audit store can use multiple databases, the presentation of session data is not affected. If a session spans two or more databases that are attached to the audit store, the Audit Analyzer console presents the data as a single, unbroken session. For example, if you change the active database during a session, some of the session data is stored in the attached database that is no longer active and some of it stored in the newly activated database, but the session data plays back as a single session to the auditor.

## Using multiple consoles in an installation

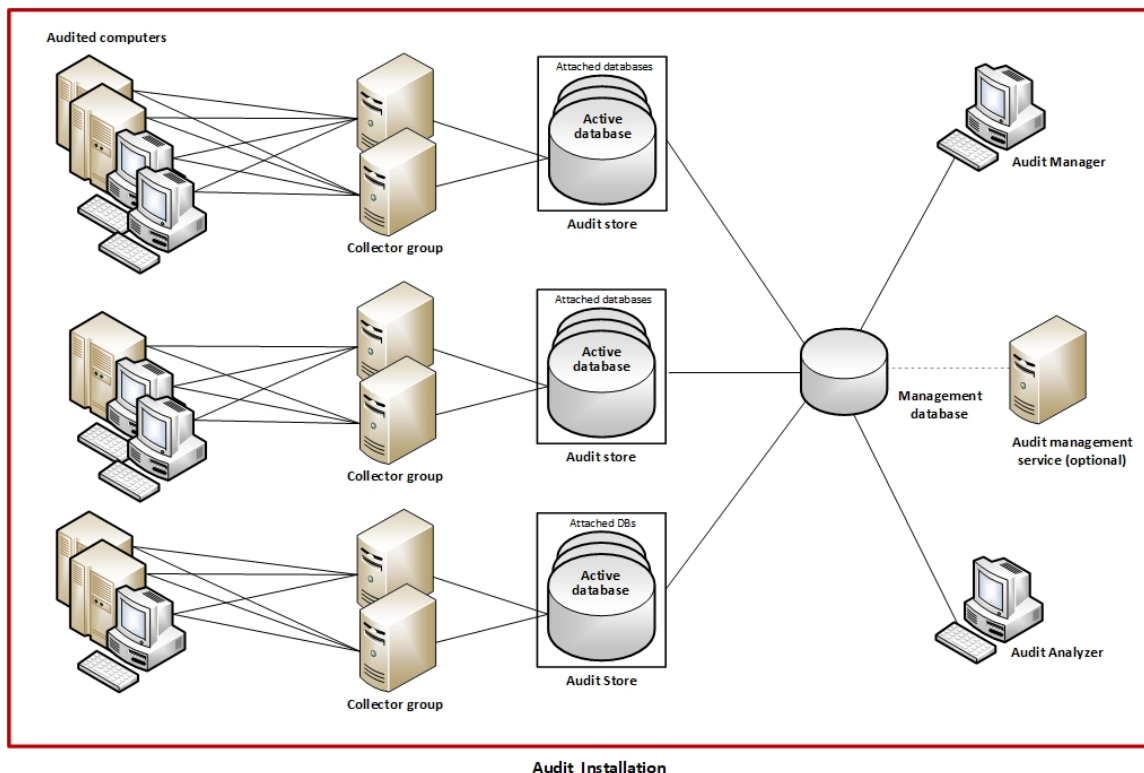
A single installation always has a single audit management database. In most cases, however, you use more than one console to request data from the audit management database. The two most important consoles in an installation are the Audit Manager console and the Audit Analyzer console.

- As the audit installation owner, you use the Audit Manager console to configure and manage the auditing components in your installation. In most organizations, there is only one Audit Manager console installed.
- Auditors use the Audit Analyzer console to search, retrieve, and play back sessions. The auditor can use predefined queries to find sessions or define

new queries. Auditors can also choose whether to share their queries with other auditors or keep them private. In most organizations, there are multiple Audit Analyzer consoles installed.

In addition to the Audit Manager and Audit Analyzer consoles, you can use the Agent Control Panel and the Collector Control Panel to configure and manage agents and collectors.

The following figure shows the architecture of a medium-size installation.



## Agent components on audited UNIX computers

To enable auditing for Linux and UNIX computers, you must install the Centrify UNIX agent on the computers you want to audit and make sure the computers are joined to an Active Directory domain. Joining a domain is required to ensure that authentication and authorization services are provided by Active Directory. To enable auditing on a computer, the Centrify UNIX agent includes the following components:

- dad—the core auditing service that collects the audit data and either sends it to a collector or spools it locally until a collector is available.



- `cdash`—the UNIX shell wrapper that intercepts all user traffic and sends it to the `dad` process.
- `dacontrol`, `dainfo`, `dareload`, and other command-line programs that enable you to manage agent operations from a login shell.

After you enable auditing on a computer, the agent captures all output (`stdout`), error messages (`stderr`), and user input (`stdin`) except for passwords. By default, the agent captures user input even if a user runs commands with `echo` turned off. For example, if a user logs on, then runs `echo off` before typing the `sudo` command, the auditing service captures the `sudo` entry as part of the user's session.

## Agent components on audited Windows computers

To enable auditing for Windows computers, you must install the Centrify Agent for Windows on the computers you want to audit and make sure the computers are joined to an Active Directory domain. Joining a domain is required to ensure that authentication and authorization services are provided by Active Directory. If you enable auditing for the Centrify Agent for Windows, the agent includes the following components:

- `wdad`—the Windows audit data collection service.
- `wash`—the Windows service that intercepts all user traffic and sends it to the Windows audit data collection service.
- The Agent Control Panel—an applet that enables you to configure and manage the agent.

For example, you can use the Agent Control Panel to configure the color depth of audit data to achieve the desired balance between playback screen resolution and audit store database size.

# Planning an audit installation

This chapter describes the decisions you need to make during the planning phase of a deployment and summarizes what's involved in deploying audit and monitoring service components and auditing-related services on the computers to be audited. It includes simplified diagrams that highlight the steps involved.

The following topics are covered:

Decide on the scope of the installation .....	24
Decide where to install the management database .....	25
Decide where to install collectors and audit stores .....	26
Decide where to install agents .....	31
Decide where to install consoles .....	31
Make sure you have a supported edition of SQL Server .....	32
Check SQL Server logins for auditing .....	32
Determining storage requirements for auditing .....	34
What's involved in the deployment process .....	36

## Decide on the scope of the installation

Before you deploy any part of the auditing infrastructure, you should decide on the scope of the audit installation and whether you want to use a single installation for your entire Active Directory site, or separate audit installations for different geographical areas or functional groups.



The most common deployment scenario is a single installation for each Active Directory forest, so that auditors can query and review information for the entire organization. However, if your Active Directory site has more than one forest, you might want to use more than one installation. If you want to use more than one installation, you should determine the subnetwork segments that will define the scope of each installation.

In Active Directory, a site represents the collection of Internet Protocol (IP) addresses that describe the physical structure of your network. If you are not familiar with how Active Directory sites are defined, you should consult Microsoft documentation for more information.

## Decide where to install the management database

Each audit installation has a single audit management server and audit management database. The management database is a Microsoft SQL Server database that stores information about the installation such as the Active Directory sites or subnets associated with each audit store.

The computer you use for the audit management database should have reliable, high-speed network connectivity. The management database does not store the captured sessions, and is, therefore, much smaller than the audit store databases. There are no specific sizing requirements or recommendations for the management database.

You can use the following guideline as the recommended minimum hardware configuration for the computer you use as the management database:

Computer used for	Number of concurrent sessions	CPU cores	CPU speed	Memory
Management database	Any	1 to 2	2.33 GHz	8 GB

The audit management server is a Windows service that performs two main tasks:

- The service collects audit trail events on the management database, then sends them to the audit store database.
- The service automatically calculates the approximate disk space used by audited sessions.

## Decide where to install collectors and audit stores

Although a collector and an audit store database can be installed on the same computer for evaluation, you should avoid doing so in a production environment. As part of the planning process, therefore, you need to decide where to install collectors and audit store databases. In designing the network topology for the installation, there are several factors to consider. For example, you should consider the following:

- Database load and capacity
- Network connectivity
- Port requirements
- Active Directory requirements

The next sections provide guidelines and recommendations to help you decide where to install the collectors and audit store databases required to support the number of computers you plan to audit.

### Use separate computers for collectors and audit store databases

To avoid overloading the computers that host collectors and audit store databases, you should install collectors and audit store SQL Server databases on separate computers. Because SQL Server uses physical memory to store database information for fast query results, you should use a dedicated computer for the audit store database, and allocate up to 80% of the computer's memory to SQL Server. In most installations, you also need to plan for more than one audit store database and to periodically rotate from one database to another to prevent any one database from getting too large. For more information about managing audit store databases, see [Managing audit store databases](#).

### Plan for network traffic and default ports

You should minimize the distance network packets have to travel between an agent and its collector. You should also minimize the distance between collectors and their audit stores. If possible, you should not have more than one gateway or router hop between an agent and its collector.



To help you plan for network traffic, the following ports are used in the initial set of network transactions:

- Directory Service - Global Catalog lookup request on port 3268.
- Authentication Services - LDAP sealed request on port 389.
- Kerberos – Ticket Granting Ticket (TGT) request on port 88.
- Network Time Protocol (NTP) Server – Time synchronized for Kerberos on port 123.
- Domain Name Service (DNS) – Host (A), Pointer (PTR), Service Location (SRV) records on port 53.

Depending on the specific components you deploy and operations performed, you might need to open additional ports. The following table summarizes the ports used for Centrify software.

This port	Is used for	Centrify software component
23	TCP communication for Telnet connections	Centrify authentication service, privilege elevation service, and audit and monitoring service.  By default, <b>telnet</b> connections are not allowed because passwords are transferred over the network as plain text.
53	TCP/UDP communication	Clients use the Active Directory DNS server for DNS lookup requests.
88	Encrypted UDP communication	Kerberos ticket validation and authentication, agents, Centrify PuTTY
123	UDP communication for simple network time protocol (NTP)	Keeps time synchronized between clients and Active Directory for Kerberos ticketing.
389	Encrypted TCP/UDP communication	Active Directory authentication and client LDAP service.
443	Cloud proxy server to Centrify cloud service	Centrify for mobile device management.
445	Encrypted TCP/UDP communication for delivery of group policies	The <b>adclient</b> and <b>adgpupdate</b> use Samba (SMB) and Windows file sharing to download and update group policies, if applicable.
464	Encrypted TCP/UDP communication for Kerberos password changes	Kerberos ticket validation and authentication for agents, Centrify PuTTY, <b>adpasswd</b> , and <b>passwd</b> .
500	Internet Key Exchange (IKE) for UDP	Centrify Isolation and Encryption Service to protect data-in-motion
1433	Encrypted TCP communication for the collector connection to	The collector service sends audited activity to the database

This port	Is used for	Centrify software component
	Microsoft SQL Server	
3268	Encrypted TCP communication	Active Directory authentication and LDAP global catalog updates.
4500	Internet Key Exchange (IKE) for NAT-T	Centrify Isolation and Encryption Service to protect data-in-motion
5063	Encrypted TCP/RPC communication for the agent connection to collectors	The auditing service records user activity on an audited computer.
none	ICMP (ping) connections	To determine whether if a remote computer is reachable.

## Identify an Active Directory site or subnets

Depending on the size and distribution of your Active Directory site, an audit store might cover an entire site or specific subnet segments. If you have a large, widely distributed site, you should consider network connectivity and latency issues in determining which subnets each audit store should serve. In addition, you should always place collectors in the same site as the agents from which they receive data. Collectors and agents must always be in the same Active Directory forest. If possible, you should put collectors and agents in the same domain.

**Note:** If you deploy agents in a perimeter network, such as a demilitarized zone (DMZ), that is separated from your main network by a firewall, put the collectors in the same Active Directory domain as the audited computers. The collectors can communicate with the audit store database through a firewall.

## Determine how many collectors and audit stores to install

Although you can add collectors and audit stores to your audit installation after the initial deployment, you might want to calculate how many you will need before you begin deploying components. You should always have at least two collectors to provide redundancy. As you increase the number of agents deployed, you should consider adding collectors.



## Estimate the number of agents and sessions audited

If you plan to use more than the minimum number of collectors, the most important factor to consider is the number of concurrent sessions you expect to monitor on audited computers. The number of concurrent sessions represents the number of agents that are actively capturing user sessions in a site at the same time.

## Guidelines for Linux and UNIX computers

You can use the following guidelines as a starting point and adjust after you have observed how much audit data you are collecting and storing for Linux and UNIX computers:

Number of concurrent sessions	Recommended number of collectors	Recommended number of audit stores
500 (or less) agents	2	1
up to 1000 agents	2	1
more than 1000 agents	2 for every 500 agents	1 for every 1000 agents

## Guidelines for Windows computers or mixed environments

You can use the following guidelines as a starting point and adjust after you have observed how much audit data you are collecting and storing for Windows computers:

Number of concurrent sessions	Recommended number of collectors	Recommended number of audit stores
100 (or less) agents	2	1
more than 100 agents	2 for every 100 agents	1 for every 100 agents

If you auditing Linux, UNIX, and Windows computers, use the numbers of collectors and audit stores recommended for Windows agents unless you have significantly fewer Windows agents.

## Determine the recommended hardware configuration

The hardware requirements for collectors and audit store servers depend on the size of the installation and where the components are installed on the network. For example, the requirements for a computer that hosts the collector service are determined by the number of audited computers the collector



supports, the level of user activity being captured and transferred, and the speed of the network connection between the agents and the collector and between the collector and its audit store.

## Guidelines for Linux and UNIX computers

You can use the following guidelines as the recommended hardware configuration for the computers you use for collectors and audit store servers when auditing Linux and UNIX computers:

Computer used for	Number of concurrent sessions	CPU cores	CPU speed	Memory
Collectors	Up to 250 active UNIX agents	2	2.33 GHz	8 GB
	250 to 500 active UNIX agents	4	2.33 GHz	16 GB
Audit store	Up to 250 active UNIX agents	2	2.33 GHz	8 GB
	250 to 500 active UNIX agents	4	2.33 GHz	16 GB
	500 to 1000 active UNIX agents	4	2.33 GHz	32 GB

## Guidelines for Windows computers

You can use the following guidelines as the recommended hardware configuration for the computers you use as collectors and audit store servers when auditing Windows computers:

Computer used for	Number of concurrent sessions	CPU cores	CPU speed	Memory
Collectors	Up to 100 active Windows agents	2	2.33 GHz	8 GB
Audit store	Up to 200 active Windows agents	2	2.33 GHz	8 GB
	200 to 500 active Windows agents	4	2.33 GHz	32 GB

## Guidelines for storage

Because audit and monitoring service collectors send captured user sessions to the active SQL Server database, you should optimize SQL Server storage for fast data logging, if possible. For the active database, you get the most benefit from improvements to disk write performance. Read performance is secondary. Fibre Attached Storage (FAS) and Storage Area Network (SAN) solutions can provide 2 to 10 times better performance than Direct Attached Storage (DAS), but at a higher cost. For attached databases that are only used to store information for queries, you can use lower-cost storage options.

## Guidelines for disk layout

The following table outlines the recommended disk arrays:

Application	Disk configuration	Use the disk for
Operating system	C: RAID 1	Operating system files, page file, and SQL Server binaries.
Microsoft SQL Server	D: RAID 10 (1+0)	Audit store database.
	E: RAID 10 (1+0)	Audit store database log files.
	F: RAID 1 or 10 (1+0)	Temporary database space (tempdb) for large queries for reports.
	G: RAID 1	Database dump files.

The size of disk needed depends on the number, length, and types of sessions recorded each day, the selected recovery model, and your data retention policies. For more information about managing audit store databases, see [Managing audit store databases](#).

## Decide where to install agents

The Centrify agent must be installed on all of the computers you want to audit. Therefore, as part of your planning process, you should decide whether you want to audit every computer on the network or specific computers, such as the computers used as servers or used to run administrative software.

Before installing the Windows agent, verify the following:

- The computer is joined to Active Directory.
- The computer has .NET 4.5.2 or later installed.
- The computer has Windows Installer version 3.1 or newer.

Agents can communicate with a collector only if the agents and collector are in the same Active Directory forest.

## Decide where to install consoles

You can install and run the Audit Manager console and the Audit Analyzer console on the same computer or on different computers. The computers where you install the consoles must be joined to the Active Directory domain and be able to access the management database that serves the installation.



You can also use the Audit Analyzer console to run queries from any additional computers with network access to the management database. Therefore, you should decide where it would be convenient to have this capability.

## Make sure you have a supported edition of SQL Server

The current release of the Centrify Audit & Monitoring Service supports 64-bit versions of the following SQL Server editions:

- SQL Server 2008 Express with Advanced Services
- SQL Server 2008
- SQL Server 2008 R2 Express with Advanced Services (Service Pack 2 or higher recommended)
- SQL Server 2008 R2 (Service Pack 2 or higher recommended)
- SQL Server 2012 Express with Advanced Services
- SQL Server 2012 (All SP levels)
- SQL Server 2014 Express with Advanced Services
- SQL Server 2014 (All SP levels)
- SQL Server 2016 -- all SP levels for SQL Server 2016 Standard and Enterprise including the latest 2016 SP2 CU7 version.

**Note:** SQL Server 2008 and 2008 R2 are not compatible with Windows 10

## Check SQL Server logins for auditing

An audit installation requires at least two Microsoft SQL Server databases: one for the management database and at least one for the first audit store database. To successfully connect to these databases, you must ensure that the appropriate users and computers have permission to read or to read and write for the databases that store audit-related information.

The simplest way to manage SQL logins for auditors and administrators is to do the following:





- Ensure you have a SQL login account for the NT Authority\System built-in account.
- Add the NT Authority\System account to system administrator role.
- Use Audit Manager to grant Manage SQL Logins permissions to the Active Directory users and groups that require them.

If you use Audit Manager to manage SQL logins, you can use Active Directory membership to automatically add and remove the permissions required for auditing activity. There is no requirement to use the SQL Server Management Studio to manage logins or permissions. Since it is recommended that you have a dedicated SQL Server instance for auditing, giving the NT Authority\System account a SQL login and system administrator role is an acceptable solution for most organizations.

## Create security groups for auditing

Depending on whether you configure Microsoft SQL Server to use Windows only authentication or Windows or SQL Server authentication, your SQL Server login credentials might be a Windows account or a SQL Server login account that is not associated with a Windows account.

To facilitate communication and the management of SQL logins, you can create Active Directory security groups for the following users and computers:

- **Centrify-Admins** for the user accounts that perform administrative tasks using Audit Manager.
- **Centrify-Auditors** for the user accounts that use Audit Analyzer.
- **Centrify-TrustedCollectors** for the computers accounts that host the collector service.

If you create these Active Directory security groups, you can then use Audit Manager to grant Manage SQL Login permissions for each group to allow its members to connect to the appropriate SQL Server database. Creating Active Directory security groups with SQL Server logins enables you to manage access to the databases required for auditing through Active Directory group membership without the help of the database administrator.

Any time you want to add an administrator, auditor, or collector computer to the installation, you simply add that user account or computer object to the appropriate Active Directory group. If an administrator or auditor leaves or if you want to stop using the collector on a particular computer, you can remove



that user or computer from its Active Directory security group to prevent it from accessing the database.

## Determining storage requirements for auditing

There are two important policy decisions your organization must make to determine how much disk space you need for storing audit data and how frequently you should plan to rotate the active database. Early on in the deployment, your organization should consider the following policy decisions:

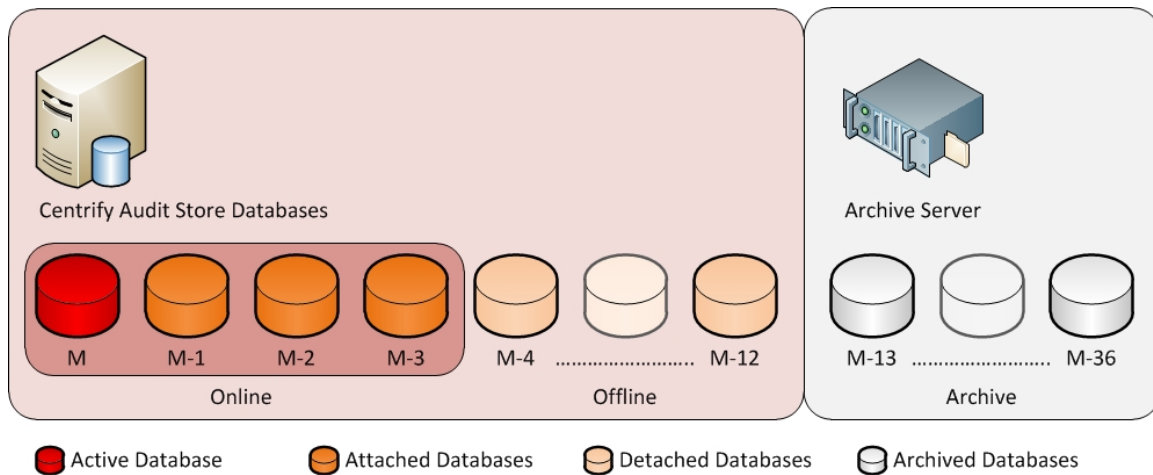
- What is your rotation policy?

To answer this question, you should decide the period of time audited sessions should be available in the active and attached database for auditors to review using the Audit Analyzer console. For example, you might decide that you want to be able to query audited activity for a minimum of 90 days. Alternatively, you might want to define a rotation policy that is based on the size of the database, so that the active database is not allowed to exceed a specific size. For example, you might decide that the database should not exceed 4GB to optimize performance for archiving.

- What is your retention policy?

To answer this question, you should decide the period of time to keep audited data available in attached databases and the maximum period of time to keep archived audit data available before purging data that's no longer needed.

To illustrate how these policies affect database management, consider a rotation policy based on a monthly schedule. In this example, an organization decides that audit data must be available for querying for a minimum of 90 days. On the first of each month, a new active database is brought online and the previous 3 months remain available as attached databases to support querying 90 to 120 days of audit data.



In this model, there are four databases online at the same time. This example organization has also decided on a two-stage retention policy. In the first stage, older databases are detached from Audit Analyzer, but remain stored on the SQL Server instance for up to one year. The detached databases provide up to a year of audit history and can be reattached, if that data is needed. In the second stage of the retention policy, the organization archives the audit store databases for up to 3 years. After three years, the oldest data is permanently purged.

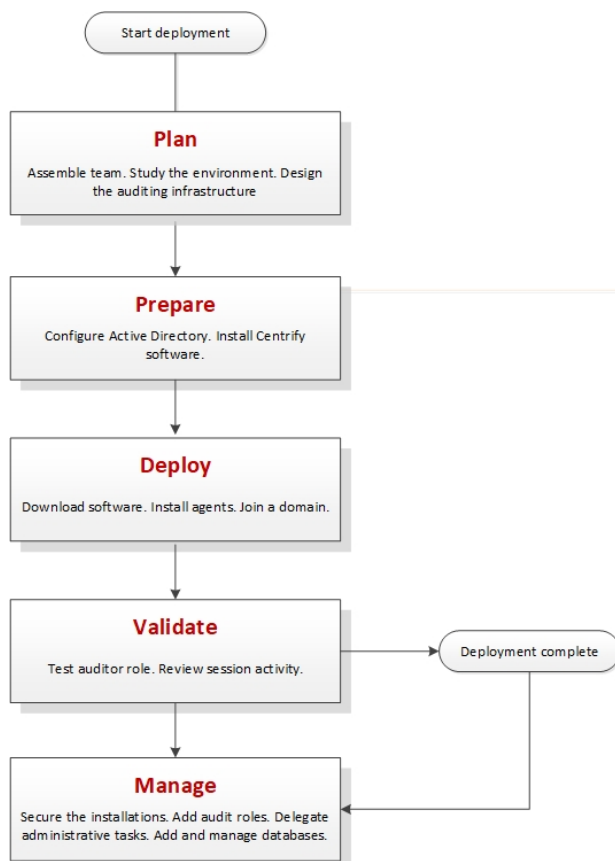
Depending on your requirements, you might use a similar retention policy or have different policies based on the session activity you are capturing. For example, you might keep sessions that capture normal user activity for three years, but keep sessions that capture SOX compliance for ten years.

To project your storage requirements, you will need additional information that is specific to your organization, including the number of computers you plan to audit, the number of sessions that are active on audited computers, and whether you record all activity using video capture or only summaries of user activity. To collect this information, you should monitor a pilot deployment. You can then use the information from the pilot deployment as described in [Estimating database requirements based on the data you collect](#) to estimate your storage requirements based on how much audit data you are generating. The decisions you make for the rotation and retention policies will help you further refine those estimations as you expand the deployment.

**Note:** If you define a rotation policy similar to this example, you can automate the monthly database rotation using Centrify application programming interfaces or using scheduled SQL Server jobs or scripts that perform database maintenance operations. For more information, see the Database Management Guide.

## What's involved in the deployment process

Most of the planning in this chapter has focused on designing the auditing infrastructure and deciding where to install components. The following illustration provides a visual summary of the complete deployment process and highlights the keys to success. The sections after the flowchart provide additional details about what's involved in each phase or the decisions you will need to make, such as who should be part of the deployment team, where to install the software, and who has permission to do what.



### Plan

During the first phase of the deployment, you collect and analyze details about your organization's requirements and goals. You can then also make preliminary decisions about sizing, network communication, and where to install components.

Here are the key steps involved:



- Identify the goals of the deployment.
  - Is auditing important for specific computers?
  - Is auditing important for computers used to perform administrative tasks?
  - Is auditing important for computers that host specific applications or sensitive information?
  - Should auditing be required for users in specific groups or with specific roles?
- Assemble a deployment team with Active Directory, UNIX, and other expertise, including at least one Microsoft SQL Server database administrator.
- Provide basic training on Centrify architecture, concepts, and terminology.
- Analyze the existing environment to identify target computers where you plan to install Centrify auditing infrastructure components.
  - Plan for permissions and the appropriate separation of duties for your organization.
  - Review network connections, port requirements, firewall configuration.
  - Identify computers for Audit Manager and Audit Analyzer consoles.
  - Identify computers to be used as collectors, audit stores, and the management Database.
  - Verify that you have reliable, high-speed network connections between components that collect and transfer audit data and sufficient disk storage for the first audit store database.
  - Identify the initial target group of computers to be audited.
- Define and document your data archiving and data retention policies.

## Prepare

After you have analyzed the environment, you should prepare the Active Directory groups to use. You can then install administrative consoles and the auditing infrastructure.

Here are the key steps involved:



- (Optional) Create the additional Active Directory security groups for your organization.
- Groups can simplify permission management and the separation-of-duties security model.
- Install Audit Manager and Audit Analyzer on at least one administrative Windows computer.
- Create a new audit installation and a management database on one computer.
- Create an audit store and audit store database on at least one computer.
- Install a collector on at least two computers.

## Deploy

After you have prepared Active Directory, installed administrative consoles on at least one computer, and created at least one installation, you are ready to deploy agents on the computers to be audited.

Here are the key steps involved:

- Install the agent on the computers you want to audit.
- Join the appropriate domains and zones.
- Prepare a Group Policy Object for deploying agents remotely using a group policy.
- Assign the appropriate permissions to the users and groups who should have access to audit data.

## Validate

After you have deployed agents on target computers, you should test and verify operations before deploying on additional computers.

Here are the key steps involved:

- Log on locally to a target computer using an Active Directory user account and password to verify Active Directory authentication.
- Open Audit Analyzer and query for your user session.



## Manage

After you have tested and verified auditing operations, you are ready to begin managing your audit installation.

Here are the key steps involved:

- Secure the installation.
- Add auditor roles and assign permissions to the appropriate users and groups.
- Create new databases and rotate the active database.
- Archive and delete old audit data.

# Installing Centrify Audit & Monitoring Service

This chapter describes how to install Centrify Audit & Monitoring Service in a production environment. In production environments, you should use a different computer for each component. For example, you should install the collector on its own computer separate from the computer used for the audit store database, and on a separate computer from the audit management database.

To create a simpler installation with all components on the same computer for evaluation purposes, see the *Evaluation Guide for Linux and UNIX*. For evaluation of auditing features in a Windows-only environment, see the *Evaluation Guide for Windows*.

The following topics are covered:

Installation preview .....	41
Installing and configuring Microsoft SQL Server for auditing .....	43
Installing the Audit Manager and Audit Analyzer consoles .....	48
Creating a setup user account for installation .....	50
Creating a new installation .....	50
Installing the audit collectors .....	61
Installing the Centrify Agent for Windows .....	64
Installing the Audit Management Server .....	82
Enabling or disabling auditing on Windows computers .....	83
Installing an Centrify Agent for *NIX .....	84
Installing additional Audit Manager or Audit Analyzer consoles .....	86
Checklist for auditing systems outside of Active Directory .....	87



## Installation preview

As a preview of what's involved in the installation process, the following steps summarize what you need to do and the information you should have on hand for a successful deployment of Centrify software.

### To prepare for deployment:

1. Analyze your network topology to determine where to install components and services and any hardware or software updates required.

For a review of the decisions to make and recommended hardware configuration, see [Planning an audit installation](#).

2. Create a list of the computers where you plan to install different components.

For example, list the computers where you plan to install agents, collectors, audit store databases, and consoles.

For a review of the requirements associated with each component, see [Planning an audit installation](#).

3. Determine the scope of the audit installation.

The most common deployment scenario is a single installation for an Active Directory site, but you can have more than one installation, if needed, and use subnets to limit the scope of the installation.

For a review of what constitutes an installation, see [Deploying auditing components in an audit installation](#) and [Decide on the scope of the installation](#).

4. Create Active Directory security groups for managing the permissions that are required for accessing the databases that store audit-related information.

For a review of the Active Directory security groups to create, see [Check SQL Server logins for auditing](#).

5. Install Microsoft SQL Server.



If you are not a database administrator in your organization, you should submit a service request or contact an administrator who has permission to create databases.

For more information about preparing a SQL Server database engine for auditing, see [Installing and configuring Microsoft SQL Server for auditing](#).

6. Install the Audit Manager and Audit Analyzer consoles.

For more information about installing the consoles, see [Installing the Audit Manager and Audit Analyzer consoles](#).

7. Create a service account with the permissions to create a new installation. For details, see [Creating a setup user account for installation](#).
8. Open Audit Manager to create a new installation.

For more information about using Audit Manager to create a new installation and audit store, see [Creating a new installation](#).

9. Install the audit collector service on at least two Windows computers.

You can add collectors to the installation at any time. For more information about installing and configuring collectors, see [Installing the audit collectors](#).

10. Install the Audit Management Server on a Windows computer.

For more information, see [Installing the Audit Management Server](#).

11. Install a Centrify agent on each Windows, Linux, or UNIX computer you want to audit.

For more information about installing Centrify agents, see [Installing the Centrify Agent for Windows](#) and [Installing an Centrify Agent for \\*NIX](#).

12. Make sure agents are enabled for auditing. For details, see [Enabling or disabling auditing on Windows computers](#) and [Enabling and disabling auditing on Linux and UNIX computers](#).

13. Install additional Audit Manager or Audit Analyzer consoles on any Windows computer that you want to use to manage the installation or query and play back session data.

After the initial deployment, you can add new agents, collectors, audit stores, and audit store databases to the installation or create additional installations.

## Installing and configuring Microsoft SQL Server for auditing

If you want to audit user activity on Windows, you must have at least one Microsoft SQL Server database instance for the audit management database and audit store databases. Centrify recommends that you use a dedicated instance of SQL Server for the audit management database. A dedicated SQL Server instance is an instance that does not share resources with other applications. The audit store databases can use the same dedicated instance of SQL Server or their own dedicated instances.

There are three database deployment scenarios for your audit installation:

- **Evaluation**—You can install Microsoft SQL Server Express with Advanced features directly from the configuration wizard or by running the `SQLEXPRADV_x64_ENU.exe` setup program to create a new Microsoft SQL Server Express database instance for testing. However, if you are auditing a production environment, you should not use Microsoft SQL Server Express.

If you choose to install a different version of Microsoft SQL Server Express for an evaluation and the version requires .NET version 3.5 SP1, you will need to manually install the .NET files yourself (the installer doesn't include these files)..

- **Manual installation with system administrator privileges**—Install a Microsoft SQL Server database instance for which you are a system administrator or have been added to the system administrator role.
- **Manual installation without system administrator privileges**—Have the database administrator (DBA) install an instance of Microsoft SQL Server and provide you with system administrator credentials or information about the database instance so that you can create the management database and audit store databases.

## Downloading and installing SQL Server manually

You can use an existing instance of Microsoft SQL Server or install a new instance. You can install Microsoft SQL Server directly from the Centrify ISO or ZIP, or download it from the Microsoft web site. In selecting a version of SQL Server to download, you should be sure it includes Advanced Services.



Advanced Services are required to support querying using SQL Server full-text search.

After downloading an appropriate software package, run the setup program using your Active Directory domain account and follow the instructions displayed to complete the installation of the Microsoft SQL Server instance.

When selecting the components to install in the setup program, expand the Database Services and select Full Text Search as a feature to be installed. For the authentication mode, select Windows authentication if all connections between auditing components will be in the same forest. If any communication will be outside of the forest, use Mixed Mode authentication and select the option to add the current user to the SQL Server Administrator role.

**Note:** Centrify does not recommend running SQL Server under a high privilege account such as a LocalSystem account.

## Configuring SQL Server to prepare for auditing

After you install the SQL Server database engine and management tools, you should configure the SQL Server instance for auditing. For example, depending on the version of SQL Server you install, you might need to manually enable full-text search.

To prepare a Microsoft SQL Server database instance for storing audit data:

- Use SQL Server Surface Area Configuration for Services and Connections to check the status and start the database engine, full-text search, and SQL Server Browser services.
- Use SQL Server Surface Area Configuration for Services and Connections or SQL Server Configuration Manager to enable remote connections for TCP/IP.
- Verify whether SQL Native Client Configuration Client Protocol is using the default TCP port 1433 for network communications. If you use a different port, you should note the port number because you will need to specify it in the server name when you create the management and audit store databases.
- Use SQL Server Configuration Manager to restart the SQL Server and SQL Server Browser services.
- Create a database backend service account in the system administrator (sa) fixed server role on the selected database server; you'll specify this



account when you create the audit installation. This account is used to run backend stored procedures. If desired, this can be the same account that you use to create the audit installation, as mentioned in [Creating a setup user account for installation](#).

## Configuring Amazon RDS for SQL Server for auditing

You can deploy audit store databases on Amazon RDS instances, if desired. Centrify supports Amazon RDS for 2016 and earlier versions (not 2017).

You must host the audit management database on a traditional SQL Server, such as SQL Server Express, Standard, or Enterprise.

If you want to use an instance of Amazon RDS for SQL Server for audit store databases you need to do the following configurations:

- After you set up your Amazon RDS for SQL Server, join the RDS SQL server to AWS Microsoft Active Directory.
- Enable these DB Parameter Group settings on RDS SQL Server:
  - `clr enabled`
  - `show advanced options`

You can use the AWS Management Console, API, or the AWS command line interface to enable these settings.

For more details, see

[http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_WorkingWithParamGroups.html](http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithParamGroups.html).

- Set up a one-way or two-way forest trust between the AWS Microsoft Active Directory and your on-premise Active Directory forest so that users of your on-premise Active Directory forest can access resources in the AWS Microsoft Active Directory.

**Note:** Amazon RDS for SQL Server with High Availability is supported.

## Amazon RDS for SQL Server required permissions

The permissions for Amazon RDS for SQL Server vary a little from the permissions for local or network instances of SQL Server. This section covers the Amazon RDS for SQL Server permission required or granted for each auditing component.



## Permissions to the audit store database stored procedures service account

The stored procedures service account (in other words, the 'execute as' account) no longer requires the sysadmin server role permission if the audit store database is on Amazon RDS for SQL Server.

The service account requires only the db\_owner database role permission and the account will be added to be member of db\_owner database role by Add Audit Store Database wizard.

**Note:** You do not need to grant the permissions manually. The Audit Manager console, Powershell cmdlet, or SDK grants the permissions to the service account.

## Collector account permissions for audit store databases on Amazon RDS for SQL Server

The collector account requires the following server level permissions on the Amazon RDS for SQL Server:

- 'View Any Definition' server level permission
- 'View Server State' server level permission

The collector account requires the following database level permissions on the audit store database:

- A member of the 'collector' database role

**Note:** You do not need to grant the permissions manually. The Audit Manager console, Powershell cmdlet, SDK, or the Collector Configuration wizard grants the permissions to the collector account.

## Management Database Account permissions for audit store databases on Amazon RDS for SQL Server

The management database account requires the following server level permissions on the RDS SQL server:

- 'Alter Trace' server level permission
- 'Alter Any Login' server level permission
- Grant permission of 'Alter Any Login' server level permission
- Grant permission of 'View Any Definition' server level permission
- Grant permission of 'View Server State' server level permission



The management database account requires the following database level permissions on the audit store database:

- A member of 'managementdb' database role

**Note:** You do not need to grant the permissions manually. The Audit Manager console, Powershell cmdlet, or SDK grants the permissions to the management database account.

### **Permissions to create the audit store database on Amazon RDS for SQL Server**

In order to create an audit store database on Amazon RDS for SQL Server, you must have the following permissions:

- 'Create Any Database' server level permission to create the database on the server
- 'Alter Any Login' server level permission to create the login for the management database account and the collector account
- 'Alter Any Login' server level permission to grant the 'Alter Any Login' permission to the management database account
- 'Alter Trace' server level permission to grant the 'Alter Trace' permission to the management database account
- 'View Any Definition' server level permission to grant the 'View Any Definition' (with grant) permission to the management database account and also to grant the 'View Any Definition' permission to the collector account
- Grant permission of 'View Server State' server level permission to grant the 'View Server State' (with grant) permission to the management database account and also to grant the 'View Server State' permission to the collector account

### **Permissions to upgrade the audit store database on Amazon RDS for SQL Server**

The required permission to upgrade the audit store database on Amazon RDS for SQL Server is the 'db owner' permission on the database. No server level permissions are required

## Installing the Audit Manager and Audit Analyzer consoles

You can install Audit Manager and Audit Analyzer on the same computer or on different computers. The computers where you install the consoles must be joined to the Active Directory domain and be able to access the management database.

In most cases, the consoles are installed together on at least one computer.

You can use either the individual console installers or the main installer.

- [Install Audit Manager using the console installer](#)
- [Install Audit Analyzer using the console installer](#)
- [Install both consoles using the main installer](#)

### To install Audit Manager using the individual console installer:

1. Log on using an Active Directory domain account.
2. Open the ISO file, and navigate to the following folder:  
`\DirectAudit\Console\`
3. Run the Audit Manager installer : `Centrify DirectAudit Administrator Console64.exe`.
4. At the Welcome page, click **Next**.
5. Review the terms of the license agreement, click **I accept the terms in the license agreement**, then click **Next**.
6. On the Destination Folder page, review the installation location and click **Next** to continue.
7. If you want to install the console in a different location, click **Change** and navigate to the desired folder.
8. Click **Install** to begin the installation.
9. The installer installs the necessary files. To open the console, keep the **Launch Centrify Audit Manager** option selected. Otherwise, deselect the option.
10. Click **Finish** to close the installer.





After you install Audit Manager, you can open Audit Manager to create a new installation.

## To install Audit Analyzer using the individual console installer:

1. Log on using an Active Directory domain account.
2. Open the ISO file, and navigate to the following folder:  
`\DirectAudit\Console\`
3. Run the Audit Manager installer : `Centrify DirectAudit Auditor Console64.exe`.
4. At the Welcome page, click **Next**.
5. Review the terms of the license agreement, click **I accept the terms in the license agreement**, then click **Next**.
6. On the Destination Folder page, review the installation location and click **Next** to continue.
7. If you want to install the console in a different location, click **Change** and navigate to the desired folder.
8. Click **Install** to begin the installation.
9. The installer installs the necessary file. To open the console, keep the **Launch Centrify Audit Analyzer** option selected. Otherwise, deselect the option.
10. Click **Finish** to close the installer.

## To install Audit Manager and Audit Analyzer on the same computer using the main installer:

1. Log on using an Active Directory domain account.
2. Open the ISO file.  
If you created a physical CD from the ISO file that you downloaded, the Getting Started page is displayed automatically. If the page is not displayed, open the `autorun.exe` file to start the installation.
3. On the Getting Started page, click **Audit & Monitor** to start the setup program for audit and monitoring service components.
4. At the Welcome page, click **Next**.



5. Review the terms of the license agreement, click **I accept the terms in the license agreement**, then click **Next**.
6. Select **Centrify Administration** to install both Audit Manager and Audit Analyzer, then click **Next**.
7. In the rare case where the administrator should not have access to the Audit Analyzer, select Audit Manager, then click **Next**.
8. After you install Audit Manager, you are prompted to create a new installation. If you want to create the installation at a later time, you can run the setup program again to create a new installation.

## Creating a setup user account for installation

You'll need to create an account to use when you create the audit installation, set up audit stores, and so forth. This account needs to have the following permissions:

- Active Directory:
  - Permission to create serviceConnectionPoint objects on the container or organizational unit you select for publishing installation information
- SQL Server:
  - Be a member of the system administrator (sa) fixed server role

This user account needs these permissions for the initial installation and some maintenance tasks. It's a good practice to add this account to your Centrify-admins security group, as mentioned in [Create security groups for auditing](#).

## Creating a new installation

Before you can begin auditing, you must create at least one audit installation and a management database. Creating the management database, however, requires SQL Server system administrator privileges on the computer that hosts the SQL Server instance. If possible, you should have a database administrator add your Active Directory domain account to the SQL Server system administrators role.

If you have not been added to the system administrators role, you should contact a database administrator to assist you. For more information about



creating a new installation when you don't have system administrator privileges, see [How to create an installation without system administrator privileges](#).

## To create a new installation and management database as a system administrator:

1. Log on using an Active Directory account with permission to install software on the local computer and permissions listed in [Creating a setup user account for installation](#).

2. Open Audit Manager.

**Note:** If you haven't configured an audit installation yet, the New Installation wizard opens automatically.

3. If this isn't your first audit installation: in Audit Manager, right-click **Centrify Audit Manager** and select **New Installation** to open the New Installation wizard.

4. Enter a name for the new installation, then click **Next**.

**Tip:** Name the installation to reflect its administrative scope. For example, if you are using one installation for your entire organization, you might include the organization name and All or Global in the installation name, such as AcmeAll. If you plan to use separate installations for different regions or divisions, you might include that information in the name, for example AcmeBrazil for a regional installation or AcmeFinance for an installation that audits computers in the Finance department.

5. Select the option to create a new management database and verify the SQL Server computer name, instance name, and database name are correct.

If the server does not use the default TCP port (1433), you must provide the server and instance names separated by a backslash, then type a comma and the appropriate port number. For example, if the server name is ACME, the instance name is BOSTON, and the port number is 1234, the server name would be ACME\BOSTON,1234.

If you're installing on a SQL cluster, enter the SQL cluster name in the SQL Server computer name field.



If you're connecting to a SQL Server availability group listener, click Options (next to the Server Name) and enter the following connection string parameters:

`MultiSubnetFailover=Yes`

Click **Next** to continue.

6. Select **Use the default NT AUTHORITY\SYSTEM account** to use the internal account or select a specific SQL login account with sufficient privileges, then click **Next**.

A SQL login account is required to run the stored procedures that read and write information to the management database. The account must be a member of the system administrator (sa) fixed server role on the selected database server, as mentioned in [Configuring SQL Server to prepare for auditing](#).

7. Type the license key you received, then click **Add** or click **Import** to import the keys directly from a file, then click **Next**.
8. Accept the default location or click **Browse** to select a different Active Directory location for publishing installation information, then click **Next**.

You must have the Active Directory permission to Create serviceConnectionPoint objects on the container or organizational unit you select for publishing installation information.

9. Select the installation-wide auditing options you want to enable, then click **Next**.
  - Select **Enable video capture recording of user activity** if you want to capture shell or desktop activity on computers when users are audited, then click **Next**.

Selecting this option enables you to review everything displayed during an audited user session, but will increase the audit store database storage requirements for the installation. You can deselect this option if you are only interested in a summary of user activity in the form of audit trail events. Audit trail events are recorded when users log on, open applications, and select and use role assignments with elevated rights.
  - Select **Do not allow any users to review their own sessions** to prevent all users from updating the review status for their own sessions or adding comments to their own sessions.



- Select **Do not allow any users to delete their own sessions** to prevent all users from deleting their own sessions.

If you set either of the installation-wide policies disallowing user activity, the policy takes precedence over any rights provided by a user's audit role.

10. Review details about the installation and management database, then click **Next**.

If you have SQL Server system administrator (sa) privileges and can connect to the SQL Server instance, the wizard automatically creates the management database.

11. Select the **Launch Add Audit Store Wizard** option if you want to start the Add Audit Store wizard, then click **Finish**

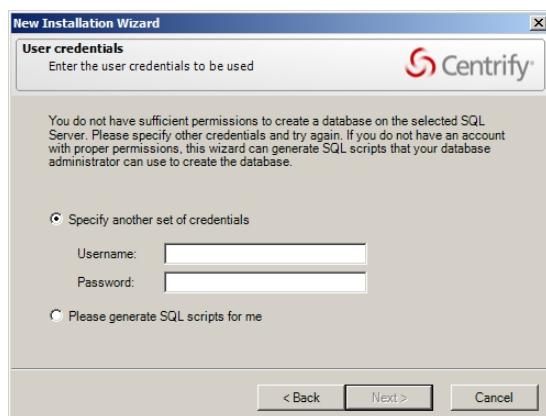
If you want to create the first audit store database on a different SQL Server instance, you should deselect the **Launch Add Audit Store Wizard** option and click **Finish**.

For more information about adding the first audit store database, see [Creating the first audit store](#).

## How to create an installation without system administrator privileges

If you do not have the appropriate permission to create SQL Server databases, you cannot use the New Installation wizard to create the management database without the assistance of a database administrator.

If you do not have system administrator privileges, the wizard prompts you to specify another set of credentials or generate SQL scripts to give to a database administrator. For example:





If you don't have a database administrator immediately available who can enter the credentials for you, you cannot continue with the installation.

## To create an installation when you don't have system administrator privileges:

1. Select the option to generate the SQL scripts, then click **Next**.
2. Select the folder location for the scripts, then click **Next**.
3. Review details about the installation and management database you want created, then click **Next**.

The wizard generates two scripts: Script1 prepares the SQL Server instance for the management database and Script2 creates the database.

4. Click **Finish** to exit the New Installation wizard.
5. Send the scripts to a database administrator with a service or change-control request.

**Note:** You should notify the database administrator that the scripts must be run in the proper sequence and not modified in any way. Changes to the scripts could render the database unusable.

6. After the database administrator creates the database using the scripts, open the Audit Manager console to run the New Installation wizard again.
7. Type the name of the installation, then click **Next**.
8. Select **Use an existing database** and verify the database server and instance name, then click the Database name list to browse for the database name that the database administrator created for you.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to ACME\BOSTON,1234.

If you're installing on a SQL cluster, enter the SQL cluster name in the SQL Server computer name field.

9. Select the database name from the list of available databases, click **OK**, then click **Next**.

You should only select an existing database if the database was created using scripts provided by Centrify.



10. Select **Use the default NT AUTHORITY\SYSTEM account** to use the internal account or select a specific SQL login account with sufficient privileges, then click **Next**.  
A SQL login account is required to run the stored procedures that read and write information to the management database. The account must be a member of the system administrator (sa) fixed server role on the selected database server.
11. Type a license key or import licenses from a file, then click **Next**.
12. Review details about the management database to be installed, then click **Next**.
13. Select the **Launch Add Audit Store Wizard** option if you want to start the Add Audit Store wizard, then click **Finish**.

## Creating the first audit store

If you selected the Launch Add Audit Store Wizard check box at the end of the New Installation Wizard, the Add Audit Store Wizard opens automatically. You can also open the wizard at any time by right-clicking the Audit Stores node in the Audit Manager console and choosing Add Audit Store.

### To create the first audit store:

1. Type a display name for the audit store, then click **Next**.  
**Tip:** If your plan specifies multiple audit stores, use the name to reflect the sites or subnets serviced by this audit store. Note that an audit store is actually a record in the management database. It is not a separate process running on any computer. You use a separate wizard to create the databases for an audit store.

2. Select the type of systems that the audit store will serve.

You can choose to separate Windows traffic from UNIX traffic if both types of agents belong to the same site or subnet.

The options are:

- Windows and UNIX
- Windows



- UNIX

Click **Next** to continue.

3. Click **Add Site** or **Add Subnet** to specify the sites or subnets in this audit store.
  - If you select Add Site, you are prompted to select an Active Directory site.
  - If you select Add Subnet, you are prompted to type the network address and subnet mask.

After you make a selection or type the address, click **OK**. You can then add more sites or subnets to the audit store. When you are finished adding sites or subnets, click **Next** to continue.

The computer you use to host the audit store database should be no more than one gateway or router away from the computers being audited. If your Active Directory sites are too broad, you can use standard network subnets to limit the scope of the audit store.

4. Review information about the audit store display name and sites or subnets, then click **Next**.
5. Select the **Launch Add Audit Store Database Wizard** option if you want to create the first audit store database, then click **Finish**.

## Creating the first audit store database

If you selected the Launch Add Audit Store Database Wizard check box at the end of the Launch Add Audit Store Wizard, the Add Audit Store Database Wizard opens automatically. You can also open the wizard at any time from the Audit Manager console by expanding an audit store, right-clicking the Databases node, and choosing Add Audit Store Database.

### To create the first audit store database:

1. Type a display name for the audit store database, then click **Next**.

The default name is based on the name of the audit store and the date the database is created.
2. Select the option to create a new database and verify that the SQL Server computer name, instance name, and database name are correct.





The default database name is the same as the display name. You can change the database name to be different from the display name, if you want to use another name.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to `ACME\BOSTON,1234`.

If you're installing on a SQL cluster, enter the SQL cluster name in the SQL Server computer name field.

When entering the SQL Server host computer name, note that you can enter either the server short name (which is automatically resolved to its fully qualified domain name, or FQDN) or the actual server FQDN or the CNAME alias for the server.

If the database is an Amazon RDS SQL Server:

- a. Select the **This is an Amazon RDS SQL Server** option.
- b. In the Server Name field, enter the RDS SQL Server database instance endpoint name used for Kerberos authentication.  
For example, if the database host name is `northwest1` and the domain name is `sales.acme.com`, then the endpoint name would be `northwest1.sales.acme.com`.

Click **Options** to enter additional connection string parameters or to enable data integrity checking.

- If you're connecting to a SQL Server availability group listener, click Options (next to the Server Name) and enter the following connection string parameters:  
`MultiSubnetFailover=Yes`
- You can enable or disable data integrity checking once, when you create the audit store database. To change the state, you must rotate to a new audit store database.

When you create your audit store database, you have the option to enable data integrity checking. Data integrity checking provides the ability to detect if auditing data has been tampered. For example, data integrity checking can detect if a user who has write privileges over the Audit Store database directly manipulates the audited session data by making a direct connection to the Microsoft SQL

Server database. Data integrity checking cannot detect tampering if a database administrator deletes an entire session or database.

Click **Next** to continue.

3. Because this is the first audit store database, you also want to make it the active database. This option is selected by default. If you are creating the database for future use and don't want to use it immediately, you can deselect the **Set as active database** option. The option to create a new database is also selected by default.

Click **Next** to continue.

4. Specify the stored procedures services account:

- Select **Use the default NT AUTHORITY\SYSTEM account** to use the internal account
- Or, select **Specify a SQL Login account** and enter a specific SQL login account with sufficient privileges.

A SQL Server login account is required to run the stored procedures that read and write information to the management database.

For local or network databases, the account must be a member of the system administrator (sa) fixed server role on the selected database server.

If the database is an Amazon RDS for SQL Server, the account you specify will be added as a member of the db\_owner fixed database role in Amazon RDS for SQL Server.

Click **Next** to continue.

5. Review details about the audit store database, then click **Next**.

If you have the correct privileges and can connect to the SQL Server instance, the wizard automatically creates the audit store database.

## Connecting to SQL Server on a remote computer

To create an audit store database on a remote computer, there must be a one-way or two-way trust between the domain of the computer on which you are running the Add Audit Database wizard and the domain of the computer hosting SQL Server. The Active Directory user account that you used to log on to the computer where the Audit Manager is installed must be in a domain trusted by the computer running SQL Server. If there is no trust relationship, you must log on using an account in the same domain as the computer running SQL Server. If you are accessing the computer running SQL Server remotely, you can



use the Run As command to change your credentials on the computer from which you are running the wizard.

## Verify network connectivity

The computer hosting the SQL Server database for the active audit store server must be online and available from the Audit Manager console and from the clients in the Active Directory site or the subnet segments you have defined for the audit store. You should verify that there are no network connectivity issues between the computers that will host collectors and those hosting the SQL Server databases.

## How to create the database without system administrator privileges

If you do not have system administrator privileges, the wizard prompts you to specify another set of credentials or generate SQL scripts to give to a database administrator. If you don't have database administrator credentials or a database administrator immediately available who can enter the credentials for you, you should generate the scripts, then follow the prompts displayed to exit the wizard.

## To add the database to the audit store after you have generated the scripts:

1. Send the scripts to a database administrator with a service or change-control request.  
You should notify the database administrator that the scripts must be run in the proper sequence and not modified in any way. Changes to the scripts could render the database unusable.
2. After the database administrator creates the database using the scripts, open the Audit Manager console.
3. Expand the installation node, then expand Audit Stores and the specific audit store you for which you want a new database.
4. Select **Databases**, right-click, then click **Add Audit Store Database**.
5. Type a display name for the audit store database, then click **Next**.
6. Enter the database server name:



The default database name is the same as the display name. You can change the database name to be different from the display name, if you want to use another name.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to `ACME\BOSTON,1234`.

If you're installing on a SQL cluster, enter the SQL cluster name in the SQL Server computer name field.

If the database is an Amazon RDS SQL Server:

- a. Select the **This is an Amazon RDS SQL Server** option.
- b. In the Server Name field, enter the RDS SQL Server database instance endpoint name used for Kerberos authentication.  
  
For example, if the database host name is `northwest1` and the domain name is `sales.acme.com`, then the endpoint name would be `northwest1.sales.acme.com`.

Click **Options** to enter additional connection string parameters or to enable data integrity checking.

- If you're connecting to a SQL Server availability group listener, click Options (next to the Server Name) and enter the following connection string parameters:

`MultiSubnetFailover=Yes`

- You can enable or disable data integrity checking once, when you create the audit store database. To change the state, you must rotate to a new audit store database.

When you create your audit store database, you have the option to enable data integrity checking. Data integrity checking provides the ability to detect if auditing data has been tampered. For example, data integrity checking can detect if a user who has write privileges over the Audit Store database directly manipulates the audited session data by making a direct connection to the Microsoft SQL Server database. Data integrity checking cannot detect tampering if a database administrator deletes an entire session or database.

7. Select **Use an existing database** and select the database that the database administrator created for you.

Because this is the first audit store database, you also want to make it the active database. This option is selected by default. If you are creating



the database for future use and don't want to use it immediately, you can deselect the **Set as active database** option.

If the server does not use the default TCP port, specify the port number as part of the server name. For example, if the port number is 1234, the server name would be similar to ACME\BOSTON,1234.

The installation, management database, and first audit store database are now ready to start receiving user session activity. Next, you should install the collectors and, finally, the agents to complete the deployment of the auditing infrastructure.

## Installing the audit collectors

After you have created a new installation, with an audit management database and at least one audit store and audit store database, you must add the collectors that will receive audit records from the agents and forward those records to the audit store. For redundancy and scalability, you should have at least two collectors. For more information about planning how many collectors to use and the recommended hardware and network configuration for the collector computers, see [Decide where to install collectors and audit stores](#).

### Set the required permission

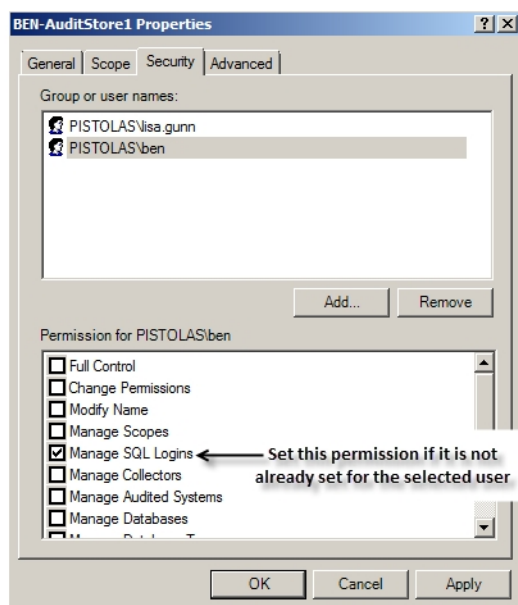
Before you configure a collector, you should check whether your user account has sufficient permissions to add new collector accounts to the audit store database. If you are a database administrator or logged on with an account that has system administrator privileges, you should be able to configure the collector without modifying your account permissions. If you have administrative rights on the computer that hosts Audit Manager but are not a database administrator, you can set the appropriate permission before continuing.

### To set the permission required to add accounts to the audit store database:

1. Open Audit Manager.
2. Expand the installation, then expand Audit Stores.

• • • • •

3. Select the audit store that the collector will connect to, right-click, then click **Properties**.
4. Click the **Security** tab.
5. Click **Add** to search for and select the user who will configure the collector.
6. Select the **Manage SQL Logins** right, then click **OK**.



## Install the collector service using the setup program

If your user account has sufficient permissions to add new collector accounts to the audit store database, you can install a collector by running the setup program on the computer on which you want to install the collector. When you are prompted to select components, select Audit Collector and deselect all of the other components, then click **Next**. Follow the instructions in the wizard to select the location for installing files and to confirm your selections, then click **Finish** to complete the installation.

The collector installer is in the `\DirectAudit\Collector` folder in your installation media.

## Configure the audit collector service

By default, when you click **Finish**, the setup program opens the Collector Configuration Wizard. Alternatively, you can launch the configuration wizard at any time by clicking **Configure** in the Collector Control Panel.

## To configure the collector service:

1. On the first screen of the Collector Configuration Wizard, select the DirectAudit installation to assign this collector to.

If the computer is also enrolled in the Centrify Cloud Platform and you have already enabled auditing in the Admin Portal, you can choose which kind of audit installation to assign the collector to:

- **Automatic:** This option configures the collector to receive audit data from systems that are enrolled in the Centrify Cloud Platform and systems that are joined to Active Directory.

You use the Admin Portal to configure which installation is used by these systems. The systems have either the Centrify Client for Linux or Centrify Client for Windows and the audit packages installed so that auditing is enabled. These systems do not have to be joined to Active Directory.

- **Manual:** This option configures the collector to receive audit data from systems that are joined to Active Directory and have either the Centrify Agent for \*NIX or Centrify Agent for Windows installed and the system is enabled for auditing. For this option, select the audit installation.

Computers that are not enrolled in the Centrify Cloud Platform have a single list of audit installations to pick from.

Click **Next** to continue.

The configuration wizard verifies that the specified installation has an audit store that services the site that the collector is in and that the collector and its audit store database are compatible.

2. Enter the port number(s) that the collector will use to communicate with the audited systems.
  - The default port is 5063 for systems that have either the Centrify Agent for \*NIX or Centrify Agent for Windows installed.
  - If the computer is also enrolled in the Centrify Cloud Platform, the default port is 5064 for systems that have either the Centrify Client for Linux or Centrify Client for Windows installed.
  - If you set the installation to Manual in the previous step, Centrify Client System port is greyed out.



For either port, if you specify a different port and have the default Windows firewall turned on, the wizard checks whether the port is open. If the port isn't open, the wizard offers to open it for you.

If you are using another vendor's firewall, open the port with the tools provided by that vendor. If there's an upstream firewall—such as a dedicated firewall appliance—between the collector and the computers to be audited, contact the appropriate personnel to open the port on that firewall.

Click **Next** to continue.

3. If the computer where you're configuring a collector belongs to multiple audit stores in the auditing installation, choose which audit store this collector will connect to, then click **Next**.

For example, two audit stores can have an overlapping scope if one audit store scope is configured for Active Directory sites and another one is set by subnets.

4. Select whether you want to use Windows authentication or SQL Server authentication when the collector authenticates to the audit store database, then click **Next**.

In most cases, you should choose Windows authentication to add the computer account to the audit store database as a trusted, incoming user.

If Microsoft SQL Server is in a different forest or in an untrusted forest, you should use SQL Server Management Studio to set up one or more SQL Server login accounts for the collector. After you create the SQL Server login account for the collector to use, you can select SQL Server authentication, then type the SQL Server login name and password in the wizard.

5. Type the maximum number of connections for the Microsoft SQL Server connection pool, then click **Next**.
6. Review the settings for the collector, then click **Next**.
7. Click **Finish** to close the wizard and start the collector service.

## Installing the Centrifify Agent for Windows

You must install an agent on every Windows computer that you want audit. You can install the agent in the following ways:





- **Interactively**, by running the Centrify setup program on each computer.

When the installation finishes, the agent configuration wizard launches automatically. You can configure the agent right away, or exit the configuration wizard and configure the agent later. See [Installing interactively using the setup program](#) for details.

- **Silently**, by executing appropriate commands in a terminal window on each computer.

You can install silently on a local computer or use a software distribution product, such as Microsoft System Center Configuration Manager (SCCM), to execute the appropriate commands remotely to deploy agents on remote computers. After installation, you can change the default agent settings, if needed. See [Installing silently by using the Microsoft Windows Installer](#) for details.

- **Silently and centrally**, by using a group policy to execute commands remotely on the computers in a domain or organizational unit.

If you use the Centrify Group Policy Deployment files, you can both install and configure the registry on remote computers from a central location without a separate software distribution product. However, you must configure the Windows agent registry settings in a file before deploying. See [Installing from a central location by using group policy](#) for details.

Regardless of the deployment method you choose, you should first make sure that the computers where you plan to deploy meet all of the installation prerequisites.

## Verify prerequisites

Before installing the Windows agent, verify the computer on which you plan to install meets the following requirements:

- The computer is running a supported Windows operating system version.
- The computer is joined to Active Directory.
- The computer has sufficient processing power, memory, and disk space for the agent to use.
- The computer has the .NET Framework, version 4.5.2 or later.
- The computer has Windows Installer version 3.1, or later.

If you are installing interactively using the setup program, the setup program can check that the local computer meets these requirements and install any



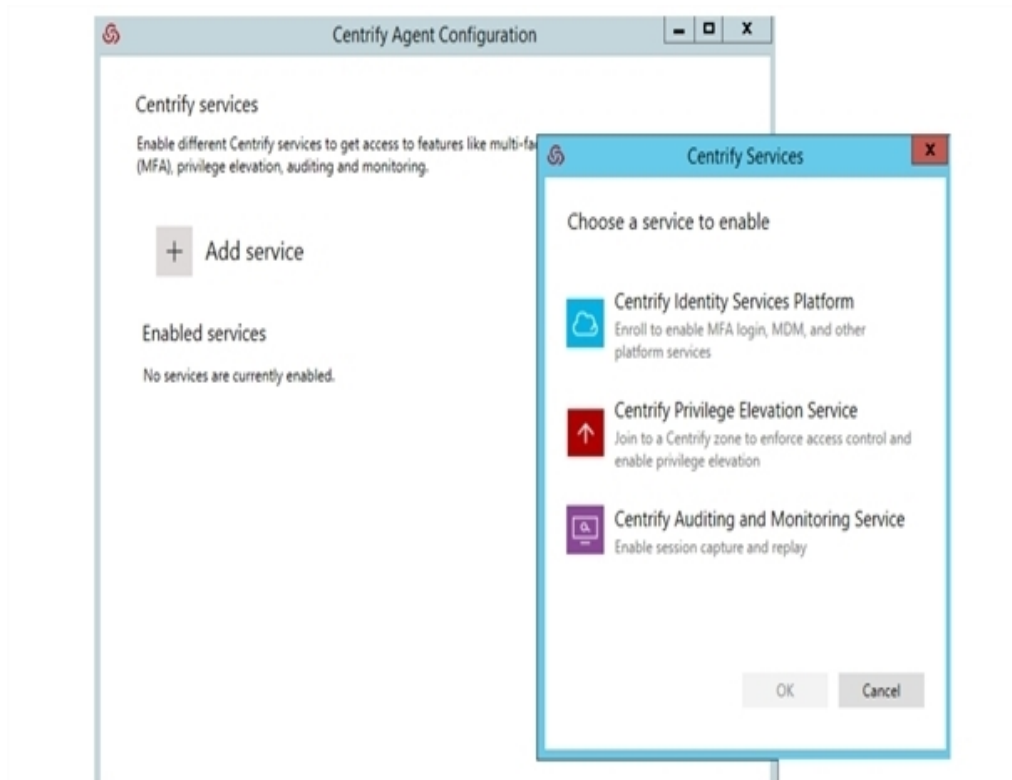
missing software. If you are installing silently from the command line or by using a Group Policy Object, you should verify the computers where you plan to install meet these requirements. If you are installing silently and a computer does not meet these requirements, the installation will fail.

## Installing interactively using the setup program

If you select auditing when you install the Windows agent, the agent starts capturing user session activity immediately after it is installed. Therefore, you should be sure that you have an installation, audit store database, and collector prepared and available before installing an agent. If the agent cannot connect to an installation, it stores the captured session data locally and can quickly overload the local computer's resources.

### To install the agent on Windows using the setup program:

1. Log on to the computer and insert the CD or browse to the location where you have saved downloaded Centrify files.  
If the Getting Started page is not displayed automatically, open the `autorun.exe` file.
2. On the Getting Started page, click **Agent** to start the setup program for the Windows agent.
3. At the Welcome page, click **Next**.
4. Review the terms of the license agreement, click **I accept the terms in the License Agreement**, then click **Next**.
5. Verify the location where files will be installed, then click **Next**.  
If you want to install in a location other than the default location, click **Browse**, select a different location, then click **Next**.
6. Click **Install**.
7. Click **Finish** to complete the installation and start the agent configuration wizard.
8. In the Centrify Agent Configuration window, click **Add Service**.



9. In the dialog box that opens, select the Centrify Auditing and Monitoring Service option and click **OK**.
10. In the Enable session capture and replay window, select the auditing installation to which you want the agent on this computer to connect.  
Click **Next** to continue.

The Centrify Auditing and Monitoring Service is now listed as an enabled service.

11. Close the Agent configuration window and click **Exit** in the installer window.

## Configuring the agent settings for auditing

The agent configuration wizard automatically configures several default settings in the agent registry. If you want to view or change the agent settings for auditing on a Windows computer after running the configuration wizard—or if you did not use the configuration wizard immediately after installation—you can use the Agent Configuration Wizard.

## To configure the agent settings for auditing:

1. Click **Start > All Programs > Centrifys Infrastructure Services 19.9 > Centrifys Agent for Windows Configuration > Agent Configuration**.
2. In the Centrifys Agent Configuration window, locate the Centrifys Auditing and Monitoring Service option, and click **Settings**.  
The Centrifys Auditing and Monitoring Service Settings window opens.
3. On the General tab, click **Configure**.
4. Select the maximum color quality for recorded sessions, then click **Next**.

If your audit installation has video capture auditing enabled, you can configure the color depth of the sessions to control the size of data that must be transferred over the network and stored in the database. A higher color depth increases the CPU overhead on audited computers but improves resolution when the session is played back. A lower color depth decreases network traffic and database storage requirements, but reduces the resolution of recorded sessions.

The default color quality is Low (8-bit).

5. Specify the offline data location and the maximum percentage of disk that the offline data file should be allowed to occupy, then click **Next**.

If the agent cannot connect to a collector, it saves session activity in the offline data location you specify until it can contact a collector.

The spool threshold defines the minimum percentage of disk space that should be available to continue auditing. It is intended to prevent audited computers from running out of disk space if the agent is sending data to its offline data storage location because no collectors are available.

For example, if you set this threshold to 10%, auditing will continue while spooling data to the offline file location as long as there's at least 10% disk space is available on the spool partition. When the disk space available reaches the threshold, auditing will stop until a collector is available.

The agent checks the spool disk space by periodically running a background process. By default, the background process runs every 15 seconds. Because of the delay between background checks, it is possible for the actual disk space available to fall below the threshold setting. If this were to occur, auditing would stop at the next interval. You can configure the interval for the background process to run by editing the



HKLM\Software\Centrify\DirectAudit\Agent\DiskCheckInterval registry setting.

6. Select the installation that the agent belongs to, then click **Next**.
7. If the computer where you're configuring an agent belongs to multiple audit stores in the auditing installation, choose which audit store this agent will connect to, then click **Next**.
8. In the Summary page, review your settings, then click **Next**.  
The agent is now configured and enabled for auditing.
9. Click **Finish** to close the agent configuration wizard, then click **Close** to exit the Centrify Auditing and Monitoring Service Settings window.

## Deciding to install with or without joining the computer to a zone

Before you begin a silent installation, you should decide whether you will wait until later to join the computer to a zone, or join the computer to a zone as part of the installation procedure.

### If you install without joining a zone during installation:

See [Installing silently by using the Microsoft Windows Installer](#) for details about the registry settings that you can configure manually after the installation finishes.

See [Installing silently without joining a zone](#) for details about performing the installation.

### If you install and join a zone during installation:

You use a transform (MST) file that is provided with Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service to configure a default set of agent-specific registry keys during the silent installation.

You can optionally edit the MST file before performing the installation to customize agent-specific registry settings for your environment.

You can optionally use the agent configuration control panel or the registry editor to configure registry settings after the installation finishes.



See [Installing silently by using the Microsoft Windows Installer](#) for details about the registry settings that you can configure by editing the MST file.

See [Installing silently by using the Microsoft Windows Installer](#) for details about how to edit the MST file before you perform the installation.

See [Installing and joining a zone silently](#) for details about performing the installation.

## Installing silently without joining a zone

This section describes how to install the agent silently without joining the computer to a zone. This procedure includes configuring registry settings manually using the registry editor or a third-party tool.

**Note:** To install the agent and join the computer to a zone during installation, see [Installing and joining a zone silently](#) for more information.

### Check prerequisites:

1. Verify that the computers where you plan to install meet the prerequisites described in [Verify prerequisites](#). If prerequisites are not met, the silent installation will fail.
2. If you are installing audit and monitoring service, verify that the following tasks have been completed:
  - a. Installed and configured the SQL Server management database and the SQL Server audit store database.
  - b. Installed and configured one or more collectors.
  - c. Configured and applied the Centrify DirectAudit Settings group policy that specifies the installation name.

### To install the Centrify Agent for Windows silently without joining the computer to a zone:

1. Open a Command Prompt window or prepare a software distribution package for deployment on remote computers.

For information about preparing to deploy software on remote computers, see the documentation for the specific software distribution product you



are using. For example, if you are using Microsoft System Center Configuration Manager (SCCM), see the Configuration Manager documentation.

2. Run the installer for the Centrify Agent for Windows package. For example:

```
msiexec /qn /i "Centrify Agent for windows64.msi"
```

By default, none of the services are enabled.

3. Use the registry editor or a configuration management product to configure the registry settings for each agent.

For example, under HKEY\_LOCAL\_

MACHINE\Software\Centrify\DirectAudit\Agent, you could set the DiskCheckThreshold key to a value other than the default value of 10%.

## To install the Centrify Agent for Windows and add a computer to a zone during installation:

1. Prepare a computer account in the appropriate zone using Access Manager or the PowerShell command `New-CdmManagedComputer`.
2. You will use the default transform file `Group Policy Deployment.mst` in Step 3 to update the MSI installation file so that the computer is joined to the zone in which it was pre-created in Step 1. You can optionally modify `Group Policy Deployment.mst` to change or add additional registry settings during installation.

If you want to edit `Group Policy Deployment.mst` to change or add additional registry settings and have not yet done so, edit it now as described in [Installing silently by using the Microsoft Windows Installer](#).

In order for the computer to join the zone from Step 1, the `Group Policy Deployment.mst` file must specify the `GPDeployment` property with a value of 1.

3. Run the following command:

```
msiexec /i "Centrify Agent for windows64.msi" /qn  
TRANSFORMS="Group Policy Deployment.mst"
```

## Installing and joining a zone silently

This section describes how to install the agent and join the computer to a zone at the same time. The procedure described here includes the following steps in addition to executing the MSI file:



- You first prepare (pre-create) the Windows computer account in the appropriate zone.

You execute an MST file together with the MSI file to join the computer to a zone and configure registry settings during the installation.

## Installing silently by using the Microsoft Windows Installer

If you want to perform a “silent” (also called *unattended*) installation of the Centrify Agent for Windows, you can do so by specifying the appropriate command line options and Microsoft Windows Installer (MSI) file to deploy. You must execute the commands on every Windows computer that you want to audit.

You can also use silent installation commands to automate the installation or upgrade of the Windows agent on remote computers if you use a software distribution product, such as Microsoft System Center Configuration Manager (SCCM), that enables you to run commands remotely to deploy software packages. However, only the command-line instructions are covered in this guide.

## Configuring registry settings

When you perform a silent installation, several registry settings specific to the agent are configured by the default MSI file. In addition, a default transform (MST) file is provided for you to use if you join the computer to a zone as part of the installation procedure. When executed together, the default MSI and MST files ensure that the computer is joined to a zone, and that a default set of agent-specific registry keys is configured.

If your environment requires different or additional registry settings, you can edit the MST file before performing an installation. Then, when you execute the MSI and MST files to perform an installation, your customized registry settings are implemented. For details about how to edit the MST file, see [Editing the default transform \(MST\) file](#).

**Note:** If you do not join the computer to a zone during installation, you do not use the MST file. In this situation, you can create or edit registry keys manually after the installation finishes by using the , or the registry editor.





The following table describes the agent-specific registry settings that are available for you to configure during installation (by using the MST file) or after installation (by using the or the registry editor). Use the information in this table if you need to configure registry settings differently than how they are configured by the default MSI and MST files. Keep the following in mind as you review the information in the table:

- The default MSI file is named `Centrify Agent for windows64.msi`, and is located in the **Agent** folder in the Centrify download location.
- The default MST file is named `Group Policy Deployment.mst`, and is located in the **Agent** folder in the Centrify download location.
- All of the settings in the following table are optional, although some are included in the default MSI and MST files so that they are configured when the MSI and MST files execute during an installation.
- Settings that are included in the default MSI and MST files are noted in the table.
- Some settings are environment-specific, and therefore do not have a default value. Others are not environment-specific, and do have a default value.
- The settings described in the table are located in the MSI file's Property table.
- The **Setting** column shows both the property name in the MSI file, and the name (in parentheses) of the registry key in the Windows registry.

Service	Setting	Description
Auditing and Monitoring	REG_MAX_FORMAT (MaxFormat)	<p>Specifies the color depth of sessions recorded by the agent.</p> <p>The color depth affects the resolution of the activity recorded and the size of the records stored in the audit store database when you have video capture auditing enabled. You can set the color depth to one of the following values:</p> <ul style="list-style-type: none"> <li>■ 0 to use the native color depth on an audited computer.</li> <li>■ 1 for a low resolution with an 8-bit color depth</li> <li>■ 2 for medium resolution with a 16-bit color depth (default)</li> <li>■ 4 for highest resolution with a 32-bit color</li> </ul> <p><b>This setting is included in the default MSI file.</b> In the registry, this setting is specified by a numeral (for example, 1). In the MSI file Property table, it is specified by the # character and a numeral (such as #1). The default value is 1.</p>
		<p>Specifies the minimum amount of disk space that must be available on the disk volume that contains the offline data storage file. You can change the percentage required to be available by modifying this registry key value.</p> <p><b>This setting is included in the default MSI file.</b> In the registry, this setting is specified by a numeral (for example, 1). In the MSI file Property table, it is specified by the # character and a numeral (such as #10). The default value is 10, meaning that at least 10% of the disk space on the volume that contains the offline data storage file must be available. If this threshold is reached and there are no collectors available, the agent stops spooling data and audit data is lost.</p>
Auditing and Monitoring	REG_SPOOL_DIR (SpoolDir)	<p>Specifies the offline data storage location.</p> <p>The folder location you specify will be where</p>

Service	Setting	Description
		<p>the agent saves (“spools”) data when it cannot connect to a collector.</p> <p><b>This setting is not included in the default MSI file.</b> To use it, you must edit the default transform (MST) file so that it is processed together with the MSI file during installation, or create it manually in the registry after the installation finishes.</p>
Auditing and Monitoring	REG_INSTALLATION_ID (InstallationId)	<p>Specifies the unique global identifier (GUID) associated with the installation service connection point.</p> <p><b>This setting is not included in the default MSI file.</b> To use it, you must edit the default transform (MST) file so that it is processed together with the MSI file during installation, or create it manually in the registry after the installation finishes.</p>
Auditing and Monitoring	REG_LOG_LEVEL_DA (LogLevel)	<p>Specifies what level of information, if any, is logged. Possible values are:</p> <ul style="list-style-type: none"> <li>■ off</li> <li>■ information</li> <li>■ warning</li> <li>■ error</li> <li>■ verbose</li> </ul> <p><b>This setting is included in the default MSI file.</b> The default value is <b>information</b>.</p>
Authentication & Privilege	REG_RESCUEUSERSIDS (RescueUserSids)	<p>Specifies which users have rescue rights. Type user SID strings in a comma separated list. For example:</p> <p><i>user1SID,user2SID,usersnSID</i></p> <p><b>This setting is not included in the default MSI file.</b> To use it, you must edit the default transform (MST) file so that the setting is processed together with the MSI file during installation, or create it manually in the registry after the installation finishes.</p>
Authentication & Privilege	REG_LOG_LEVEL_DZ (LoggingLevel)	<p>Specifies what level of information, if any, is logged. Possible values are:</p> <ul style="list-style-type: none"> <li>■ off</li> </ul>

Service	Setting	Description
		<ul style="list-style-type: none"> <li>■ information</li> <li>■ warning</li> <li>■ error</li> <li>■ verbose</li> </ul> <p><b>This setting is included in the default MSI file.</b> The default value is information.</p>
Authentication & Privilege	GPDeployment	<p>Specifies whether the computer is joined to the zone where the computer was pre-created. This setting is used only during installation and does not have a corresponding registry key. Possible values are:</p> <ul style="list-style-type: none"> <li>■ 0 - The computer is not joined to the zone.</li> <li>■ 1 - The computer is joined to the zone.</li> </ul> <p><b>This setting is included in the default transform (MST) file.</b> To use it, you must execute the MST file when you execute the default MSI file. The default value is 1, meaning that the pre-created computer is joined to the zone.</p>

## Editing the default transform (MST) file

The default transform file, `Group Policy Deployment.mst`, enables you to specify registry key settings that are different from the default settings that are defined in the MSI file. You can use the `Group Policy Deployment.mst` file to customize a silent installation for a specific environment.

If you want to customize the agent settings for your environment, you should edit the `Group Policy Deployment.mst` file before executing the command to perform a silent installation. If you want to use the default settings specified in the MSI file, you can skip this section and go directly to **Installing silently from the command line**.

You must use the Orca MSI editor to edit the `Group Policy Deployment.mst` file. Orca is one of the tools available in the Windows SDK. If you do not have the Windows SDK or Orca installed on your computer, you can download and install it from this location: [http://msdn.microsoft.com/en-us/library/aa370557\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/aa370557(v=vs.85).aspx).



## To edit the default MST file:

1. In the Agent folder in the Centrify download location, create a backup copy of the default `Group Policy Deployment.mst` file.
2. Open a Command Prompt window and execute the following command to launch Orca:  
`orca.exe`
3. In Orca, select **File > Open** and open the Centrify windows `Agent64.msi` file located in the Agent folder in the Centrify download location.
4. In Orca, select **Transform > Apply Transform**.
5. In Orca, navigate to the Agent folder in the Centrify download location and open `Group Policy Deployment.mst`.

The file is now in transform edit mode, and you can modify data rows in it.

6. In the Orca left pane, select the Property table.

Notice that a green bar displays to the left of “Property” in the left pane. This indicates that the Property table will be modified by the MST file.

The right pane displays the properties that configure registry keys when you execute the command to install the agent using the MSI file. Notice that the last property in the table, `GPDeployment`, is highlighted in a green box. This indicates that the `GPDeployment` property will be added to the MSI file by the MST file.

7. In the right pane, edit or add properties as necessary to configure registry keys for your environment.

Property	Description
REG_MAX_FORMAT	<p>Sets the <b>MaxFormat</b> registry key to specify the color depth of sessions recorded by the agent.</p> <p>The color depth affects the resolution of the activity recorded and the size of the records stored in the audit store database when you have video capture auditing enabled.</p> <p>In the MSI file Property table, you can set the color depth to one of the following values:</p> <ul style="list-style-type: none"> <li>■ #0 to use the native color depth on an audited computer.</li> <li>■ #1 for a low resolution with an 8-bit color depth.</li> <li>■ #2 for medium resolution with a 16-bit color depth.</li> <li>■ #4 for highest resolution with a 32-bit color.</li> </ul> <p>The default value is #1. To edit this property, double-click the Value column and type a new value.</p>
REG_DISK_CHECK_THRESHOLD	<p>Sets the <b>DiskCheckThreshold</b> registry key to specify the minimum amount of disk space that must be available on the disk volume that contains the offline data storage file.</p> <p>In the MSI file Property table, the default value is #10, meaning that at least 10% of the disk space on the volume that contains the offline data storage file must be available. You can change the percentage required to be available. To edit this property, double-click the Value column and type a new value.</p>
REG_SPOOL_DIR	<p>Sets the <b>SpoolDir</b> registry key to specify the offline data storage location.</p> <p>The folder location you specify will be where the agent saves data when it cannot connect to a collector.</p> <p>To add a this property to the transform file, right-click anywhere in the property table, then select <b>Add Row</b>.</p>

Property	Description
REG_INSTALLATION_ID	<p>Sets the <code>InstallationId</code> registry key to specify the unique global identifier (GUID) associated with the installation service connection point.</p> <p>This property is not required if you are using the Installation group policy to identify the audit installation to use. If you are not using group policy to identify the audit installation, you can add a this property to the transform file. Right-click anywhere in the property table, then select <b>Add Row</b> to add the property and value to the file.</p>
REG_LOG_LEVEL_DA	<p>Sets the <code>LogLevel</code> registry key to specifies what level of information, if any, is logged. Possible values are:</p> <ul style="list-style-type: none"> <li>■ <code>off</code></li> <li>■ <code>information</code></li> <li>■ <code>warning</code></li> <li>■ <code>error</code></li> <li>■ <code>verbose</code></li> </ul> <p>The default value is <code>information</code>. To edit this property, double-click the Value column and type a new value.</p>

- After you have made the necessary modifications, select **Transform > Generate Transform** to save your modifications to the default MST file. Be sure to save the MST file in the same folder as the MSI file. If the MST and MSI files are in different folders, the MST file will not execute when you execute the MSI file.

The MST file is now ready to be used as described in [Installing silently from the command line](#).

## Installing silently from the command line

If you want to perform a “silent” or unattended installation of the Centrify Agent for Windows, you can do so by specifying the appropriate command line options and Microsoft Windows Installer (MSI) file to deploy.

Before running the installation command, you should verify the computers where you plan to install meet the prerequisites described in [Verify prerequisites](#). If the prerequisites are not met, the silent installation will fail. You should have also completed the following tasks:

- Installed and configured the SQL Server management database and the SQL Server audit store database.
- Installed and configured one or more collectors.



- Configured and applied the Centrify DirectAudit Settings group policy that specifies the installation name.

You can use similar steps to install the Centrify Common Component using the `Centrify Common Component64.msi` file before you install the agent. If you install the common component first, information about the agent installation is recorded in a log file for troubleshooting purposes. However, you are not required to install the common component separately from the agent.

## To install the Centrify Agent for Windows silently:

1. Open a Command Prompt window or prepare a software distribution package for deployment on remote computers.
2. Run the installer for the Centrify Agent for Windows package for a 64-bit architecture with the appropriate command line options.

For example, to install the Centrify Common Component on a computer with 64-bit architecture, run the following command:

```
msiexec /i "Centrify Common Component64.msi" /qn
```

If you want to enable both auditing and access control features on a computer with a 64-bit operating system and use the values defined in the `Group Policy Deployment.mst` file, you would run the following command:

```
msiexec /i "Centrify windows Agent64.msi" /qn TRANSFORMS="Group Policy Deployment.mst"
```

## Installing from a central location by using group policy

You can use a Group Policy Object (GPO) to automate the deployment of Centrify Agents for Windows. Because automated installation fails if all the prerequisites are not met, be sure that all the computers on which you intend to install meet the requirements described in [Verify prerequisites](#).

You can use similar steps to install the Centrify Common Component using the `Centrify Common Component64.msi` file before you install the agent. If you install the common component first, information about the agent installation is recorded in a log file for troubleshooting purposes. However, you are not required to install the common component separately from the agent.

In most cases, you can use the default agent settings defined in the `Group Policy Deployment.mst` transform file. If you want to modify the





default settings prior to installation, see the instructions in [Installing silently by using the Microsoft Windows Installer](#).

## To create a Group Policy Object for the deployment of Centrify Agents for Windows:

1. Copy the Centrify windows Agent64.msi and Group Policy Deployment.mst files to a shared folder on the domain controller or a location accessible from the domain controller.

When you select a folder for the files, right-click and select **Share with > Specific people** to verify that the folder is shared with Everyone or with appropriate users and groups.

2. On the domain controller, click **Start > Administrative Tools > Group Policy Management**.
3. Select the domain or organizational unit that has the Windows computers where you want to deploy the Centrify agent, right-click, then select **Create a GPO in this domain, and Link it here**.

For example, you might have an organizational unit specifically for Centrify-managed Windows computers. You can create a group policy object and link it to that specific organizational unit.

4. Type a name for the new Group Policy Object, for example, Centrify Agent Deployment, and click **OK**.
5. Right-click the new Group Policy Object and click **Edit**.
6. Expand **Computer Configuration > Policies > Software Settings**.
7. Select **Software installation**, right-click, and select **New > Package**.
8. Navigate to the folder you selected in Step 1, select the Centrify windows Agent64.msi file, and click **Open**.
9. Select **Advanced** and click **OK**.
10. Click the **Modifications** tab and click **Add**.
11. Select the Group Policy Deployment.mst file, click **Open**, and click **OK**.
12. Close the Group Policy Management Editor, right-click the Centrify Agent Deployment group policy object, and verify that **Link Enabled** is selected.

By default, when computers in the selected domain or organizational unit receive the next group policy update or are restarted, the agent will be



deployed and the computer will be automatically rebooted to complete the deployment of the agent.

If you want to test deployment or deploy immediately, you can open a Command Prompt window to log on to a Windows client as a domain administrator and force group policies to be updated immediately by running the following command:

```
gpupdate /force
```

After installation, all of the registry settings that were specified in the MSI and MST files are configured. If you need to change any of the default agent settings, open the DirectAudit Agent Control Panel or the Registry Editor.

For more information about how to configure and use Group Policy Objects, see the documentation on the Microsoft Windows website.

## Installing the Audit Management Server

It's a best practice to install the Audit Management Server after you've installed your audit stores, audit store databases, and installed your collectors. You can install the Audit Management Server either on a new computer or one where you've installed a collector.

### To install the Audit Manager Server:

1. Log on using an Active Directory domain account.
2. Open the ISO file, and navigate to the following folder:  
    \DirectAudit\Audit Management Server\  
3. Run the Audit Management Server installer : Centrif y DirectAudit  
    Audit Management Server64.exe.
4. At the Welcome page, click **Next**.
5. Review the terms of the license agreement, click **I accept the terms in the license agreement**, then click **Next**.
6. On the Destination Folder page, review the installation location and click **Next** to continue.
7. If you want to install the console in a different location, click **Change** and navigate to the desired folder.
8. Click **Install** to begin the installation.



9. The installer installs the necessary files. To open the console, keep the **Run Audit Management Configuration Wizard** option selected. Otherwise, deselect the option.
10. Click **Finish** to close the installer.

## Configuring the Audit Management Server

By default, when you finish installing the Audit Management Server, the installer opens the Audit Management Server Configuration Wizard.

### To configure the Audit Management Server:

1. On the first page, select the installation for which you want to configure the Audit Management Server.  
  
If you have one installation, it's already selected.  
  
Click **Next** to continue.
2. On the Authentication Type page, specify which kind of authentication that the Audit Management Server will use. The choices are:
  - **Windows Authentication:** Specify the computer account that will run the Audit Management Server.
  - **SQL Server Authentication:** Specify the SQL Server user name and password to use. Click Test Connection to make sure that the login credentials work.  
Click **Next** to continue.
3. On the Summary page, review the Audit Management Server configuration details, and click **Next** to continue.
4. Click **Finish** to close the configuration wizard.

## Enabling or disabling auditing on Windows computers

You enable or disabling auditing for a Windows computer by adding or removing the audit and monitoring service from the agent configuration.



## To enable auditing on a Windows computer:

- Use the Agent Configuration wizard to configure the Centrify Agent for Windows to connect to the Centrify Audit & Monitoring Service.

The agent configuration wizard runs automatically after you've installed the Centrify Agent for Windows.

## To disable auditing on a Windows computer:

- In the Centrify Agent Configuration window, select Centrify Audit & Monitoring Service and click **Remove**.

To enable or disable video capture editing for an entire installation, see [Enabling or disabling video capture auditing](#). To enable or disable auditing on a per-user basis you can use a group policy and the audited user list and non-audited user lists. For details, see the Group Policy Guide.

## Installing an Centrify Agent for \*NIX

You can install the auditing services for Linux or UNIX computers interactively the agent installation script, `install.sh`. If you want to run the installation script silently or use a native package manager to install UNIX agents, see [Installing the UNIX agent on remote computers](#).

The steps in this section describe how to install interactively using the `install.sh` script, which automatically installs platform-specific software packages and invokes the proper installation mechanism and options for a computer's operating system.

## To install the agent using the installation script:

1. Log on as a user with root privileges.
2. Mount the cdrom device using the appropriate command for the local computer's operating environment, if necessary.

**Note:** If you are not using the CD, verify the location and go on to the next step.



3. Change to the appropriate directory.

For example, to install on an AIX computer from the Centrifify CD or ISO file, change to the UNIX directory:

```
cd Agent_Unix22
```

4. Run the installer and respond to its questions:

```
./install.sh
```

If there is an installation with the name `DefaultInstallation`, the UNIX agent uses it by default. If you are using an installation with a name other than `DefaultInstallation`, you must identify the installation by using `dacontrol` or group policy after installing the agent. For more information, see [Checking the status of the UNIX agent](#).

5. After installing the package, use `dainfo` to verify that the agent is installed and running. You should see output similar to the following that indicates the agent is `Online`:

```
Pinging adclient:  adclient is available
```

```
Daemon status:      Online
```

```
Current installation: 'PistolassF' (configured locally)
```

```
Current collector: DC2008r2-LG.pistolas.org:5063:HOST/dc2008r2-  
1g@PISTOLAS.ORG ...
```

If the output of `dainfo` indicates that the agent is `Offline` or that auditing is not enabled, verify your network connections and try restarting the auditing service or run the command to enable auditing manually as described in [Enabling and disabling auditing on Linux and UNIX computers](#).

You must adjust the disk space requirements higher if you allocate a large amount of offline storage to use when none of the collectors servicing the audit store can be reached. This and other parameters are in a text file named `centrifida.conf` in `/etc/centrifida` on each audited computer that has the UNIX agent installed. For more information about setting configuration parameters, see [Configuring the UNIX agent off-line database](#). For information about all of the configuration parameters available to customize auditing, see the *Configuration and Tuning Reference Guide*.

## Enabling and disabling auditing on Linux and UNIX computers

After you install the agent, you can enable auditing with the `dacontrol` command. The `dacontrol` command links all shells to the `cdash` shell wrapper



by way of NSS. When a user opens a terminal, `cdash` is automatically loaded instead of the user's shell, then `cdash` loads the appropriate shell for the user and begins auditing the session.

## To enable auditing on a Linux or UNIX computer:

1. Log on as a user with root privileges.
2. Run `dacontrol` with the `-e` option:
3. Run `dacontrol` again to verify that auditing has been enabled.

For example:

```
dacontrol --query
```

```
This machine has been configured through group policy to use  
installation 'DefaultInstallation'
```

```
DirectAudit NSS module: Active
```

```
DirectAudit is not configured to audit individual commands.
```

After you enable auditing on a Linux or UNIX computer, you can control whether the auditing of shell activity applies for all users or for selected users by using role assignments. If auditing is enabled and the agent is not running, users with an active role assignment that requires logging are not allowed to log in.

For more information about configuring and assigning roles, see the *Administrator's Guide for Linux and UNIX*.

## Installing additional Audit Manager or Audit Analyzer consoles

If you need to make Audit Manager or Audit Analyzer consoles available to other users, you can install additional consoles on other computers. For example, install Audit Analyzer on computers used by auditors in your organization.

## Checklist for auditing systems outside of Active Directory

Here is the overall process for auditing a computer that isn't joined to Active Directory, including links to documented procedures.

Step #	Actions	Details
<b>Create the audit installation</b>		
1	For the audit store that includes the collector that you will enroll to the Centrify Cloud Platform, edit the audit store scope so that it includes the following: <ul style="list-style-type: none"> <li>■ The site or subnet that the collector is in</li> <li>■ The IP address or subnet of the system to be audited (the one that isn't in Active Directory)</li> </ul>	<a href="#">Creating a new installation</a>
<b>Add the audit installation to the Admin Portal and enable auditing</b>		
2	Install a connector on a Windows computer in the Active Directory domain  Note: For now, do not install a connector on the same computer as a collector.	"How to install a connector" in the Privileged Access Service help ( <a href="https://docs.centrify.com">docs.centrify.com</a> )
3	In the Admin Portal, enable auditing for the audit installation.	"Enabling auditing for remote sessions" in the Privileged Access Service help ( <a href="https://docs.centrify.com">docs.centrify.com</a> )
4	Verify the connector status in the Admin Portal.	"Reference content - Connector configuration program" in the Privileged Access Service help ( <a href="https://docs.centrify.com">docs.centrify.com</a> )
<b>Configure the collector</b>		
5	On the computer where the collector is or will be, install the Centrify client and enroll the computer in the cloud platform.  The collector needs to be joined to Active Directory and enrolled in the cloud platform.	"Installing and using the Centrify Client for Windows" in the Privileged Access Service help ( <a href="https://docs.centrify.com">docs.centrify.com</a> )

Step #	Actions	Details
6	Install a new collector or reconfigure an existing collector so that the collector receives audit data according to the cloud settings.	<a href="#">Configure the audit collector service</a>
<b>Configure the computer to be audited</b>		
7	In the Admin Portal, download the Centrify Client installers and get an enrollment code	<p>"Installing and using the Centrify Client for Windows" in the Privileged Access Service help (<a href="https://docs.centrify.com">docs.centrify.com</a>)</p> <p>"Enrolling and managing computers using Centrify Clients for Linux" in the Privileged Access Service help (<a href="https://docs.centrify.com">docs.centrify.com</a>)</p> <p>"Enrolling a computer" in the Privileged Access Service help (<a href="https://docs.centrify.com">docs.centrify.com</a>)</p>
8	In the Admin Portal, make sure that the user account you'll use to run the installer has the permissions to enroll the system.	"Admin Portal administrative rights" in the Privileged Access Service help ( <a href="https://docs.centrify.com">docs.centrify.com</a> )
9	On the computer to be audited, make sure that its DNS setting are set so that it can contact and be contacted by the collector computer.	On the computer to be audited, make sure that its DNS settings are set so that it can contact the collector computer by its fully qualified domain name (FQDN).
10	Install the client and enroll the computer in the cloud platform.	<p>"Installing and using the Centrify Client for Windows" in the Privileged Access Service help (<a href="https://docs.centrify.com">docs.centrify.com</a>)</p> <p>"Enrolling and managing computers using Centrify Clients for Linux" in the Privileged Access Service help (<a href="https://docs.centrify.com">docs.centrify.com</a>)</p>
11	In the Admin Portal, verify the enrollment.	In the Admin Portal, go to Resources > Systems to verify the enrollment status.
12	Install the audit client package(s): <ul style="list-style-type: none"> <li>■ Windows: Install the Windows audit package.</li> <li>■ Linux: First install the OpenSSL package, and then install the Linux audit package..</li> </ul>	"Downloading the audit packages for the Centrify Clients" in the Privileged Access Service help ( <a href="https://docs.centrify.com">docs.centrify.com</a> )
13	In Audit Manager, verify that the computer is being audited.	<a href="#">Managing audited computers and agents</a>



## Auditing systems that are inside a DMZ

If you have Windows or UNIX/Linux systems that are deployed inside of a networking DMZ, you can audit those systems without having to set up a separate audit installation.

Organizations often use a DMZ to host a group of systems in a section of the corporate network in between the intranet and the public internet access. Firewall settings define the perimeter of the DMZ; the firewall helps limit access to internal networks from the outside network.

In order to audit systems inside of a DMZ, the following must be true for your deployment:

- All the Windows or UNIX/Linux systems in the DMZ are joined to the DMZ domain (for example, `acme.dmz`).
- You've already set up the audit installation in your main domain for your organization (for example, `acme.corp`) and you're auditing systems in that domain.
- The SQL Server that hosts the audit databases is also joined to the main domain.
- There's either no Active Directory trust between the main and DMZ domains or there's a one-way trust where the DMZ domain trusts the main domain (for example, `acme.dmz` trusts `acme.corp`).
- All the audit administrator and auditor accounts belong to the main domain.

Before you go to set up auditing on DMZ systems, be sure to do the following:

- Deploy at least one audit collector on a system that's joined to the DMZ domain. This is because an audited system can only look for audit collectors in its own forest.
- Configure the SQL Server to use mixed-mode authentication. This is because a collector in a DMZ cannot authenticate with SQL Server in the main domain using Windows authentication.
- Configure the necessary firewall exceptions for the SQL Server deployed in the main domain so that the audit collector in the DMZ can connect to the SQL Server. This includes the firewall exceptions for the SQL Server listener port as well as other ports, such as UDP 1434 (which is used by the SQL browser service).

## To audit systems in a DMZ:

### 1. Prepare the audit store:

- a. Set up an audit store that contains the audited data for the systems in the DMZ. You can either create a new audit store or modify an existing one so that the audit store scope includes the sites or subnets of the systems in the DMZ.
- b. Add a new audit store database to the DMZ audit store and mark the database as active.

For more information, see [Creating the first audit store](#).

### 2. Prepare the SQL authentication account:

- a. In Audit Manager, right-click the audit store database that you just created and select **Properties**.
- b. In the Advanced tab, under the Allowed incoming collectors, click **Add**.
- c. For the authentication, select **SQL Server authentication**. Select an existing account or click the list to create a new SQL Login account.

This SQL Login account is what the collectors in the DMZ domain will use to authentication with the SQL Server in the main domain. As a best practice, it's recommended to create a dedicated incoming collector account for all collectors in the DMZ.

### 3. Publish the audit installation information to the DMZ domain:

- If there's a one-way trust between the DMZ and main domains:
  - a. In Audit Manager, right click the installation name and click **Properties**.
  - b. In the Publication tab, click **Add**.
  - c. Select an OU or container in the DMZ domain to which you'll publish the audit installation information. Click **OK** to continue, and click **OK** again to close the dialog box and publish the audit installation information to the DMZ.

For more information, see [Publishing installation information](#).

- If there's no trust between the DMZ and main domains:
  - a. In Audit Manager, right-click the installation name and click **Properties**.



- b. In the Publication tab, click **Export** to export the audit installation information to an LDIF file.
- c. Provide the LDIF file to the Active Directory administrator of the DMZ domain and request that they manually import the file into an OU or container in the DMZ domain. They can import the LDIF file using the LDIFDE.exe utility.

For more information, see [Exporting installation information](#).

4. Install a collector on at least one Windows system in the DMZ:
  - a. Run the Collector Configuration wizard, and select the audit installation and specify the port number.
  - b. In the Authentication type screen, select **SQL Server authentication** and enter the credentials for the SQL authentication account that you created earlier.
  - c. Click **Test Connection** to ensure that the credentials work and the SQL Server is reachable.
  - d. Finish the rest of the wizard. If there are any warnings when validating the permissions, you can safely ignore them.

If you login to the collector computer as a user from your DMZ domain, that user will most certainly not have the permissions to connect to the audit installation and, as a result, the Collector Configuration wizard (which runs in context of the logged-in user) may fail to validate certain permissions and show warning messages instead.

For details about configuring a collector, see [Installing the audit collectors](#).

5. Install and configure the agent on the systems in the DMZ.

For details, see [Installing the Centrify Agent for Windows](#).

# Managing an installation

This chapter describes how to secure and manage an audit installation after the initial deployment of Centrify software. It includes tasks that are done by users assigned the Master Auditor role for an installation and users who are Microsoft SQL Server database administrators.

The following topics are covered:

Securing an installation .....	93
Configuring selective auditing .....	98
Configuring agents to prefer collectors .....	100
Audit license enforcement .....	101
Enabling audit notification .....	102
Enabling or disabling video capture auditing .....	103
Preventing users from reviewing or deleting sessions .....	104
Adding an installation .....	105
Publishing installation information .....	106
Removing or deleting an installation .....	108
Managing audit store databases .....	108
Managing audit stores .....	119
Managing the audit management database .....	122
Maintaining database indexes .....	125
Managing collectors .....	126
Managing audited computers and agents .....	128
Delegating administrative permissions .....	130
Managing audit roles .....	131

## Securing an installation

For production deployments, you can take the following steps to secure the installation:

- Use the Installation group policy to specify which installation agents and collectors are part of. By enabling the Installation group policy you can prevent local administrators from configuring a computer to be part of an unauthorized installation.
- Configure a trusted group of collectors to prevent a hacker from creating a rogue collector to collect data from agents.
- Configure a trusted group of agents to prevent a hacker from performing a Denial of Service attack on the collector and database by flooding a collector with bogus audit data.
- Encrypt all data sent from the collector to the database.

Before you can follow these steps to secure an installation, you must have access to an Active Directory user account with permission to create Active Directory security groups, enable group policies, and edit Group Policy Objects.

### To secure an installation using Windows group policy:

1. Open the Group Policy Management console.
2. Expand the forest and domains to select the Default Domain Policy object.
3. Right-click, then click **Edit** to open Group Policy Management Editor.
4. Expand **Computer Configuration > Policies > Centrify Audit Settings**, then select **Common Settings**.
5. Double-click the **Installation** policy in the right pane.
6. On the Policy tab, select **Enabled**.
7. Click **Browse** to select the installation you want to secure, then click **OK**.
8. Click **OK** to close the Installation properties.

## Securing an audit store with trusted collectors and agents

By default, audit stores are configured to trust all audited computers and collectors in the installation. Trusting all computers by default makes it easier



to deploy and test auditing in an evaluation or demonstration environment. For a production environment, however, you should secure the audit store by explicitly defining the computers the audit store can trust.

You can define two lists of trusted computers:

- Audited computers that can be trusted.
- Collector computers that can be trusted.

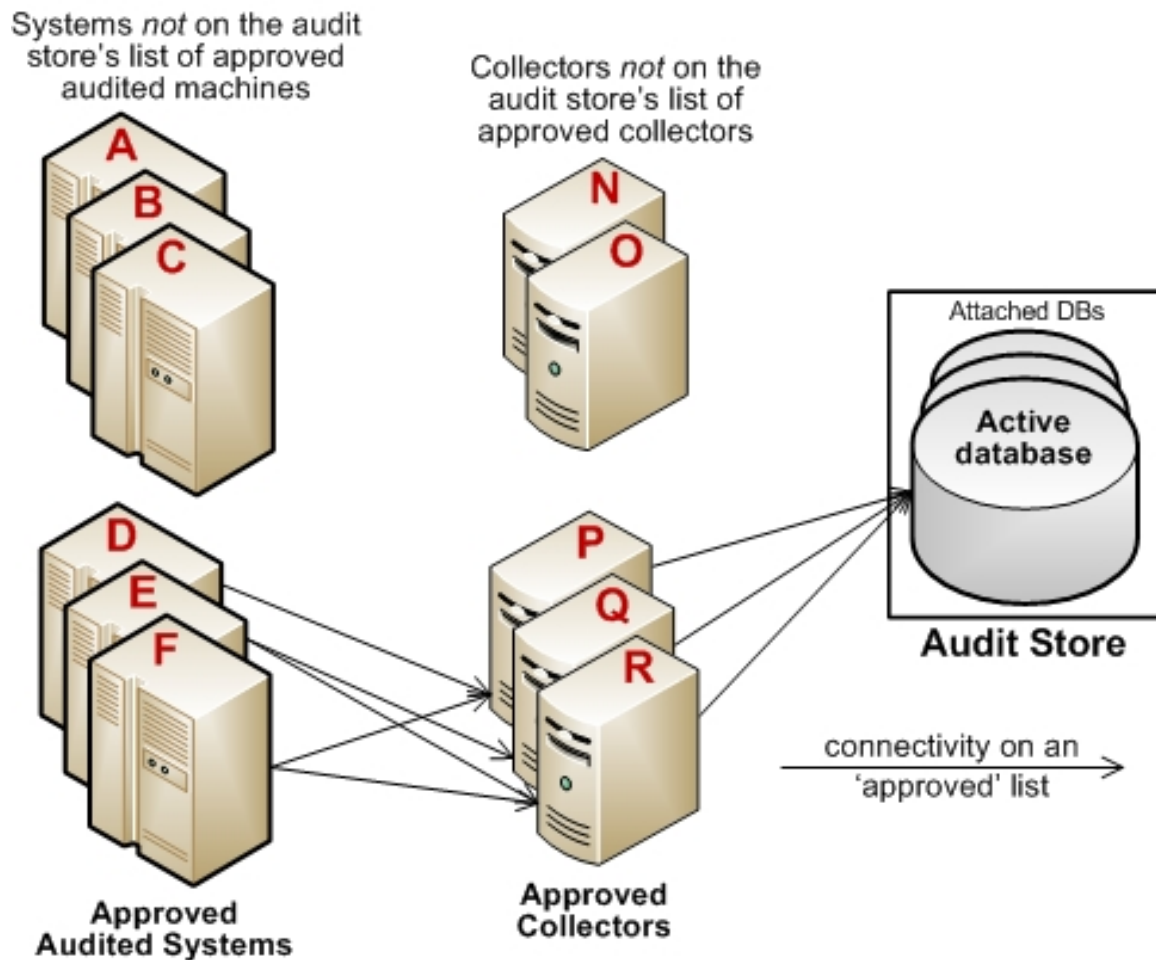
## To secure an audit store:

1. Open the Audit Manager console.
2. Expand the installation and Audit Stores nodes.
3. Select the audit store you want to secure, right-click, then select **Properties**.
4. Click the **Advanced** tab.
5. Select **Define trusted Collector list**, then click **Add**.
6. Select a domain, click **OK**, then search for and select the collectors to trust and click **OK** to add the selected computers to the list.

Only the collectors you add to the trusted list are allowed to connect to the audit store database. All other collectors are considered untrusted and cannot write to the audit store database.
7. Select **Define trusted Audited System list**, then click **Add**.
8. Select a domain, click **OK**, then search for and select the audited computers to trust and click **OK** to add the selected computers to the list.

Only the audited computers you add to the trusted list are allowed to connect to the trusted collectors. All other computers are considered untrusted and cannot send audit data to trusted collectors.
9. Click **OK** to close the audit store properties dialog box.

The following example illustrates the configuration of trusted collectors and trusted audited computers.



In this example, the audit store trusts the computers represented by P, Q, and R. Those are the only computers that have been identified as trusted collectors in the audit store Properties. list. The audit store has been configured to trust the audited computers represented by D, E, and F. As a result of this configuration:

- Audited computers D, E, and F only send audit data to the trusted collectors P, Q, and R.
- Trusted collectors P, Q, and R only accept audit data from the trusted audited computers D, E, and F.
- The audit store database only accepts data for its trusted collectors P, Q, and R, and therefore only stores audit data that originated on the trusted audited computers D, E, and F.

## Disabling a trusted list

After you have added trusted collectors and audited computers to these lists, you can disable either one or both lists at any time to remove the security restrictions. For example, if you decide to allow auditing data from all audited



computers, you can open the audit store properties, click the Advanced tab, and deselect the **Define trusted Audited System list** option. You don't have to remove any computers from the list. The audit store continues to only accept data from trusted collectors.

## Using security groups to define trusted computers

You can use Active Directory security groups to manage trusted computer accounts. For example, if you create a group for trusted audited computers and a group for trusted collectors, you can use those groups to define the list of trusted collectors and audited computers for the audit store. Any time you add a new computer to one of those groups, thereafter, it is automatically trusted, without requiring any update to the audit store properties.

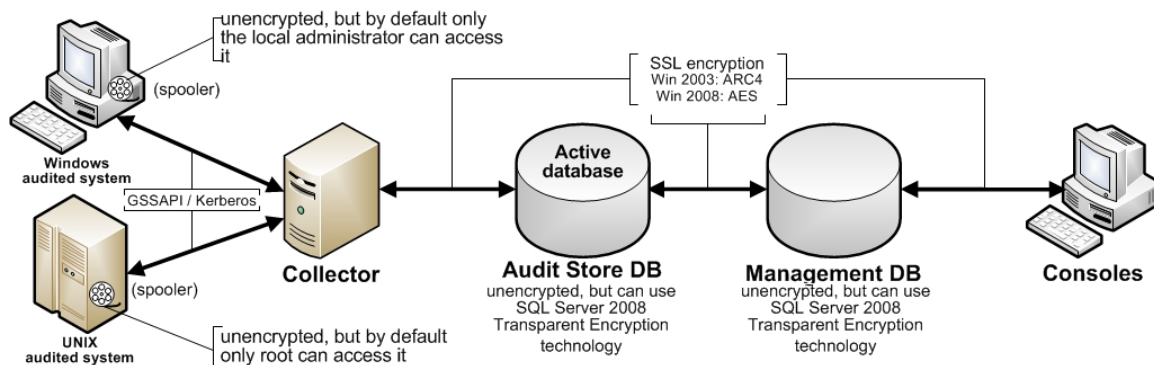
## Securing network traffic with encryption

The last step in securing an installation is to secure the data collected and stored through encryption. The following summarizes how data is secured as it moves from component to component:

- Between an audited computer and the spooler that stores the data locally when no collectors are available, audit data is not encrypted. Only the root user or local Administrator account can access the data by default.
- Between the audited computer's data collection service (dad on UNIX or wdad on Windows) and the collector, data is secured using Generic Security Services Application Program Interface (GSSAPI) with Kerberos encryption.
- Between the collector and the audit store database, data can be secured using Secure Socket Layer (SSL) connections and ARC4 or AES encryption if the database is configured to use SSL connections.
- Between the audit store and management databases, data can be secured using Secure Socket Layer (SSL) connections and ARC4 or AES encryption if the database is configured to use SSL connections.
- Between the management database and the Audit Manager console, data can be secured using Secure Socket Layer (SSL) connections and ARC4 or AES encryption if the database is configured to use SSL connections.

The following illustration summarizes the flow of data and how network traffic is secured from one component to the next.





## Enabling Secure Socket Layer (SSL) communication

Although the database connections can be secured using SSL, you must configure SSL support for Microsoft SQL Server as part of SQL Server administration. You must also have valid certificates installed on clients and the database server. If you are not the database administrator, you should contact the database administrator to determine whether encryption has been enabled and appropriate certificates have been installed. For more information about enabling SSL encryption for SQL Server and installing the required certificates, see the following Microsoft support article:

<https://support.microsoft.com/en-us/help/316898/how-to-enable-ssl-encryption-for-an-instance-of-sql-server-by-using-mi>

## Enabling encryption for Microsoft SQL Server Express

If you use Microsoft SQL Server Express, encryption is turned off by default. To secure the data transferred to the database server, you should turn encryption on.

## To enable encryption for each audit store and management database:

1. Log on to the computer hosting an audit store or management database with an account that has database administrator authority.
2. Open **SQL Server Configuration Manager**.
3. Select the SQL Server Network Configuration node, right-click **Protocols for DBINSTANCE**, then select **Properties**.
4. On the **Flags** tab, select **Yes** for the **Force Encryption** option, then click **OK** to save the setting.

## Using a service account for Microsoft SQL Server

When you install Microsoft SQL Server, you specify whether to use Windows authentication or a mix of Windows and SQL Server authentication. You also specify the accounts that the database services should use. By default, system accounts are used. If SQL Server uses a domain user account instead of a system account, you should ensure that the account has permission to update the SQL Server computer object in Active Directory. If the account has permission to update the computer where SQL Server is running, SQL Server can publish its service principal name (SPN) automatically. Getting the correct service principal name is important because Windows authentication relies on the SPN to find services and audit and monitoring service uses Windows authentication for console-to-audit management database connections. If the SPN is not found, the connection between the console and audit management database fails.

The audit management database-to-audit store connection and the collector-to-audit store connection can use either Windows authentication or SQL Server authentication. If SQL Server authentication is used, it does not matter whether the SQL Server instance uses a system account or a service account. If you have configured SQL Server to use Windows authentication only, be sure that the Windows account is allowed to connect to the audit management database and to the audit store database.

If the domain user account running SQL Server services does not have permission to update the computer object, see the following Microsoft knowledge base article for information about how to manually register the SPN for SQL Server:

<https://support.microsoft.com/en-us/help/909801/how-to-make-sure-that-you-are-using-kerberos-authentication-when-you-c>

## Configuring selective auditing

By default, the agent captures activity for all users on audited computers, but you can limit auditing to specified users. If you are using authentication and privilege elevation, you can control auditing by configuring role definitions with different audit requirements then assigning those role definitions to different sets of Active Directory users.

If you are using the Centrify Audit & Monitoring Service without access management:



- You can use group policies to specify which Windows users to audit and which Windows users should not be audited.

For information about configuring group policies to customize auditing, see the *Group Policy Guide*.

- For UNIX users, you can use the `dash.user.skiplist` configuration parameter to specify the UNIX user accounts and Active Directory UNIX names that you don't want to audit.

For more information about setting the `dash.user.skiplist` parameter, see the comments in the `/etc/centrifyda/centrifyda.conf` file. For information about all of the configuration parameters available to customize auditing, see the *Configuration and Tuning Reference Guide*.

## To control auditing by using group policies:

1. Open the Group Policy Management console.
2. Expand the forest and domains to select the Default Domain Policy object.
3. Right-click, then click **Edit** to open Group Policy Management Editor.
4. Expand **Computer Configuration > Policies > Centrify Audit Settings**, then select **Windows Agent Settings**.

5. Select the Audited user list policy and change the policy setting from Not Configured to **Enabled**, then click **Add** if you want to identify specific users to audit.

When you enable this group policy, only the users you specify in the policy are audited. If this policy is not configured, all users are audited.

6. Select the Non-audited user list policy and change the policy setting from Not Configured to **Enabled**, then click **Add** if you want to identify specific users that should not be audited.

When you enable this group policy, only the users you specify are not audited. If this policy is not configured, all users are audited. If you enable both the Audited user list and the Non-audited user list policies, the users you include in the Non-audited user list take precedence over the Audited user list.

The following table details the effect of choosing to enable the Audited user list policy, the Non-audited user list policy, or a combination of both policies.

Non-audited user list	Audited user list	How the setting affects auditing
Not configured	Not configured	No users are defined for either policy, so all users accessing audited computers are audited.
Not configured	Enabled	Only the users you specify in the Audited user list policy are audited. If you do not specify any users when you enable this policy, no users are audited.
Enabled	Not configured	Only the users you specify in the Non-audited user list are exempt from auditing. If you enable this policy but do not specify any users, no users are exempt from auditing. All users are audited.
Enabled	Enabled	If both policies are enabled, the non-audited user takes precedence over the audited list of users.
		If a user is specified in the audited list, that user is explicitly audited.
		If a user is specified in the non-audited list, that user is explicitly not audited.  If the same user is specified in both lists or no users are specified for either policy, no users are audited because the non-audited user takes precedence.

## Configuring agents to prefer collectors

If desired, you can specify that agents first use the collectors that are in the same site as the agent. You configure this option for each audit store.

For example, consider the following installation setup:

- One audit store
- Two sites (SantaClara and SanDiego)
- Two collectors in SantaClara, and two collectors in SanDiego

If you enable the option for the agents to prefer collectors in the same site as the agent, the agents in the SantaClara site use the collectors in that site, and the agents in the SanDiego site use the collectors there.

If for some reason all collectors in a site are down, the agents use collectors in another site or configured subnet.

Once an agent fails over and uses a collector in another site, the agent continues to use that collector until a rebinding occurs. You can do a rebinding



with the `dareload -b` command. During the time that the agent is using a collector in another site, `dadiag` displays a warning message.

If your installation uses agents older than version 2017, those older agents ignore the collector preference setting.

## To specify agents use collectors in the same site:

1. Open the Audit Manager console window.
2. Expand **Audit Stores**, and right-click the desired audit store and select **Properties**.
3. In the Audit Store Properties dialog box, click **Advanced**.
4. Select **Agents must prefer collectors in the same site as the agent**.  
By default, this option is not enabled.
5. Click **OK** to save the changes.

It may take several minutes for the changes to take effect, depending on Active Directory replication delays and policy sets.

## Audit license enforcement

Any time you open the Audit Manager console, Audit Analyzer console, or the session player, a background process determines the availability of audit licenses. Only the audited computers that are currently connected to a collector are included in the license count to determine license usage and compliance. Computers that have been previously audited and have data in the audit store database but are not currently connected to a collector and haven't been connected to a collector for over 45 days are not included in the license count.

As you increase the number of licenses in use, license enforcement is progressive. If the number of audited computers is less than 90% of the number of licenses you have purchased, there's no affect on any auditing features. If the number of audited computers is more than 90% of the licenses purchased, enforcement depends on the number of licenses in use:

- 90-100% of the licensing limit displays a warning message that you are close to over-deployment, but you can continue to use all auditing features.



- 100-120% of the licensing limit displays a warning message that you must acknowledge by clicking **OK** when you open any console, after which you can resume using the console or session player.
- Over 120% of the licensing limit displays a warning message for 60 seconds when you open any console. If you see the 60 second warning message, use the License dialog box to add license keys to continue using auditing features.

You can contact Centrify to purchase additional licenses or remove some audited computers from the installation to bring the number of licenses used into compliance.

## Agents and licenses from previous versions

An installation can include agents and licenses from previous versions of Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service. For example, an installation might include a mix of UNIX and Windows agents from DirectAudit 2.x, or DirectAudit 3.x, or all new agents on the computers you want to audit.

## Enabling audit notification

If you enable audit notification, users see a message informing them that their actions are being auditing when they log on. After you enable notification, the message is always displayed on audited computers if the session activity is being recorded.

### To enable audit notification for an installation:

1. In the Audit Manager console, right-click the installation name, then select **Properties**.
2. Click the **Notification** tab.
3. Select **Enable notification**.  
Deselect this option to turn off notification.
4. Click the browse button to locate and select a text file that contains the message you want to display.



A notification message is required if you select the Enable notification option. The contents of the file you select are displayed below the file location. The maximum text file size is 30 KB.

5. Click the browse button to locate and select an image to appear as a banner across the top of the audit notification.

Displaying a banner image is optional when you enable notification. The maximum image file size is 15 KB. For the best image display, use an image that is 468 pixels wide by 60 pixels high.

**Note:** Animated GIF files are not supported for use as audit notifications. If you do specify an animated GIF, the image displays as a static image.

6. Click **OK** or **Apply**.

Users will see the notification message the next time they log in.

7. If you enable notification after you have deployed agents, update the local policy on the audited computers by running the following command:

```
gpupdate /FORCE
```

## Enabling or disabling video capture auditing

In most cases, you decide whether to enable video capture auditing when you create a new installation. You can, however, choose to enable or disable video capture auditing for an installation at any time. For example, you might enable full video capture auditing of user activity during your initial deployment and later find that you are capturing user activity that is of no interest or requires too much database management to store. Conversely, you might initially decide not to enable video capture and later discover that you want to record complete information about user activity when users run privileged commands or open certain applications.

You can also choose to enable video capture editing for an installation but disable it for specific computers. You disable or enable video capture auditing for a specific computer or set of computers by using group policy settings or by modifying the `agent.video.capture` setting. For details, see the *Group Policy Guide* or the *Configuration and Tuning Reference Guide*.

## To enable or disable video capture auditing for an installation:

1. In the Audit Manager console, right-click the installation name, then select **Properties**.
2. Click the **Audit Options** tab.
3. Select **Enable video capture auditing of user activity** if it is not selected to start capturing a visual record of all user activity when users perform tasks using a role that is configured to be audited.  
Deselect this option to stop all video capture auditing. If you disable video capture auditing, you will not be able to replay session activity.
4. Click **OK** or **Apply**.

## Preventing users from reviewing or deleting sessions

By default, users can update the review status, add comments, and delete their own sessions if they have an audit role with the appropriate permissions. However, there are installation-wide options to prevent any users from updating the review status or deleting their own sessions. These installation-wide options take precedence over audit role permissions for all users.

## To prevent all users from updating the review status or deleting their own sessions in an installation:

1. In the Audit Manager console, right-click the installation name, then select **Properties**.
2. Click the **Audit Options** tab.
3. Select the appropriate settings for your installation.
  - Select **Do not allow any users to review their own sessions** if you to prevent all users from updating the review status or adding comments to their own sessions in Audit Analyzer.
  - Select **Do not allow any users to delete their own sessions** if you to prevent all users from deleting their own sessions in Audit Analyzer.
4. Click **OK** or **Apply**.



## Adding an installation

Although a single installation is the most common deployment scenario, you can configure multiple installations. For example, you can use separate installations to provide concurrent production and test-bed deployments or to support multiple administrative domains within your organization.

### To create a new installation:

1. Open Audit Manager.
2. Select the root node, right-click, then select **New Installation**.
3. Follow the prompts displayed.  
The steps are the same as the first installation. For more information, see [Creating a new installation](#).
4. Choose the appropriate installation for each collector using the Collector Configuration wizard.
5. Choose the appropriate installation for each agent using the Agent Configuration wizard.

Once you have multiple installations, you can choose which one each collector is part of using the Collector Configuration wizard. You can choose which installation each agent is part of using the Agent Configuration wizard. You can also configure collectors and agents using group policy.

**Note:** Agents can communicate with a collector only if the agents and collector are in the same Active Directory forest.

### Delegating administrative tasks for a new installation

The account you use to create a new installation is the default administrator and Master Auditor with full control over the entire installation and the ability to delegate administration tasks to other Active Directory users or groups. You can grant permission to perform administrative tasks to other users by opening the Properties for each component, then clicking the Security tab.

## Opening an installation in a new console

If you create multiple installations at the same site, you can select the installation name, right-click, then select **New Window From Here** to keep consoles for different installations separate from each other. Creating a new window for each installation can help you avoid performing operations on one installation that you intended to perform on another.

## Closing an installation

The Audit Manager console allows you to manage multiple installations. To remove the current installation from the console, but not physically remove the database or the information published to Active Directory, you can select the installation name, right-click, then select **Close**.

## Publishing installation information

Centrify Audit & Monitoring Service publishes installation information to a service connection point (SCP) object in Active Directory so that audited computers and collectors can look up the information. If the published locations for multiple SCPs in the same installation are not the same, or if collectors cannot read from at least one of the published locations, the collectors are unable to determine which audit store is the best match for the sites and subnets, and so they do not attempt to connect to an audit store.

## Permission to publish to Active Directory

Only administrators who have been delegated permission to modify various attributes of the installation can publish those attributes to Active Directory.

At a minimum, you must have the Active Directory permission to Create serviceConnectionPoint objects on the container or organizational unit that you have identified for publishing installation information.

If you do not have Active Directory permission to modify the installation, the updates are kept in the audit management database, and a message is issued to notify you that the installation information could not be updated in Active Directory.



## Synchronizing installation information

If you have an Active Directory account with permission to publish information about the installation, you can update the service connection point.

### To publish the service connection point for an installation:

1. Open Audit Manager.
2. Select the installation name, right-click, then click **Properties**.
3. Click the **Publication** tab, then click **Synchronize** to publish the information.

In a multi-forest or DMZ environment, this tab lists multiple Active Directory locations to which to publish.

4. Click **OK** to close the installation properties.

## Exporting installation information

If you have an Active Directory account with permission to access installation information, you can export the service connection point that contains the installation information to a file in LDAP Data Interchange Format (LDIF). Exporting installation information can be useful if you want to add the domain for a perimeter network to an existing installation. After exporting installation information to a file, you can modify the file—for example, to use a different domain component—then import the modified file using the `ldifde` command.

### To export and import installation information:

1. Open Audit Manager.
2. Select the installation name, right-click, then click **Properties**.
3. Click the **Publication** tab.
4. Select the Active Directory location, then click **Export**.
5. Select a file location and type a file name, then click **Save**.
6. Click **OK** to close the installation properties.



7. Use a text editor to modify the file, as needed.

For example, you might use a different domain component—such as `DC=dmz1,DC=ajax, DC=org` in place of `DC=internal, DC=ajax, DC=org`—to differentiate between the perimeter and internal networks.

8. Import the modified file using a command similar to the following in a Command Prompt window:

```
ldifde -i -f C:\Users\Administrator\Desktop\sample-dmz.ldif
```

## Removing or deleting an installation

Before you can remove or delete an installation, you must do the following:

- Run the setup program to remove all agents and collectors and collector service connection points (SCPs).
- Detach and remove all audit store databases.
- Open the Installation Properties and click the **Publications** tab to make sure only one installation service connection point (SCP) is listed.

**Note:** To remove service connection points on other sites, contact an administrator with publication permission on those sites.

To remove or delete an installation, select the installation in the Audit Manager console, right-click, then select **Remove** to open the Remove installation dialog box.

- Click **Remove** to remove the installation but not delete the management database from the SQL Server instance.
- Click **Delete** to remove the installation and delete the management database from the installation of SQL Server.

**Note:** All the publications published to Active Directory are removed when you remove or delete an installation.

## Managing audit store databases

During the initial deployment, your installation only has one audit store database. As you begin collecting audit data, however, that database can quickly increase in size and degrade performance. Over time, an installation typically requires several Microsoft SQL Server databases to store the data



being captured and historical records of session activity, login and role change events, and other information. As part of managing an installation, you must manage these databases to prevent overloading any one database and to avoid corrupting or losing data that you want to keep.

One of the biggest challenges in preparing and managing Microsoft SQL Server databases for storing audit data is that it is difficult to estimate the level of activity and how much data will need to be stored. There are several factors to consider that affect how you configure Microsoft SQL Server databases for auditing data, including the recovery method, memory allocation, and your backup and archiving policies.

The sections below provide guidelines for sizing and managing the Microsoft SQL Server databases you use for audit data. For more complete information about managing and configuring SQL Server, however, you should refer to your Microsoft SQL Server documentation.

## Selecting a recovery model

Standard backup and restore procedures come in three recovery models:

- **Simple**—The Simple recovery model allows high-performance bulk copy operations, minimizes the disk space required, and requires the least administration. The Simple Recovery model does not provide transaction log backups, so you can only recover data to the point of the most recent full or differential backup. The default recovery model is Simple, but is not appropriate in cases where the loss of recent changes is not acceptable.
- **Full**—The Full recovery model has no work-loss exposure, limits log loss to changes since the most recent log backup, and provides recovery to an arbitrary time point. However, the Full recovery model uses much more disk space.
- **Bulk-logged**—The Bulk-logged recovery model provides higher performance and minimizes the log space used by disk-intensive operations, such as create index or bulk copy. With the Bulk-logged recovery model, you can only recover data to the point of the most recent full or differential backup. However, because most databases undergo periods of bulk loading or index creation, you can switch between Bulk-logged and Full recovery models to minimize the disk space used to log bulk operations.

When a database is created, it has the same recovery model as the **model** database. Although the Simple recovery model is the default, the Full and Bulk-Logged recovery models provide the greatest protection for data, and the Full recovery model provides the most flexibility for recovering databases to an earlier point in time. To change the recovery model for a database, use the `ALTER DATABASE` statement with a `RECOVERY` clause.

Regardless of the recovery model you choose, you should keep in mind that backup, restore, and archive operations involve heavy disk I/O activity. You should schedule these operations to take place in off-peak hours. If you use the Simple recovery model, you should set the backup schedule long enough to prevent backup operations from affecting production work, but short enough to prevent the loss of significant amounts of data.

## Configuring the maximum memory for audit store databases

Because Microsoft SQL Server uses physical memory to hold database information for fast query results, you should use a dedicated instance to store auditing data. Because SQL Server dynamically acquires memory whenever it needs it until it reaches the maximum server memory you have configured, you should set constraints on how much physical memory it should be allowed to consume.

The maximum server memory (`max server memory`) setting controls the maximum amount of physical memory that can be consumed by the Microsoft SQL Server buffer pool. The default value for this setting is such a high number that the default maximum server memory is virtually unlimited. Because of this default value, SQL Server will try to consume as much memory as possible to improve query performance by caching data in memory.

Processes that run outside SQL Server, such as operating system processes, thread stacks, socket connections and Common Language Runtime (CLR) stored procedures are not allowed to use the memory allocated to the Microsoft SQL Server buffer pool. Because those other processes can only use the remaining available memory, they might not have enough physical memory to perform their operations. In most casts, the lack of physical memory forces the operating system to read and write to disk frequently and reduces overall performance.

To prevent Microsoft SQL Server from consuming too much memory, you can use the following formula to determine the recommended maximum server memory:



- Reserve 4GB from the first 16GB of RAM and then 1GB from each additional 8GB of RAM for the operating system and other applications.
- Configure the remaining memory as the maximum server memory allocated for the Microsoft SQL Server buffer pool.

For example, if the computer hosting the Microsoft SQL Server instance has 32GB of total physical memory, you would reserve 4GB (from first 16 GB) + 1GB (from next 8 GB) + 1 GB (from next 8 GB) for the operating system, then set the Maximum server memory for Microsoft SQL server to 26GB (32GB – 4GB – 1GB – 1GB = 26).

For more information about how to configure Microsoft SQL Server maximum memory setting and other memory options, see the following Microsoft article:

[http://msdn.microsoft.com/en-us/librms178067\(v=sql.105\).aspx](http://msdn.microsoft.com/en-us/librms178067(v=sql.105).aspx)  
[ms178067\(v=sql.105\).aspx](http://msdn.microsoft.com/en-us/librms178067(v=sql.105).aspx)

You should configure the maximum memory allowed for the Microsoft SQL Server instances hosting audit store databases and the management database. However, this setting is especially important to configure on the Microsoft SQL Server instance hosting the active audit store database.

## Using Transact-SQL to configure minimum and maximum memory

You can control the minimum and maximum memory that the SQL Server buffer manager uses by issuing Transact-SQL commands. For example:

```
sp_configure 'show advanced options', 1
reconfigure
go
sp_configure 'min server memory', 60
reconfigure
go
sp_configure 'max server memory', 100
reconfigure
go
```

For more information about configuring SQL Server and setting minimum and maximum server memory using T-SQL, see <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options?view=sql-server-2017>

## Estimating database requirements based on the data you collect

To determine how auditing will affect database capacity, you should monitor a pilot deployment of 20 to 25 agents with representative activity to see how much data is produced daily. For example, some audited computers might have few interactive user sessions or only short periods of activity. Other audited computers might have many interactive user sessions or long sessions of activity on average.

During the pilot deployment, you want to the following information:

- How many interactive user sessions occur daily on each computer?
- How long do sessions last on average?
- What are the activities being captured, and what is the average size of each session being captured?
- How long do you need to store the captured data to balance performance and storage?
- What is the data retention period for audited data?

From the information you collect in the pilot deployment and the data retention policy for your organization, you can estimate the database size using the following guideline:

**(number of agents) x (number of sessions per agent) x (average data size per session) x (retention days)**

Results in the estimated size of the Microsoft SQL Server database for the number of days in the retention policy

For example, if an average session generated 100 KB in the database and the installation had 250 agents, 10 sessions per agent, and a six-month retention period (about 130 working days), the storage requirement for the audit store database would be 36.9 GB:

250 agents x 10 sessions/agent each day x 100 KB/session x 130 days =  
32,500,000 KB

The following table shows examples of the data storage requirement in an installation with Windows agents, typical levels of activity with an average of one session per day on each audited computer, and the recovery mode set to Simple:



Agents	Average session length	Average session size	Daily	Weekly	6 Months
100	20 minutes	806 KB - low activity	79 MB	394 MB	10 GB
50	25 minutes	11.56 MB - high activity	578 MB	2.81 GB	73.36 GB
100	20 minutes	9.05 MB - high activity	905 MB	4.42 GB	115 GB

In this example, an installation with 100 Windows agents with low activity would require approximately 10 GB for the audit store database to keep audit data for 6 months. An increase in the number of interactive sessions, session length, or average session size would increase the database storage required.

If SQL Server requires more space to accommodate the new data, it expands the database file immediately, which can cause degraded performance. To reduce the effect of database expansion on performance, allocate sufficient space to support database growth. In addition, monitor database space and when space is low, schedule a database expand operation for an off-peak time.

## Reducing color depth to decrease disk usage

If you enable video capture auditing of user activity for an installation, the color depth setting affects the size of sessions stored in the audit store database. Depending on whether you want higher quality video playback or lower disk consumption, you can modify this setting. The growth rate is linear as you increase or decrease the color depth.

Based on a simulation of user activity, changing the color depth from 16-bit to 8-bit reduces disk space by 42%. Changing the color depth from 32-bit to 16-bit reduces disk space by 34 to 39%. If you can accept the lower quality video playback, changing the color depth from 32-bit to 8-bit reduces disk space by 62 to 65%.

## Using SQL Server availability groups with multi-subnet failover for audit store databases

If you add an audit store database to a SQL Server availability group that has multiple subnet failover functionality, the SQL Server that hosts the management database must be SQL Server 2012 or above. This restriction applies only to availability groups that have multi-subnet failover configured.

For details about availability group multi-subnet failovers, see <https://msdn.microsoft.com/en-us/library/hh213417.aspx#SupportAgMultiSubnetFailover>.

## Adding new audit store databases to an installation

When you first set up an installation, you also create the first audit store and audit store database. By default, that first database is the active database. As you begin collecting audit data, you might want to add databases to the audit store to support a rolling data retention policy and to prevent any one database from becoming a bottleneck and degrading performance.

Only one database can be the active database in an audit store at any given time. The computer hosting the active database should be optimized for read/write performance. As you add databases, you can change the older database from active to attached. Attached databases are only used for querying stored information and can use lower cost storage options.

**Note:** A single instance of Microsoft SQL Server can host multiple databases. Those databases can support different versions of the agent.

Audit store databases have the following characteristics:

- A database can be active, attached, or detached.
- Only one database can be actively receiving audit data from collectors.
- A database cannot be detached while it is the active database.
- A database that was previously the active database cannot again be the active database.
- If a detached database contains parts of sessions presented to the Audit Analyzer, a warning is displayed when the auditor replays those sessions.

## Rotating the active database

Database rotation is a management policy to help you control the size of the audit store database and the performance of database operations. There are several reasons to do database rotation:



- It is more difficult to manage one large database than multiple small databases.
- Performance is better with multiple small databases.
- Backing up, restoring, archiving, and deleting data all take significantly more time if you work with one large database.
- Database operations take very little time when you work with multiple small databases.

For audit and monitoring service, you can implement a database rotation policy by having the collector write data to a new database after a certain period of time. For example, the collector in site A writes data to the database `siteA-2015-11` in November, then write data to database `siteA-2015-12` in December and to the database `siteA-2016-01` in January. By rotating from one active database to another, each database stays more compact and manageable.

## Creating a new database for rotation

You can rotate from one active database to another at any time using the Audit Manager console.

### To create a new database for rotation:

1. Open Audit Manager.
2. Expand the installation node, then expand Audit Stores and a specific audit store name.
3. Select **Databases**, right-click, then select **Add Audit Store Database** to create a new database.  
For details on setting up the database, see [Creating the first audit store database](#).
4. Select the **Set as Active database** option so collectors start writing to the newly created database.

You can also use Centrify application programming interfaces (APIs) to write a script that automates the database rotation process. For API details and sample code, see the Centrify SDK documentation.

## Database archiving

To implement periodic archiving, add a new active database, leave one or more previous databases attached, and take the oldest database off-line for archiving.

## Queries during rotation and archiving

If the database backup program supports online backups, the Audit Analyzer can still query the database while the backup is in progress. However, the backup program may block updates to the session review status. If the backup program does not support online backup, the database will be offline until the backup is complete.

## Database backups

You can back up a database whether it is attached to the audit store or detached from the audit store.

## Reattaching a restored backup of a database

If you need to query sessions from an older database that is offline and detached, you can restore the database from a backup and reattach it to your auditing installation. You might need to do this if your auditing installation is large, you do frequent database rotation, and you don't keep many databases attached and online.

Understand that after you restore a database from a backup, you need to fix a couple of settings in the database before you can reattach it to your auditing installation. During the backup operation, the database owner and trustworthy properties get set in such a way that prevents you from reattaching the database to your auditing installation unless you fix these properties.

## To reattach a restored database to your auditing installation:

1. Run the following command to reset the database owner to [sa]:

```
ALTER AUTHORIZATION ON DATABASE::<db_name> TO [sa]
```



2. Run the following command to reset the trustworthy property:

```
ALTER DATABASE <db_name> SET TRUSTWORTHY ON
```

You can now reattach the database to your auditing installation.

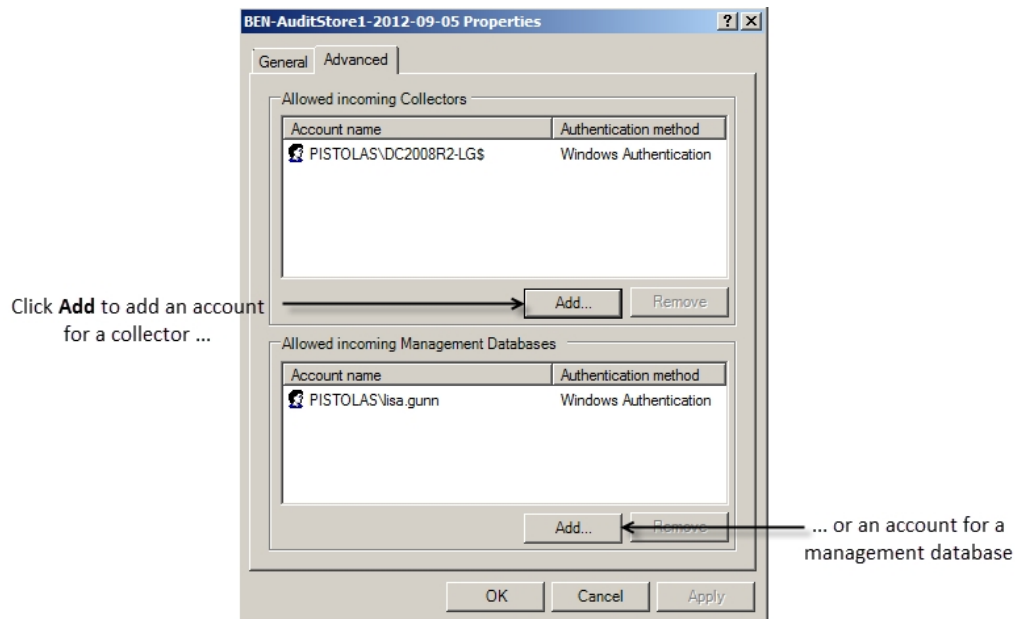
## Allowed incoming accounts

You can specify the accounts that are allowed to access the audit store database. By configuring these accounts, you can control which collector computers can connect to the audit store database and which management databases have access to the data stored in the audit store database.

Your account must have Manage SQL Login permission to configure the incoming accounts.

### To configure allowed accounts:

1. Open Audit Manager.
2. Expand the installation node, then expand Audit Stores and select a specific audit store name.
3. Select a database under the audit store, right-click, then select **Properties**.
4. Click the **Advanced** tab.
5. Click **Add** to add a collector or management database account. For example:



## 6. Select an authentication type.

- If you select Windows authentication, you can browse to select a computer, user, or group to add.
- If you select SQL Server authentication, you can select an existing SQL Server login or create a new login.

Connections should use Windows authentication whenever possible. However, computers in an untrusted forest cannot connect to an audit management database using Windows authentication. To allow connections from an untrusted forest, add a SQL Server login account as the incoming account for the management database.

## Detecting data tampering and verifying session integrity

When you create your audit store database, you have the option to enable data integrity checking. Data integrity checking provides the ability to detect if auditing data has been tampered with.

For example, data integrity checking can detect if a user who has write privileges over the Audit Store database directly manipulates the audited session data by making a direct connection to the Microsoft SQL Server database.

Session data that is stored in audit store databases is typically accessible to database administrators and/or database owners in an unrestricted fashion. For these users with write privileges on the audit store database, it's fairly easy



to tamper with data in such a way that it can help manipulate the outcome of an AQL query.

For example, someone could change the searchable tags in such a way so that the session is never returned by a query. Or, someone could remove suspicious activity from a recorded session, such as by changing the list of commands that are executed or changing the command output.

**Note:** Data integrity checking cannot detect tampering if a database administrator deletes an entire session or database. Also, data integrity checking is not yet available for audit trail events.

Once you enable data integrity checking, you can do the following:

- Use the Audit Analyzer console or a PowerShell cmdlet to check the integrity of audited sessions.
- Determine if any data in the following tables has been modified and where it was modified:
  - Session
  - RawData
  - Command
  - SyscallCommand
  - SyscallFilemon
  - WashData
  - WashEvent
- Determine if any database rows belonging to an audited session were permanently deleted.

If you have not enabled an audit store database for data integrity checking and you try to check session integrity in Audit Analyzer, an error message appears.

## Managing audit stores

An audit store is a collection of databases that contain audit data. All attached databases in the audit store are available to the audit management database. Typically each site has one audit store, but you can add audit stores as required for large or multi-site installations. For details, see [Adding more audit stores to an installation](#).

## Configuring audit store scope

The scope of an audit store defines which audited computers send their audit data to the audit store, and which collectors are assigned to the audit store. The scope is a set of Active Directory sites and/or subnets. To configure the scope for an audit store, open its **Properties** page and select the **Scope** tab. To add a site, click **Add Site** and select the site from the list. To add a subnet, click **Add Subnet** and type a subnet address and mask.

## Configuring permissions for an audit store

To configure audit store security, open the audit store's **Properties** page and select the **Security** tab.

Only users with Change Permission permission on the audit store are allowed to modify the user rights on the Security tab of the audit store's Properties page.

The following table lists the rights that can be granted to active Directory users or groups, and the operations that the users granted such rights ("trustees") are allowed to perform.

The audit store administrator by definition has all of these user rights (Full Control).

User Right	Allowed Operations
Full Control	<ul style="list-style-type: none"> <li>■ All of the operations listed in the following rows of this table</li> </ul>
Change Permissions	<ul style="list-style-type: none"> <li>■ Modify permissions on this audit store</li> </ul>
Modify Name	<ul style="list-style-type: none"> <li>■ Modify display name for this audit store</li> </ul>
Manage Scopes	<ul style="list-style-type: none"> <li>■ Add a subnet or active Directory site</li> <li>■ Remove a subnet or active Directory site</li> </ul>
Manage SQL Logins	<ul style="list-style-type: none"> <li>■ Set the allowed incoming accounts for this audit store's databases</li> <li>■ Set the allowed incoming accounts for collectors</li> </ul>
Manage collectors	<ul style="list-style-type: none"> <li>■ Enable collector trusted group for this audit store</li> <li>■ Add collector to the trusted collector group in this audit store</li> <li>■ Remove collector from the trusted collector group in this audit store</li> <li>■ Remove disconnected collector record from this audit store</li> </ul>
Manage Audited	<ul style="list-style-type: none"> <li>■ Enable audited computers trusted group for this audit store</li> </ul>

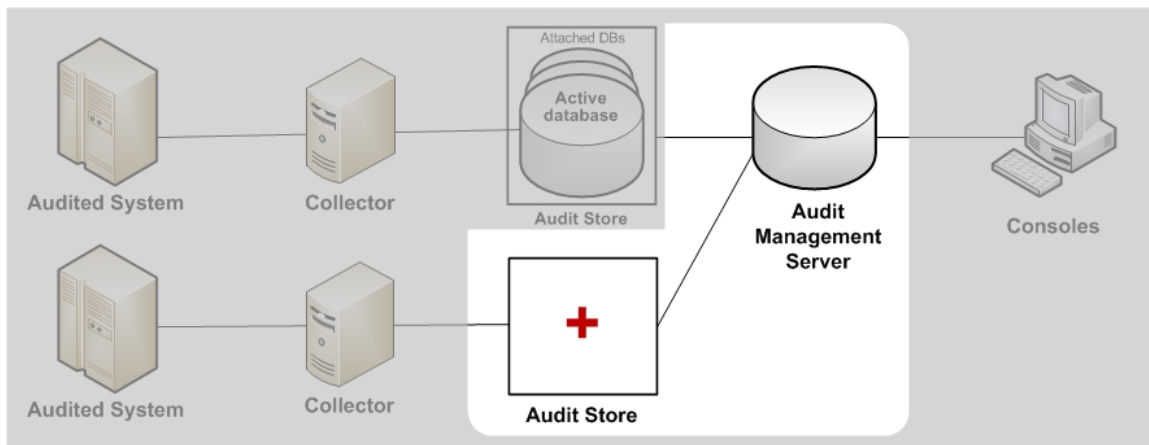


User Right	Allowed Operations
Systems	<ul style="list-style-type: none"> <li>■ Add audited computer to the trusted audited computer group in this audit store</li> </ul>
	<ul style="list-style-type: none"> <li>■ Remove audited computer from the trusted audited computer list in this audit store</li> </ul>
	<ul style="list-style-type: none"> <li>■ Remove disconnected audited computer record from this audit store</li> </ul>
Manage Databases	<ul style="list-style-type: none"> <li>■ Add audit store database to this audit store</li> </ul>
	<ul style="list-style-type: none"> <li>■ Attach audit store database to this audit store</li> </ul>
	<ul style="list-style-type: none"> <li>■ Detach an audit store database from this audit store</li> </ul>
	<ul style="list-style-type: none"> <li>■ Change active database in this audit store</li> </ul>
Manage Database Trace	<ul style="list-style-type: none"> <li>■ Modify the display name of a version 2 audit store database</li> </ul>
	<ul style="list-style-type: none"> <li>■ Enable or disable database trace</li> </ul>
	<ul style="list-style-type: none"> <li>■ Export database trace</li> </ul>

## Adding more audit stores to an installation

The audit store typically maps one-to-one with an Active Directory site. However, in some situations it is desirable to define the scope of an audit store differently:

- A subnet that Active Directory considers part of a site may be connected over a slow link. In this situation, you probably want to configure another audit store and collectors that service audited computers in the remote subnet.
- A very large site may require multiple audit stores for load distribution. You can accomplish this by partitioning an Active Directory site into multiple audit stores based on subnets. Each subnet has its own audit store and set of collectors and audited computers.



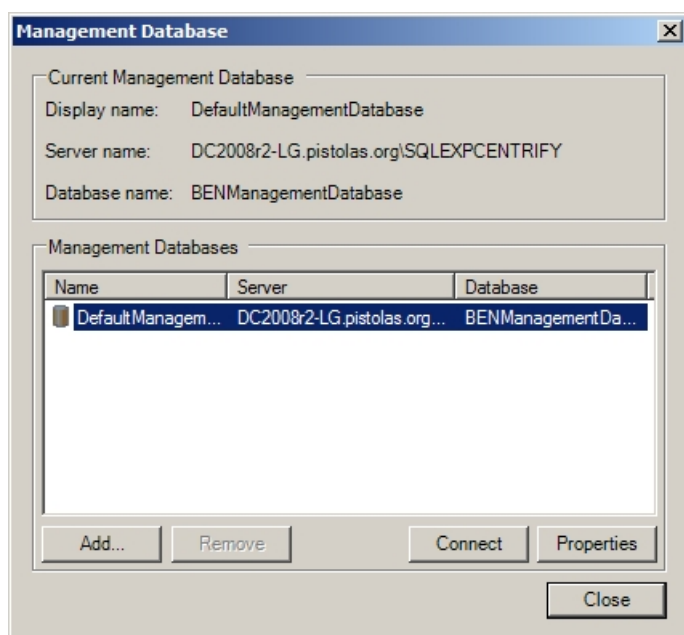
Two common audit store actions are:

- Adding a new audit store in a new site, and using the **Select Scope** page in the **Add Audit Store Wizard** to configure the site settings.
- Splitting an audit store in two, using the audit store's **Property** page to adjust the scope of the existing audit store, and then adding a new audit store.

To configure the audit store to support a particular subnet, click the **Subnet** radio button, and fill in the subnet IP address and mask.

## Managing the audit management database

The audit management database keeps track of where components are installed and information about the installation. To connect to the database or manage its properties, select a specific installation name in Audit Manager, right-click, then select **Management Databases**. From this dialog box, you can view information about the current audit management database, remove or connect to a management database, or change the properties for a management database.



## Configuring audit management database scope

Select the audit management database you want to configure, then click **Properties**. From the Properties, click the **Scope** tab to configure audit management database scope. Click Add Site if you want to add a new Active Directory site to the management database or click Add Subnets to add a subnet for the management database to serve. Select the site or subnet from the list of sites or subnets found, then click **OK**. You can add or remove sites and subnets from the management database at any time using the Scope tab.

**Note:** All components use Windows authentication whenever possible. However, an audit management database in another forest cannot connect to an audit store database using Windows authentication.

## Setting audit management database security

Select the audit management database you want to configure, then click **Properties**. From the Properties, click the **Security** tab to configure security settings for the management database. Click the **Add** page to add groups or users to the list of trustees who can manage, modify, or remove installation-wide components. Type all or part of the user or group name, select the appropriate user or group from the results, then click **OK**.



Select the appropriate rights you want to grant to the selected Active Directory users or groups, and the operations that the users granted such rights (“trustees”) are allowed to perform.

Select this right	To grant permission for these operations
Full Control	■ All of the operations listed in the following rows of this table.
Change Permissions	■ Modify permissions on this audit management database.
Modify Name	■ Modify display name for this audit management database.
Manage Sites	■ Add a subnet or Active Directory site. ■ Remove a subnet or Active Directory site.
Remove Database	■ Remove this audit management database from the installation.
Manage SQL Logins	■ Set the allowed incoming accounts for this audit management database. ■ Set the outgoing account for this audit management database.
Manage Database Trace	■ Enable or disable database trace ■ Export database trace

Only users with Change Permission permission on the audit management database can modify the user rights on the Security tab. By definition, the management database administrator has Full Control over all of the user rights and is an allowed incoming user.

## Configuring the maximum memory for the management database

Because SQL Server dynamically acquires memory whenever it needs it until it reaches the maximum server memory you have configured, you should set constraints on how much physical memory it should be allowed to consume. You can use the formula described in [Configuring the maximum memory for audit store databases](#) to determine the maximum memory you should allow for the Microsoft SQL Server instances hosting the management database.

For more information about how to configure Microsoft SQL Server maximum memory setting and other memory options, see the following Microsoft article:

[https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms178067\(v=sql.105\)](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ms178067(v=sql.105))

## Removing an audit management database

Select a specific installation name in Audit Manager, right-click, then select **Management Databases**. Select the audit management database you want to remove, then click **Remove**.

Because it is not recommended that you have multiple management databases in a single installation, you ordinarily would not separately remove an audit management database, but rather remove it as part of deleting an installation.

## Maintaining database indexes

To ensure better performance and prevent database corruption, Centrify recommends you rebuild the database indexes for all the audit store databases and the management database as a regularly scheduled task that you run at least once a week. Rebuilding the indexes is especially important for the active audit store database to reduce fragmentation, but as a best practice you should rebuild indexes for all attached databases and the management database.

The following sample SQL statements illustrate how to rebuild all indexes on all the databases in one script:

```
=== BEGIN SQL statements ===
DECLARE @Database NVARCHAR(128)
DECLARE @Table NVARCHAR(128)
DECLARE @Command NVARCHAR(500)

-- To skip index rebuilding for a database, add its name to the list
below
DECLARE DatabaseCursor CURSOR FOR
SELECT name FROM master.dbo.sysdatabases
WHERE name NOT IN ('master','msdb','tempdb','model')
ORDER BY 1

OPEN DatabaseCursor
FETCH NEXT FROM DatabaseCursor INTO @Database
WHILE @@FETCH_STATUS = 0
BEGIN
    PRINT 'Processing database ' + @Database
    SET @Command = 'DECLARE TableCursor CURSOR FOR SELECT
        ''[' + TABLE_CATALOG + '].[' + TABLE_SCHEMA
        + '].[' +
        TABLE_NAME + ']' as TableName FROM [' + @Database
        + '].INFORMATION_SCHEMA.TABLES
        WHERE TABLE_TYPE = ''BASE TABLE'''
    EXEC (@Command)
    OPEN TableCursor
```



```
FETCH NEXT FROM TableCursor INTO @Table
WHILE @@FETCH_STATUS = 0
BEGIN
    PRINT 'Rebuilding all indexes on ' + @Table
    SET @Command = 'ALTER INDEX ALL ON ' + @Table
        + ' REBUILD'
    EXEC (@Command)
    FETCH NEXT FROM TableCursor INTO @Table
END

CLOSE TableCursor
DEALLOCATE TableCursor

FETCH NEXT FROM DatabaseCursor INTO @Database
END
CLOSE DatabaseCursor
DEALLOCATE DatabaseCursor
=== END SQL statements ===
```

## Managing collectors

You can select the Collector node in Audit Manager to view details about each collector you have added to the installation. You can then expand the Collectors node and select an individual collector in the left pane to display information about the audited computers that send sessions to that collector in the right pane.

The following table describes the columns available in the right pane for collectors.

Column name	Description
Collector	Name of the collector
IP Address	Location of the collector on the network
Status	Whether the collector is disconnected from or connected to the audit store. If a collector has never been successfully assigned to an audit store, it is not even shown in the left-pane list.
Uptime	How long a connected collector has been running since it was last booted
Last Update Time	The date and time of the last update received by the collector.
Port Number	The port through which the collector communicates with its assigned audited computers and audit store. Default is 5063.
Audit Store	The audit store to which this collector is assigned
Audit Store Database	The active database to which the collector is currently sending audit data
Connected	The number of audited computers currently connected to this collector.

Column name	Description
Machines	Because agents can communicate with a collector only if the agents and collector are in the same Active Directory forest, this column only includes audited computers that are in the same forest as the collector.
Disconnected Machines	The number of audited computers of which the collector is aware but that are not currently connected to this collector. Note that the collector is only aware of audited computers that were at one time connected to it.
Collector Version	The version of the collector software installed on the computer.

## Monitoring collector status

The Collector Control Panel is available from the Start menu on any Windows computer on which you have installed a collector.

The Collector Control Panel enables you to monitor the local collector by giving you an overview of collector connectivity and status, including the collector's current installation, audit store, audit store database, port number, and service status. To change the collector's port number, installation, or authentication, click **Configure**. If you change the collector configuration, it might take a minute for the change to be reflected in the Collector Control Panel.

You can also use the Collector Control Panel to start, stop, or restart the collector service, and to generate more detailed information about the status of the collector. To see detailed information about the installation, audit store, audit store database, trusted agents, and connectivity between components, click the **Troubleshooting** tab, then click **Diagnostics**. The collector will generate a report and display the information in a separate window.

## Modifying the command prompt recognized by the collector

For the collector to identify the command events executed in a session, it must also be able to identify the command prompt. Although there are several characters that are commonly used and recognized by default, most computers also allow you to customize the command prompt. If a customized command prompt is not detected by the collector, commands will not be displayed properly in the session Events list, making it difficult for auditors to see the commands executed in a selected session.



To enable the collector to detect custom or unusual command prompts, you can add a registry key on the computer where the collector is installed and specify a text string or a regular expression that will match the command prompt.

## To specify a regular expression for the command prompt:

1. Log on to the computer where the collector component is installed and running.
2. Open the Registry Editor.
3. Expand the **HKEY\_LOCAL\_MACHINE > SOFTWARE > Centrify > DirectAudit** registry.
4. Select the Collector component, right-click, then select **String Value**.
5. Type Prompt as the new key name.
6. Select the new Prompt key, right-click, then select **Modify**.
7. Type a text string or regular expression that will enable the collector to identify the command prompt you are using on computers you are auditing.

If you don't define a registry value, the default regular expression `^[^#%>\$]*[#%>\$]\s*` is used to detect the command prompt.

## Removing collectors

If you want to remove a collector, go to the installer and select the collector. The Collector Setup wizard Welcome page appears.

Because a collector is present on the computer, the next page enables you to select Change, Repair, or Remove the collector. Click **Remove**.

## Managing audited computers and agents

You can monitor agent status from the Audit Manager console. With audited computers selected in the left pane, Audit Manager displays the name and IP address for audited computers, whether the agent is currently connected or disconnected, and how long the agent has been running since last restarted. You can also see the collector to which the agent is sending data, the audit





store and audit store database where the audit data is stored, and the version of the agent software installed on the computer.

Audited systems can be either a computer or a network device. Audit Manager displays two kinds of audited systems:

- **System-based:** A Windows or UNIX computer that is running an agent. You can access these systems either directly or from the Privileged Access Service Admin Portal.
- **Vault-based:** A Windows or UNIX computer or a network device that is not running an agent (agentless). You can access these systems from the Privileged Access Service Admin Portal.

Because agentless systems do not have an agent installed, the Audit Manager displays slightly different information for these kinds of systems. For these systems, you can see the name, IP address, the collector, audit store, and audit store database.

## Monitoring agent status

You can use the `dainfo -d` command on audited Linux and UNIX computers to view information about the configuration, connectivity, and auditing status of the agent.

## Configuring the UNIX agent off-line database

If the UNIX agent is unable to connect to a collector, it spools the session data to local storage. When a collector becomes available, it then sends the spooled data to that collector.

By default, the minimum amount of allocated disk space that must be available to the offline database before spooling stops and warnings are posted to the agent error log is 10%. You can change this percentage by assigning a different value to `spool.diskspace.min` in the `/etc/centrifyda/centrifyda.conf` file. For example, to change the minimum to 15%, set the following value:

```
spool.diskspace.min: 15
```

If the threshold is reached and a collector is still not available, the agent stops spooling data, and further audit data is lost. If this happens frequently or unexpectedly, you may want to increase the disk space allocation.

## Removing an audited computer

If an audited computer has been removed from the audit installation, the audited computer will continue to be listed on the Audit Manager as **Disconnected**. To remove the decommissioned audited computer, select **Delete** from its context menu.

## Delegating administrative permissions

You can facilitate the administration of a large installation by delegating tasks and, if needed, setting up additional Audit Manager consoles.

Whoever creates the installation is the first administrator in the system, with full control of the entire installation and the ability to delegate administration tasks to any Active Directory user or group. You can grant permissions to other users on the **Security** tab of the **Properties** page for each component.

## Publishing installation information

Audit Manager publishes information about your installation to a service connection point (SCP) object in Active Directory so that audited computers and collectors can look up the information. If the published locations for multiple SCPs in the same installation are not in synch, or if agents cannot read from at least one of the published locations, the agents are unable to determine which audit store is the best match for the sites and subnets, and so they do not attempt to connect to an audit store.

### Permission to publish to Active Directory

Only administrators who have been delegated permission to modify various attributes of the installation can publish those attributes to Active Directory.

If you do not have Active Directory permission to modify the installation, the updates are kept in the audit management database, and a message is issued to notify you that the installation information could not be updated in Active Directory.

## Synchronizing installation information

If you have an Active Directory account with permission to modify the installation, you can click Synchronize the Installation Properties page Publication tab to publish the information.

In a multi-forest or DMZ environment, this tab lists multiple Active Directory locations to which to publish.

## Managing audit roles

By default, each installation automatically has a Master Auditor role that has access to all audit data. The Master Auditor can read, replay, update review status, and delete all audit sessions in the installation. You cannot delete or change the permissions for the Master Auditor role itself. You can change the users or groups who are assigned to the Master Auditor role and the permissions granted to each role member, but you cannot make any other changes to this role. You can, however, create your own custom audit roles for the installation.

## Creating custom audit roles

Audit roles allow specific auditors to search and replay specific sessions, review specific events, or generate reports using the Audit Analyzer console based on the criteria you define. Each role specifies the criteria to use, the users and groups that are assigned to the role, and the specific permissions those users and groups have been granted.

For example, you might specify the criteria for filtering sessions to be only the session activity recorded on a particular audited computer or all UNIX sessions recorded after a specific date and time.

The collection of auditors is identified by specifying either explicit auditors, or an Active Directory group of auditors. Using Active Directory groups is recommended because this puts all of a user's privileges under the common Active Directory infrastructure.

For each audit role, you can also configure the specific permissions granted to each member of the role. For example, some audit roles might permit auditors to read and replay sessions but not update the status, add review comments, or delete the sessions to which they have access.

## To create and assign audit roles:

1. Open Audit Manager and expand the audit installation to which you are connected.
2. Select Audit Roles, right-click, then select **Add Audit Role**.
3. Type a name and, optionally, a description of the audit role, then click **Next**.
4. Select the type of sessions—UNIX sessions, Windows sessions, or both UNIX and Windows sessions—to include for auditors assigned to this audit role, then click **Add** to specify filtering criteria for the role.
5. Select an attribute for filtering information from the list of Attributes.  
For example, you can match sessions based on the period of time in which they were active, based on a specific state, or based on Active Directory group membership. You can also match sessions based on the specific activity that took place during the session. For example, you can find sessions where specific UNIX commands or Windows applications were used.
6. Select the appropriate criteria for the attribute you have selected, then click **OK**.

The specific selections you can make depend on the attribute selected. For example, if the attribute is **Review Status**, you can choose between “Equals” and “Not equals” and the specific review status you want to find, such as “To be Reviewed.” If you select the attribute **Comment**, you can specify “Contains any of” and type the text string that you want to find any part of. If you select the attribute **Group**, you can select “Is (exactly)” and the user principal name (UPN) of an Active Directory group, such as `adm-sf@acme.com`.

You can specify multiple attributes, by clicking Add and selecting additional attributes and criteria. You can test the filtering criteria you have added by clicking **Execute Query** and examining the results. When you have finished adding filters, click **Next**.

7. Select the privileges for the audit role, then click **Next**.
8. Review your settings for the audit role, click **Next**, then click **Finish**.

You can assign users and groups to the audit role immediately by running the Assign users and Groups wizard or at a later time by right-clicking on the role name.



9. Type all or part of name to search for and select Active Directory users and groups to assign to the audit role.

## Changing audit role properties

After creating an audit role, you can modify its properties.

### To change properties for an audit role:

1. Open Audit Manager and expand the audit installation to which you are connected.
2. Expand Audit Roles, select an audit role name and right-click, then select **Properties**.
3. Click the General tab to change the name or description of an audit role.
4. Click the Access tab to change the filtering attributes and criteria an audit role.
5. Click the Privilege tab to change what members of the audit role can do with the sessions matching the criteria you specify.
6. Click the Security tab to change permissions for the audit role itself.

For example, you allow another user or group to change role membership for an audit role, you would click Security, then click Add to search for and select a user or group, then select the Change Role Membership permission to allow the selected user or group to modify the membership of the audit role.

## Granting permissions to manage audit roles

Anyone you assign the Manage Audit Roles permission on an installation has full control over all of the audit roles for that installation. After you grant users or groups the Manage Audit Roles permission, they can create and remove roles, change the filtering criteria, modify audit role permissions for other users and group, and select the users or groups who are assigned to the role.

The following examples illustrate how users or groups granted the Manage Audit Roles permission might modify the audit roles for an installation:



- Assign the Master Auditor role to other users and groups.
- Create a UNIX Session Viewer role for UNIX auditors that allows them to view (read) UNIX sessions—but not replay, update, or delete—all UNIX sessions in the installation.
- Create a Finance Managers role that includes both UNIX and Windows sessions filtered by the Active Directory group Finance Operators, so that users assigned to the Finance Managers audit role can read, replay, update, and delete all of the session activity generated by members of the Finance Operators group, but no other groups.
- Create an audit role that enables investigators who are assigned to the role to read and replay only the activity captured when a specific command or application is used.

These are only a few examples of how you can use the Manage Audit Roles permission to define filtering criteria and privileges that control what different users or groups who are assigned to audit roles can see and do.

# Querying and reviewing audited activity

This section describes how to use Audit Analyzer to find and review the audited sessions and audit trail events in which you are interested. If you are the Master Auditor or been assigned an audit role, you can use Audit Analyzer to create and store queries that retrieve information from one or more audit stores. When you locate sessions or events of interest, you can review a summary of activity, play back all or part of the session, mark the session for follow-up, or change the status of the session.

The following topics are covered:

Accessing audited sessions .....	136
Predefined queries for audit sessions .....	136
Predefined queries for audit events .....	138
Predefined queries for reports .....	138
Creating new session queries .....	143
Creating queries for audit events .....	149
Organizing queries in custom folders .....	151
Exporting and importing query definitions .....	152
Displaying session information .....	153
Adding session reviewers without designating auditing roles .....	153
Changing the review status for audited sessions .....	154
Playing back a session .....	156
Exporting sessions .....	160
Deleting sessions .....	162

## Accessing audited sessions

Your access to audited sessions is controlled either through the audit roles you have been assigned, or through designation as a reviewer if you do not have an auditing role assigned to you. For more information on designating audit session reviewers, see [Adding session reviewers without designating auditing roles](#).

If you have been assigned at least one audit role, or have been designated as a reviewer without an audit role, you can use Audit Analyzer to search for and replay the audited session activity collected from audited computers.

Depending on the permissions defined for your audit role, you might also be able to annotate, update the status of, or delete the audited sessions to which you have access. If you have been designated as a reviewer of an audit session, you can only review and updated the status of the sessions to which you have access.

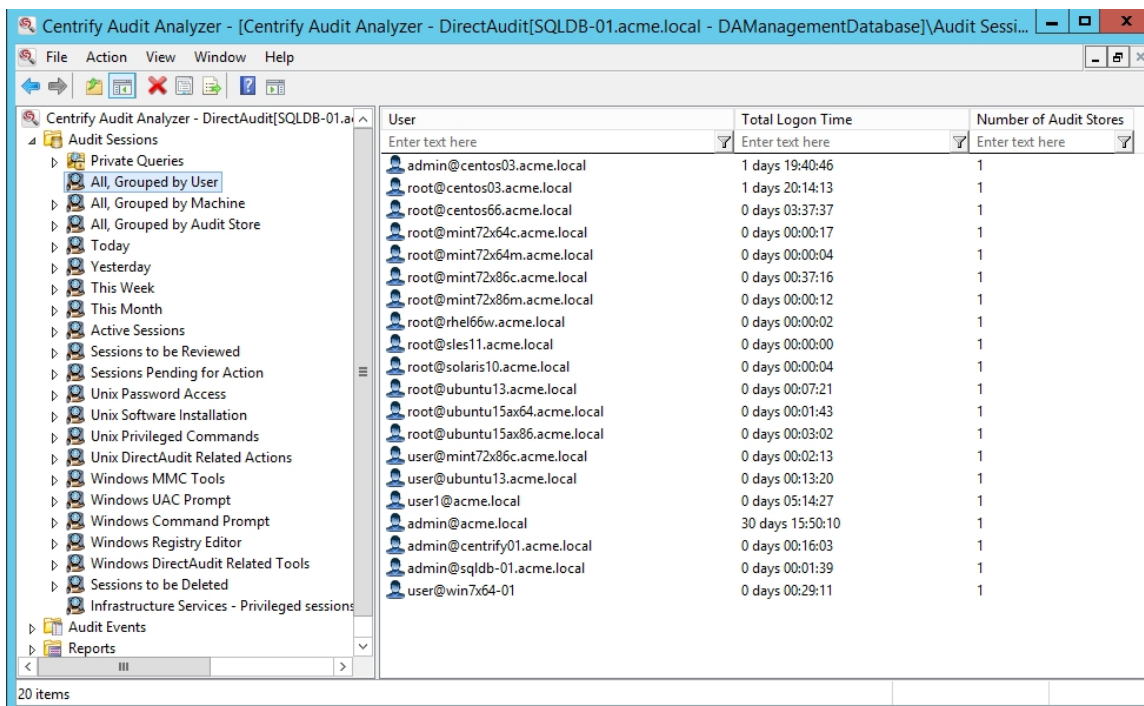
The first time you start Audit Analyzer, you are prompted to select an installation. If you have an audit role in that installation and the connection is successful, Audit Analyzer opens and displays the default categories for predefined queries:

- Audit Sessions
- Audit Events
- Reports

## Predefined queries for audit sessions

Audit Analyzer includes many predefined queries that you can use to find the sessions in which you are interested. To access the predefined queries, expand Audit Sessions. You can then select a predefined query to display a list of the audited sessions that meet the conditions of that query. For example, if you want to search for sessions by user, you can use the All, Grouped by User, then select the specific user whose sessions are of interest to see a list of all the sessions captured for that user. For example, in the right pane, you would select a user from the list:





After you select the user, Audit Analyzer displays detailed information about each of that user's sessions. For each session, Audit Analyzer lists the user name who started the session, the user display name, the account name used during the session, the name of the audited computer, the audit store where the session is stored, the start and end time for the session, current state, whether the audited session is a console or terminal client session, the review status of the session, any comments that have been added to the session, and the session size. For example:

User	Display Name	Account	Machine	Audit Store	Start Time	End Time	State	Client Name
Enter text here	Enter te...	Enter text here	Enter text here	Enter text here	Enter text here	Enter text here	Enter te...	Enter text h...
maya@pistolas.org	Maya Sanders	maya	firefly-sf.pistolas.org	Default-First-Site-Name@...	4/14/2015 2:54:54 PM	4/15/2015 12:06:32 PM	Completed	Xterm (:0.0)
maya@pistolas.org	Maya Sanders	maya	firefly-sf.pistolas.org	Default-First-Site-Name@...	3/31/2015 3:54:27 PM	4/15/2015 12:06:32 PM	Completed	Xterm (:0.0)
maya@pistolas.org	Maya Sanders	maya	firefly-sf.pistolas.org	Default-First-Site-Name@...	1/21/2015 10:53:20 AM	1/21/2015 10:55:06 AM	Completed	Xterm (:1.0)
maya@pistolas.org	Maya Sanders	maya	firefly-sf.pistolas.org	Default-First-Site-Name@...	1/21/2015 10:43:27 AM	1/21/2015 10:46:14 AM	Completed	Xterm (:1.0)
maya@pistolas.org	maya	maya	firefly-sf.pistolas.org	Default-First-Site-Name@...	10/9/2014 2:18:07 PM	10/9/2014 2:25:01 PM	Completed	Xterm (:0.0)
maya@pistolas.org	Maya Sanders	maya@pistolas.org	dc2008r2-lg	Default-First-Site-Name@...	2/18/2015 3:41:25 PM	2/24/2015 10:33:32 AM	Completed	Console
maya@pistolas.org	Maya Sanders	maya@pistolas.org	dc2008r2-lg	Default-First-Site-Name@...	2/18/2015 1:58:20 PM	2/18/2015 2:23:18 PM	Completed	Console

Note that only completed sessions display the session size in Audit Analyzer.

Depending on the permissions associated with your audit role, you can right-click any session to view an indexed list of the activity captured, export the session activity to a comma-separated values file, update the review status for the session, or delete the session. If you have video capture auditing enabled for the installation, you can also select a session, right-click, then select **Replay** to review the session in the session player.

To view a description and definition for any predefined query, select the query, right-click, then select **Properties**. You can also export the query definition or the results from a query and perform other tasks on predefined queries. To



perform any of these additional tasks, select the predefined query, right-click, then select the action you want to take.

## Predefined queries for audit events

Audit Analyzer includes predefined queries that you can use to find the sessions that recorded audit trail events. To access the predefined queries for locating audit trail events, expand Audit Events. You can then select a predefined query to display a list of the audit trail events that meet the conditions of that query. You navigate to indexed lists of commands and events and replay sessions of interest for audit event queries in exactly the same way as audit session queries and you have the same options for viewing the activity captured. However, the details displayed for audit event queries are different from audit session queries.

For each event, Audit Analyzer lists the name of the user, the name of the audited computer, the time of the event, the event name and description, and whether access was successful.

## Predefined queries for reports

Audit Analyzer includes predefined queries for generating reports. By default, the reports include information for all audited users, computers, and sessions. Select the type of report you are interested in generating, then specify additional criteria for filtering the report output. You can then save the modified report query or show the report.

If you click Show Report, the report is generated and displayed in a new window. You can then save the report as an HTML, PDF, CSV, or XML document.

### User activity report

The default User Activity Report provides a detailed record of user actions for all audited users. The report includes the user name, the computer where the activity occurred, the time at which the activity occurred, and the event recorded. For example, if a user opened a Windows application or ran a UNIX



command, the event would be recorded and included in the report you generate.

You should note that the User Activity Report does not include all desktop changes, such as navigation through directories using Windows Explorer. Instead, the report provides information about specific events. For example, the report will include information about when an application is opened, operations are performed, and when the application is closed. For more detailed information about user activity, you can enable video capture auditing for the installation and for specific desktops, applications, or commands using roles in Access Manager.

For information about enabling video capture auditing, see [Enabling or disabling video capture auditing](#).

You can customize and filter the information included in a User Activity Report by specifying the query criteria and saving the report definition.

## **Privileged activity report**

The default Privileged Activity Report provides a record of all actions taken with elevated privileges for all audited users and computers. The report includes the user name, the computer where the activity occurred, the time at which the activity occurred, and the event recorded. For example, if a user selected a role with administrative privileges, the event would be recorded and included in the report you generate.

You can customize and filter the information included in a Privileged Activity Report by specifying the query criteria and saving the report definition.

## **Centrify zone administration activity report**

The default Centrify Zone Administration Activity Report provides a record of all zone-related administrative actions taken for all audited users and computers. The report includes the user name, the computer where the activity occurred, the time at which the activity occurred, the client name, and the event recorded. For example, if an administrator created a new zone or delegated a management task to another user or group, the event would be recorded and included in the report you generate.



You can customize and filter the information included in a Centrify Zone Administration Activity Report by specifying the query criteria and saving the report definition.

## **Login by user report**

The default Login By User Report provides a record of both successful and failed login attempts for all audited users, computers, and sessions. The report includes the user name, the computer where the user attempted to log on, the time of the login attempt, and whether access was granted.

You can customize and filter the information included in a Login By User Report by specifying the query criteria and saving the report definition.

## **Login by computer report**

The default Login By Computer Report provides a record of both successful and failed login attempts for all audited users, computers, and sessions. The report includes the user name, the computer where the user attempted to log on, the time of the login attempt, and whether access was granted.

You can customize and filter the information included in a Login By Computer Report by specifying the query criteria and saving the report definition.

## **Authorization failure report**

The default Authorization Failure Report provides a record of authorization failure events for all audited users, computers, and sessions. The report includes the user name, the computer where the user attempted to log on or use a role, the time of the attempt, and the reason the user was denied access.

You can customize and filter the information included in a Authorization Failure Report by specifying the query criteria and saving the report definition.

## **Monitored execution report**

If you have configured your auditing installation for advanced monitoring, then this Monitored Execution report shows the monitored commands being



executed on the audited computers. This report includes information on commands that are run individually or as part of scripts. This report shows who ran one of the monitored commands even if that person is not an audited user.

The Monitored Execution report includes the user name, the computer where the commands were run, the time the command was run, the name of the command and the command arguments used, the process and parent process IDs, the “run as” user, the directory in which the command run, and whether the command was successful.

**Note:** In the report, the Access Status column lists out whether the command was started successfully or not. This field does not describe whether the command completed successfully or not.

**Note:** Advanced monitoring does not generate an audit trail event for commands for which you’ve enabled per-command auditing.

You can customize and filter the information included in a Monitored Execution report by specifying the query criteria and saving the report definition.

## Detailed execution report

If you have configured your auditing installation to perform advanced monitoring, then this Detailed Execution report shows all of the commands being executed on the audited machines—including commands that are run as part of scripts or other commands.

The Detailed Execution report includes the user name, the computer where the activity occurred, the time at which the activity occurred, the command that was entered, the process and parent process IDs, the current directory, the actual command that was executed, the command arguments, the “run as” user, whether the command started or not (access status), and any additional access status details (such as “permission denied” if the access status is “failed”).

**Note:** In the report, the Access Status column lists out whether the command was started successfully or not. This field does not describe whether the command completed successfully or not.

**Note:** Advanced monitoring does not generate an audit trail event for commands for which you’ve enabled per-command auditing.



You can customize and filter the information included in a Detailed Execution report by specifying the query criteria and saving the report definition.

## File monitor report

If you have configured your auditing installation to perform advanced monitoring, the File Monitor report shows the sensitive files being modified by users on the audited machines. The File Monitor report includes any activity by any user (except root, -1) in the following protected areas on audited machines:

- /etc/
- /var/centrify/
- /var/centrifydc/
- /var/centrifyda/

The report includes the user name, the computer where the activity occurred, the time at which the activity occurred, the filename, the current directory, the kind of file access was attempted, if the file access was successful or not, the command that was used, the process and parent process IDs, and the “run as” user.

**Note:** If a monitored file is renamed, the report displays both the original and new filename. The order of filenames may differ slightly on each operating system.

## MFA Failure Report

The default MFA Failure Report provides a record of multi-factor authentication (MFA) failure events for all audited users, computers, and sessions. The report includes the user’s name, the computer where the user attempted to log on or use a role, the time of the attempt, and the reason that MFA authentication failed.

You can filter the information included in a MFA Failure Report by specifying the query criteria and saving the report definition.

## Creating new session queries

You can create your own queries from existing queries or based on the criteria you define. Depending on the type of information you want to define as search criteria and whether you want to make the queries private or public, there are different type of queries you can define.

To search for audited sessions, you can create:

- Quick queries
- Private queries
- Shared queries

If you create a quick, private, or shared query, a new node is added to the Audit Analyzer console for that type of query under the Audit Sessions node. If you want to search for audit trail events, you can also create queries for audit events, which are added to Audit Analyzer under the Audit Events node.

### Creating a new quick query

A quick query is a full-text search of the audit store database for a simple string or keyword. With a quick query, you can start typing the search string and see a list of potential matches from which you can select an item to look for sessions that contain the item. You should use quick queries when you want to find sessions based on a simple text string, such as a captured input or output, or based on a particular attributes, such as a user name or application, rather than using complex expressions.

#### To create a new quick query:

1. Open Audit Analyzer, select Audit Sessions, right-click, then select **New Quick Query**.
2. Type a search string into the search field.

As you type, the Quick Query displays a list of possible matches that start with the text you are typing. For example, if you start typing the string “da” as the search term, the Quick Query list displays captured commands such as `dacontrol`, `dad`, and `daddebug` as potential matches:



The quick query uses SQL Server full text search.

The list of potential matches can include captured input and output, application names, user names, computer names, time stamps, and any other information stored in the audit store database.

If a text string in the list is what you are looking for, select it. By default, the query will search for sessions that contain all of the text specified. If you want to search for any portion of the text specified, select **Find sessions containing ANY instead of ALL of the search terms**.

3. Click **Find** to display the matching logon sessions in the right pane.

## Searching for a specific string

If you want to search for a specific string, you can enclose the command line string with quotation marks. For example, you can type “dacontrol -i” to only return sessions that captured dacontrol with the -i option. If you type the same search string without quotation marks and select **Find sessions containing ANY instead of ALL of the search terms**, the quick query will return sessions that include dacontrol with and without the -i option.

## Modifying a quick query

You can edit a quick query by selecting the query in the left pane, right-clicking, then selecting **Properties**. You can change the name and add a description on the **General** tab. Click the **Definition** tab to change the query text.

## Creating a new private query

A private query is a set of search criteria that you define for your own use. Private queries are only visible to the auditor who creates them. You create private queries by selecting options in Audit Analyzer dialog boxes. Your selections are translated into complex expressions in the SQL Server query language. You can also save any predefined or shared query as a private query if you want to modify an existing query for private use.





## To create a new private query:

1. Open Audit Analyzer, select Audit Sessions, right-click, then select **New Private Query**.
2. Type a name and description for the query.

After you save the query, this information is available for viewing and editing on the General tab when you display the query's properties.
3. Select the type of sessions that you want the query to find.

You can search for UNIX sessions, Windows sessions, or both UNIX and Windows sessions. By default, new queries search for both UNIX and Windows sessions.
4. Select an attribute for grouping query results, if applicable.

You can select one or more attributes for grouping query results. If you specify more than one attribute, results are displayed as nested groups according to the order in which you specified the attributes. For example, if you select audit store, then user, then date, the query results are grouped by audit store, then by user for each audit store, then by date for each user.
5. Select an attribute for ordering query results within each group, if applicable.

You can select ascending or descending sort order for each attribute. For example, you might group query results by user name and set the sort order for user to ascending, but the sort order for time to descending.
6. Click **Add** to add search criteria to filter the results of the query.
7. Select an appropriate attribute from the Attribute list based on the sessions you want to find.

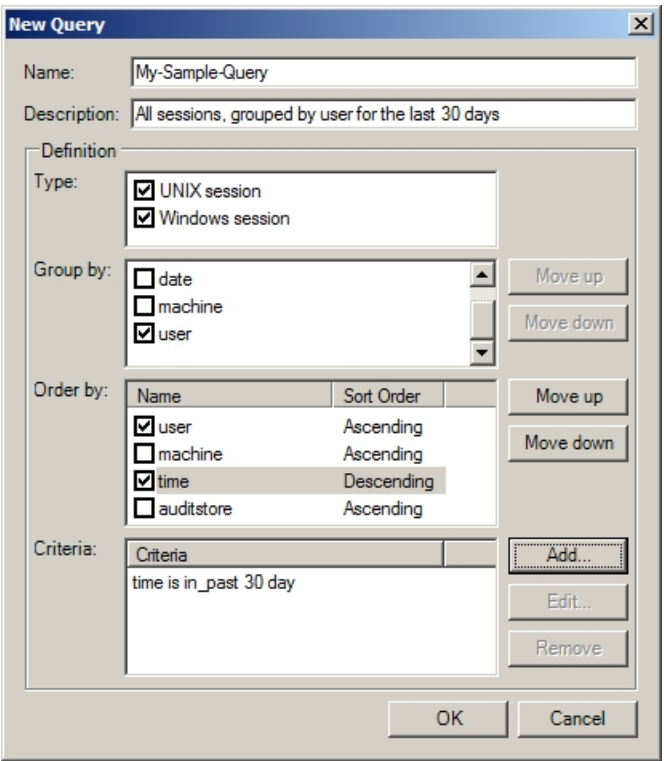
For example, you can search for sessions based on the period of time in which they were active or based on a specific state. You can also search for sessions based on the activity that took place during the session. For example, you can find sessions where specific UNIX commands or Windows applications were used.
8. Select the appropriate criteria for the attribute you have selected, then click **OK**.

The specific selections you can make depend on the attribute selected. For example, if the attribute is **Review Status**, you can choose between "Equals" and "Not equals" and the specific review status you want to find.,

such as “To be Reviewed.” If you select the attribute **Comment**, you can specify “Contains any of” and type the text string that you want to find any part of.

When creating queries for user names or computers, you might want to use the “Starts with” option. If you use the default to match “Is (exactly)”, you must include the fully qualified domain name of the user or computer.

9. Click **Add** to add another filter to the criteria for the query, or click **OK** to save the query and find the sessions that match the criteria you have specified.



### Adding multiple filters to the query criteria

If you have more than one filter, different criteria attributes, such as Time and State, are separated by an implicit AND operation. Only sessions that match both criteria are returned. If you have repeated criteria attributes, for example, if you have two Time filters (time is not in past 10 days; time is in last month), the attributes are separated by an implicit OR operation. Sessions that match either criteria are returned.

### Editing and removing filters from the query criteria

You can edit and remove any of the filters you specify. For example, if you are not finding the appropriate sessions, you might need to change or remove the



criteria you have defined. After you have saved a query, you can right-click the query name, then select **Properties** to modify the query definition.

## Specifying command or application filters in the query criteria

When you specify criteria for commands, applications, or outputs, the entry field displays a list of possible matches from audited sessions based on the text you are typing. For example, if you select “**windows Applications**” as the attribute and “**Contains any of**” and start typing “**word**” as the text string, the entry field displays a list of possible matches that contain “**word**” in the application name. You can select a potential match or continue typing to specify the application by its display name or the executable file name. For example, you can specify **winword.exe**, **Microsoft Word**, or both.

## Creating a new shared query

A shared query is a set of search criteria that you define for other auditors to use. Shared queries are visible to the auditors you specify. Only the auditor who creates a query can grant permission to other auditors to use the query. You create shared queries by selecting options in Audit Analyzer dialog boxes in exactly the same way as you create private queries. Your selections are then translated into complex expressions in the SQL Server query language. You can also convert a private or quick query to a shared query.

### To create a new shared query:

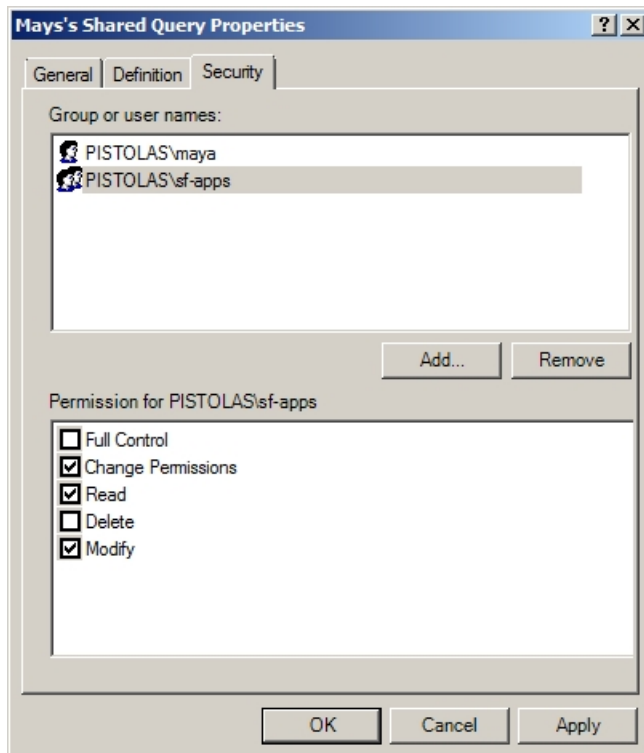
1. Open Audit Analyzer, select **Audit Sessions**, right-click, then select **New Shared Query**.
2. Type the query name and select the session type, grouping, ordering, and other criteria for the query.  
If you need more information about specifying information for any field in the new query, .
3. Click **Add** to add another filter to the criteria for the query, or click **OK** to save the query and find the sessions that match the criteria you have specified.
4. Expand **Shared Queries**, select the query name you specified in Step 2, right-click, then select **Properties**.
5. Click the **Security** tab.



6. Click **Add**.
7. Type the user or group name to identify the auditors who should have permission to use this query, then click **OK**.

You can add multiple users or groups from the Select Users or Groups dialog box. You can also type part of the name, then click **Check Names** to look up user and group names.

8. Select each user or group, then select the appropriate permissions.



## Searching for shared queries

After you publish queries and give other users permission to access them, other auditors can search for and select the shared queries they want to use. The shared queries are not automatically visible to users who have permission to use them.

### To find shared queries you have permission to use:

1. Open Audit Analyzer, select Audit Sessions, right-click, then select **Open Shared Queries**.
2. Type the query name or click **Show existing queries**, then click **Find Now**.
3. Select one or more queries from the results returned, then click **OK** to add the query to your list of Shared Queries.

## Creating queries for audit events

In addition to the predefined queries for audit events, you can create your own queries based on the criteria you define. Audit events are recorded for many activities, including both successful and failed operations. For example, you can search for events that are recorded when users attempt to log on and authentication fails or when users run commands or use applications with a role that grants elevated privileges. Audit trail events are also recorded when there are changes to the auditing infrastructure, and when there are changes to Centrify zones.

### To specify the search criteria for a new audit event query:

1. Open Audit Analyzer, select Audit Events, right-click, then select **Query Audit Events**.
2. Type the query name and, optionally a description for the query.
3. Type a user name if you want to filter the event query by user name.  
You can specify one or more user names in `userPrincipalName` format (`user@domain`). Use semi-colons (;) to separate multiple user names. For example, to limit the search for audit events to events recorded for actions taken by the users ben, maya, and fred, you could type the following:  
`ben;maya;fred`
4. Type a computer name if you want to filter the event query by computer.  
You can specify multiple computer names separated by semi-colons.
5. Select the Event time option if you want to specify a time frame to filter the query based on when the event occurred.  
If you select this option, you can search for events that occurred:
  - before, not before, after, not after, between, or not between specific dates and times.
  - in or not in the last specified number of days, hours, or minutes.
  - during the specified period of time.
6. Select the Type option to search for events based on the type of activity performed.  
If you select this option, you must click > to view and select the event categories in which you are interested. For details about the type of



events recorded in each category, select the category and review the Description displayed for that category.

7. Select the Result option to search for events based on the result of the activity performed.

For example, you can use this option in combination with other options to search for only successful or failed operations.

8. Select the Role option, then a role name and zone if you want to filter the event query by role.
9. Select the Parameter option if you want to filter the query based on a specific parameter.

If you select this option, you must click > to view and select the event parameters that are currently available and in which you are interested.

10. Click **OK** to save and run the new query.

After you create a new query, you can export the query definition or its results, email it to others, or modify its properties.

## How Access Manager roles affect audit trail events

If you only enable auditing without access control and privilege management features, audit trail events are recorded for all successful and failed operations on audited computers. The events are stored in the audit store database and can be returned in response to queries. These events are not associated with roles, so you should not use the Role filter in your query definition.

If you enable auditing with access control and privilege management, however, user activity is only recorded when a role with “auditing required” or “audit if possible” setting is used to perform one or more tasks. In most cases, roles that allow users to perform tasks using elevated privileges or in a restricted shell environment are configured with one of these audit settings. By default, the Windows Login and UNIX Login roles are also configured to “audit if possible” to capture all audit trail events on the computers where the auditing service is running. If a role is configured with audit not requested or required, only audit trail events are recorded.

If the auditing service is running on the computer where the user logs on or where the administrative tasks are performed, the audit trail event is collected and transferred to the audit store database. Only the audit trail events that are captured and stored in the audit store database can be returned in response to



audit event queries. Therefore, from Audit Analyzer, you can only query and report on audit trail events that are stored in the audit store database while a user performs tasks in an audited role on an audited computer.

## Querying by audit event type or by role

In many cases, querying for audit trail events by event type produces more predictable results than querying for events by role. For example, to query for successful and failed login attempts, select Type, then select the Login Event category. In this particular case, the Windows Login and UNIX Login roles do not—as a user’s effective role—capture successful and failed login attempts, so they should not be used as filters for querying successful and failed login events.

If you query using the Role filter, Audit Analyzer only returns the audit trail events associated with the selected role. In some cases, this might be the information you are looking for—for example, to review the execution of commands using a role with elevated privileges. On UNIX computers, however, many audit trail events are not linked directly to the actions taken with a specific role. For example, on a Linux or UNIX computer with the auditing service running, many command-line activities record audit trail events. These events are stored in the audit store database and can be queried, but are not associated with any role and not reported if you select a role filter.

## Populating and deleting the roles available

The list of roles available for querying is based on the roles you have defined using Access Manager. If you add a role definition, the new role displays in the list of roles when an audit trail about the role is generated.

If you delete a role from all zones, however, it will remain in the list until the last session that has events associated with that role is deleted or the audit store database is detached.

## Organizing queries in custom folders

By default, queries are organized into folders by type. You can choose to organize your queries in other ways. For example, you can create a custom hierarchy of folders and move your queries into those folders. The folder information is stored locally and does not affect other auditors, so each auditor can have a private folder structure for favorite queries.



## To create a custom folder hierarchy:

1. Open Audit Analyzer, select Audit Sessions, right-click, then select **New Folder**.
2. Select the new folder, right-click, then select **Rename** and type a new folder name.
3. Right-click the new top-level folder, then select **New Folder** to create sub-folders.

## Exporting and importing query definitions

You can export and import query definitions from one Audit Analyzer console to another to make queries available to different groups of auditors. You can also export query definitions for individual queries or for queries stored in a custom folder hierarchy. For example, if you have a custom “Queries Required at All Sites” folder, you can select that folder and only export those query definitions.

### To export query definitions:

1. Open Audit Analyzer, select the Audit Analyzer root node, right-click, then select **Export Query Definitions**.
2. Select a location and type a file name, then click **Save**.  
All of the query definitions are saved to an xml file.

### To import query definitions:

1. Open Audit Analyzer, select the Audit Analyzer root node, right-click, then select **Import Query Definitions**.
2. Navigate to the location that contains the .xml file you want to import, then click **Open**.

The imported queries are created as private queries. If you have an audit role with Manage Shared Query privileges, you can publish the imported queries as shared queries.



## Displaying session information

After you select a query to see a list of sessions, such as the **Today** query to see a list of today's sessions or an individual user to see a list of sessions for that user, you can view an indexed list of the activity that took place during any of the individual UNIX or Windows sessions captured.

For example, you can select a Windows session, right-click, then select **Indexed Event List** to review a list of the applications that were opened during the session, in the order in which they were opened, the title of the active window, the type of activity, the desktop role used to access the application, and whether audit data was captured for the role being used. If you have video capture auditing enabled for the installation, you can replay the session entirely or from any point in the indexed list.

Similarly, for UNIX sessions, you can select a specific session, right-click, then select **Indexed Command List** to display a list of commands executed and the order they occurred. If you have video capture auditing enabled for the installation, you can replay the session entirely or from any point in the indexed list.

## Adding session reviewers without designating auditing roles

If you have been assigned an auditing role that allows you to replay, delete, and update the status of an auditing session, you can also designate users or groups the permission to replay and update the status of that session, even if they do not have an assigned auditing role.

**Note:** Users and groups assigned as session reviewers cannot delete auditing sessions, and therefore cannot change the reviewer list for the sessions available to them.

### To designate users or groups as reviewers of one or more auditing sessions:

1. In Audit Analyzer, select the session or sessions you want to be reviewed. You can do this by selecting the predefined groupings or by defining specific criteria using a query.



2. Right-click the selected sessions and select **Set Reviewers**.
3. Type all or part of the name of the user or group that you want to add to the list of reviewers and click **Check Names**.  
If you would like to add multiple reviewers, separate the full or partial names by semicolons.
4. Click **OK**.

To remove reviewers from a session, right-click the session and select **Clear Reviewers**.

## Changing the review status for audited sessions

You can use the review status to keep track of audited sessions. For example, if you have a formal review process, you can change the state of sessions to indicate whether they are in the queue to be reviewed, have been reviewed, are awaiting some type of action, or should be deleted. For each change of state, you can add comments to more fully document what's been done or if any follow-up by another auditor is required.

By default, all audited sessions start with a review status of **None**.

### To update the review status for a session:

1. Open Audit Analyzer and navigate to the session.
2. Select the session in the right pane, right-click, then select **Update Review Status**.
3. Select the appropriate new status.  
For example, select **To be Reviewed** if the session requires a review or **To be Deleted** if the session has no activity requiring further review or data that must be retained.
4. Type any notes for yourself or other auditors in the Comments dialog box, then click **OK**.

## Viewing status history

The changes you and other auditors make to the review status for a session are recorded and cumulative, so that you can view the complete status change



history for any session.

## To view the status change history for a session:

1. Open Audit Analyzer and navigate to the session.
2. Select the session in the right pane, right-click, then select **Properties**.
3. Click the **Review Status** tab.

Changes to the review status are listed with the most recent change at the top of the list and proceeding back in historical order. You can select any review status change in the list to see who made the change and any comments recorded when the change was made.

## Adding comments to a session

The comments associated with a session are cumulative. For example, if you select **To Be Reviewed** and type a comment, then later change the state to **Reviewed** with another comment, both comments are displayed on the **Comments** tab if you view the session's Properties.

You can also add comments to a session without changing its review status. To add comments to a session without changing the review status, right-click the session, select **Properties**, then click the **Comments** tab. You can use this tab to record detailed information about sessions of interest. You can also use the **Review Status** attribute to find sessions by review status, and the **Comment** attribute to find sessions by comment text.

## Reviewing and deleting your own sessions

By default, you can update the review status, add comments, and delete your own sessions if you have an audit role with the appropriate permissions. However, there are installation-wide options to prevent any users from updating the review status or deleting their own sessions. These installation-wide options take precedence over your audit role permissions. Depending on how these options are set, you might be prevented from updating the review status and adding comments to your own sessions, prevented from deleting any of your own sessions, or prevented from both. If either installation-wide option is set, you might be blocked when you attempt to add a comment or delete a session.



## Playing back a session

If you select the **Enable video capture auditing option** for an installation, you can replay session activity captured on audited Windows or UNIX computers.

For Windows computers, the video record captures desktop activity when users select roles with auditing enabled.

For UNIX sessions, the video record captures complete input and output typed in a UNIX shell during a session.

If the Replay option is available for a session on the right-click menu, you can view a summary of the commands executed or applications opened in the session player. You can also search for commands, parameters, or events, control the playback speed and magnification from the session player, and update the session review status.

### To play back a session when video capture auditing is enabled:

1. Open Audit Analyzer and navigate to the session.
2. Select the session in the right pane, right-click, then select **Replay** to open the session player.

The left pane of the session player displays a summary of activity similar to the indexed list. For example, if the session is a Windows session:

• • • • •

**Summary**

User: admin@acme.local  
Machine: centryfy01.acme.local  
Start time: 5/9/2019 2:41:59 PM  
Last event time: 5/9/2019 2:48:00 PM  
Review status: Reviewed  
DirectAuthorize desktop: Default

**Events**

Time	Application	Title	Type	Desktop	Audited
5/9/2019 2:41:59 PM	Microsoft Mana	Centrif Audit Anal	Application	Default	Y
2:42:03 PM	Console Window	Access Module for P	Application A	Default	Y
2:42:03 PM	Windows Power	Access Module for P	Application A	Default	Y
2:42:35 PM	Microsoft Mana	Centrif Audit Analy:	Application A	Default	Y
2:42:37 PM	Microsoft Mana	Centrif Audit Analy:	Title Change	Default	Y
2:43:19 PM	Microsoft Mana	Indexed Event List	Window Acti	Default	Y
2:43:23 PM	Microsoft Mana	Centrif Audit Analy:	Window Acti	Default	Y
2:43:28 PM	DirectAudit Sessi	Centrif DirectAudit	Application A	Default	Y
2:47:13 PM	Microsoft Mana	Centrif Audit Analy:	Application A	Default	Y
2:47:13 PM	Microsoft Mana	Centrif Audit Analy:	Title Change	Default	Y
2:47:13 PM	DirectAudit Sessi	Centrif DirectAudit	Application A	Default	Y
2:47:15 PM	Windows Explore	Program Manager	Application A	Default	Y
2:47:17 PM	Consent UI for a	User Account Contr	Application A	Default	Y

The current event displayed in the player is highlighted in the list of events.

You can search on any column to find events of interest. If the session is a UNIX session, you can search the full session for any text string. For example, if you are playing a UNIX session, the right pane displays the shell session and a search field.

**Summary**

User: admin@centos03.acme.local  
Machine: centos03.acme.local  
Start time: 5/9/2019 4:05:50 PM  
Last event time: 5/9/2019 4:06:39 PM  
Review status: Reviewed


**Events**

Time	Command
5/9/2019 4:05:50 PM	/bin/bash
4:05:53 PM	adinfo
4:06:21 PM	dainfo
4:06:31 PM	dainfo
4:06:39 PM	dacontrol -e

Search the full record of the session by typing a search string here

Search the event list here



3. Click the **Play/Pause** icon () at the bottom of the session player to start or stop the session you are viewing.

You can also fast forward session playback by clicking the **Speed control** icon to play back at 2x or 3x the normal speed. The dark blue playback line across the bottom of the window represents the total time of the session. You can drag the **Timepoint needle** to go directly to a specific point in the session.

The **Real-time** icon toggles to allow you to play back a session as it was recorded in real time or move swiftly from one user action to the next. The **Session point** in the lower right corner identifies the date and time of the current point in the session playback.

4. To update the session review status:
  - a. Select **Session > Update Review Status**, and then select the desired review status.
  - b. Add your review comments and click **OK**.

The updated session review status displays in the session player.

5. Close the session player.

## Starting the session player separately

In most cases, you start the session player from Audit Analyzer. However, you can also start the session player from a Windows command prompt using standard Windows command line options or by specifying a Uniform Resource Identifier (URI).

### Using Window command line options

If you use the Windows command line to start the session play, the installation name and session ID are required. The other arguments are optional.

```
daplayer /installation=installation_name /id=session_guid  
[/conn=auditserver_connection_string]  
[/store=auditstore_ID]  
[/time=timestamp]
```

For example:

```
daplayer.exe /installation=MyInstallation  
/id="{f533142a-d3e8-4b4a-ae9f-86ce156bdad0}"  
/store=1
```

If you don't specify the audit server connection string, the session player attempts to bind to an appropriate audit management database. The session player can replay sessions from only one audit store, but the audit store ID is optional because sessions usually reside in a single audit store. An individual session can span multiple audit store databases within a single audit store. If a session spans multiple audit stores, that is, different subnets or sites, you should specify which audit store to play it from.

The timestamp option is a 32-bit integer that tells the session player to jump to the point where the event of interest occurred.

## Using the Uniform Resource Identifier (URI)

The Uniform Resource Identifier identifies the session player, the installation name, and the session GUID for each session. This format is especially useful when used with the **Copy Session URI** menu item. The URI link can then be pasted into an email or instant messenger message. On a computer where Audit Analyzer is installed, the recipient can simply click on the URI link and the session player starts automatically.

### Playing back a session from a web browser

On computers that have Audit Analyzer installed, you can also play back sessions from a web browser. Because the `cda://` protocol is automatically registered on the computer with Audit Analyzer, you can use a web browser to replay a specific session. If you want to play back a session from a web browser, you can extract the installation and session identifier from the session URI.

## To get the installation and session identifier:

1. Select a session and right-click or open the session in the session player, then select **File > Copy Session URI**.
2. Open a text editor and paste the session URI into the file.
3. Delete the portion of the URI that identifies the player, so that only the installation and the object GUID remain.

For example, if the URI looks like this:

```
rep://myInstallation/b62bc280-678c-439a-aec3-09a9b7ee4395
```

Remove the first part of the URI so that you only have the installation name and session identifier:

```
//myInstallation/b62bc280-678c-439a-aec3-09a9b7ee4395
```

• • • • •

## To play back a specific session from a web browser:

1. Open a web browser.
2. Type the installation name and session ID in the address bar of the web browser:

```
cda://<installationName>/<session_id>
```

For example:

```
cda://myInstallation/b62bc280-678c-439a-aec3-09a9b7ee4395
```

The session player opens and plays the specified session.

## Exporting sessions

Depending on whether you have selected the **Enable video capture auditing option** for an installation, you might have different options for exporting session data to a file. The options available also depend on whether the session activity was captured on an audited Windows computer or an audited UNIX computer.

To view your export options, select the session and right-click or open the session in the session player, then click the File menu. Depending on the session type or installation settings, you might see the following export options:

### Export to Command List

Exports the time stamp and UNIX shell commands as comma separated values (csv) in a text file. The file contains the same information as displayed in the Indexed Command List for UNIX sessions.

### Export to Event List

Exports the time stamp, application name, and other details as separated values (csv) in a text file. The file contains the same information as displayed in the Indexed Event List for Windows sessions.



• • • • •

## Copy Session URI

Copies the URI of the selected session to the clipboard. You can then paste the URI into a web browser to open the session.

## Check Session Data Integrity

Checks the session for any possible data tampering. If the session is fine, a message displays that the data integrity check passed. If the session has been tampered with, a message displays with details of what data was affected.

## Export to TXT

Saves the selected UNIX session(s) or UNIX session(s) and user input (stdin) as a plain text file.

If you selected multiple sessions, a message displays that asks you if you want to export the multiple sessions to a single file. Click **Yes** to save the sessions in a single file or **No** to save the sessions in separate files.

If you select the Export Session with User Inputs option, user input is noted with a line number of K or “keyboard” input.

## Export Detailed Executions

Saves the session in HTML, PDF, CSV, or XML format if you have enabled advanced monitoring and the session includes any detailed executions.

## Export to CDF

Saves the selected Windows session in Computable Document Format. You can then open the CDF file with the session player (`daplayer filename.cdf`). Because the session player reads the session information directly from the CDF file, you don't need to specify an installation name or connect to a database to replay the session.

## Export to WMV

Saves the selected session in Microsoft Windows Media Video format. You can use Windows Media Player or other media players to play back sessions in this format. However, sessions exported to WMV files do not include the summary information such as the user name, the computer name, start and end times, or the list of events captured.

## Deleting sessions

Auditing allows you collect detailed information about activity in your organization. In some cases, however, you might have sessions that collect information that you are not interested in capturing or include information that you don't want to store or make available to other auditors. For example, you might find there are sessions with very little activity or sessions that have been reviewed and are no longer needed. You might also notice that there are sessions that captured personally-identifying or medical data that other auditors should not be allowed to see. To handle these cases, you can selectively delete sessions from the audit store database.

In most cases, if you are the Master Auditor or have been granted permission to change the status of a session, you can mark sessions for deletion in Audit Analyzer. As noted in [Reviewing and deleting your own sessions](#), however, you might be prevented from deleting your own sessions if the installation-level setting prevents users from deleting their own sessions.

### To delete a specific session:

1. Open Audit Analyzer console, then use a predefined or custom query to find the sessions that you want to delete.
2. Select the sessions that you want to delete.
3. Right-click, then select **Delete**.  
Audit Analyzer displays a confirmation message indicating that the deletion cannot be reversed.
4. Click **Yes** to continue.

## To delete all sessions in a query:

1. Open Audit Analyzer, right-click a query node, then select **Delete All Sessions**.  
Audit Analyzer prompts you to confirm the deletion of all sessions returned by the query.
2. Click **Yes** to continue.  
Audit Analyzer prompts you to confirm the deletion of sessions with a review status of To be Reviewed or Pending for Action.
3. Click **Yes** to delete those sessions, or click **No** to continue the deletion of other sessions but preserve the sessions marked for retention.  
While the delete operations runs, you can click Stop Delete if needed.  
Sessions are partially deleted up until the point where the delete operation was cancelled.

## Viewing sessions outside of Audit Analyzer

You can view audited sessions while working in other Centrify management consoles. For example, on computers that have Audit Analyzer and Access Manager installed, you can start the session player from Access Manager or from Active Directory Users and Computers. You can also launch the session player by itself or from a web page or a software program.

### Viewing sessions from Access Manager

On computers where both the Access Manager console and the Audit Analyzer console are installed, you can search for and view sessions directly from the Access Manager console.

## To view audited sessions in Access Manager:

1. Navigate to a computer, user, or role assignments node in the left pane of Access Manager.
2. In the right pane, right-click the object and select **View DirectAudit Sessions**.
3. Specify any additional criteria, then click **Find**.

## Viewing sessions in Active Directory Users and Computers

On computers where you have Active Directory Users and Computers with Access Manager properties and Audit Analyzer, you can view audited sessions directly from Active Directory Users and Computers.

### To view audited sessions from Active Directory Users and Computers:

1. Navigate to the Users node in the left pane of the Active Directory Users and Computers.
2. In the right pane, right-click the user and select **All Tasks > View DirectAuditSessions**.
3. Specify any additional criteria, then click **Find**.

## Using Find Sessions

Find Sessions is a separate executable file, installed in the same directory as Audit Analyzer, that you can use to find and open audited sessions. The program provides a graphical user interface and a command line interface for specifying the search criteria. You can use either interface to find sessions of interest. From the Find Sessions graphical user interface, you can also replay, update the review status, view the desktops used for any sessions found, display the list of indexed commands or events, and copy the session URL.

To start Find Sessions from the Windows command line, you can type the following in a Command prompt window:

```
findsessions /ia
```

### Specifying the sessions to find

You can use the Common or Advanced search criteria to find sessions of interest. The Find Sessions dialog box then displays the results that match the criteria you specify. In most cases, you can find the sessions you are interested in through some combination of user name, computer name, and session time displayed on the Common tab. If you want to specify additional criteria, such as review status or auditor name, you can click the Advanced tab.

## Using the command line interface

You can run Find Sessions as a command line utility on computers where Audit Analyzer is installed. The command line interface can be useful, for example, if you may want to find, export, or delete sessions as part of a script. You can view usage information for the command line interface using the `/help` option. Specify search criteria for finding sessions using the following format:

```
findsessions /i="InstallationName" /u="username" /m="computerName"
/t="yyyy-MM-dd"
```

## Using a web browser to access sessions

On computers that have Audit Analyzer installed, you can also find and play back sessions from a web browser. Because the `cda://` protocol is automatically registered on the computer with Audit Analyzer, you can use a web browser to open Find Sessions or to replay a specific session. For example, you can embed a `cda://` link in a web page to automatically generate a list of sessions, or you might want to embed a link to a session or set of sessions in a web-based report or event notification.

You must be able to specify a query using AQL syntax to open Find Sessions from a web browser. If you want to start playing back a session from a web browser, you must know the session identifier. You can extract the session identifier from the session URI.

## To start Find Sessions from a web browser:

1. Open a web browser.
2. Type the installation name and a search string using AQL syntax in the address bar of the web browser.

For example, if you want to search an installation named `MyInstallation5` for sessions that involved the `Administrator` user, you would type the following in the address bar:

```
cda://DefaultInstallation5/?search=\"1 user=\"Administrator*\"\""
```

3. Click **Allow** to open the Find Sessions with the Advanced tab displayed and `user=Administrator*` listed for the Define Criteria.
4. Click **Find Now** to find sessions matching the criteria you specified.

For more information about using Find Sessions, see the Find Sessions help.

# Advanced monitoring

The Centrify Audit & Monitoring Service captures input and output for audited users and commands and then uses this information to provide a history of executed commands.

However, you may want to gather additional information about which users and what programs are accessing or modifying production systems. For example, you may want to know when any user runs a highly privileged program, even if the user runs it from a script or by modifying system configuration files. You can use advanced monitoring to capture these kinds of activities.

One of the big differences in advanced monitoring is that you can track when any user performs a particular activity, not just an audited user.

Advanced monitoring uses the Linux system auditing tools to capture the following user and program activity:

Use case	Where to review the user activity	Are audit trail events generated for this activity?
When any user executes a particular program, not just audited users.	<ul style="list-style-type: none"> <li>■ Audit Analyzer</li> <li>■ Linux agent syslog</li> <li>■ Monitored Execution report</li> <li>■ Monitored Execution List</li> </ul>	yes
When any user (not just audited users) attempts to modify system configuration files in monitored directories specified by an administrator.	<ul style="list-style-type: none"> <li>■ Audit Analyzer</li> <li>■ Linux agent</li> </ul>	yes

Use case	Where to review the user activity	Are audit trail events generated for this activity?
	syslog	
	■ File Monitor report	
Which programs are executed in an audited session, regardless of how the program is invoked-- whether it's run by way of a script, the use of a command alias, and so forth.	<ul style="list-style-type: none"> <li>■ Audit Analyzer</li> <li>■ Detailed Execution report</li> </ul>	no - there would be too many events for the information to be useful.

The following topics are covered:

Set up advanced monitoring .....	167
Using the advanced monitoring reports .....	169

## Set up advanced monitoring

To configure advanced monitoring, make sure that your computer meets the requirements, make some configuration changes in the `centrifyda.conf` file, and then enable advanced monitoring either by using the `dacontrol` command or the “Enable Advanced Monitoring” group policy.

### Advanced monitoring requirements

- Currently, Centrify supports only 64-bit Linux distributions from RedHat (RHEL, Fedora, CentOS). For more information about supported platforms and versions, please refer to the current Centrify Audit & Monitoring Service release notes.
- Verify that you have the Linux audit package running. For example, run this command:  
`rpm -qa audit`
- Ensure that the Linux audit package that you have is supported for use with Centrify Audit & Monitoring Service. Version 1.2.8 or later of Linux audit package is required. However, Centrify Audit & Monitoring Service



prefers the Linux audit package version 2.4.5 or later because earlier versions may have issues with startup.

- Ensure that your collector and audit store database are running Centrify Server Suite 2017 or 2017.1, or Centrify Infrastructure Services 2017.2 or later.

## Configuring advanced monitoring

You have some options and choices as to how you configure advanced monitoring. To use any of these parameters, you must also enable advanced monitoring (by using the `dareload -m` command or the “Enable Advanced Monitoring” group policy). Here’s a list of the configuration parameters that you can edit in the `centrifyda.conf` file:

- **event.file.monitor**

Use the `event.file.monitor` parameter to enable advanced monitoring for configuration files.

- **event.file.monitor.process.skiplist**

For any areas that you’ve specified to monitor (using `event.file.monitor`), use the `event.file.monitor.process.skiplist` parameter to ignore any specific processes in those areas.

- **event.file.monitor.user.skiplist**

Use the `event.file.monitor.user.skiplist` parameter to specify a list of users to exclude from advanced monitoring for files. For these users, the auditing service does not record any write access to directories specified in `event.file.monitor`.

- **event.execution.monitor**

Use the `event.execution.monitor` parameter to monitor all programs that users run in an audited session.

- **event.monitor.commands**

Use the `event.monitor.commands` parameter to specify a list of commands to monitor. Be sure to list each command using the full path name of the command. The auditing service generates an audit trail event when a user runs any of these monitored commands, unless the user is listed in the `event.monitor.commands.user.skiplist` parameter.





- **event.monitor.commands.user.skiplist**

Use the `event.execution.monitor.user.skiplist` parameter to specify a list of users to exclude from advanced monitoring for program execution. For these users, the auditing service does not record any programs that they run, even when the parameter `event.execution.monitor` is set to `true`.

After you make the configuration changes in the `centrifyda.conf` file, run the `dacontrol -m` command to apply the changes.

## Enabling advanced monitoring

After you've made your configuration changes in the `centrifyda.conf` file, the next step is to enable advanced monitoring.

### To enable advanced monitoring:

- Run the following command:  
`dacontrol -m`
- Or, use the Enable Advanced Monitoring group policy.

### To disable advanced monitoring:

- Run the following command:  
`dacontrol -n`
- Or, discontinue using the Enable Advanced Monitoring group policy.

## Using the advanced monitoring reports

These reports provide details on what your advanced monitoring configuration has tracked:

- **Monitored execution report**

If you have configured your auditing installation for advanced monitoring, then this Monitored Execution Report provides a detailed record of the sessions where a user ran one of the commands that you've configured to



monitor. This report shows who ran one of the monitored commands even if that person is not an audited user. Also, this report includes information on commands that are run individually or as part of scripts.

- **Detailed execution report**

If you have configured your auditing installation to perform advanced monitoring, then this Detailed Execution 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**

The File Monitor report shows the sensitive files being modified by users on the audited machines. The File Monitor report includes any activity by any user (except root) in the following protected areas on audited computers:

- `/etc/`
- `/var/centrifydc/`
- `/var/centrifyda/`
- `/var/centrify/`

# Troubleshooting and common questions

This chapter describes how to view and manage log files and diagnostics for components of the auditing infrastructure on UNIX computers. This chapter also describes how to identify and resolve common problems you might encounter when auditing user activity or managing the auditing infrastructure.

The following topics are covered:

Checking the status of the UNIX agent .....	171
Viewing and changing log file settings .....	174
Tracing database operations .....	179
Stopping auditing on a computer .....	182
Determining collector status and connectivity .....	183
Managing Microsoft SQL Server databases .....	187
Publishing installation information in Active Directory .....	189
Monitoring file system disk space usage .....	189

## Checking the status of the UNIX agent

After you install and enable auditing for a UNIX computer, you can check the status of the agent using the `daifno` command to verify the connection to the correct installation. For example, the agent might not automatically connect to the installation if you use an installation name other than `DefaultInstallation`.

To check the status of the agent and the auditing infrastructure, run the following command as a user with root privileges:

• • • • •

```
dainfo --diag
```

The `--diag` option returns detailed information about the local computer and about the installations, audit stores, trusted collectors, trusted agents, and the active audit store database that the agent is sending its data to. The diagnostic output also includes details about the Active Directory location and object identifier for each installation.

## Configuring the installation for an agent

If the command indicates that the status is offline or the installation is not configured, use `dacontrol` to explicitly identify the correct installation. For example:

```
dacontrol -i installation_name
```

You can then rerun `dainfo --diag` to verify the installation is configured correctly. Note that you cannot use `dacontrol` to connect to a different installation name if the installation is configured using the Installation group policy. In a secure installation, the Installation group policy identifies the Active Directory location that contains the service connection point object for the installation. If you are not using group policy to identify the installation, you can manually configure agents and collectors to use a specific installation name.

## Checking for disconnected agents using Audit Manager

You can also use Audit Manager to see the status of all agents in the installation. If any agent is listed as Disconnected, you should check whether the audited computer is shut down. If the audited computer is not shut down, the agent might be outside the scope of any audit store or unable to find a collector. Use the diagnostic services to check communication between components.

## Starting and stopping the UNIX agent

In most cases, the UNIX agent is automatically started when an audited computer is first powered on and remains running until the audited computer is shut down. Starting the agent when a computer starts up ensures the agent can capture activity for all shell sessions.



Although you typically start and stop the dad process as part of a computer's startup and shutdown scripts, you can also start the agent directly from the command line on a local computer.

If the agent is not running, run the following command to start it:

```
/usr/share/centrifydc/bin/centrifyda start
```

## **Detecting the authentication, privilege elevation, and audit and monitoring services installation status**

If you're encountering any issues with your authentication, privilege elevation, and audit and monitoring services installation, you can run the dacheck program on your UNIX computers. The dacheck command detects the following errors in your authentication, privilege elevation, and audit and monitoring services installation:

- Auditing binaries linkage problems
- Disk space
- DNS, collector, dad, adclient health
- Logging status
- Auditing file permissions/ownership
- Auditing installation configuration
- If ActiveDirectory joined
- Auditing database integrity
- If root in user.ignore and other criteria that affect root login
- var/centrifyda, /tmp write permission
- nsswitch.conf (or method.cfg, user.cfg for AIX)
- Selinux status
- Nscd (pwgrd) status
- User's cdax/real shell existence, permission, ownership.
- DNS Reverse lookup for collector's hostname
- Report Domain Controller

To check the status of the agent and the auditing infrastructure, run the following command as a user with root privileges:



- dacheck

The dacheck command is available in the same location as the adcheck command: `/usr/share/centrifydc/bin`.

## Viewing and changing log file settings

Log files are text files that record information about operations performed by auditing components on a local computer. If you have administrative privileges on a computer, you can open log files with any text editor.

You can view log files, change the location of the log file, and change the level of detail recorded in the log file from the Log Settings dialog box. Depending on the computer you are using, there are different ways to open the Log Settings.

### Audit Manager

By default, the log file for Audit Manager is located in the `C:\Users\User\AppData\Roaming\Centrify\DirectAudit\Log` directory. Select the Audit Manager top-level node, right-click, then select **Log Settings** to change the location or the level of detail recorded in the log file. By default, only error and warning messages are logged. You should only modify log settings if instructed to do so by Centrify Support.

### Audit Analyzer

By default, the log file for Centrify Audit Analyzer is located in the `C:\Users\User\AppData\Roaming\Centrify\DirectAudit\Logs` directory. Select the Audit Analyzer top-level node, right-click, then select **Options** to display the Log Settings tab. You can use the tab to change the location or the level of detail recorded in the log file. By default, only error and warning messages are logged. You should only modify log settings if instructed to do so by Centrify Support.

### Audit Management Server

By default, the log file for the audit management server is located in the `C:\Program Files\Common Files\Centrify Shared\Log` directory. You can



open the Audit Management Server Control Panel, click the **Troubleshooting** tab, then click the **Options** to display Log Settings if you want to change the location or the level of detail recorded in the log file. By default, error, warning, and informational messages are logged. You should only modify log settings if instructed to do so by Centrify Support.

## Collectors

By default, the log file for the collector service is located in the C:\Program Files\Common Files\Centrify Shared\Log directory. You can open the Collector Control Panel, click the **Troubleshooting** tab, then click the **Options** to display Log Settings if you want to change the path to the log file or change the level of detail recorded in the log file. By default, error, warning, and informational messages are logged. You should only modify log settings if instructed to do so by Centrify Support.

## Audited computers

By default, the log file for the Centrify Agent for Windows is located in the C:\Program Files\Common Files\Centrify Shared\Log directory. You can open the auditing Agent Control Panel, click the **Troubleshooting** tab, then click **Options** to display Log Setting if you want to change the path to the log file or change the level of detail recorded in the log file. By default, error, warning, and informational messages are logged. You should only modify log settings if instructed to do so by Centrify Support. On UNIX computers, detailed logging is disabled by default. For information about enabling logging, see [Enabling detailed logging for Linux and UNIX computers](#).

**Note:** A list of auditing agent error codes is available in KB-7541 in the Centrify Knowledge Base.

## Enabling detailed logging for Linux and UNIX computers

In most cases, troubleshooting auditing-related issues requires information about the operation of the agent, the collector service, and database activity. For performance reasons, you should only enable agent logging when you need to capture detailed information about agent operations. For troubleshooting



purposes, however, you can use the `dadebug` command to turn on detailed logging.

## To enable audit-related logging on audited Linux or UNIX computers:

1. Switch to the root user.
2. Run the `dadebug clear` command to remove any existing detailed logging from previous operations.  
`dadebug clear`
3. Run the `dadebug on` command to enable detailed logging on for audit-related agent operations.  
`dadebug on`  
  
Detailed messages are recorded in the `/var/log/centrifydc.log` file. You can view the contents of the log file with a text editor. In most cases, however, you should collect additional information and send all of the logged information to Centrify Support.
4. Restart the auditing service.  
`/usr/share/centrifydc/bin/centrifyda restart`
5. Run the `dainfo` diagnostic command and save the output to a text file.  
`dainfo --diag > /tmp/dainfo.txt`
6. Run the `adinfo` diagnostic command and save the output to a text file.  
`adinfo --diag > /tmp/adinfo.txt`
7. Stop detailed logging of audit-related activity.  
`dadebug off`
8. Send an email to Centrify Support with the log files and the agent configuration file as an attachment.  
`/var/log/centrifydc.log`  
`/tmp/dainfo.txt`  
`/tmp/adinfo.txt`  
`/etc/centrifyda/centrifyda.conf`





## To check whether detailed logging is enabled:

1. Run `dadebug` without parameters to see if detailed logging is currently enabled.

`dadebug`

Centrify DirectAudit debug logging is on.

2. Run `addebug` without parameters to see if detailed logging is currently enabled.

`addebug`

3. Run `addebug off` to disable logging, if needed.

## Enabling detailed logging for the collector service

If you are troubleshooting an auditing-related issue, you should enable detailed logging for the collector service on the computers where the collector service runs.

## To enable detailed logging on a collector:

1. Log on to a computer with a collector service.
2. Click **Start > All Programs > Centrify Infrastructure Services 19.9 > Centrify Audit & Monitoring Service > Audit Collector Control Panel** to open the Collector Control Panel.
3. Click the **Troubleshooting** tab.
4. Click **Options**, change the logging level to **Trace messages**, then click **Apply**.
5. Note the log folder location or click **Browse** to specify a different location for the log file, then click **OK**.
6. Click **View Log** to view the current log file.  
From the log file window, you can also click **File > Save As** to save the log file.
7. Click **Close** to close the Collector Control Panel.
8. Send an email to Centrify Support with the log file from the location specified in Step 5 as an attachment.
9. Open the Collector Control Panel, click the **Troubleshooting** tab, click



**Options**, change the logging level back to its default setting of **Informational messages**, then click **OK**.

## Enabling detailed logging for auditing consoles

In most cases, troubleshooting auditing-related issues requires information about the operation of the agent and the collector or database activity. However, in some cases, it might be necessary to capture detailed information about the operation of Audit Manager or Audit Analyzer.

### To capture detailed information for Audit Manager:

1. Log on to a computer with the Audit Manager console.
2. Click **Start > All Programs > Centrify Infrastructure Services 19.9 > Audit Manager** to open the Audit Manager console.
3. Select the Audit Manager node, right-click, then click **Log Settings**.
4. Change the logging level to **Trace messages**, then click **Apply**.
5. Note the log folder location or click **Browse** to specify a different location for the log file, then click **OK**.
6. Send an email to Centrify Support with the log file from the location specified in [Enabling detailed logging for the collector service](#) as an attachment.
7. Right-click Audit Manager, click **Log Settings**, change the logging level back to its default setting of **Warning messages**, then click **OK**.

### To capture detailed information for Audit Analyzer:

1. Log on to a computer with the Audit Analyzer console.
2. Click **Start > All Programs > Start > All Programs > Centrify Infrastructure Services 19.9 > Audit Analyzer>** to open the Audit Analyzer console.
3. Select the Audit Analyzer node, right-click, then click **Options**.
4. Change the logging level to **Trace messages**, then click **Apply**.
5. Note the log folder location or click **Browse** to specify a different location for the log file, then click **OK**.



6. Send an email to Centrify Support with the log file from the location specified in [Enabling detailed logging for the collector service](#) as an attachment.
7. Right-click Audit Analyzer, click **Options**, change the logging level back to its default setting of **Warning messages**, then click **OK**.

## Tracing database operations

Database traces are used to help diagnose problems in the management database or audit store databases. For example, database traces can help to identify inconsistencies caused by hardware errors or network interruptions. After you enable database tracing, Audit Manager tracks all of the SQL statements and debug messages from the audit management database or audit store, and records the information in the database server.

**Note:** Tracing database operations affects database performance. You should only activate a database trace if you require this information for troubleshooting. Before you start a database trace, try to reduce the load on the database instance as much as possible, then only perform the actions needed to reproduce the issue you are troubleshooting. Turn off database tracing as soon as you have logged the activity you need for the analysis of database operations. The trace for each database can take up to 800MB of server disk space. After you turn off database tracing, restart the SQL Server instance to reset the disk space.

### Starting a database trace

You can start a database trace for a management database or an audit store database.

#### To start database tracing:

1. Open Audit Manager.
2. Select an installation name, right-click, then click **Properties**.



3. Click the **Database Trace** tab.

This tab displays basic information about the management databases and audit store databases for the selected installation. In the Trace Status column, you can see whether tracing is enabled or disabled for each database.

4. Select a management or audit store database in the list, then click **Enable** to start tracing on the database selected.
5. Click **OK**, then perform the database actions for which you want to capture information.

## Stopping the database trace

You should turn off database tracing immediately after you have logged the activity you need for the analysis of database operations.

### To stop database tracing:

1. Open Audit Manager.
2. Select the installation name, right-click, then click **Properties**.
3. Click the **Database Trace** tab.
4. Select the management or audit store database that has tracing enabled, then click **Disable** to stop tracing on the database selected.
5. Click **Export** to save the database trace from the selected databases to a file with comma-separated values (.csv).
6. Follow the prompts displayed in the Export Database Trace wizard to save the information to a file.

## Exporting the database trace for a management database

The Export Database Trace wizard prompts you for different information depending on whether the database trace is for a management database or an audit store database. For example, if you generate a database trace for a management database then click **Export**, the Export Database Trace wizard prompts you for user accounts.

## To export the database trace:

1. Select a start date and time for the **From** filter and an end date and time for the **To** filter, then click **Next**.
2. Click **Add** to search for and select users, then click **Next**.  
By default, you can search for users in the entire directory, you can click **Object Types** or **Locations** to change the scope of the search scope, or click **Advanced** specify other criteria.
3. Accept the default folder location or click **Browse** to select a different location, then click **Next**.
4. Review your selections, then click **Next**.  
By default, the wizard save the file as *installation\_name.csv* and opens the file location.
5. Click **Finish**, then click **OK** to close the installation properties.

## Exporting the database trace for audit store databases

When you select an audit store from the lower area of the **Database Trace** tab on the **Properties** page and click the lower **Export** button, the wizard opens with a date/time **Export Criteria** page. On the second page, the wizard asks you to pick the domain and computer.

## To export the database trace:

1. Select a start date and time for the **From** filter and an end date and time for the **To** filter, then click **Next**.
2. Click **Add** to search for and select collectors, then click **Next**.  
By default, you can search for computers in the entire directory, you can click **Object Types** or **Locations** to change the scope of the search scope, or click **Advanced** specify other criteria.
3. Click **Add** to search for and select management database computers, then click **Next**.
4. Accept the default folder location or click **Browse** to select a different location, then click **Next**.
5. Review your selections, then click **Next**.



By default, the wizard save the file as `audit_store_name.csv` and opens the file location.

6. Click **Finish**, then click **OK** to close the installation properties.

## Delegating database trace management

You can delegate the authority to manage database tracing by granting the Manage Database Trace permission to other users for a management database or an audit store database.

## Stopping auditing on a computer

Several actions can directly or indirectly stop auditing on a computer. For example:

- Someone powers down the audited computer.
- Someone logs in on the audited computer and stops the agent.
- The audited computer is moved to a different audit store, causing the initial audit store to consider the audited computer disconnected.
- The administrator checks the **Define trusted audited computer** list on the Advanced tab of an Audit Store Properties page, and does not include the audited computer on that list.

## Resuming auditing if the agent stops

If the dad service stops running for any reason, audited shell sessions will stop working and you will be prompted to resume or quit auditing. If you resume auditing, the `cdawatch` process attempts to start dad and connect to the installation. However, if you have manually stopped the dad process, for example by running `/usr/share/centrifydc/bin/centrifyda stop`, you must manually restart the agent.

If you decide to quit auditing when the dad service has stopped running, you are prompted to confirm that you want to terminate the session before the session ends.

## Allowing users to log in when auditing is stopped

If auditing is required but the agent is not running, users might be prevented from logging in. You can log in as a user with root privileges and either restart the agent or temporarily disable auditing using `dacontrol -d` to allow users to log in.

You can also run `dainfo --diag` or check the log file to get more information. For example, if the `adclient` process is not running, you might be unable to restart auditing.

If you cannot immediately correct the problem, you can temporarily disable all auditing.

## Determining collector status and connectivity

You can use the Collector Control Panel to generate a complete diagnostic check of the collector. The diagnostic report includes detailed information about the current status of the collector and the installation and audit store to which the collector sends data.

### To generate diagnostics on a collector:

1. Log on to a computer with a collector service.
2. Click **Start > All Programs > Centrify Infrastructure Services 19.9 > Centrify Audit & Monitoring Service > Audit Collector Control Panel** to open the Collector Control Panel.
3. Click the **Troubleshooting** tab.
4. Click **Diagnostics**.

The results are displayed in a Diagnostic Information window. If connections are successful and components are configured correctly, you should see results similar to this:

```
Establishing connection with collector: Success
Getting collector's current status: Running
Getting collector's current installation: DefaultInstallation (locally
configured)
Getting collector's current Audit Store: Data
Source=pysql.py.dev\CENTRIFYSUITE;Initial Catalog=AuditStoreWindows-2018-
11-02
Machine IP address(es): 10.140.16.59
```

• • • • •

```
Machine is joined to: py.dev
Forest: py.dev
Using Domain Controller: pydc.py.dev
Is Global Catalog Available: True
Using Global Catalog: pydc.py.dev
Machine is in site: Default-First-Site-Name@py.dev
Installations:
DefaultInstallation
AD Object: py.dev/Program Data/Centrify/DirectAudit/Vegas-Installation-
d97d8fc9-7876-4f5b-b161-4a7b3736b8ec
Object GUID: 1563b2e1-1ea3-4307-ac51-7c92fdf5cb8a
Installation ID: f7b36b73-0384-4283-b6f7-63a1cdb77b17
Audit Stores:
AuditStoreUNIX
Site(s): (Default-First-Site-Name@py.dev)
Subnet(s): None configured
Affinity: UNIX
Trusted Agents: None configured
Trusted Collectors: None configured
Audit Store Active Database:
Data Source=pysql.py.dev\CENTRIFYSUITE
Initial Catalog=AuditStoreUNIX-2018-11-02
Additional Connection Parameters=<none>
    AuditStoreWindows
    Site(s): (Default-First-Site-Name@py.dev)
    Subnet(s): None configured
    Affinity: Windows
    Trusted Agents: None configured
    Trusted Collectors: None configured
    Audit Store Active Database:
    Data Source=pysql.py.dev\CENTRIFYSUITE
    Initial Catalog=AuditStoreWindows-2018-11-02
    Additional Connection Parameters=<none>
    Machine's Installation: DefaultInstallation (locally configured)
    This machine's Audit Store is 'AuditStoreWindows' based on preferred
Audit Store (locally configured)
    Attempting to connect to Audit Store:
    Data Source=pysql.py.dev\CENTRIFYSUITE
    Initial Catalog=AuditStoreWindows-2018-11-02
    Integrated Security=TRUE
    Pooling=True
    Max Pool Size=1000
    Encrypt=True
    TrustServerCertificate=True
    Additional Connection Parameters=<none>
    Connected to Audit Store successfully
```

Done.

You can copy the results to a file and send them to Centrify Support for help.

## Resolving connectivity issues between a collector and an audit store

If the diagnostic report or the Collector Configuration wizard indicates that the collector cannot connect to an audit store database, check the following:



- Verify the account you logged in with has permission to add a collector.
- Verify the collector service has permission to connect to the active audit store database. You can grant this permission from Audit Manager.
- Check whether the SQL Server instance needs to be restarted. For example, make sure the SQL Server instance is not waiting for a restart to complete ASP.NET registration changes.
- Check whether there is a firewall between the collector and the SQL Server instance blocking access.
- Check whether SQL Server is configured to allow named pipes and TCP/IP connections.
- Check whether SQL Server is configured to allow remote connections.
- Compare the site or subnet that the collector is configured to use with the scope of the audit store. For example, make sure the audit store site or subnet matches the site or subnet in the audit store properties.

```
AuditStore
  Site(s): (Default-First-Site-Name@pistolas.org)
  Subnet(s): None configured
```

## Resolving authentication issues

If you configure the collector service to use an Active Directory account instead of the local system account, you might encounter problems with Kerberos authentication when the collector attempts to connect to the audit store database. Kerberos authentication uses the service principal names (SPN) registered for the SQL Server account to authenticate a service. When the collector (client) wants to connect to SQL Server, it locates an instance of the service, composes an SPN for that instance, connects to the service, and presents the SPN for the service to authenticate. If the collector service account does not have any SPNs, the Kerberos authentication request fails.

To resolve this problem, go to KB-1311 in the Centrify Knowledge Base, select **Attachments**, and click **View > Open > Run** to run the `checkspn.vbs` script on a computer that is joined to Active Directory.

**Note:** The user who is running this command must have permission to register the SPN on the service account.

By default, this script runs in report-only mode. It checks whether the required SPNs are present on the service account in question and issues a prompt to fix



it, if not. This script registers the SPN in the service account `servicePrincipalName` attribute in the format:

```
MSSQLSvc/<FQDN>:<tcpport>
```

## Monitoring collector performance counters

If you have enabled auditing and installed the collector service on a local Windows computer, you can add audit-specific performance counters to Performance Monitor to help you analyze and resolve audit-related issues. When you install the collector, the performance counters are added automatically, if you uninstall the collector, the counters are also automatically removed from Performance Monitor.

### To add authentication, privilege elevation, and audit and monitoring services performance counters:

1. Log on to a computer with a collector service.
2. Click **Start > Administrative Tools > Performance Monitor**.
3. Expand Monitoring Tools and select **Performance Monitor**.
4. Click the green plus (+) icon in the toolbar.
5. Find the Audit Collector from the list, and expand it to show the list of available performance counters.

The performance counters generally fall into one of three categories; agent information, packet volume, and data loads. For example, if you add the counter # Connected Agent, you will be able to view the number of agents currently connected. If you add the counter # Unix Meta Message Packet, you will be able to view the number of Unix meta message packets. If you add the counter, Bytes Unix Command, you will be able to view Unix command data in bytes.

6. Choose the performance counter you would like to add and click **Add**.
7. Repeat Step 6 until you have added the counters you want to monitor.
8. Click **OK**.

## Managing Microsoft SQL Server databases

Managing an audit installation requires permission to create new SQL Server databases on a SQL Server instance. In a production environment, this is an ongoing process to keep databases small and efficient. Because the management of the audit databases is not a one-time setup operation, Centrify recommends that you have at least one dedicated SQL Server instance for the audit administrator to use. The audit administrator should also be a member of the SQL Server system administrator role to ensure full control over the databases created and archived.

### Selecting SQL Server or Windows authentication

When you configure the Microsoft SQL Server instance to use for auditing, you must specify the type of authentication to use. The appropriate type of authentication depends on how your production environment is configured. For example, if you have a firewall between components or one-way trust relationship between forests, you must allow SQL Server authentications.

To support the auditing infrastructure, you can use the following types of authentication:

- Windows authentication for creating new databases.
- Windows authentication or both SQL Server authentication and Windows authentication for connections between collectors and audit stores.
- Windows authentication or both SQL Server authentication and Windows authentication for connections between audit stores and the audit management database.
- SQL Server authentication for collectors in an untrusted forest and an audit store in a trusted forest.
- SQL Server authentication for audit store databases in a trusted forest and audit management database in an untrusted forest.

If you choose Windows authentication, you can perform actions with your own logon account or using another Windows account name and password.

## Connecting to an installation or database

If you are unable to connect to the SQL Server database, the problem might be caused by one of the following issues:

- A firewall blocking access to the SQL Server instance.
- TCP/IP has not been enabled for the SQL Server instance of SQL Server
- Remote connections have not been enabled for the SQL Server instance.

For information about areas to check, see the following article:

<https://blog.sqlauthority.com/2009/05/21/sql-server-fix-error-provider-named-pipes-provider-error-40-could-not-open-a-connection-to-sql-server-microsoft-sql-server-error/>

## Assigning the service principal name for SQL Server

If you get error messages when performing database operations, such as creating a new audit management database using Audit Manager, the problem is likely because the service principal name (SPN) for the SQL Server instance is assigned to the wrong Active Directory container.

- If the SQL Server startup account is a local system account, the appropriate container is the computer name.
- If it is any other account, the appropriate container is the SQL Server startup account.

Because authentication tries to use the first SPN it finds, make sure that no SPNs are assigned to inappropriate containers. Usually this error occurs when the administrator does not remove a manually added SPN from the Active Directory container after changing the SQL Server service account.

For help troubleshooting this problem, read the following article:

<https://support.microsoft.com/en-us/help/811889/how-to-troubleshoot-the-cannot-generate-sspi-context-error-message>

## Publishing installation information in Active Directory

The default location for publishing audit installation information in Active Directory is:

`domain/Program Data/Centrify/DirectAudit`

In most cases, this location is accessible to any administrative user. If you cannot access the publication location, check the following:

- Make sure you have permission to publish information to Active Directory.
- Verify that the publication location exists in Active Directory.
- Check the network for problems.

Moving a service connection point from its published location can result in connection problems. If you delete the default publication location and add a new publication location, you might not have permissions on the new location. If you do not have the appropriate permissions on the new location, ask the Active Directory administrator to grant you such permissions before running any of the wizards to reconfigure agents and collectors.

**Note:** A new location might not be reflected immediately in the list current published locations. However, this has no any adverse effects apart from not being able to see the published location.

## Monitoring file system disk space usage

Like most software applications, Centrify agents require adequate disk space to be available to operate properly. For example, agents read and write temporary files to authenticate processes and ensure data integrity. If your operating system does not have enough disk space to accommodate these temporary files, the agent might be unable to run and prevent users from logging on or activity from being audited.

To prevent problems with disk space allocation, you should monitor key directories, such as the `/tmp` and `/var` directories, to ensure free space is available. The disk space required by different directories depends on the configuration and operating systems of the computer and the Active Directory environment. However, if any directory approaches 100% of its allocation, you

• • • • •

should allocate more disk or remove older files to free up space for continued operation.

# Command line programs for managing audited sessions

This chapter provides an overview of the command line interface that you can use to manage audited computers. For complete reference information about the required and optional parameters for each command, see the `man` page provided locally on the Centrify-managed computer.

The following topics are covered:

How to use command line programs .....	191
Displaying usage information and man pages .....	192
Using commands for administrative tasks .....	192

## How to use command line programs

Command-line programs allow you to perform administrative tasks directly from a UNIX shell or by using a shell script. These programs are installed when you install the Centrify UNIX agent, and are installed by default in the following directories:

- `/usr/sbin`
- `/usr/bin`

You can use the UNIX command-line programs to take action directly on a local UNIX computer, for example to enable or disable auditing manually on a local computer. You can also use these programs to perform administrative or diagnostic tasks when it is more convenient to run them on the UNIX computer than through Audit Manager. For example, you might find it more convenient to



view details about the agent configuration or diagnostic information directly on a local computer rather than through Audit Manager or the Agent Control Panel.

## Displaying usage information and man pages

You can display a summary of usage information for any UNIX command-line program by typing the command plus the `--help` or `-h` option. For example, to see the usage information for the `dacontrol` command:

```
dacontrol --help
```

For more complete information about any command, read the command's man page. For example, to see the man page for the `dacontrol` command, type:

```
man dacontrol
```

## Using commands for administrative tasks

The command-line programs allow you to perform administrative tasks—such as enable or disable shell auditing on UNIX computers or generate diagnostic information—directly on an audited computer. The following table provides a summary of the auditing-related programs installed with the Centrify Agent for \*NIX and the Centrify Client for Linux audit package. For complete information about the syntax and options for any command, see the man page for that command.

Use this command	To do this
<code>dacheck</code>	<p>The <code>dacheck</code> command performs operating system, network, and Active Directory tests to verify a computer meets the system requirements for a successful installation. For example, the <code>install.sh</code> script runs the <code>dacheck</code> program.</p> <p>The <code>dacheck</code> command is located in the same place as the <code>adcheck</code> command: <code>/usr/share/centrify/dc/bin</code>.</p>
<code>dacontrol</code>	<p>Enable or disable session or individual command auditing on a computer. You can also use this command to manually configure the audit installation to use for a local computer if you are not identifying the installation by group policy.</p> <p>Only users with <code>root</code> privileges can run the <code>dacontrol</code> command.</p>

**Note:** If the audited system is not joined to Active Directory and



Use this command	To do this
	it is audited by way of the Centrify Client for Linux, you cannot change the audit installation with the <b>dacontrol</b> command.
<b>dad</b>	<p>Start the <b>dad</b> process manually.</p> <p>The <b>dad</b> process records terminal activity on the UNIX computer and transfers the data to a collector. In most cases, it is automatically started when the computer is first booted. However, you can run this command to manually start the audit process on a local computer.</p> <p>Only users with <b>root</b> privileges can run the <b>dad</b> command.</p>
<b>dadebug</b>	<p>Enable or disable logging for the <b>dad</b> process on an audited computer.</p> <p>If you enable logging, the <b>dad</b> process writes messages to the <b>/var/log/centrifydc.log</b> file. If you run <b>dadebug</b> without specifying an option, the command returns a status message that indicates whether logging is currently enabled or disabled.</p> <p>Only users with <b>root</b> privileges can run the <b>dadebug</b> command.</p>
<b>dadiag</b>	<p>Display detailed information about the configuration and current auditing status for a local computer.</p> <p>This command displays the same information as <b>dainfo --diag</b>.</p>
<b>daflush</b>	<p>Clear the auditing service in-memory cache of name service queries and installation information.</p> <p>If you run this command without any arguments, it removes both auditing-related name service query results and audit installation information from the in-memory cache. If you run this command with no arguments or specify the <b>--name-service</b> option, the command also automatically clears the cache for common name services—such as <b>nscd</b> and <b>pwgrd</b>—if those services are running on the local computer.</p> <p>Clearing the cache of name service query results is useful if you make changes that would affect the results of a name service query, and want to ensure you get updated information. For example, if you remove the UNIX Login role for an Active Directory user, some information for that user might remain in the auditing service cache and be returned when you run a command such as <b>getent passwd</b> for that user. You can run <b>daflush</b> to ensure the user is removed completely from the local computer cache, including the auditing service cache.</p> <p>Only users with <b>root</b> privileges can run the <b>daflush</b> command.</p>
<b>dainfo</b>	Display detailed information about the status and configuration of an audited computer.
<b>dareload</b>	Force the <b>dad</b> process to reload configuration properties from the <b>/etc/centrifyda/centrifyda.conf</b> file or the advanced monitoring properties from <b>/etc/centrifyda/libaudit.conf</b> .

Use this command	To do this
	<p>This command enables you to apply configuration changes without restarting the agent.</p> <p>Only users with <b>root</b> privileges can run the <b>dareload</b> command.</p>
<b>dashe11fix.sh</b>	<p>Reset shells to their source shell on computers that are not being audited in an audited zone.</p> <p>On audited computers, the <b>cdash</b> shell is used to capture and forward audit data instead of the original shell. This script enables you to restore the user's original shell choice if the auditing service and wrapper shell are removed.</p>
<b>daspool</b>	<p>Display information about the size and content of the auditing-related offline cache (spool) files.</p> <p>If an audited computer cannot contact a collector service, it caches session, audit trail, and other information locally until a collector becomes available. This command enables you to review information about these offline cache files.</p> <p>Only users with <b>root</b> privileges can run the <b>daspool</b> command.</p>

## Configuring duplicate audit session cleanup

Sometimes the auditing service records duplicate sessions if your auditing installation includes one or more UNIX computers where both of the following situations occur:

- The DirectAudit agent is installed.
- A user can log in to the computer from the Admin Portal and the cloud tenant is enabled for auditing.

To avoid this situation, add the following environment variable to your `/etc/centrifydc/ssh/sshd_config` file:

```
AcceptEnv centrify_cip_da_data
```

Note that the above `/etc/centrifydc/ssh/` path applies if you're using the Centrify OpenSSH server. If you're using a different SSH server, the file path may be different-- so be sure to update the appropriate SSH daemon configuration file for your system.

With the environment variable set, the agent uses that to verify the SSH public key of the associated tenant. That way the auditing service can determine which sessions are duplicated and remove them. Also, the agent on the UNIX



computer will no longer record sessions that originate from the Admin Portal on the same computer.

## Downloading the tenant SSH public key

There's a script called `dadownloadsshpublickey.tcl` that downloads the tenant's SSH public key. With the public key and the `centrify_cip_da_data` environment variable, the auditing service can determine which audit sessions are duplicates and remove them.

The agent installer puts this tcl script into `/usr/bin`, except for CoreOS systems where the installer puts the script into `/opt/centrify/bin`. This script requires root privilege to run. The output file specified by dad for the script is `/var/centrifyda/tenant_rsa.pub`.

If dad fails to download the public key or if you need to change the public key after dad has started, you can manually run this tcl script.

```
/usr/bin/dadownloadsshpublickey.tcl --output-file  
/var/centrifyda/tenant_rsa.pub
```

Use the following options when you run this script:

- `--cip, --i <cloud tenant URL>`

This option is optional.

If the computer is not joined to the domain currently, use this option to specify the cloud tenant URL. If you don't use this option, the script finds the URL automatically if the computer is joined to the domain.

- `--output-file, -o <file>`

This option is required.

Use this option to specify the output filename for the tenant's SSH public key. This file must be in a parent directory that is writable by root only and the directory cannot be a symlink.

# Installing the UNIX agent on remote computers

In most cases, you install the UNIX agent locally on a computer using the `install.sh` script interactively. You can install the UNIX agent on remote computers using the `install.sh` script and a configuration file or using virtually any software distribution or package installer program. This chapter provides an overview of these alternatives for installing the agent on UNIX or Linux computers.

The following topics are covered:

Installing the agent silently using a configuration file .....	196
Using other programs to install the UNIX agent .....	197

## Installing the agent silently using a configuration file

You can automate agent installation by running the `install.sh` script in non-interactive mode:

```
install.sh -n
```

In this mode, the script uses configuration details specified in the `centrifda-install.cfg` file. If this file is not found, the `install.sh` script uses its built-in default values.

To specify configuration values, edit the sample `centrifda-install.cfg` file in its default location, or create a new text file with the same name, and then run the `install.sh` script.

In the file, `INSTALL=Y` installs the agent, and `INSTALL=U` upgrades the agent.



By default, the script returns an exit code of 0 if the operation is successful. To return exit codes that provide more detailed information about the result, use:

```
install.sh -n --custom_rc
```

This return code	Indicates
CODE_ SIN=0	Successful install
CODE_ SUP=0	Successful upgrade
CODE_ SUN=0	Successful uninstall
CODE_ NIN=24	Did nothing during install
CODE_ NUN=25	Did nothing during uninstall
CODE_ EIN=26	Error during install
CODE_ EUP=27	Error during upgrade
CODE_ EUN=28	Error during uninstall
CODE_ ESU=29	Error during setup; for example, unsupported operating environment or invalid arguments

## Using other programs to install the UNIX agent

Auditing-related files are bundled with the core Centrify agent files into a platform-specific software package. You must install the Centrify agent on the audited computer before you enable the auditing service.

### To install auditing using a native installation mechanism:

1. Log on as a user with root privileges.
2. If you want to install from a CD and the drive is not mounted automatically, use the OS-specific command to mount the cdrom device.
3. Copy the appropriate package to a local directory.

For Solaris 10:

```
cp /cdrom/cdrom0/Unix/centrifyda-n.n.n-sol10-sparc-local.tgz .
```

For Red Hat Enterprise Linux:



```
cp /mnt/cdrom/Unix/centrifyda-n.n.n-rhel5-x86_64.rpm .
```

For SuSE Linux:

```
cp /mnt/cdrom/Unix/centrifyda-n.n.n-suse11-x86_64.rpm .
```

4. If the software package is a compressed file, unzip and extract the contents. For example, on Solaris:

```
gunzip -d centrifyda-n.n.n-sol10-local.tgz  
tar -xf centrifyda-n.n.n-sol10-sparc-local.tar
```

5. Run the installation command appropriate to the operating environment.

For Red Hat Linux, you can use:

```
rpm -ivh centrifyda-n.n.n-rhel5-x86_64.rpm
```

For SuSE Linux, you can use:

```
rpm -ivh centrifyda-n.n.n-suse11-x86_64.rpm
```

For Solaris, you can use:

```
pkgadd -d CentrifyDA -a admin
```

**Note:** You can also use other programs, such as SMIT or YAST, to install the agent package.

6. If you are using an installation with a name other than `DefaultInstallation`, you need to configure it with `dacontrol` or using group policy.

If there is an installation with the name `DefaultInstallation` the UNIX agent uses it by default. For more information about specifying the installation, see [Configuring the installation for an agent](#).

7. After installing the package, use `dainfo` to verify that auditing is installed and running. You should see output similar to the following:

```
Pinging adclient:    adclient is available  
Daemon status:      Online  
Current collector:   DC2008r2-LG.pistolas.org:  
                    5063:HOST/dc2008r2-lg@PISTOLAS.ORG  
Session offline store size:    0.00 Bytes  
Session despool rate:         0.00 Bytes/second  
Audit trail offline store size: 0.00 Bytes  
Audit trail despool rate:      0.00 Bytes/second  
Getting offline database information:  
    Size on disk: 52.00 KB  
    Database filesystem use: 3.06 GB used,  
    15.52 GB total, 12.45 GB free  
DirectAudit NSS module: Active  
User (root) audited status: Yes  
DirectAudit is not configured for per-command auditing.
```

# Permissions required to perform administrative and auditing tasks

This chapter describes the permissions required to perform various auditing-related activities.

The following topics are covered:

Setting and synchronizing audit-related permissions .....	199
Installation permissions .....	200
Management database permissions .....	202
Audit store and audit store database permissions .....	204
Audit role permissions .....	205
Auditor permissions .....	205

## Setting and synchronizing audit-related permissions

As a Master Auditor, you can set the permissions that control what all other administrators and auditors can do. In most cases, you set these permissions by making selections in Audit Manager. Your selections are saved in the management database for each installation, then published in Active Directory whenever you synchronize the management database with the service connection point for the installation.



The permissions you can set consist of a specific action that can be taken, a scope to which the action applies, and the specific Active Directory user or group to which you are granting the permission.

For example, a permission might specify an action, such as ability to modify a name or detach a database with a scope such as a specific installation or audit store database. For each action and scope, you select the Active Directory user or group to be granted that permission. After users or groups are granted a permission, they are called a trustee for that action and scope.

## Installation permissions

Installation permissions allow users or groups to modify different aspects of an installation's properties. By default, the Master Auditor and the management database administrator have Full Control over the installation and can assign the following permissions to other users and groups:

This permission	Enables trustees to do this
Full Control	Perform all administrative tasks on the selected installation and assign permissions to other users and groups.
Change Permissions	Add, modify, or remove Active Directory users and groups that have specific permissions. A user or group granted this permission can display the properties for the installation, then click the <b>Security</b> tab to select permissions for other users and groups.
Modify Name	Modify the name of the selected installation. A user or group granted this permission can display the properties for the installation, then click the <b>General</b> tab to change the installation name.
Manage Management Database List	Add or remove a management database for the selected installation. A user or group granted this permission can right-click the installation name in Audit Manager and select <b>Management Databases</b> to add or remove a management database. Deleting the management database from Microsoft SQL Server requires additional SQL Server permissions.
Manage Audit Store List	Add, modify, or remove audit stores and audit store databases for the selected installation. A user or group granted this permission can use the Add Audit Store wizard or right-click the installation name in Audit Manager, select <b>Management Databases</b> , then click <b>Properties</b> to add or remove sites or subnets associated with the installation.



This permission	Enables trustees to do this
Manage Collectors	Add, modify, or remove collectors for the selected installation.
Manage Audited Systems	Add, modify, or remove audited computers for the selected installation.
Manage Audit Roles	Add, modify, or remove audit roles for the selected installation.
Manage Queries	Add, modify, or remove queries for the selected installation.
Manage Publications	<p>Add, modify, or remove publication locations in Active Directory for the service connection point associated with the selected installation.</p> <p>A user or group granted this permission can display the properties for the installation, then click the <b>Publication</b> tab to change the publication location in Active Directory for the installation.</p> <p>A user or group granted this permission can also update the information stored in Active Directory to keep the information in Active Directory synchronized with the information stored in the management database. However, users or groups with this permission must have sufficient Windows rights to be able to update objects in Active Directory.</p>
Manage License	<p>Add or remove license keys for an installation.</p> <p>A user or group granted this permission can display the properties for the installation, click the <b>General</b> tab, then click <b>Details</b> to manage licenses for the installation.</p>
Modify Notification	<p>Enable or disable the audit notification message for the selected installation.</p> <p>A user or group granted this permission can display the properties for the installation, then click the <b>Notification</b> tab to manage the notification message and image for the installation.</p>
Modify Audit Options	<p>Enable or disable video capture auditing for the selected installation.</p> <p>Control whether users are allowed to update the review status of their own sessions.</p> <p>Control whether users are allowed to delete their own sessions.</p> <p>A user or group granted this permission can display the properties for the installation, then click the <b>Audit Options</b> tab to manage installation-wide auditing options.</p>
View	<p>Enable read-only permission for the selected installation.</p> <p>If a user has only View permission, they can see all the auditing components in the Audit Manager console, but they do not have access to audited sessions nor can they change any installation details.</p>

## Setting installation permissions

You can set installation permissions for a specific installation, by selecting the installation name in Audit Manager.

### To set permissions on an installation:

1. Open Audit Manager and select the installation name.
2. Right-click, then click **Properties**.
3. Click the **Security** tab.
4. Click **Add** to open Select Users and Groups.
5. Type the user or group name who should be granted installation permissions, then click **OK**.

You can add multiple users or groups from the Select Users or Groups dialog box. You can also type part of the name, then click **Check Names** to look up user and group names.

6. Select the specific permissions you want to grant to the selected user or group.

## Management database permissions

Management database permissions allow users or groups to modify different aspects of an installation's management database. By default, the Master Auditor and the management database administrator have Full Control over the management database and can assign the following permissions to other users and groups:

This permission	Enables trustees to do this
Full Control	Perform all administrative tasks on the selected management database and assign permissions to other users and groups.
Change Permissions	Add, modify, or remove Active Directory users and groups that have specific permissions. A user or group granted this permission can display the properties for the management database, then click the <b>Security</b> tab to select permissions for other users and groups.
Modify	Modify the name displayed for the selected management database.

This permission	Enables trustees to do this
Name	A user or group granted this permission can display the properties for the management database, then click the <b>General</b> tab to change the management database name.
Manage Scopes	Add, modify, or remove sites or subnets for a management database. A user or group granted this permission can display the properties for the management database, then click the <b>Scope</b> tab to add or remove sites and subnets.
Remove Database	Remove a management database from an installation. Deleting the management database from Microsoft SQL Server requires additional SQL Server permissions.
Manage SQL Logins	Add or remove the Allowed incoming users for the selected management database. A user or group granted this permission can display properties for the management database, then click the <b>Advanced</b> tab to add or remove allowed accounts, or to change the outgoing account or authentication type.
Manage Database Trace	Enable, disable, or export database traces for the selected management database.

## Setting management database permissions

You can set management database permissions for a specific installation, by selecting the installation name in Audit Manager.

### To set permissions on an management database:

1. Open Audit Manager and select the installation name.
2. Right-click, then click **Management Databases**.
3. Select the management database, click **Properties**, then click the **Security** tab.
4. Click **Add**, type the user or group name who should be granted permissions, then click **OK**.
5. Select the specific permissions you want to grant to the selected user or group.

## Audit store and audit store database permissions

Audit store permissions allow users or groups to modify different aspects of an audit store or audit store database. By default, the Master Auditor and the audit store database administrator have Full Control over the audit store and its database and can assign the following permissions to other users and groups:

This permission	Enables trustees to do this
Full Control	Perform all administrative tasks on the selected audit store database and assign permissions to other users and groups.
Change Permissions	Add, modify, or remove Active Directory users and groups that have specific permissions. A user or group granted this permission can display the properties for the audit store, then click the <b>Security</b> tab to select permissions for other users and groups.
Modify Name	Modify the name displayed for the selected audit store. A user or group granted this permission can display the properties for the audit store, then click the <b>General</b> tab to change the audit store name.
Manage Scopes	Add, modify, or remove sites or subnets for the audit store. A user or group granted this permission can display the properties for the audit store, then click the <b>Scope</b> tab to add or remove sites and subnets.
Manage SQL Logins	Add or remove the allowed incoming collectors and management database logins for the selected audit store database. A user or group granted this permission can display properties for the audit store database, then click the <b>Advanced</b> tab to add or remove accounts for collectors and management databases.
Manage Collectors	Add, modify, or remove trusted collectors for the audit store. A user or group granted this permission can display properties for the audit store, then click the <b>Advanced</b> tab to add or remove accounts trusted collectors.
Manage Audited Systems	Add, modify, or remove trusted audited computers for the audit store. A user or group granted this permission can display properties for the audit store, then click the <b>Advanced</b> tab to add or remove accounts trusted audited computers.
Manage Databases	Add, attach, detach, or delete audit store databases for the selected audit store.
Manage Database Trace	Enable, disable, or export database traces for the selected audit store.

## Audit role permissions

Audit role permissions allow users or groups to modify different aspects of an audit role. By default, the Master Auditor has Full Control over the audit roles and can assign the following permissions to other users and groups:

This permission	Enables trustees to do this
Full Control	Perform all administrative tasks on the selected audit role and assign permissions to other users and groups.
Change Permissions	<p>Add, modify, or remove Active Directory users and groups that have specific permissions.</p> <p>A user or group granted this permission can display the properties for the audit role, then click the <b>Security</b> tab to select permissions for other users and groups.</p>
Change Role Membership	<p>Add, modify, or remove Active Directory users and groups that are assigned to the selected role.</p> <p>A user or group granted this permission can use the Add Audit Role wizard to assign users and groups to an audit role or select an audit role name, right-click, then select <b>Assign Users and Groups</b> to modify the role membership.</p>
Change Role Definition	<p>Modify the name, description, access, or privileges for the selected audit role.</p> <p>A user or group granted this permission can display the properties for the audit role, then:</p> <ul style="list-style-type: none"> <li>■ Click the <b>General</b> tab to modify the role name or description.</li> <li>■ Click the <b>Access</b> tab to modify the type of session and other criteria.</li> <li>■ Click the <b>Privileges</b> tab to modify what users and groups assigned to the role can do.</li> </ul>

## Auditor permissions

Auditor permissions allow users or groups to view, create, share, and delete queries. For an installation, the Master Auditor can control access to Audit Analyzer and queries using the Manage Queries permission and the assignment of audit roles. The privileges associated with an audit role also control whether auditor can update the review status or replay sessions. By default, the Master Auditor has Full Control over the auditor permissions and audit roles and can assign the following permissions to other users and groups:

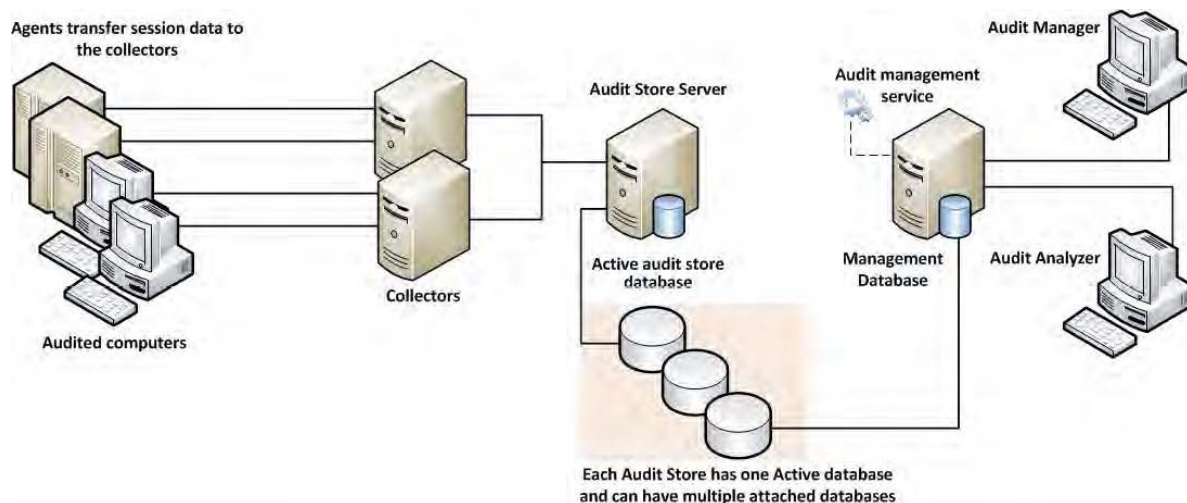
This permission	Enables trustees to do this
Full Control	Perform all administrative tasks on the selected query and assign permissions to other users and groups.
Change Permissions	Add, modify, or remove Active Directory users and groups that have specific permissions. A user or group granted this permission can display the properties for the query, then click the <b>Security</b> tab to select permissions for other users and groups.
Read	Read the selected query definition, session results, and indexed commands.
Delete	Delete the selected query definition, session results, and indexed commands.
Modify	Modify the selected query definition, session results, and indexed commands.

# Sizing recommendations for audit installations

A typical deployment of Centrify Audit & Monitoring Service consists of a number of components such as one or more audited Systems (UNIX/Linux or Windows), one or more collectors, audit management server, management database, one or more audit store databases and consoles (the Audit Manager and the Audit Analyzer consoles) which all communicate with each other. Given the complexity of this communication and number of components involved, good planning is important for a successful deployment of the product. When planning a deployment, some of the most common questions that we asked are below:

- Will just one installation of Centrify Audit & Monitoring Service suffice? Or are multiple installations needed or recommended?
- How many audit stores need to be provisioned in each of the installations and how should their scope be configured?
- How many collectors will be needed and what kind of hardware is recommended for each of them?
- What is the recommended version/edition of SQL Server and what kind of hardware is recommended to host this SQL Server?

You must take into consideration a number of factors when deciding how to plan and configure the audit and monitoring service deployment and what kind of hardware will be needed to deploy the key components. This section will help you understand these factors in detail and come up with answers to such questions.



The following topics are covered:

Planning an audit and monitoring service deployment .....	208
Best practices for an audit installation .....	212
Creating an initial estimate of your database storage needs .....	216
Guidelines for determining hardware configuration .....	216
Identifying typical deployment issues .....	220
Settings to adjust for performance improvement .....	222
Conclusion .....	225

## Planning an audit and monitoring service deployment

System Integrators often rely on the number of audited systems to estimate the hardware requirements and to come up with the overall strategy of audit and monitoring service deployment. For example, an environment with 100 audited systems may look like a small setup and one may incorrectly conclude that it's a small scale deployment that won't require a powerful hardware to support it. Once setup however, such assumptions may turn it into a deployment that seldom scales and often produces poor performance, both when capturing the audit activity and when querying the already captured audit data.





Below are a few factors that you must consider before making any deployment decisions,

## SQL Server

Out of all the components in the audit and monitoring service ecosystem, SQL is the most heavyweight and will share most of the burden when it comes to workload. Using a properly equipped and optimally configured SQL Server is very important. The version and edition of SQL Server being used (such as Express or Standard or Enterprise) or the type of machine being used to host the SQL Server (such as a virtual or physical machine) can noticeably improve the overall performance. On the contrary, a poorly configured SQL Server may produce a very poor performance no matter how powerful the underlying hardware is.

## Number of concurrently audited users

Relying on the number of audited systems is not always a good assumption. For example, an environment may have just a handful of systems but may have a large number of users logging into these systems on a daily basis. A jumpbox scenario such as Citrix XenApp Server is a perfect example. When planning, you should plan for the number of concurrently audited users, not just the total number of audited systems. User activity patterns and behaviors also play an important role in overall performance and storage requirements. For example, the audited data will be much smaller in an environment where no logins are expected most of the time as compared to a network control systems wherein audited users are logging on and logging out throughout the day. The sizing guidelines specified in the later section of this whitepaper have all been based on workload simulations for the exact same reason.

## What needs to be captured

What's being captured controls the overall workload on various components. Capturing video is more expensive than not doing so in terms of disk usage and load on collectors and SQL Server. Similarly, capturing interactive sessions is always going to produce more audited data when compared to capturing a handful of commands thus putting system under more pressure. Capturing large quantities of data has another side effect; it slows down database



backups and other maintenance processes which is not always liked by the database administrators.

## Who needs to be audited

Who is being audited is equally important. Under default settings, the audit and monitoring service audits everything and everybody and this may not be a practical solution in many large environments. In production environments, it's very common to see processes or scheduled tasks that periodically monitor UNIX/Linux or Windows systems for their health by remotely executing certain commands (System Monitoring and Management software, such as BMC Patrol that periodically runs vmstat or iostat command on each of the UNIX/Linux systems is a good example). Activities like these needlessly generate thousands of Audited sessions on a daily basis and in many cases create tremendous load on an entire audit and monitoring service system.

## UNIX/Linux and Windows

The type of system being audited influences the amount of data that will be captured from that system and the overall CPU load on collectors. For example, a Windows audited system almost always generates more data per day compared to a UNIX audited system with comparable number of concurrent users. This also means that an environment with Windows audited systems will most likely be more demanding (in terms of hardware resources) compared to an environment with same number of UNIX/Linux audited systems.

## Query performance

Query performance is one factor that often gets ignored. Capturing user activity and storing it in the database in a reasonable time is important. What's also important is to be able to search these records in a predictable time frame irrespective of the combined size and number of all the databases in the Centrify Audit & Monitoring Service system.

## Audit data retention policy

Audit data retention policy dictates how many days of data should be online and readily available for querying purpose and this number varies from one enterprise to another. Pay special attention to data retention policy requirements in the target environment. A longer retention policy typically results in large databases which also suffer from poor query performance if databases are not well maintained. On the contrary, too frequent rotation will also result in poor query performance if you keep too many inactive databases attached to the audit store.

## System overheads

Keep in mind the overhead that is caused by the Centrify Audit & Monitoring Service system itself; there are a number of background jobs carried out by various components of the audit and monitoring service system, including the audited systems themselves, collectors, and the Audit Management Server. This includes activities such as sending the audited system's heartbeat to the database (by way of collector), sending the collector's heartbeat to the database, processing active sessions list, processing and synchronizing information of audit roles with Active Directory Group criteria, calculating effective size of audited sessions, storing license usage information in Active Directory, and many more.

## Latency

Geography/Network topology play an important role as it introduces latency. For example, an environment may well have just a handful of audited systems but if they're not geographically co-located, you may see delays in getting the audited user activity to its final destination (the database server); the same may happen if audited systems are not connected to collectors by a network link with reasonable bandwidth. A general rule of thumb is to group together audited systems, collectors and databases that are connected by a high speed network using the concept of audit store.

## Best practices for an audit installation

The previous section listed out a number of factors that may affect how a audit and monitoring service system will be deployed. Below is a set of best practices that are derived from these factors. Follow these practices for planning any audit and monitoring service deployment (large or small). You can also refer to the last section of this whitepaper that discusses how to tweak settings in an existing environment to improve performance.

### Plan based on concurrently audited users

When planning, always focus on the number of concurrently audited users, not just the total number of audited systems. Take into consideration user sessions that might be generated as a result of automated monitoring activity from System Monitoring and Management software, such as BMC Patrol etc.

### Avoid single box deployment

Always avoid installing key components such as SQL Server, collectors and Audit Management Server on the same system, especially in environments with heavy workload. Keep in mind that a collector's workload is CPU intensive and SQL Server's workload is CPU, IO, and memory intensive. If both a collector and SQL Server are installed on the same system, they'll slow each other down.

### Control the amount of data

It's always a good practice to establish rules to avoid capturing unnecessary data. This typically includes blacklisting commands such as top or tail (which generate large outputs and seldom contain any meaningful user activity) or enable per-command auditing instead of session auditing. Also, compile a list of users that do not really need to be audited and add them to the non-audited user's list. This often includes user accounts that are used to run automated jobs from System Monitoring and Management software, such as BMC Patrol and so forth.

## Scope the audit stores efficiently

Always visualize the flow of traffic, not just when audited activity is being captured but also when it's being searched and replayed. It's better to avoid traffic over slow links by splitting the audited systems into multiple audit stores based on their geographic location, even if it may mean that you'll be deploying more collectors and SQL Servers. In certain cases, splitting audited systems into multiple audit stores may not be sufficient enough and you may even need to consider provisioning multiple audit and monitoring service installations. When audited data is being queried, all calls are routed to the audit store databases by way of the Management database. If the Management database is not connected to the console or to the audit store databases by way of a fast network link, the queries will always return the results slowly no matter how good the performance of SQL Server is.

## Estimate storage requirement based on pilot data

No two customers are the same and you can never accurately predict how much data will be collected over a period of time in each environment. Hence, it's important to analyze existing data in a customer's environment (from pilot project) to predict the future data growth. A pilot testing is an effective way to help you understand a number of things such as the following factors:

- Understand workload patterns and come up with an overall configuration strategy that determines how the audit stores will be scoped, which users should or should not be audited, which commands should be blacklisted and so forth.
- Database storage requirement – Roughly, how much data will be collected over the retention policy period? This will also help you establish the active audit store database rotation policy.
- What kind of hardware will be needed for the SQL Server to serve the production workload?
- How many collectors will be needed in each audit store (this number is especially important when auditing Windows systems)?

The Centrify Audit & Monitoring Service Data Analysis tool (see [KB-4496](#)) can be very helpful to understand data trends. If the Centrify Audit & Monitoring Service Data Analysis tool reveals that more than anticipated amount of data is being captured, you can always use the database rotation to keep the active



audit store database's size in control thus controlling the storage requirements for all attached databases.

## **Maintain databases periodically**

Apart from taking regular backups, it's also important to keep the databases healthy by maintaining them periodically. This includes activities such as reorganizing or rebuilding indexes; these tasks must be done by a customer's DBA periodically. Centrify recommends reorganizing indexes if they are 5% to 30% fragmented and rebuilding indexes if they are more than 30% fragmented.

## **Control the size of active databases**

A large active audit store database often results in poor performance as a result of fragmented indexes, lengthy backups, and out of date database statistics, especially when the databases are not maintained periodically. Centrify recommends keeping the active audit store database size between 250GB-500GB (as of Suite 2016). Consider rotating databases whenever the size exceeds the recommended thresholds. You can rotate databases programmatically by using either the Centrify DirectManage SDK or the Centrify Audit PowerShell Module, or manually using the Audit Manager console). It's also a good practice not to keep too many audit store databases attached to an audit store, because doing so affects query performance.

## **Plan database rotation based on retention policy**

Always try to align the audit data retention policy with the active audit store database rotation. For example, if the audit data retention policy requires last 90 days of data to be online, try to rotate the active audit store database every 90 days. This strategy makes it easy to find achieved data if it's ever needed for reviewing purpose in the future. One exception to this strategy is an environment where the audit data retention policy is so long that the active audit store database is guaranteed to exceed the recommended maximum size of the active audit store database (as mentioned in the previous section). In such cases, you can divide the entire retention policy period into small periods (for example, one database for each month) and continue to rotate the active audit store database at the recommended intervals. Irrespective of



which strategy you choose and implement, it's always recommended to detach all audit store databases that contain data outside of the retention policy period. This not only improves the query performance but also reduces the disk usage on the database server.

## **Configure SQL Server optimally**

Centrify recommends setting the SQL Server machine's power plan settings (Control Panel > Power Options) to High Performance.

SQL Server has a setting called Max Server Memory that controls the maximum amount of physical memory that can be consumed by the SQL Server's buffer pool. An incorrectly configured Max Server Memory may either result in the SQL engine causing high IO or OS/other programs starving for more memory. It's critical to configure the Max Server memory correctly based on the amount of total physical memory available. Always configure this value as recommended before deployment begins.

Centrify recommends storing the transaction logs and data files that are associated with any SQL Server database on two separate volumes. For more information, see the Microsoft Knowledge base article <https://support.microsoft.com/en-us/kb/2033523>.

## **Other recommendations**

Centrify recommends deploying at least two collectors per audit store for redundancy purpose.

## **Understand that any hardware has its limits**

It's entirely possible that even after following all the best practices, the Centrify Audit & Monitoring Service system continues to perform poorly. In such cases, you must consider splitting the workload by deploying additional SQL Servers or collectors, depending on where the bottleneck is. Deploying an additional SQL Server will almost always result in reconfiguring scope of the audit stores (in order to redirect some traffic to the new SQL Server) and it must be done with careful planning.

## Creating an initial estimate of your database storage needs

Here's a way that you can do an initial but rough guess of your recommended storage needs. For a more detailed estimate, please refer to [Guidelines for determining hardware configuration](#).

- 1 MB per minute per Windows session with nominal activity  
You could need considerably more storage than this if sessions will include flash animation, video replay, and so forth.
- Use a ratio of users to number of systems
  - For example, you could have 50 users for 1000 systems, which would be a 5% ratio; you would then multiply the number of users with the above estimates.
  - 50 Windows users would require 50 MB/minute, or 120 GB/week, or 1.5TB/quarter.

## Guidelines for determining hardware configuration

The overall performance of the audit and monitoring service ecosystem ultimately depends on the performance of SQL Server and the collectors. To come up with guidelines for hardware, we have created a test environment wherein the SQL Server hardware configuration has been categorized into three variants: a low end SQL Server, a high end server SQL Server, and a mid-level SQL Server. Below are the test environment configuration details:

	Low end hardware specification	Mid-level hardware specification	High end hardware specification
Physical machine	DIY PC	S5000 Intel Xeon	Dell R730
Physical memory	8 GB (2x4GB)	16 GB (2x8GB)	32 GB (2x16GB)
CPU	Intel i5-650, 3.2 GHz	E5420 (2.5 GHz)	2xIntel Xeon E5-1620 v3 (2.4 GHz, 8C/16T)
HDD	1x1TB (7200 rpm SATA)	1x1TB (7200 rpm SATA)	1x1TB (7200 rpm SAS 6Gbps)

The Hardware configuration depicted in the above table reflects the sizing test environment. Centrifify cannot make specific recommendations (such as physical





memory, CPU frequency, or CPU type) for purchasing hardware; use these numbers only as a guideline.

The table below lists the test conditions along with the outcome of tests, and this roughly indicates the recommended number of audited systems that can be supported in this test environment.

	<b>UNIX Agent (session auditing)</b>	<b>UNIX Agent (command auditing)</b>	<b>Windows Agent (video enabled)</b>	<b>Windows Agent (video disabled)</b>
Test conditions	60% agents are idle 35% agents are running simple commands 5% agents are running tail command	5% agents are idle 2% agents are running "su" sessions 93% agents are running "dzdo" command sessions	60% agents are idle 40% agents are active	100% agents are active
Low end SQL Server	1100	1800	400	1300
Mid-range SQL Server	1500	3600	400	2400
High end SQL Server	2000	4500	640	3000

- The numbers depicted in the above table reflects the outcome of a sizing test in a very specific test; use these numbers only as a guideline.
- Refer to the table in the next section for actual recommendations.

Based on these test results, Centrify recommends using the table below when planning a deployment of Centrify Audit & Monitoring Service. Please note that the recommended SQL Server configuration is only applicable to the SQL Server hosting the audit store database. It's generally a good practice to host the Management database on the same SQL Server where the other audit store databases are hosted.

Audited System Type	Audit Type	Number of Audited Systems	Expected Activity	Recommended SQL Server Configuration	Recommended Number of Collectors	Average Response Time (ms)
UNIX	Command auditing	1800	5% agents are idle 2% agents are running "su" sessions 93% agents are running "dzdo" command sessions	Low end	2	83
UNIX	Command auditing	3600	5% agents are idle 2% agents are running "su" sessions 93% agents are running "dzdo" command sessions	Mid-range	2	60
UNIX	Command auditing	4500	5% agents are idle 2% agents are running "su" sessions 93% agents are running "dzdo" command sessions	High end	4	102
UNIX	Session auditing	1100	60% agents are idle 35% agents are running simple commands 5% agents	Low end	2	87

Audited System Type	Audit Type	Number of Audited Systems	Expected Activity	Recommended SQL Server Configuration	Recommended Number of Collectors	Average Response Time (ms)
			are running tail command			
UNIX	Session auditing	1500	60% agents are idle 35% agents are running simple commands 5% agents are running tail command	Mid-range	2	76
UNIX	Session auditing	2000	60% agents are idle 35% agents are running simple commands 5% agents are running tail command	High end	4	104
Windows	Video disabled	1300	100% agents are active	Low end	2	91
Windows	Video disabled	2400	100% agents are active	Mid-range	3	67
Windows	Video disabled	3000	100% agents are active	High end	4	100
Windows	Video enabled	400	60% agents are idle 40% agents are active	Low end	5	85
Windows	Video enabled	400	60% agents are idle 40% agents are	Mid-range	5	88

Audited System Type	Audit Type	Number of Audited Systems	Expected Activity	Recommended SQL Server Configuration	Recommended Number of Collectors	Average Response Time (ms)
			active			
Windows	Video enabled	640	60% agents are idle 40% agents are active	High end	8	113

- Expected activity is based on 8 hours of work every day. Results may vary if the target environment has a different pattern for user activity/behavior, different workload/ratio of idle to active systems compared to the test environment.
- Average response time is the total time taken in milliseconds to send a unit of data from audited system to the SQL Server by way of collector.
- All recommended numbers are based on the assumption that the target environment is stable in terms of performance of individual components and network throughput. Intermittent transient errors are expected and typically do not impact the sizing assessments.
- Windows audited system generates large amount of audit data when video capture is enabled and such environments require high performance SQL Server storage. This is the primary reason why the number of agents supported between the low and medium SQL Server configuration are similar. The artificial load generated by the test simulators is also higher than the expected daily activity in a typical production environment. With high performance storage, the total number of Windows audited systems supported will likely be higher compared to the numbers recommended in this whitepaper.
- When monitoring both Windows and UNIX/Linux audited systems in the same environment, use the Windows numbers as a guideline.

## Identifying typical deployment issues

It's fairly easy to identify scaling/performance issues with a Centrifry Audit & Monitoring Service system that are typically a result of poor planning or deployment. Below are some of the most common deployment issues.

## Large spool files on audited systems

A healthy audit and monitoring service system should be able to keep up the pace with users' audited activity. When the system cannot keep up the pace, it means either the user's audited activity is generating too much data (such as when a user runs the `cat` command on a very large file) or the audit and monitoring service system components (such as collectors and databases) are not able to process and store the generated data fast enough. In such cases, you'll typically see large spool files on the audited systems that often need more time to get despoiled completely.

## Constant high CPU on collector/SQL Server

It's perfectly normal to see high CPU activity on collector and SQL Server machines during peak hours as this is the time when data is continuously getting pumped from the audited system to the collector and finally to the database. However, when you see similar activity during off-peak hours (especially when it doesn't correspond to the number of active users in that environment at that time), it indicates that the audit and monitoring service system is getting backlogged.

## Low despool rate

The despool rate largely depends on the type of data being captured, the speed of network/latency between audited system and collector, the speed of the network/latency between the collector and the database, and ultimately the performance of the SQL Server itself. Because of these factors, there's no ideal value or range for the despool rate. However, you should not see a despool rate that's significantly lower than the rate of data capture, especially when there are no known issues related to network speed or SQL Server performance.

## False "Agent disconnected" alerts

Each Agent periodically sends its heartbeat to the database (by way of collector) and the Audit Manager console relies on this ping to determine if the Agent is connected or not. If there are deployment issues with audit and monitoring service, the Agent heartbeat may not get registered even if the



Agent is online, and this may raise false alarms as the system will be shown as disconnected in Audit Manager Console. Whenever you see such contradicting information regarding the status of the audited system, it typically is indicative of underlying deployment issues.

## Too many SQL Server tasks in queue

SQL Server has a fixed set of worker threads that it can use to perform its job and this number depends on the CPU architecture, such as 32-bit or 64-bit, and the total number of CPUs on the SQL Server. If SQL Server is given more tasks than it can finish, they'll end up waiting at the bottom of this queue, thus consuming memory and degrading overall system performance. Always consult the DBA to confirm if the environment is consistently showing a lot of tasks in the worker queue; this can indicate that the workload is too much for this SQL Server to handle. For more information, see the Microsoft article [https://msdn.microsoft.com/en-us/library/ms177526\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms177526(v=sql.105).aspx).

## Settings to adjust for performance improvement

In an environment where Centrifry Audit & Monitoring Service is already deployed and experiencing scalability/performance issue, it's not always possible to re-architect the deployment or make significant configuration changes (such as re-scoping the audit stores or adding a new SQL Server may not be practical); this is true especially in large environments. The table below that lists some key settings that you may try to change in order to improve the overall performance of various audit and monitoring service components.

Title	Summary	When to adjust	Component
Agent Settings			
Agent heartbeat interval for Unix/Linux Audited Systems (dad.timer.update.agent.status)	Controls the interval for sending Unix/Linux Audited System's heartbeat to the Collector	When SQL activity monitor shows high CPU usage at a predictable interval as a result of heartbeat registration or when Collector logs reveal repeated failures in registering Audited System's heartbeat or when Audit Manager	Unix/Linux Agent (centrifryda.conf)

Title	Summary	When to adjust	Component
		console frequently shows a lot of disconnected Audited Systems even if they are all online.  For more details about the configuration parameter, see the Configuration and Tuning Reference Guide.	
Agent heartbeat interval for Windows Audited Systems (SessionPingInterval)	Controls the interval for sending Windows Audited System's heartbeat to the Collector	When the SQL activity monitor shows high CPU usage at a predictable interval as a result of heartbeat registration or when Collector logs reveal repeated failures in registering Audited System's heartbeat or when Audit Manager console frequently shows a lot of disconnected Audited Systems even if they are all online.	Windows Agent (registry setting)
User blacklisting (dash.user.skiplist)	Allows specifying blacklist of users that should not be audited on Unix/Linux systems	Useful in preventing capture of audit activity of users such as BMC Patrol agent or ServiceNow service accounts or users that do not really need to be audited.  For more details about the configuration parameter, see the Configuration and Tuning Reference Guide.	Unix/Linux Agent (centrifyda.conf) and also available via Group Policy
Audited/Non-audited users list	Allows specifying whitelist or blacklist of users that should or	Useful in preventing capture of audit activity of unwanted users.	Group Policy

Title	Summary	When to adjust	Component
	should not be audited on Windows systems		
BindingCheckInterval	Controls the interval at which Agent checks if it's connected to the correct Collector or not	When binding check causes load on the Domain Controller as a result of periodic Active Directory calls (for example, when you notice an Active Directory call from each Audited System every 10 seconds)	Windows Agent (registry setting)
<b>Collector settings</b>			
Agent global heartbeat interval (AgentMinimumUpdateInterval)	Controls the interval for sending Audited System's heartbeat to the Collector at the Collector level (in case it's not practical to tweak this setting on each of the Audited Systems)	When SQL activity monitor shows high CPU usage at a predictable interval as a result of heartbeat registration or when Collector logs reveal repeated failures in registering Audited System's heartbeat or when Audit Manager console frequently shows a lot of disconnected Audited Systems even if they are all online.	Collector (registry setting)
Maximum concurrent SQL connections per Collector (MaxPoolSize)	Controls how many SQL connections (maximum) can be opened by the Collector at a time	In order to reduce the workload caused by Collector on the SQL Server. Reducing the MaxPoolSize will reduce the total number of connections open on the SQL Server but may also reduce the despool rate.	Collector (registry setting)
<b>Installation level settings</b>			
Command blacklisting	Allows specifying one or more commands whose output	When you see large audited sessions that are a result of running commands with large	Group Policy



Title	Summary	When to adjust	Component
	is not required to be captured	output (for example, commands such as tail or top) and you need to control disk space consumed by such audited activity.	
Enable/Disable video audit	Allows enabling or disabling video capture (at installation level or on a per machine basis) when storing audited user activity in the database	When video capture is resulting into large sessions consuming a lot of disk space and/or it's not desirable to store the video.	Audit Manager console or group policy

- Not all configuration parameters/settings are available in releases prior to Suite 2015.1. Please contact Centrify Support for additional information on older releases.
- Agent heartbeat interval can configured per audited system or globally by configuring it in collector's registry setting. Centrify recommends configuration the heartbeat interval on the collector if you want all the audited systems to send their heartbeat at an identical interval.
- Tweaking the configuration settings may not always help or eliminate the deployment issues completely. In such cases, making significant deployment/configuration changes may be the only option. Please contact Centrify Support to evaluate possible solutions.

## Conclusion

This sizing recommendation section has provided some information as to what factors can affect Centrify Audit & Monitoring Service performance. Keep in mind, however, that every installation is unique and we cannot anticipate every use case. If you continue seeing performance degradation after following the best practices outlined in this document, contact Centrify Support for assistance.

# Glossary

**Administrator console** An earlier version of the Audit Manager console used to configure and monitor audit installations and to grant and manage auditor rights for users and groups.

**Audit Analyzer console** A GUI that auditors use to search audit data. The console enables auditors to query audit store databases, select sessions to replay, and flag sessions for follow-up.

**Audit Manager console** The management console that is used to configure and monitor the audit installation and to grant and manage auditor rights for users and groups.

**Audit management database** The audit management database is a Microsoft SQL Server database instance that keeps track of all of the components in a single audit installation. When users query and display audit data using Audit Analyzer, the audit management database connects to the appropriate audit stores to respond to the requests. In previous versions, the component was called the audit server.

**Audit management server** The Windows service that collects audit trail events when there are no audit store databases available. Only one instance of this service should run for a single audit installation.

**Audit role** A specification that defines a set of audit data and access privileges for an assigned set of users or groups. Users or groups who are assigned to one or more audit roles are identified as auditors. An administrator creates different audit roles to give auditors specific access rights to appropriate audit data.

**Audit store** A component of the auditing infrastructure that defines a scope of audit data in a Microsoft SQL Server database. An audit store can encompass an entire Active Directory site or a specific subnet. Only one SQL Server database can be actively receiving audit data from collectors at a time. However, an audit store can have multiple attached databases. All attached databases in the audit store are available to the audit management database,



which presents audit data to auditors in response to requests from Audit Analyzer. Typically, each Active Directory site has one audit store.

**Audit store database** A Microsoft SQL Server database that contains captured session data.

**Audited computer** A Windows, Linux, or UNIX computer that has an agent installed to capture user activity. When auditing is enabled, it starts when a user logs on.

**Audited system** Another term used interchangeably with audited computer to describe a Windows, Linux, or UNIX computer that has an agent installed to capture user activity.

**Auditor console** An earlier version of the Audit Analyzer console that auditors use to search audit data, select sessions to replay, flag sessions for follow-up, and query audit store databases.

**Audit trail** The list of commands that were audited.

**Centrify Agent for \*NIX** The collection of components on a UNIX computer responsible for access control, privilege management, and sending audit data to a collector. The Centrify Agent for \*NIX encompasses all required and optional services that provide authentication and privilege elevation and audit and monitoring service features on Linux and UNIX computers. On audited UNIX computers, these components include the service that intercepts traffic (cdash), the data collection service (dad), the agent configuration file (centrifyda.conf), and command line programs.

**Centrify Agent for Windows** The collection of components on an audited Windows computer responsible for sending audit data to a collector. On Windows, these components include the service that intercepts traffic (wash), the data collection service (wdad), and the agent configuration control panel.

**Collector** A Windows service that collects audit data from audited systems and sends it to an audit store.

**Common component** A Windows service that captures diagnostic log information from all auditing-related components.

**DirectAudit installation** A named collection of audited computers, collectors, audit stores, and an audit management database that interact. Each installation has a Master Auditor with full control over all of the components in the installation. The installation defines the boundary of audit data available. An organization can have multiple installations. For example, two corporate



divisions can deploy isolated installations; or a test installation can be maintained separately from the production deployment.

**Installation** A named collection of audited computers, collectors, audit stores, and an audit management database that interact. Each installation has a Master Auditor with full control over all of the components in the installation. The installation defines the boundary of audit data available. An organization can have multiple installations. For example, two corporate divisions can deploy isolated installations; or a test installation can be maintained separately from the production deployment.

**Management database** The Microsoft SQL Server database instance that keeps track of all of the components in a single installation. When users query and display audit data, the management database connects to the appropriate audit stores to respond to the requests. In previous versions, the component was called the audit server.

**Master Auditor role** The user account that has full administrative control over an installation. You cannot modify the permissions associated with the Master Auditor role. You can change who is assigned to the role.