Centrify Server Suite 2017

Evaluation Guide for Linux and UNIX

February 2017

Centrify Corporation

Legal notice

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

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

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

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

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

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

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

Contents

Index

About this guide

The *Centrify Server Suite Evaluation Guide for Linux and UNIX* describes how to install and configure the Centrify software on a Windows computer joined to an Active Directory domain controller and on the Linux and UNIX computers you want to manage. After you install the software, you can follow the steps in this guide to create Active Directory users and groups and set up a test environment with Centrify zones, roles, privileges, and group policies. Through this test environment, you can see how Centrify enables you to control users access, manage privileges, and monitor activity on UNIX and Linux computers in your organization.

Intended audience

This guide is for system and network administrators who want to evaluate Centrify software. The guide assumes you have a working knowledge of Windows Server and Active Directory and are familiar with Active Directory features, functionality, and terminology. This guide also assumes you are familiar with the Linux or UNIX-based computers you plan to manage and how to perform common administrative tasks.

Using this guide

Centrify provides an integrated set of software components that centrally control, secure, and audit user access to servers, workstations, mobile devices, and applications through Microsoft Active Directory. The purpose of this guide is to give you hands-on experience using Centrify software to manage identities, access privileges, and administrative tasks on UNIX and Linux computers.

The guide is divided into the following chapters:

- Chapter 1, "Preparing hardware and software for an evaluation," describes what you will need and how to prepare for the evaluation.

- Chapter 2, "Configuring the basic evaluation environment," provides step-by-step instructions for setting up the evaluation environment.
- Chapter 3, "Exploring additional management tools," describes the features of Centrify software that reduce complexity and ease the workload in large organizations.
- Chapter 4, "Auditing sessions," describes how you can audit user activity and search and replay user sessions.
- Chapter 5, "Frequently asked questions," provides answers to the most common questions about Centrify products and features.
- Chapter 6, "Removing software after an evaluation," describes how to optionally uninstall Centrify software.

To complete your evaluation, be sure to review the Evaluation Checklist spreadsheet. The Evaluation Checklist provides a summary of the features that enable you to centrally manage the computers and users in a complex environment. With the spreadsheet, you can rate and score features to quantify your evaluation.

Conventions used in this guide

The following conventions are used in this guide:

- `Fixed-width font` is used for sample code, program names or output, file names, and commands that you type at the command line. When *`italicized`*, the fixed-width font is used to indicate variables.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- ***Italics*** are used for book titles and to emphasize specific words.

Finding more information

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

demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

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

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

Contacting Centrify

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

Getting additional support

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

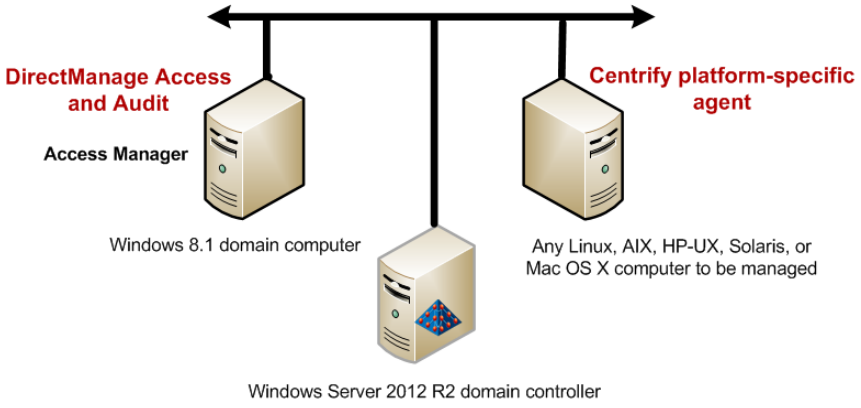
To connect with other Centrify users, ask questions, or share information, visit the Centrify Community website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.

Preparing hardware and software for an evaluation

This chapter describes the hardware and software you need to prepare for the evaluation of Centrify software. It includes instructions for downloading Centrify software from the Centrify website if you do not have the CD and the permissions required to install and configure the evaluation environment.

What you need for the evaluation

To follow the instructions in this guide, you need a simple configuration of networked Windows domain computer, Windows Server domain controller, and a Linux, UNIX, or Mac OS X computer to manage as illustrated in the following example.



To complete this evaluation, you install Centrify software on two physical or virtual computers:

- **DirectManage Access** and **Audit** components on a Windows computer joined to an Active Directory domain.
- **Centrify UNIX agent** on a supported Linux-based or UNIX-based platform that you want to manage.

In most organizations, Centrify software is not installed on the domain controller. However, you must be able to connect to a domain controller from the other two computers to complete the evaluation.

Windows computer requirements

You use the Windows computer where DirectManage Access Manager is installed to perform most of the procedures described in this guide.

Before installing on Windows, check that you have a supported version of one of the Windows operating system product families. For example, you can use Windows 7 or later, or Windows 8 or 8.1 for DirectManage components. Alternatively, you can install components on computers in the Windows Server product family—such as Windows Server 2008 or 2008 R2, or Windows Server 2012 or 2012 R2—so that your administrative computer can be configured with additional server roles.

For more detailed information about supported platforms for specific components, see the Resources section on the Centrify website.

http://www.centrify.com/resources

You should also verify that you have the .NET Framework, version 4.5 or later, installed. If the .NET Framework is not installed, the setup program can install it for you. Alternatively, you can download the .NET Framework from the Microsoft Download Center, if needed.

The Windows computer should have the following minimum hardware configuration:

Component	Minimum requirement
CPU speed	550 MHZ
RAM	256 MB
Disk space	1.5 GB

You should also verify that the Windows computer you plan to use for the evaluation is joined to the Active Directory domain.

Note If you are installing the software on virtual computers, see “Using a virtual environment” on page 13 for additional guidelines.

Linux and UNIX computer requirements

A platform-specific Centrify agent must be installed on each computer you want to manage through Active Directory. Centrify supports several hundred distributions of popular operating systems, including AIX, HP-UX, and Solaris versions of the UNIX operating environment and both commercial and open source versions of the Linux operating system. For the most complete and most up-to-date list of supported operating systems and vendors, see the supported platforms listed on the Centrify website.

You can download platform-specific agent packages from the Centrify C**ustomer Download Center** if you register for a free centrify.com account. You can also download agents for free from the Centrify Express website.

The UNIX or Linux computer must be connected to the same network as the domain controller.

Domain controller requirements

For the Active Directory domain controller, you should verify that you have access to a computer with a supported version of the Windows Server product family—such as Windows Server 2008 or Windows Server 2012—and is configured with the domain controller and DNS server roles.

In addition, you should verify that the domain functional level is at least Windows Server 2003.

To determine the domain functional level:

1. Open Active Directory Users and Computers (dsa.msc).
2. Select the domain.
3. Select **Action**, then click **Raise domain functional level**.

   If the current domain functional level is not at least Window Server 2003, use the drop down list to raise the level.

Verify administrative access for the evaluation

To prepare for the evaluation, you should confirm that you have the local Administrator account and password for the root domain of the Active Directory forest. The forest root Administrator account is the account created when you install the first Windows Server in a new Active Directory site.

If you set up a separate Active Directory domain for testing purposes, you should have this account information. If you are using an existing Active Directory forest that was not expressly created for the evaluation, you should identify the forest root domain and confirm that you have an account that is a member of the Domain Admins group on the Windows computer you use for the DirectManage Access Manager console. This ensures that you have all the permissions you need to perform the procedures in this evaluation.

If you are not a member of the Domain Admins group on the Windows computer you use for the DirectManage Access Manager console, have the Active Directory administrator create a separate organizational unit for Centrify objects and delegate control of that organizational unit to the user account you are using the for evaluation. For more information about delegating control, see “Delegate control for the Centrify organizational unit” on page 19.

You should also verify that Administrative Tools are visible in the Start menu on the Windows computer you are using for the evaluation. If the Administrative Tools option is not displayed, download and install the Microsoft Remote Server Administrator Tools from the Microsoft website. For download and installation instructions, see http://www.microsoft.com/en-us/download/details.aspx?id=7887.

Checking the DNS environment

DirectManage and the Centrify agent are designed to perform the same set of DNS lookups that a typical Windows computer performs in order to find the nearest domain controller for the local site. For example, the Centrify UNIX agent looks for service locator (SRV) records in the DNS server to find the appropriate controller for the domain it has joined.

In most cases, when you configure the DNS Server role on a Windows computer, you configure it to allow dynamic updates for Active Directory services. This ensures that the SRV records published when a domain controller comes online are available in DNS. If your DNS Server is configured to prevent dynamic updates, however, or if you are not using the Window computer as the DNS server, the Centrify UNIX agent might not be able to locate the domain controller.

Do the following to ensure the UNIX computer can look up the SRV records in the DNS server for the evaluation environment:

- Configure the DNS Server role on the Windows computer to **Allow secure dynamic updates**.
- Make sure that each UNIX or Linux computer you are using includes the Windows DNS server as a `nameserver` in the `/etc/resolv.conf` file.

When you configure the DNS Server, you should configure it to perform both forward and reverse lookups and to allow secure dynamic updates.

Using a virtual environment

To simplify the hardware requirements, you might find it useful to set up your evaluation environment using either Microsoft Virtual PC or VMware Workstation. To set up a virtual environment, you need a computer with enough CPU, RAM, and available disk space to run three virtual machines simultaneously. Centrify recommends the following minimum configuration:

- CPU: at least 1.70 GHz
- RAM: at least 8 GB
- Available disk space: 15 GB

The virtual environment should also be configured to run as an isolated evaluation environment using **Local/Host-only** or **Shared/NAT** networking.

In addition, because the virtual environment runs as an isolated network, each virtual machine should be manually assigned its own static TCP/IP address and host name.

Downloading Centrify software

If you do not have the physical media for Centrify software, you can download all of the files you need for the evaluation from the Centrify website.

Downloading Centrify Server Suite

You can download all of the components for Centrify Server Suite Enterprise Edition from the Centrify website to your Windows computer. Before you begin, be sure you have the email address and password you used to register for the evaluation.

To download Enterprise Edition

1. Open a browser on the Windows computer you plan to use for the evaluation.
2. Click the Support tab and select the Centrify Customer Support Portal link.
3. Type your email address for user name and your account password, then click Login.
4. Click Customer Download Center, then click Centrify Server Suite.
5. Select the product bundle for Windows computers.
6. Click Download ISO or Download ZIP and open or save the file to download the file.
7. Close the window when the download is complete.

Downloading Centrify Linux and UNIX agents

If you do not have the physical media for Centrify platform-specific agents, you can download individual platform-specific packages directly from the Centrify website to a local Linux or UNIX computer or use DirectManage Deployment Manager to download the agent packages to a Windows computer, then deploy agents from that central Windows location to remote Linux and UNIX computers. If you

are using DirectManage Deployment Manager, you can skip this section.

To download platform-specific agent packages

1. Open a browser on the Linux or UNIX computer you plan to use for the evaluation.
2. Click the Support tab and select the Centrify Customer Support Portal link.
3. Type your email address for user name and your account password, then click **Login**.
4. Click Customer Download Center and locate **UNIX/Linux/Mac Agents** under Centrify Server Suite.
5. Select either the **All Agents Disk** or **One at a Time** link.

   If you select One at a Time, you can scroll through and select from the list of platforms to view the packages available for each operating system version. You can then select the specific packages to download.
6. At a minimum, select **Centrify Agent Installer** for the Linux or UNIX computers you want to include in the evaluation.
7. If necessary, copy the downloaded files to the Linux or UNIX computer.

Verifying you have Active Directory permissions

Many of the procedures in this guide add or modify Active Directory user, group, and computer accounts. You should verify you have the appropriate Active Directory permissions to make these kinds of changes in the evaluation environment. If you are not an Active Directory administrator or a domain administrator, you might not have access to the domain controller or sufficient permission to modify Active Directory objects and attributes.

To conduct the evaluation, have an Active Directory administrator create an organizational unit for you to use and delegate full control of the organizational unit to you. For more information about creating an organizational unit and delegating control, see the following topics:

- “Create an organizational unit for Centrify” on page 17
- “Delegate control for the Centrify organizational unit” on page 19

In addition to the organizational unit for Centrify objects, you need to have **Log on as a service** user access rights to start the Zone Provisioning Agent included in the package.

To confirm that your account has “Log on as a service” access rights

1. Open the Windows Administrative Tools Local Security Policy.
2. Expand the Local Policies node and select User Rights Assignments.
3. Scroll down to Log on as a service and double-click to display properties for this right.
4. Click **Add User or Group**.
5. Type the user or group name or click **Browse** to search for and select your account, then click **OK** to add this right to your account in the Local Security Setting.

Next steps

This concludes the site preparation, Centrify software download, and permissions assessment. You are now ready to install the software and create the fundamental elements of the evaluation environment.

Configuring the basic evaluation environment

In this chapter, you install Centrify software on your evaluation computers and configure users, groups, roles, and group policies to integrate the UNIX environment into Active Directory. After you complete these steps, your UNIX or Linux computer will be a Centrify-managed computer that is joined to the Active Directory domain, allowing UNIX users to log in using their Active Directory credentials.

To configure a basic evaluation environment, you will complete the following tasks:

- Create an organizational unit for Centrify
- Delegate control for the Centrify organizational unit
- Install and configure DirectManage Access
- Install Centrify UNIX agent
- Add and provision an evaluation user and group
- Create a UNIX administrator role
- Create child zones and service administrator role
- Deploy group policies to UNIX computers

You should perform these tasks in the order listed.

Create an organizational unit for Centrify

To isolate the evaluation environment from other objects in Active Directory, you can create a separate organizational unit for all of the Centrify-specific objects that are created and managed throughout the evaluation. You must be the Active Directory administrator or have Domain Admins privileges to perform this task.

To create an organizational unit for Centrify

1 Open Active Directory Users and Computers and select the domain.

2 Right-click and select **New > Organizational Unit.**

3 Deselect **Protect container from accidental deletion.**

4 Type the name for the organizational unit, for example, `Centrify`, then click **OK**.

Create additional organizational units

Additional organizational units are not required for an evaluation. In a production environment, however, you might create several additional containers to control ownership and permissions for specific types of Centrify objects. For example, you might create separate organizational units for UNIX Computers and UNIX Groups. To illustrate the procedure, the following steps create an organizational unit for the Active Directory groups that will be used in the evaluation to assign user access rights to the Centrify-managed computers within the top-level organizational unit for Centrify-specific objects.

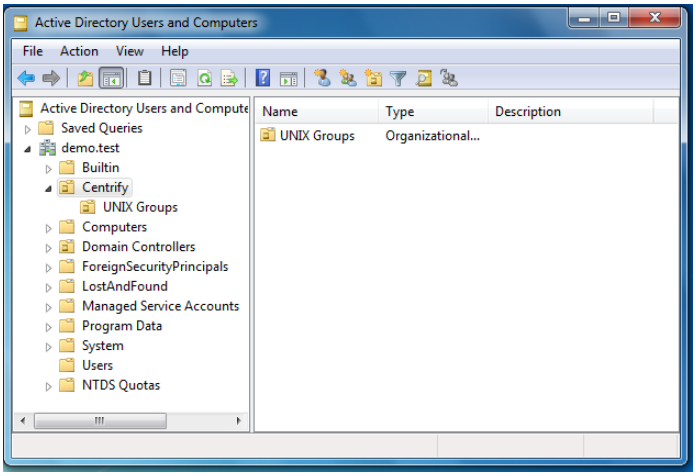
To create an organizational unit for evaluation groups

1 In Active Directory Users and Computers, select the top-level organizational unit you created in "Create an organizational unit for Centrify" on page 17.

2 Right-click and select **New > Organizational Unit.**

3 Deselect **Protect container from accidental deletion.**

4 Type the name for the organizational unit, for example, `UNIX Groups`, then click **OK**.



In later exercises, you will use this organizational unit and add other containers to manage additional types of information.

Delegate control for the Centrify organizational unit

To allow another person who is not an Active Directory administrator to perform all of tasks in the evaluation, you can delegate control of the Centrify organizational unit to that person. If you are an Active Directory administrator or a member of the Domain Admins group in the evaluation domain, you can skip this step.

To delegate control of the organizational unit for Centrify

1 Open Active Directory Users and Computers and select the domain.

2 Select the top-level organizational unit for Centrify objects, `Centrify`.

3 Right-click, then select **Delegate Control**.

4 In the Delegation of Control wizard, click **Next**.

5 Click **Add**.

6 Search for and select the user or group for delegation, then click **Next**.

7 Select the tasks to delegate, then click **Next**.

At a minimum, select the following common tasks:

- Create, delete, and manage user accounts
- Reset user passwords and force password change at next logon
- Read all user information
- Create, delete, and manage groups
- Modify the membership of a group

8 Click **Finish.**

Install and configure DirectManage Access

You are now ready to install DirectManage Access components on the Windows computer you are using for the evaluation.

To install DirectManage Access on the Windows computer

1 On the physical or virtual computer where you downloaded Enterprise Edition software, double-click **autorun.**

2 On the **Getting Started** page, click **Access**.

3 On the **Welcome to Centrify DirectManage** window click **Next**.

4 Review the terms of the license agreement, click **I agree to these terms**, then click **Next**.

5 Type your name and organization, then click **Next**.

6 Verify that the top-level DirectManage Access - Administration option is selected and expand **DirectManage Access - Utilities** and select Centrify Zone Provisioning Agent in addition to the default components, then click **Next**.

7 Accept the default **C:\Program Files\Centrify** location for installing components, or click **Browse** to select a different location, then click **Next**.

8 Click **Next** to disable publisher verification.

9 Review the components you have selected, then click **Next** to begin installing components.

10 Deselect the Configure and start Zone Provisioning Agent option, then click **Finish**.

Because you are going to configure the service account for the Zone Provisioning Agent in a later exercise, click **Yes** to dismiss the warning about the Zone Provisioning Agent running as the local system account.

11 Click **Exit** to close the Getting Started page.

Start DirectManage Access Manager for the first time

After installing DirectManage Access components, you should have the following new icons on your desktop:

- DirectManage Access Manager
- DirectManage Deployment Manager

You are now ready to start using DirectManage Access Manager. The first time you open DirectManage Access Manager it creates Active Directory containers to store Centrify licenses and zone information.

To start DirectManage Access Manager for the first time

1 Open DirectManage Access Manager by double-clicking the icon on the desktop.

2 Verify the name of the domain controller, then click **OK**.

The default is the domain controller to which the Windows computer is joined. If you want to connect to a different forest, type the name of a domain controller in that forest. If you want to connect to the forest with different credentials, select **Connect as another user**, then type a user name and password to connect as.

3 In the Setup Wizard Welcome page, click **Next**.

4 Verify that **Use currently connected user credentials** is selected to use your current logon account, then click **Next**.

   You must be logged on with an account that has Active Directory administrator rights in the target organizational unit. If your logon account does not have those rights, select **Specify alternate user credentials** and enter a different user name and password.

5 Select **Generate Centrify recommended deployment structure** and **Generate default deployment structure**, then click **Next**.

6 Select a location for installing license keys in Active Directory, then click **Next**.

   The Setup Wizard displays information about the Read permissions that must be granted on the container. Click **Yes** to continue.

7 Type or copy and paste the license key you received, click **Add**, then click **Next**.

   If you received the license key in a text file, you can click **Import** to import the key directly from the file, then click **Next**.

8 Click **Next** to use the default container for the Centrify zones.

9 Accept the default permission delegation and click **Next**.

10 Review the summary of your selections, then click **Next**.

11 Click **Finish**.

After you click Finish, DirectManage Access Manager is displayed.

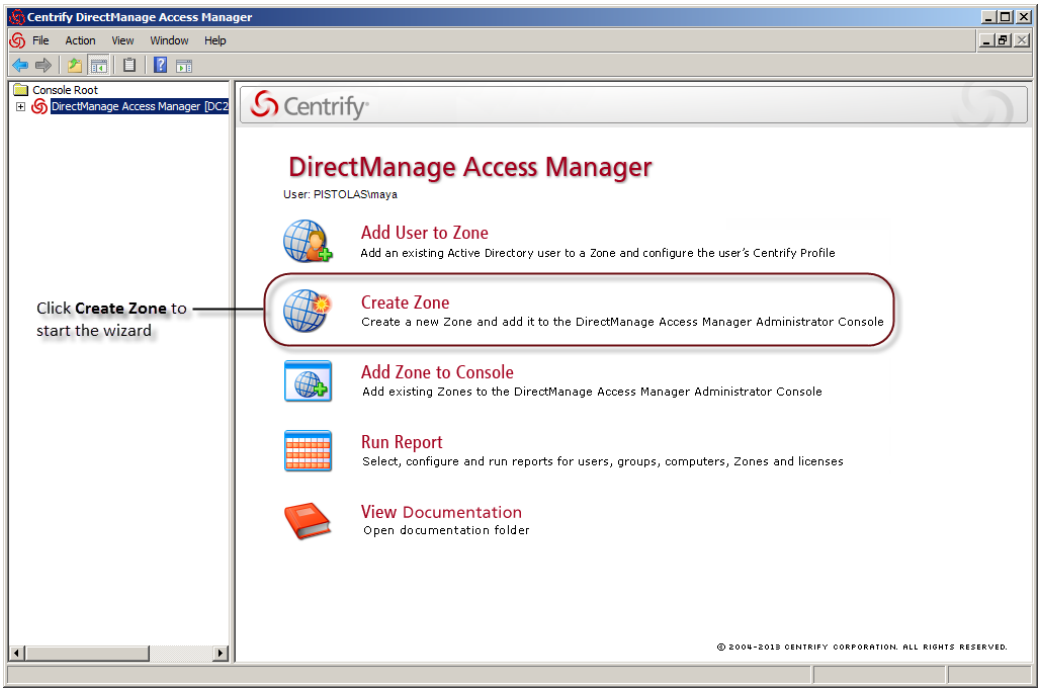
Create the first zone

The next step in configuring your evaluation for access control and privilege management is to create a Centrify zone. Zones enable you to define and control access privileges for users and groups in your organization. By using zones, you can limit who has access to different computers and where users have permission to exercise elevated privileges.

To create a parent zone

1 Open DirectManage Access Manager.

2 Click **Create Zone**.

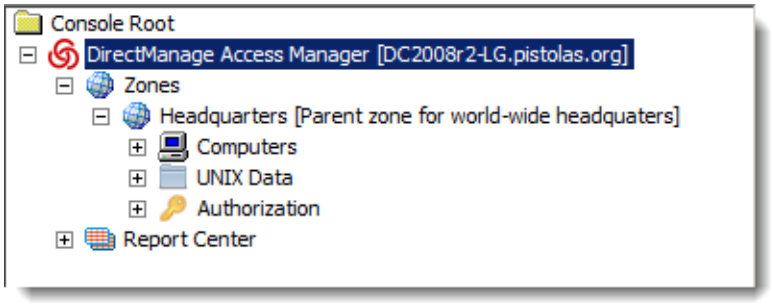


3 Type a name and description for the zone, for example `Headquarters`, then click **Next**.

4 Leave **Use default zone type** selected, and click **Next**.

5 Verify information about the zone you are creating, then click **Finish**.

You now have one parent zone. You can have multiple parent zones or a single parent zone, depending on your needs. If you expand the **Zones** node, the left pane displays your new zone.



DirectManage Access Manager automatically creates the Computers, UNIX Data and Authorization nodes for each zone you create. These

nodes enable you specify precise access privileges for computer and application administrators in each zone.

A parent zone can have one or more child zones. Child zones inherit information from the parent zone. For example, you can define access rights, roles, and role assignments in a parent zone and use them or change them in a child zone. You will work with child zones in a later exercise.

Now that you have DirectManage Access Manager installed and have configured your first zone, you are ready to install the Centrify agent on a UNIX or Linux computer.

Install Centrify UNIX agent

The Centrify agent must be installed on each UNIX or Linux computer you want to manage. After you have downloaded platform-specific agents for the operating systems you want to evaluate, you should make sure the software is on the physical or virtual UNIX or Linux computer you are using for the evaluation.

To install the agent package

1. Log on to the UNIX or Linux computer with `root` privileges.
2. Copy the Centrify UNIX agent package for the local operating system to the computer and change to that directory.
3. Extract the contents of the package.

   For example, if you have a Red Hat Enterprise Linux based computer with a 32-bit processor, you would enter the following:

   ```
   gunzip centrify-suite-2015-rhel3-i386.tgz
   ```
4. Expand the archive file.

   For example, if you have a Red Hat Enterprise Linux based computer with a 32-bit processor, you would enter the following:

   ```
   tar -xvf centrify-suite-2015-rhel3-i386.tar
   ```
5. Run the `install.sh` script.

   For example, if you are running Red Hat Enterprise Linux you would enter the following:

```
/bin/sh install.sh
```

6 Follow the prompts displayed to check whether the local computer is ready for the installation.

If there are errors, you must fix them before installing the software. Warning messages are informational, but do not prevent you from installing the software.

7 Follow the prompts displayed using the following instructions:

Prompt	Action
How do you want to proceed?	Enter `E` for the Enterprise Edition.
Do you want to run adcheck to verify your AD environment?	Enter `N` to skip post-installation checks.
Join an Active Directory Domain?	Enter N to join later.
Enable auditing on this computer (DirectAudit NSS mode)?	Enter Y to enable auditing.
Do you want to continue (Y) or re-enter information?	Enter Y to install the default packages.

If you have more than one Linux or UNIX computers included in the evaluation, repeat Step 1 through Step 7 on each computer.

8 Verify the installation by running the `adinfo` command at the UNIX command prompt.

```
adinfo
```

This command-line program displays information about the Linux or UNIX computer's status in Active Directory. At this point, the output should show you that you are not joined, but Licensed Features are enabled.

Join the domain

You are now ready to use the `adjoin` command-line program to join the Linux or UNIX computer to the Active Directory domain you are using for evaluation.

The most basic syntax for the `adjoin` command is:

`adjoin` *`domain`* `-z` *`zone`* `-u` *`username`*

For more information about `adjoin` syntax and options, see the `man` page for the `adjoin` command.

To join an Active Directory domain from a Linux or UNIX computer

1. Log on to the UNIX or Linux computer with `root` privileges.
2. Run the `adjoin` command, specifying the domain, zone, and the account name for an Active Directory administrator with permission to join the domain.
3. Enter the password for the Active Directory account used to join the domain.
4. Verify the UNIX or Linux computer is joined to Active Directory by running the `adinfo` command.

   ```
   adinfo
   ```

   The output should look similar to the following:

   ```
   Local host name:   kona-sf
   Joined to domain:  pistolas.org
   Joined as:         kona-sf.pistolas.org
   Pre-win2K name:    kona-sf
   Current DC:        dc2008r2-lg.pistolas.org
   Preferred site:    Default-First-Site-Name
   Zone:            pistolas.org/Centrify Pubs/Zones/Headquarters
   Last password set: 2013-11-18 15:27:18 PST
   CentrifyDC mode:   connected
   Licensed Features: Enabled
   ```

5. Restart the Linux or UNIX computer.

   Restarting the computer is not required, but is recommended to ensure that all services are restarted.

Verify your progress in DirectManage Access Manager

You now have a Centrify-managed computer. To see the computer in DirectManage Access Manager, expand **Zones > Headquarters > Computers**. The Linux or UNIX computer is listed under the Computers node. The computer has successfully joined an Active Directory domain and is prepared for access control and privilege management. However, no Active Directory users can log on to the computer yet.

Add and provision an evaluation user and group

Before any Active Directory users can log on to the Centrify-managed computer, you must provision an Active Directory account with UNIX profile attributes and assign the user a role that has login privileges. To demonstrate the process in the evaluation, you will create a new Active Directory user, provision the user with a UNIX profile, and assign the user basic access privileges.

To create a new Active Directory user with access to the Centrify-managed computer

1. Open Active Directory Users and Computers and create a new **User** object.
   - Fill in the First, Last, and the User logon name fields**.**
   - Type and confirm a password and select the Password never expires option.
   - Acknowledge the warning, click Next, then click Finish.
2. Create a new Active Directory group in the `UNIX Groups` organizational unit you created under the `Centrify` organizational unit.
   - For the Group name enter Login Users.
   - Select Global as the scope for the group and Security for the type of group, then click OK.
3. Add the evaluation user to the Login Users group.

- Select the user you created in Step 1, right-click and select Add to a group.
- Select the Login Users group, then click OK.

4 Provision a UNIX profile for the new user using DirectManage Access Manager.

- Expand the Zones node and select the `Headquarters`, right-click, then select **Add User.**
- Select the user you created for the evaluation.
- Select Define user UNIX profile only and deselect Assign roles.
- Accept the default values for all profile properties.
- Review your selections, click Next, then click Finish.

5 Assign the default UNIX Login role to the Login Users group using DirectManage Access Manager.

- Expand the Authorization node under the `Headquarters` zone.
- Select Role Assignments, right-click, then select **Assign Role**.
- Select the UNIX Login role and click OK.
- Click Add AD account.
- Change the object to Find from User to Group, then search for and select the Login Users group, then click OK.
- Click OK to complete the role assignment.

Verify access by logging on

The Active Directory user can now log on to the UNIX or Linux computers that has joined the domain and the parent zone.

To verify the user can log on using Active Directory credentials

1 Open a terminal on your joined Linux or UNIX computer and switch to the `root` account.

2 Run `adflush` to clear the Centrify UNIX agent's cache.

This step simply ensure that the agent will make a new connection to Active Directory to get the latest user and group information.

3 Log off as `root`.

4 Log in using the Active Directory credentials for the evaluation user you created and added to the `Login User` group.

Create a UNIX administrator role

Now that you have verified an Active Directory user can access the Linux or UNIX computer you are using for the evaluation, you will see to how to create users that have elevated privileges and how you can limit the use of those privileges to specific computers.

To illustrate this scenario, you will create a UNIX administrator role that grants root privileges for the computers in a zone without requiring users to know the root password. Instead, users who are assigned the UNIX administrator role use their Active Directory credentials.

You can use the same steps to define roles with different and more granular rights. For example, you will follow similar steps to create an Apache administrator role that can only perform a limited set of tasks on computers in a child zone.

At the end of this section, you will have two accounts with UNIX Login privileges: one of which has only standard user privileges, the other account has full administrative privileges.

To create a new Active Directory user and group with administrative access

1 Open Active Directory Users and Computers and create a new **User** object.

- Fill in the First, Last, and the User logon name fields.
- Type and confirm a password and select the Password never expires option.
- Acknowledge the warning, click Next, then click Finish.

2 Open Active Directory Users and Computers and create a new **Group** object in the `UNIX Groups` organizational unit.

- For the Group name, enter EnterpriseUnixAdmins.
- Select Global as the scope for the group and Security for the type of group, then click OK.

3 Add the administrative user to the `EnterpriseUnixAdmins` group.

- Select the user you created in Step 1, right-click and select Add to a group.
- Select the `EnterpriseUnixAdmins` group, then click OK.

4 Provision a UNIX profile for the new user using DirectManage Access Manager.

- Expand the Zones node and select the `Headquarters`, right-click, then select **Add User.**
- Select the user you created for UNIX administration.
- Select Define user UNIX profile only and deselect Assign roles.
- Accept the default values for all profile properties.
- Review your selections, click Next, then click Finish.

Define a command right and a new role

You are now ready to define a new privileged command right that uses the asterisk (*) wild card to give the user the equivalent of all commands, all paths, and all hosts in the `sudoers` file. In a production deployment, you would define more specific sets of privileged commands and run them using accounts with no restricted access than the root user.

To create new UNIX right definition for the administrative role

1 Create a new privileged command using DirectManage Access Manager.

- Expand the Authorization node under the `Headquarters` zone, then expand UNIX Right Definitions and select Commands.
- Right-click then select New Command. For this example, you will only set information on the General tab.
- Type a command name and description, for example `root_any_command` and `All commands, all paths, all hosts`.
- Type an asterisk (*) in the Command field to match all commands.

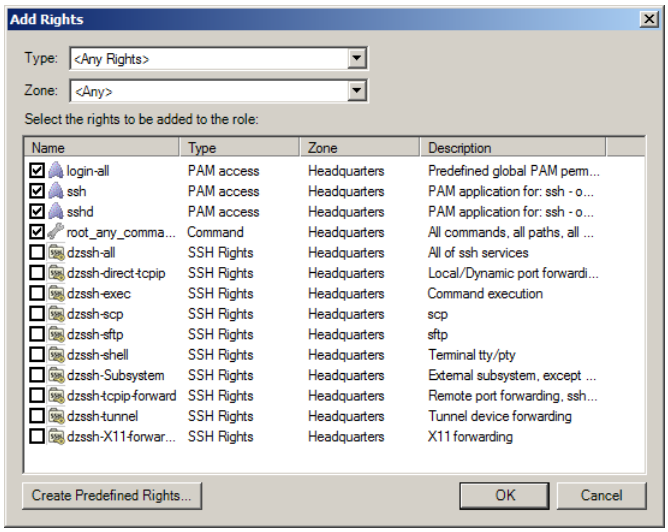
- Leave the default setting for Glob expressions.
- Select the Specific path options and type an asterisk (*) to match all command paths, then click OK.

You now have a `root_any_command` that grants privileges to run any command in your role definitions. In the next steps, you create a role that will give members of the `EnterpriseUnixAdmins` group the `root_any_command` privileges.

To create and assign the UNIX administrators role

1. Create a new role definition using DirectManage Access Manager.
   - Expand the Authorization node under the `Headquarters` zone, select Role Definitions, right-click, then select Add Role.
   - Type a role name (`UnixAdminRights`) and a description (`Set of rights for UNIX administrators`) for the new role.
   - Click the System Rights tab and select all of the UNIX rights and the Rescue right.
   - Click the Audit tab and select Audit if possible, then click OK.
2. Add the `root_any_command` and several default rights to the new role.
   - Select the `UnixAdminRights` role, right-click, then select Add Right.

- Use CTRL-click to select rights, including login-all, secure shell (ssh, sshd, and dzssh-all) rights, and the `root_any_command` right you just created, then click **OK**.



3 Assign the `UnixAdminRights` role to the enterprise UNIX administrators group using DirectManage Access Manager.

- Expand the Authorization node under the `Headquarters` zone, select Role Assignments, right-click, then select Assign Role.
- Select the `UnixAdminRights` role and click OK.
- Click Add AD Account.
- Change the object to Find from User to Group, then search for and select the EnterpriseUnixAdmins group, then click OK.
- Click OK to complete the role assignment.

Verify administrative privileges

You now have two role assignments—`Login Users` and `EnterpriseUnixAdmins`—in the zone. Any Active Directory user you add to the `Login Users` group and provision a UNIX profile for will have access rights but no administrative privileges on the computers in the zone. Any Active Directory users you add to the `EnterpriseUnixAdmins` group and provision a UNIX profile for will be able to run any command with root-level permissions using their Active Directory credentials.

The Active Directory user you added to the `EnterpriseUnixAdmins` group can now log on and run privileged commands on the UNIX or Linux computers you are using for evaluation.

To verify the user can run privileged commands using Active Directory credentials

1 Log on to the Linux or UNIX computer using the Active Directory logon name and password you created for the UNIX administrator.

2 Open a terminal on the Linux or UNIX computer.

3 Run a command that requires root-level privileges.

For examples, run the `dzinfo` command to view the rights and roles for the UNIX Login user you created "Add and provision an evaluation user and group" on page 27.

```
dzinfo user_name
```

Because you are logged on as the Active Directory user and not invoking the command using your role assignment, the command displays an error message indicating that you are not allowed to view authorization information for another user.

4 Re-run the command using your role assignment by typing `dzdo` before the command.

```
dzdo dzinfo user_name
```

The command runs successfully and returns information about the evaluation user similar to this partial output.

```
User: lois.lane
Forced into restricted environment: No

  Role Name              Avail Restricted Env
  ---------------        ----- --------------
  UNIXLogin/Headquarters Yes   None

  Effective rights:
    Password login
    Non password login
    Allow normal shell

  Audit level:
    AuditIfPossible
```

View effective rights

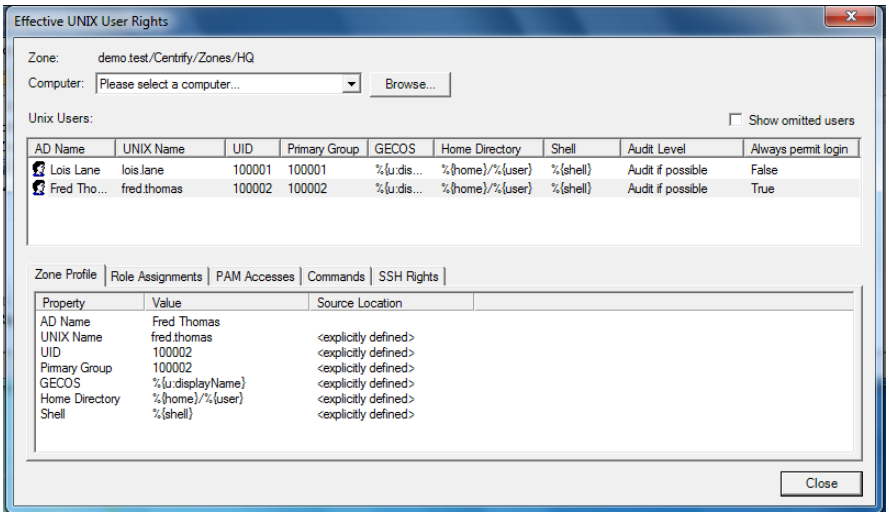
Often, you need to see which users have what privileges in a zone. DirectManage Access Manager provides you a single view of all of the effective users in a zone and lets you tab through their account properties.

To view effective rights for Linux and UNIX users

1 Open DirectManage Access Manager.

2 Expand Zones, right-click your parent zone name, then select **Show Effective UNIX User Rights**.

For example, the following illustrates the effective users in the evaluation zone.



3 Select a user, then click the tabs to see details about that user's profile, role assignments and UNIX rights.

Create child zones and service administrator role

In many cases, you don't want a service administrator to have `root` privileges. For example, there's no reason to give database or web service administrators root-level privileges if their role only requires limited access to a few privileged operations.

To illustrate how to grant more limited privileges to an administrator, you will now create a role that gives an Apache server administrator permission a few specific tasks, such as edit the Apache configuration file and start and stop the Apache service. In this scenario, you will also create child zones to further limit the Apache administrator's authority to just the computers in the child zones.

To create child zones

1. Open DirectManage Access Manager.
2. Expand Zones, right-click your parent zone name, then select **Create Child Zone.**
3. Type a Zone name (`Nevada`) and a brief description (`Western field office`), then click **Next**.
4. Click **Finish**.
5. Repeat Step 1 through Step 4 giving the second child zone a different name (`Delaware`) and description (`Eastern web farm office`).
6. Expand Child Zones and each new zone you created to view the nodes of the child zones.

To create a new Active Directory user and group for Apache administrators

1. Open Active Directory Users and Computers and create a new **User** object.
   - Fill in the First, Last, and the User logon name fields.
   - Type and confirm a password and select the Password never expires option.
   - Acknowledge the warning, click Next, then click Finish.
2. Open Active Directory Users and Computers and create a new **Group** object in the `UNIX Groups` organizational unit.
   - For the Group name, enter `ApacheAdmins`.
   - Select Global as the scope for the group and Security for the type of group, then click OK.
3. Add the web administrator to the `ApacheAdmins` group.

- Select the user you created in Step 1, right-click and select Add to a group.
- Select the `ApacheAdmins` group, then click OK.

4 Provision a UNIX profile for the new user using DirectManage Access Manager.

- Expand the Zones node and select the `Headquarters`, right-click, then select **Add User.**
- Select the user you created for web administration.
- Select Define user UNIX profile only and deselect Assign roles.
- Accept the default values for all profile properties.
- Review your selections, click Next, then click Finish.

Define command rights and a new role for Apache administrators

You are now ready to create the privileged commands and role definition for the Apache administrators much as you did for the UNIX administrators. However, in this scenario, you will add the following new commands:

Command name	Command	Purpose
web_edit_http_config	vi /etc/httpd/conf	Edit the httpd daemon configuration file
web_apachectl	apachectl *:	Front end command for managing the httpd daemon
web_httpasswd	htpasswd *	Create and update HTTP server user name and password file

These commands will be added to a new role definition, `ApacheAdminRights`. As an alternative to creating the commands and role manually using DirectManage Access Manager, as you did in the

previous section, the following steps illustrate how you can use an ADEdit script.

ADEdit is a command-line scripting environment included with the Centrify UNIX agent. You can use ADEdit commands and scripts to modify Active Directory objects interactively directly from a UNIX or Linux computer terminal. The sample script `ApacheAdminRole` illustrates how you can use an ADEdit script to create UNIX rights and an Apache administrator role. This sample script is located in the `/usr/share/centrifydc/samples/adedit` directory on the UNIX or Linux computer where you have installed the Centrify agent.

To create the ApacheAdmin commands and the ApacheAdminRights role

1. Log on to the Linux or UNIX computer using the Active Directory logon name and password you created for the UNIX administrator.
2. Open a terminal on the Linux or UNIX computer.
3. Change the directory to `/usr/share/centrifydc/samples/adedit`.
4. Run the `ApacheAdminRole` script.

   ```
   ./ApacheAdminRole
   ```

   If you see the error `/bin/env: bad interpreter: No such file or directory`, try changing the first line in the script to `#!/usr/bin/env adedit`.
5. Follow the prompts displayed to provide the following information for connecting to Active Directory:
   - Domain name.
   - The Active Directory account name that has administrator privileges in the organizational unit you're using for the Centrify zones.
   - The password for the Active Directory account.
6. Select the zone from the list of zones in your domain.

   For example, enter `2` to create the commands and role in the `Nevada` child zone or `3` to create the commands and role in the `Delaware` zone. The script then creates the commands and the role in the selected zone.

Verify the success of the script

You can verify the new command rights and role in DirectManage Access Manager.

To verify the script created command rights new role

1. Open DirectManage Access Manager.
2. Expand the `Nevada` or `Delaware` child zone, then expand Role Definitions.
3. Select the `ApacheAdminRights` role to view the new command rights in the right pane.

   The new rights are also listed in the under the child zone UNIX Right Definitions > Commands node. If the new role is not listed, right-click, then select Refresh.

Add rights to the new role definition

The `ApacheAdminRole` script created the new UNIX command rights for Apache-related tasks. However, the Apache administrators require a few more rights to do their job. For example, the `ApacheAdminRights` role created using the sample script does not include the UNIX Login right for any computers.

To add more rights to the ApacheAdminRights role

1. Open DirectManage Access Manager.
2. Expand the `Nevada` or `Delaware` child zone, then expand Role Definitions.
3. Select the `ApacheAdminRights` role, right-click, then select **Add Right**.
4. Select the `Nevada` or `Delaware` child zone from the list of zone to restrict the list of rights to the rights available in the child zone.
5. Select the following default rights:
   - `login-all` to allow Apache administrators to log on.

- `ssh` to allow Apache administrators to use the PAM secure shell client application.
- `sshd` to allow Apache administrators to use the secure shell server application.
- `dzssh-scp` to allow Apache administrators to use the secure copy application.
- `dzssh-sftp` to allow Apache administrators to use the secure file transfer application.

6 Click **OK**.

Assign the Apache administrator role to a group

You can now assign the `ApacheAdminRights` role to the Active Directory `ApacheAdmins` group. The members of this group will only have the Apache access rights on the computers in the `Nevada` or `Delaware` child zone you selected. Outside of the selected zone, members will have no access rights on any UNIX computers.

To assign the ApacheAdminRights role to the Apache administrators

1 Open DirectManage Access Manager.

2 Expand the `Nevada` or `Delaware` child zone and its Authorization node.

3 Select Role Assignments, right-click, then select **Assign Role.**

4 Select the `ApacheAdminRights` role, then click **OK**.

5 Click **Add AD Account**.

- Change the object to Find from User to Group, then search for and select the ApacheAdmins group, then click OK.
- Click OK to complete the role assignment.

Deploy group policies to UNIX computers

Centrify provides group policy templates for managing UNIX and Linux computers. The group policies are centrally managed through the

Group Policy Management Editor, but modify configuration settings on the managed computers where they are applied. This mechanism allows you to manage the group policy settings from a single location and have them applied on remote UNIX and Linux computers.

To illustrate how to configure and apply group policies, you will create a Group Policy Object for the `Centrify` organizational unit.

To load and apply group policies for UNIX and Linux computers

1. Open the Group Policy Management utility (`gpmc.msc`) and expand your evaluation domain.
2. Right-click the `Centrify` organizational unit, and select **Create a GPO in this domain, and Link it here.**
3. Type a name for the new GPO (`UNIX policies`), then click OK.
4. Expand the `Centrify` organizational unit, right-click the GPO, then select **Edit**.
5. Expand the Computer Configuration > Policies node and select **Centrify Settings**.
6. Right-click and select **Add/Remove Templates**
7. Click **Add** and select all of the templates listed, click **Open**, then click **OK**.

   This step adds both computer and user group policies under the Centrify Settings node. Expand Centrify Settings to explore the specific policies available. You can click the Explain tab for any group policy to see more information about what it does. The remainder of this section illustrates how you would enable and configure a few simple policies for centrify-managed. You should note that all policies—including Centrify group policies—are “Not configured” by default.

Configure user mapping by group policy

To illustrate how to configure a Centrify group policy, you will enable the Set user mapping policy. This policy maps a UNIX user, for example `root`, to an Active Directory user account, for example `Amy.Adams`.

After this policy is set, `root` attempts to log on must use the mapped Active Directory user's credentials.

To configure a Centrify group policy

1. Expand Centrify Settings > DirectControl Settings, scroll down and double-click the **Set user mapping** policy.
2. Select **Enabled**, then click **Add**.
3. Type the UNIX user account name (`root`).
4. Click Browse to search for and select the Active Directory account to use, then click **OK**.
5. Click **OK** to enable the policy.

Note If you enable this policy, the root user in the zone will **not** be able to log in to the managed computers in the zone.

Configuring password prompts

There are several group policies that enable you to customize the text displayed when a user attempts to log on to a managed computer. For example, you can customize the text displayed when a password is expiring in a certain number of days or when authentication fails. To illustrate how to configure the Centrify group policies for password-related prompts, you will enable the Set login password prompt policy.

1. Expand **Centrify Settings > DirectControl Settings > Password Prompts** and double-click **Set login password prompt**.
2. Select **Enabled**.
3. Type the text string you want displayed, then click **OK**.

Next steps

You now have a basic foundation for working with Centrify software. You have created a parent zone and child zones, provisioned users to log on to computers in those zones, defined rights and roles in different zones, and granted Active Directory users and groups specific rights by assigning them to roles. You've also seen how to apply and

configure group policies for Centrify-managed computers. From here, you can experiment on your own or explore some of the additional tools that Centrify provides.

Exploring additional management tools

In configuring a basic evaluation environment, you saw how you can use Active Directory to centrally manage user accounts, access privileges, and group policies on Linux and UNIX computers through Centrify zones. This chapter introduces some of the additional Centrify tools that you can use to manage the UNIX users and computers in your organization.

Evaluating security risks and vulnerabilities

You can use the Centrify Identity Risk Assessment feature to check discovered computers for a wide range of potential issues and generate a report of findings. The assessment report can help you determine the overall risk level across computers in your organization and specific areas where you have the most exposure. The report also highlights steps you can take to reduce risk and improve security, compliance, and operational efficiency.

The results of each assessment you run are stored in the DirectManage Deployment Manager database, so you have a historical record of activity and an archive of past assessment results.

With Deployment Manager, there are four simple steps to complete the security assessment:

1. Identify the computers to evaluate.

   You can specify how to find the remote computers you want to evaluate, for example, by specifying a local subnet or range of IP addresses of interest.

2. Download the assessment tools software.

   The assessment tools software package contains the platform-specific `surveyor` program for the computers you want to evaluate.

3. Start the assessment on remote computers.

The `surveyor` program runs on the computers you have selected for evaluation and checks for a wide range of potential issues that you might want to address to improve security in your organization.

4 Generate the identity risk assessment report.

After the `surveyor` program has collected information from the computers selected for evaluation, you can generate an executive summary of the results or a summary and a detailed report that includes information about the specific tests performed on individual computers.

The security assessment is an optional preliminary deployment step that helps you identify and evaluate risks before deploying Centrify software. In most cases, you should complete a security assessment once on each target set of computers where you plan to deploy the Centrify agent. You can also run the security assessment after deploying agents if you want to compare before and after results.

Consolidating information from managed computers

In addition to the risk assessment feature, you can also use DirectManage Deployment Manager to gather and manage the computer, user, and group information from all of the remote UNIX and Linux computers you choose to discover. Once discovered, you can analyze the remote computers for network or configuration issues that might prevent deployment, deploy agents from a single console, and monitor your software inventory on managed computers.

To see how Deployment Manager gives you a consolidated view of remote UNIX and Linux computers, try the following tasks:

- Discover remote UNIX and Linux computers
- Extract user and group information
- Export elevated privileges from sudoers files

Note For more information about deploying and managing the Centrify agent software on the managed computer, see the "Can I manage Centrify software from one location?" on page 70.

Discover remote UNIX and Linux computers

You can use DirectManage Deployment Manager to create an inventory of the UNIX and Linux computers that are accessible on your internal network or in a cloud. A successful discovery connects to remote computers and collects information about the computer's operating system, local users and groups, and configuration details. To collect this information, you must have `root` or similar administrative privileges for each computer you want to add to the inventory.

To add computers to DirectManage Deployment Manager

1. Double-click the DirectManage Deployment Manager icon on your desktop.
2. Click **Add Computers** in Step 1.
3. Select the method for discovering the computers to add, then click **Next**.
   - Discover computers from the network
   - Discover computers from a cloud service
   - Import a computer list from a text file
   - Add a single computer

   If adding a single computer, type the computer name or IP address, click **Next**, then continue to Step 7.
4. Specify the criteria for discovering computers of interest, then click **Next**.
   - If discovering computers on the network, select the local subnet, a subnet address and mask, or a range of IP addresses.
   - If discovering computers in a cloud, specify the cloud name and cloud service provider.
   - If importing computers from a file, browse to the location of the text file to import.
5. Review the list of computers found to see if any should be removed, then click **Next**.

   If Deployment Manager can connect to computers matching the criteria you specified, those computers are added to the computer

inventory by default. You can deselect any computer that you want to exclude from the inventory.

6 Review the list of computers matching the criteria you specified that Deployment Manager could not access to select any that should be added, then click **Next**.

If Deployment Manager cannot establish a connection using `ssh` or `telnet`, it displays the unreachable computers in a separate list. You can add computers from this list. However, you must resolve the connectivity issue before you can collect any information.

7 Type a user name with permission to log on to one or more of the computers you are adding.

In most cases, you should use your own user account or another standard user account with the ability to run privileged commands on the computers you are adding. If you are adding multiple computers, the same account for all computers or specify different account information for any of the computers you are adding.

8 Select the **Specify privileged command in tasks that require root privilege** option if you are using your own user account or another user account to execute privileged commands.

If you are using the `root` user account, you can leave this option unchecked.

9 Select **sudo** to use `sudo` and settings in the `sudoers` file or **su** to use the switch user (`su`) command to execute privileged commands.

10 Type the password for the `root` user or for your own account, then click **Next**.

11 Select the authentication method and provide the password or private key information for the user account you specified in Step 7, then click **Next**.

You can also select the **Apply the same account to other computers** option to use the same user name, privileged command, and authentication method for multiple computers.

12 Select whether you want to use the existing account information for the next computer in the list or specify new account information, then click **Next**.

13 Click **Finish** to exit the Add Computers wizard and retrieve information for the specified computers.

After you complete the step, the Deployment Manager console displays the navigational nodes for Computers, History, and Open Issues and the Welcome page displays the added computers in a graphic format, organized by platform.

Extract user and group information

During discovery, Deployment Manager also reads the `/etc/passwd` and `/etc/group` files from the computers it finds and lists the details under the Local Accounts node. For example, you can expand the Local Accounts, then Users to see details from the `/etc/passwd` files on all of the computers that have been discovered. You can then use the column headers to sort and filter the information displayed.

This information is useful, for example, when you need to create Active Directory accounts for the UNIX and Linux users that have different account names and UIDs on different computers. Deployment Manager lets you export the user list of all users found or just the users on a single computer.

To export the entire list of all UNIX users

1 Expand Local Accounts, select Users, right-click, then select **Export List**.

2 Select a folder location and type the file name.

3 Select the encoding and separator you want, then click **Save.**

You now have an editable file from which you can strip out the names for the accounts you don't need to add to Active Directory.

Export elevated privileges from sudoers files

Another important step when you're integrating UNIX or Linux users into Active Directory is identifying which users have elevated privileges on which computers. In most cases, this information is defined is the `/etc/sudoers` configuration file on individual computers or for groups of computers.

You can use Deployment Manager to download the sudoers file from discovered computers so that it can be imported into DirectManage Access Manager.

To download privileges defined in a sudoers file

1. Expand All Computers and select the target computer.
2. Right-click the computer, then select **Download Sudoers File.**
3. Click **Browse** to select a destination folder.
4. Type the file name, then click **Next**.
5. Review the content of the `sudoers` file to be saved, then click **Finish**.

You can now use DirectManage Access Manager to parse the contents of the `sudoers` file and import the aliases and user specifications. For more information about importing and converting aliases and user specifications into rights and roles, see the *Administrator's Guide for Linux and UNIX*.

Adding UNIX profiles automatically

Adding UNIX user accounts to Active Directory on a large scale poses several challenges:

- Provisioning: How do you provision large numbers of UNIX users and map them to unique Active Directory user objects?
- Assigning roles: Once the UNIX users have profiles stored in Active Directory, how do you give each user just the privileges required?

- Accommodating legacy UIDs: How do you migrate UNIX users who have different UIDs on different servers and maintain existing file ownership requirements?

One strategy for adding and managing a large number of UNIX profiles is to use the Zone Provisioning Agent and provisioning properties. The Zone Provisioning Agent can automatically provision new users with the full complement of UNIX profile attributes when you add them to an Active Directory group. Configuring the environment to illustrate automated provisioning with the Zone Provisioning Agent, however, requires several steps that are only applicable if you choose that deployment scenario.

The following steps summarize the process, but are not recommended for an evaluation.

To deploy the Zone Provisioning Agent

1. Create an Active Directory service account with the “Log on as a service” user right.
2. Open the Centrify Zone Provisioning Agent Configuration Panel and configure the service to use the service account you created for it.
3. Create or identify the Active Directory groups you will use as source groups for UNIX users.
4. Set the provisioning properties for the zone or zones where users will be automatically provisioned.

   For example, open Access Manager, select the parent zone, right-click, then select Properties to see the Provisioning properties. You can then set the Active Directory source group and how you want UNIX attributes to be automatically generated.
5. Migrate all existing users using the appropriate override attributes into zones to preserve their profiles.
6. Start the Zone Provisioning Agent service.

Keep in mind that the Zone Provisioning Agent takes over all user provisioning if enabled for a zone. After you start the service, you cannot use the Access Manager **Add User** option to add a user to the zone. This ensures that all UIDs are unique in the domain.

If you configure the Zone Provisioning Agent, you can add and remove users from selected Active Directory groups to automatically add or remove their UNIX profiles in a zone.

To add users after configuring zone provisioning

1. Open the `users.txt` file in the `/usr/share/centrifydc/samples/adedit` directory to add more or change names.

   Use an editor that does not insert a carriage return at the end of each line. Each line must end with a line feed.

2. Run the `AddUnixUsers` sample script in the directory to create the Active Directory account for each UNIX user and add each user to the Active Directory `UNIX Users` group.

   ```
   ./AddUnixUsers users.txt.
   ```

3. Follow the prompts displayed to provide the following information for connecting to Active Directory:

   - Domain name.
   - The Active Directory account name that has administrator privileges in the organizational unit you're using for the Centrify zones.
   - The password for the Active Directory account.

4. Type an initial password that meets the Active Directory requirements to be used for all of the accounts added.

5. Open the Centrify Zone Provisioning Agent Configuration Panel and click **Restart**.

6. Open Access Manager or Active Directory Users and Computers and assign users to the appropriate Active Directory groups to assign rights.

Generating compliance reports

Increasingly, companies need to file compliance reports that show which users have what rights on which computers. You can use Access Manager to help you generate these reports.

Using default reports

Access Manager includes several default reports in the Report Center. Each report title identifies a specific query. The right panel is blank until you execute the query. Once you execute the query, it is added to the reports list.

Note Query results are not updated automatically. Be sure to select the **Refresh** option often and especially if you don't get the results you expect.

To view a report that lists users privileges on a managed computer

1 Open DirectManage Access Manager.

2 Expand Report Center then **Hierarchical Zone - Computer Effective Rights**.

3 Double-click **Current** to run the query for managed computers.

4 Double-click one of the managed computers to list the effective rights defined for that computer.

For example, the right pane displays the effective rights for the selected computer:

ComputerEffectiveRight.Location	ComputerEffectiveRight.Role	ComputerEffectiveRight.Trustee	ComputerEffectiveRight.User	Right.FullName
Enter text here	Enter text here	Enter text here	Enter text here	Enter text ...
pistolas.org/Centrify Pubs/Zon...	UNIX Login/Headquarters	pistolas.org/Centrify Pubs/UNIX ...	lois.lane@pistolas.org	login-all/Headq...
pistolas.org/Centrify Pubs/Zon...	UnixAdminRights/Headquarters	pistolas.org/Centrify Pubs/UNIX ...	fred@pistolas.org	sshd/Headquar...
pistolas.org/Centrify Pubs/Zon...	UnixAdminRights/Headquarters	pistolas.org/Centrify Pubs/UNIX ...	fred@pistolas.org	ssh/Headquart...
pistolas.org/Centrify Pubs/Zon...	UnixAdminRights/Headquarters	pistolas.org/Centrify Pubs/UNIX ...	fred@pistolas.org	login-all/Headq...
pistolas.org/Centrify Pubs/Zon...	UnixAdminRights/Headquarters	pistolas.org/Centrify Pubs/UNIX ...	fred@pistolas.org	root_any_com...

5 Select the managed computer, right-click, then select **Export List**.

6 Type the file name and type, then click **Save**.

To display, print, or save a report

1 Open Access Manager.

2 Expand Report Center then **Hierarchical Zone - Computer Effective Rights**.

3 Right-click **Current**, then select the action to take.

- Display Report to generate an HTML-formatted report.
- Print Report to print the report output.
- Save Report to save the report in a supported format.

Creating your own queries

You can also create your own reports.

To create custom queries for reports

1. Open Access Manager.
2. Select Report Center, right-click then select **New Report Wizard**.
3. Follow the prompts displayed to name the report and set report options.

   Press F1 for context-sensitive help on any page. When you finish selecting report criteria, the wizard displays a summary window.
4. Review your report selections, then click **Finish** to save the query.
5. Expand the query, right-click Current, then select **Display Report** to view the report.

Managing UNIX information from a UNIX terminal

Many organizations find it least disruptive for their UNIX administrators to continue to manage their UNIX and Linux computers directly from their own computer rather than from a Windows computer. If you plan to manage zones, UNIX user and group accounts, access privileges, roles, and role assignments from a UNIX or Linux computer, you can use the command-line tools described in this section.

Using UNIX commands

This following table summarizes the most commonly used Centrify command line programs.

Command	Location	Description
adcheck	/usr/share/centrifydc/bin	Performs operating system, network, and Active Directory tests to verify a computer meets the system requirements for a successful installation. For example, the `install.sh` script runs the `adcheck` program.
adedit	/usr/bin	Starts the adedit application for interactive commands or running scripts For more information about the adedit application, see "Using ADEdit" on page 54.
adflush	/usr/sbin	Clears the computer's DirectManage cache. Use this after you have made changes to Active Directory accounts to remove and replace the previous values.
adgpupdate	/usr/bin	Retrieves group policies from the Active Directory domain controller and applies the policy settings to the local computer and current user immediately. If you do not use the command, group policies are automatically updated at a random interval between 90 and 120 minutes.
adinfo	/usr/bin	Displays summary or detailed diagnostic information for the managed computer.
adjoin	/usr/sbin	Joins the local computer to an Active Directory domain, organizational unit and zone.
adleave	/usr/sbin	Removes the local computer from the Active Directory domain.
adpasswd	/usr/bin	Changes the Active Directory account password for the current user or a specified user.

Command	Location	Description
adquery	/usr/bin	Queries Active Directory for information about users and groups.
dzinfo	/usr/bin	Displays information about the effective rights and roles for the current login account.
dzdo	/usr/bin	Enables you to run privileged commands as root or another user.

Some UNIX commands require you to be logged on as `root` or as a user with `root` privileges. Other commands allow different operations or return different results if you are logged on as `root`. For the complete list of Centrify command line programs you can run on Linux and UNIX computers, see the *Administrator's Guide for Linux and UNIX*. For detailed information about the options available for any command, see the `man` page for that command.

Using ADEdit

The Centrify UNIX agent also includes the Tcl-based ADEdit program. ADEdit has two basic components:

- the `adedit` command-line application
- the `ade_lib` Tcl library

ADEdit provides a scripting language that you can use to bind to one or more Active Directory domain controllers. You can then use ADEdit to retrieve, modify, create, and delete Active Directory objects of any kind, including Centrify-specific objects such as zones, rights, and roles. For example, you used ADEdit and a sample script to create rights and a role in "Define command rights and a new role for Apache administrators" on page 36.

The following sections introduce a few of the key features for ADEdit. For more information about using ADEdit commands and the `ade_lib` library, see the *ADEdit Command Reference and Scripting Guide*.

ADEdit application

ADEdit uses Tcl as its scripting language. The Tcl scripting language includes all standard programming features, such as variables, logical operators, and predefined functions (called “procedures” in Tcl). The ADEdit application also includes a Tcl interpreter and Tcl core commands, which allow it to execute standard Tcl scripts, and a comprehensive set of its own commands designed to manage Centrify-specific objects in Active Directory.

You can use ADEdit to execute individual commands interactively or to execute sets of commands together in the form of an ADEdit script.

ade_lib Tcl library

The `ade_lib` Tcl library is a collection of Tcl procedures that provide helper functions for common Centrify-specific management tasks such as listing zone information for a domain or creating an Active Directory user. You can include `ade_lib` in other ADEdit scripts to use its commands.

Using adedit sample scripts

The Centrify UNIX agent includes several sample `adedit` scripts that you can run in your evaluation environment. The scripts are in the `/usr/share/centrifydc/samples/adedit` directory on the UNIX or Linux computer where you have the agent installed.

To run scripts that have the .sh extension, enter `/bin/sh filename.sh`.

To run scripts that do not have an extension, you can just enter `./filename`.

Note If you get the error `/bin/env: bad interpreter: No such file or directory` when you run a script, this means that the `env` command is not in the `/bin` directory. In most cases, it is in `/usr/bin` instead. To fix this, change the first line in the script to:

```
#!/usr/bin/env adedit
```

The following table lists the sample scripts and the arguments.

Script name	Required arguments	Optional arguments
AddUnixUsers	`users.txt`	none
ApacheAdminRole	none	none
computers-report	`-domain` *`domain_name`* `-u` *`AD_user_name`* `-sep` *`separator`*	`-m` `-p` *`password`* Use `-m` if you want to authenticate using the computer account credentials instead of an Active Directory user account. If using an Active Directory user account, use `-p` if you want to include the user's password in the command line. If you don't specify this option, you are prompted for the password.
CreateChildZones	`-d` *`domain_name`* `-z` *`parent_zone_name`* `-u` *`AD_user_name`*	`-p` *`password`* Use `-p` if you want to include the user's password in the command line. If you don't specify this option, you are prompted for the password.
CreateParentZone	`-d` *`domain_name`* `-z` *`zone_name`*	none
GetChildZones	none	none
GetComputers	none	none
GetGroups	none	none

Script name	Required arguments	Optional arguments
getopt-example	`-d` *`domain_name`* `-u` *`AD_user_name`*	`-p` *`password`* Use `-p` if you want to include the user's password in the command line. If you don't specify this option, you are prompted for the password.
Getusers	none	none
GetZones	none	none
MakeRole	`Role_apacheAdmin.txt`	none
MktDept.sh	List of names, for example, Mary, Joe, and Lance	none

Script name	Required arguments	Optional arguments
useracc-report	`-domain` *`domain_name`* `-u` *`AD_user_name`* `-sep` *`separator`*	`-m` `-p` *`password`* Use `-m` if you want to authenticate using the computer account credentials instead of an Active Directory user account. If using an Active Directory user account, use `-p` if you want to include the user's password in the command line. If you don't specify this option, you are prompted for the password.
user-report	`-z` *`zone_distinguished_name`*	`-m` `-p` *`password`* Use `-m` if you want to authenticate using the computer account credentials instead of an Active Directory user account. If using an Active Directory user account, use `-p` if you want to include the user's password in the command line. If you don't specify this option, you are prompted for the password.

For more information about the sample scripts and how they can be used or modified, see the *ADEdit Command Reference and Scripting Guide*.

Next steps

You have now explored some of the additional tools available for working with Centrify-managed computers, including the basic features of Deployment Manager, ADEdit sample scripts, and default

reports. You are now ready to see how you can use auditing service to capture, replay, and manage user sessions on managed Linux and UNIX computers.

Auditing sessions

This chapter describes how to install and use the DirectManage Audit components. The auditing service is a process on each managed UNIX and Linux computer that captures user session input and output and transfers this information to a collector service. The collector service forwards the audited sessions to a database, where it is available for review and replay.

Install auditing components on Windows

For the evaluation, you are going to install the auditing infrastructure on a single Windows computer. To complete these steps, you will install a Microsoft SQL Server database for the evaluation environment, a single collector, and the Audit Manager and Audit Analyzer consoles from the DirectManage Audit setup program. You have already installed the auditing service on the Linux or UNIX computer you are using for the evaluation.

To install auditing components on the Windows computer

1. On the physical or virtual computer where you downloaded Enterprise Edition software, double-click **autorun.**
2. On the Getting Started page, click **Audit**.
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. Select both **Centrify DirectManage Audit - Administration** and **Centrify DirectManage Audit - Services** to install all components, then click **Next**.
6. Accept the default location for installing files by clicking **Next**, then click **Next** to proceed with the installation.
7. Confirm that the Launch Configuration Wizard box is selected by default, then click **Finish**.

8 Click **Exit** to close the **Getting Started** page.

Configure a new audit installation

An audit *installation* is a logical object similar to an Active Directory forest or site. It encompasses all of the auditing components you deploy—agents, collectors, audit stores, audit store databases, 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 logical boundary of the installation.

To create a new installation for auditing in the evaluation environment

1 If you have launched the new installation wizard automatically, at the **Welcome** page, click **Next**.

You can also use Audit Manager to launch the new installation wizard.

2 In the New Installation wizard, accept the default audit installation name by clicking **Next**.

For the evaluation, use the default installation name to automatically collect the sessions cached on the managed computers. If you use a different name, you must manually specify the installation an audited computer should use.

3 Select the option to create a new management database and verify the SQL Server computer name, instance name, and database name are correct, then click **Next**.

4 Select **Use the default NT AUTHORITY\SYSTEM account** to run the stored procedures that read and write information to the management database, then click **Next**.

5 Type the license key you received, then click **Add** or click **Import** to import the keys directly from a file, then click **Next**.

6 Accept the default location for publishing installation information, then click **Next**.

7 Select the installation-wide auditing options you want to enable, then click **Next**.

For the evaluation, select **Enable video capture recording of user activity** to capture shell activity on the audited computer, then click **Next**. Do not select the options that disallow the review and deletion of your own sessions.

8 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.

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

Check that auditing is enabled

After the auditing infrastructure is installed and configured, you are ready to audit activity on the managed computers where the Centrify agent is installed.

To check that auditing is enabled on the managed computer

1 Log on to the managed computer as `root`.

2 Run the following command verify auditing is enabled:

```
dacontrol -e
```

This command will enable auditing or display a message indicated that auditing is already enabled.

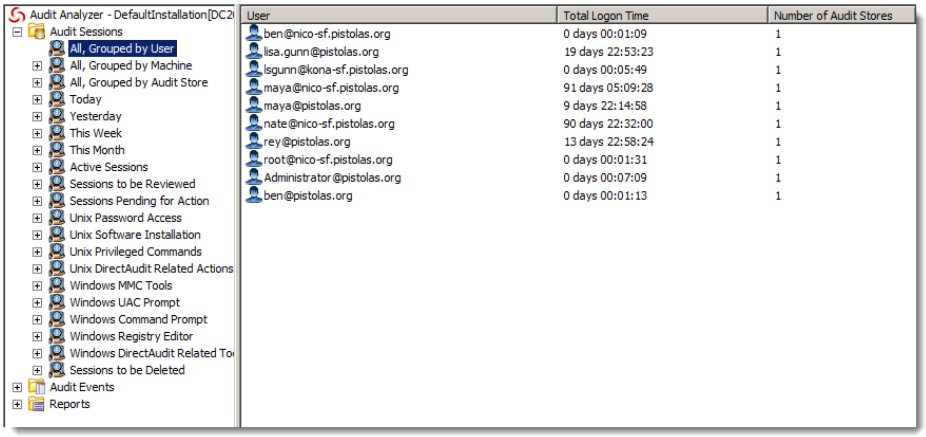
Within a few minutes the collector service should start to retrieve session activity for the managed computer. For more information about configuring and managing the auditing infrastructure, see the *Auditing with Centrify Server Suite Administrator's Guide* (`centrify-audit-adminguide.pdf`).

Viewing sessions using predefined queries

After you have started collecting user activity on a managed computer, you can use Audit Analyzer to view and replay the sessions captured.

For example, you can open Audit Analyzer and select **Active Sessions** to see sessions that are currently in progress.

Audit Analyzer includes many predefined queries like the Active Sessions query 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 select the "All, Grouped by User" query, 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 a specific 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 used, start and end time, current state, whether the audited session is a console or terminal client session, the review status of the session, the name of the user that modified the status, the size of the session in kilobytes, and any comments that have been added to the session.

In addition to the predefined queries for audited sessions, Audit Analyzer includes predefined queries for audit trail events and predefined queries for basic reports. You can explore these queries on your own as you capture additional activity.

Replaying a session

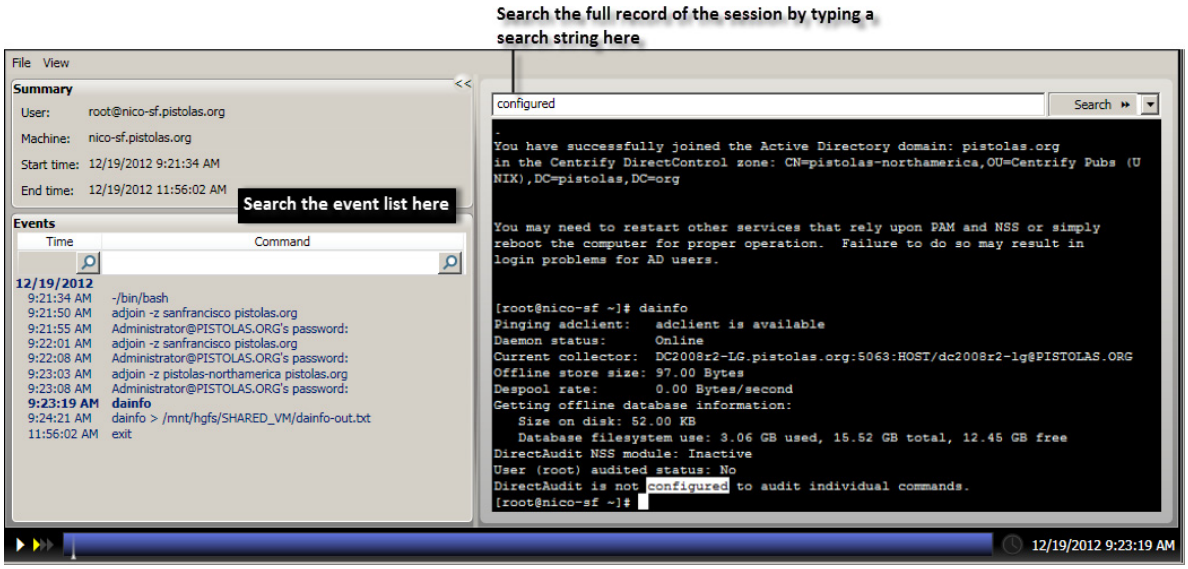
If you accepted the defaults when you created the installation for auditing, you should have video capture auditing enabled. Video capture auditing records all standard input (`stdin`), standard output (`stdout`), and standard error (`stderr`) activity that occurs on the managed computer. With video capture enabled, you can select a session, right-click, then select **Replay** to review the session in the session player.

At this point in the evaluation, you have had very limited activity on the Linux or UNIX computer you are managing and auditing. Before replaying any sessions, you might want to log on to the managed computer and run several simple UNIX shell commands, then close the UNIX terminal and log off.

To replay the sample session

1. Open Audit Analyzer from the desktop icon.
2. Click **Today** in the left pane to list the sessions that have run today.
3. Select the session that has UNIX shell command activity, right-click, then click **Replay** to display the session player.

The left pane of the session player displays a summary of activity. You can search on any column to find events of interest. You can also search for a specific text string. For example:



4 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.

5 Close the session player.

Managing audited sessions

You can right-click any session to view an indexed list of the commands captured, export the session activity to another format for sharing or further analysis, update the review status for the session, or delete the session.

Using command summaries

You can view a list of the commands the user executed in a selected session by right-clicking the session, then selecting Indexed Command List. This option provides a summary of user activity so that you can quickly scan for events of interest or for suspicious activity without replaying activity. You can then start the session player from a specific command in the list by selecting the command and clicking **Replay**.

Exporting sessions

You can export session activity to several different formats to enable you to share information for review and analysis. After selecting a session, you can right-click to export the session to the following formats:

- As a plain text (TXT) file that includes the time of each input and output event that occurred during the session.
- As a comma separated values (CSV) file where each row represents a single command input or output line from the terminal window.
- As a Microsoft Windows Media Video (WMV) file can be played by using any media player that supports the WMV format. This option enables you to share the video capture of activity with auditors or other users who don't have access to Audit Analyzer. You should note, however, that WMV files do not include all of the information available in the session player. For example, exporting a session to a WMV files does not preserve information such as the session summary that includes the user name, computer, start and end time for the session and the summary of events.
- As a uniform resource identifier (URI) by selecting **Copy Session URI**. This option enables you to share the session with auditors or other users who don't have access to Audit Analyzer. Once copied to the clipboard, you can paste the URI into a browser to open the session for replay.

Viewing and editing session properties

If you select a session, right-click, then select **Properties** you can view detailed information about the session, including the type of session, the session start and end times, the zone where the session took place, the audit store where the session is stored, details about the user whose activity was recorded and computer where the session ran, and the current status of the session. From the properties section, you can also view the current review status for the session, when the review status was last modified, and who made the change to the review status. You can also click on the Reviewers tab in Properties to see the list of users that are authorized to review the session, change the status of the session, and add comments to the session. By clicking the Comments tab, you can also view and add comments to the session. For example, you might want to use the Comments tab to add details about what to look for in a session to assist a reviewer or to provide additional information when you change the review status of a session.

Updating review status for a session

You can use the **Update Review Status** for a session to distinguish sessions that warrant attention and to mark their progress through your review cycle. For example, if you find a session that warrants analysis, you might right-click to select Update Review Status, then select **To be Reviewed**. After you select a new status, you are prompted to add comments and the session is added to the appropriate predefined query in the left pane. For example, if you selected To be Reviewed status, the session to the **Sessions to be Reviewed** list.

After you review the session and you determine it needs further action, you might select the **Pending for Action** review status. Selecting this status removes the session from **Sessions to be Reviewed** list and adds it to **Sessions Pending for Action** list.

Deleting sessions

You can select a session, right-click, then select **Delete** to delete a session after you have finished reviewing activity and taken appropriate action or when it is no longer needed. Selecting this option deletes the session from all predefined and custom query lists. For

example, if you delete the session from the results for the **Today** predefined query, the session might also be deleted from the results for the predefined **Sessions to be Reviewed** query or any shared or private queries where it was previously listed.

Creating custom queries

In addition to the predefined queries, you can use Audit Analyzer to create your own queries for locating sessions using specific criteria. For example, you might want to find all sessions that contain the string `sudo` or that ran a specific program. To search for these sessions, you can create a custom query definition.

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.

To create a new custom query

1. Open Audit Analyzer, select Audit Sessions, right-click, then select the type of session query to create.
2. Type a name and description for the query.
3. Select the type of sessions that you want the query to find.

   For example, select UNIX sessions to limit the search to only include UNIX sessions. By default, new queries search for both UNIX and Windows sessions.
4. Select an attribute for grouping query results, if applicable.
5. Select an attribute for ordering query results within each group, if applicable.

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.

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.

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.

Frequently asked questions

This chapter provides answers to common questions and information about specific features that are not applicable for all organizations. You should review the questions covered to see if there are any topics of interest or are relevant to your situation.

The following questions are covered:

Can I manage Centrify software from one location?

Yes. You can use Deployment Manager to centrally manage and deploy Centrify software for remote UNIX and Linux computers. For example, Deployment Manager can discover UNIX and Linux computers on your internal network or hosted by a cloud service, determine whether those computers meet basic system requirements or have Centrify software already installed, and deploy or update Centrify software on those computers when you are ready to do so.

You used Deployment Manager during the evaluation in "Exploring additional management tools" on page 43. You can also use Deployment Manager to download Centrify software from the Centrify website, analyze your environment, deploy and update Centrify software on remote computers, and manage those computers from a central location. From Deployment Manager, you can open remote sessions on managed computers, enable or disable auditing, or run administrative scripts.

How do I accommodate legacy or conflicting identity information?

If you plan to migrate existing UNIX and Linux users to Active Directory, you might have users that already have different login names or UIDs on multiple UNIX or Linux computers. For file and directory ownership to continue uninterrupted, those users must be able to continue using those legacy identity attributes.

To accommodate different login names and UIDs on different computers, you can create computer-level overrides that let you change just those UNIX attributes you need to change for individual UNIX or Linux computers. The legacy attributes remain tied to a single Active Directory account, but enable you to deploy with no changes to your existing environment.

To set computer-level overrides

1. Expand Zones and parent and child zones to find the zone for the computer requiring an override.
2. Expand **Computers** to display the computer requiring an override.
3. Expand the computer name and UNIX Data.
4. Right-click **Users** under the selected computer, click **Add User to Zone.**
5. Search for and select the Active Directory user.
6. Select the UNIX properties to change in the user's UNIX profile.

For example, you can change the UID used for the selected user. The new profile attribute is only used on the computer where you make the change.

7 Set the new value, then click **OK**.

For all other computers in the selected zone and in other zones, the user's UNIX profile remains unchanged. You can change any or all profile attributes on other computers to accommodate your legacy identity information.

Can I have separate role assignments for specific computers?

Yes. Centrify-managed computers get their role assignments from three places:

- Parent and child zone role assignments made in the Authorization node.
- Role assignments made at the computer level.
- Role assignments made in the zone's computer roles.

Generally, you start assigning roles at the child zone and then the computer role levels. However, there are occasions when you need to make the role assignment for a single computer. In this case, you use the computer-level override functionality.

To make a role assignment as a computer-level override

1 Expand Zones and parent and child zones to find the zone for the computer requiring an override.

2 Expand **Computers** to display the computer requiring an override.

3 Expand the computer name and select Role Assignments.

4 Right-click **Role Assignments** under the selected computer, click **Assign Role.**

5 Select the role requiring a computer-specific assignment.

6 Click **Add AD Account** to search for and select a user or group.

How can I manage access rules for computers in different zones?

You can use computer roles—groups of computers with a common purpose—to simplify assigning access roles. A computer role is simply an Active Directory group of computers. You create this group because a specific set of computers have something in common. For example, you can create a security group for all Oracle database servers in your organization, or all Oracle servers in a specific location, or all Oracle servers owned by a certain team of administrators. The same computers might be in multiple Active Directory groups, but each group defines a specific purpose. The computers might also be in the same zone or different zones.

A computer role enables you to associate an Active Directory group of computers with a specific set of access rules that apply to just that set of computers.

To create a computer role that defines access rules for a group of computers

1. Create Active Directory groups for the sets of users who have specific access rights.

   For example, you might create a group for `OracleUsers` and a group for `OracleAdmins` in the Centrify UNIX Groups organizational unit.

2. In Access Manager, expand Zones and parent and child zones to find the zone for the computer requiring a computer role.

3. Expand Authorization, right-click Computer Roles, then select **Create Computer Role**.

4. Type the name and description, then select **<Create group>** to **c**reate the Active Directory security group for the computers than share a common purpose.

   For example, create a new global group named `Oracle Servers`.

5. In Access Manager, create or identify the access rights and role definitions that will be specifically applicable for the set of computers.

For example, define the access rights appropriate for the Oracle users and for the Oracle administrators.

Add role definitions for the Oracle users (`OracleLoginRights`) and administrators (`OracleAdminRights`), then add the appropriate rights to each role.

6 Assign the role definitions to the appropriate Active Directory groups.

For example, assign the `OracleLoginRights` role to the `OracleUsers` group and the `OracleAdminRights` role to the `OracleAdmins` group.

7 Add the computers to the computer role group.

For example, expand Computer Roles and Oracle servers, right-click Members, then select **Add Computer** to add each Oracle server to the Members node.

How do I manage access privileges during application development?

In-house application development and deployment typically require three sets of computers, each with its own set of users and privileges:

- Development: The set of computers with the source code and tools for application development. You only want your developers and maybe one or two users to have access to these computers.
- Test: The set of computers used by QA to confirm that the application conforms to specifications. You only want the QA staff to have access to these computers.
- Production: The computers deployed throughout the enterprise. You don't want developers or QA to have access to these computers.

You can use computer roles to ensure that only specified users have access at each stage. In this case, you would define two computer roles in the zone:

- `DevelopmentSystems`

- `TestSystems`

Then, you would do the following:

- Create `Developer` and `Tester` groups in Active Directory.
- Create `Developer` and `Tester` roles and add the rights in Access Manager.
- Assign the roles to the groups in the `DevelopmentSystems` and `TestSystems` roles.
- Add the development and test computers as a member to each role.

Now, only the members of the `Developer` and `Tester` Active Directory groups have access to the corresponding computer role's member computers.

How do I terminate a user account but keep the account profile?

When a user leaves the company, you might want to retain their account profile to ensure all of the files they created on your organization's UNIX and Linux computers have an owner. You can use the predefined `listed` role to retain an account profile with no access privileges.

To create the group and assign the role

1. Create an Active Directory group in the UNIX Groups organizational unit called `Listed`. In the description enter, `Terminated users`.
2. In Access Manager, expand Zones and find the zone where the account profile is required.
3. Expand Authorization and Role Assignments, then select **Assign Role**.
4. Select the `listed` role, click **Add AD Account**, search for and select the select the `Listed` Active Directory group, then click **OK**.

To terminate a user

1. Remove the user account from all of the UNIX Groups that have access rights.
2. Verify that the user has no role assignments and no effective rights in any zone.
3. Add the user account to the `Listed` group.

If the user rejoins the company, you simply delete the user from the `Listed` group and add the user to groups, as needed.

Can Active Directory credentials be used to log in to applications?

Yes. Centrify provides additional packages that let you configure single sign-on for Apache, Tomcat, JBoss, WebSphere and WebLogic web servers, and for Oracle, DB2, and SAP database applications.

Can Active Directory credentials be used for phone and tablet users?

Yes. Centrify offers software that enables you to authenticate users on iOS and Android devices before they can access their company email, web, and SaaS applications. A separate evaluation package is available for you to try out mobile device management for smart phones or tablets. Contact your sales representative for a free evaluation.

How do I migrate from NIS maps to Centrify software?

Access Manager provides an extension that enables you to import and manage NIS network maps in Active Directory on a zone-by-zone basis. For UNIX and Linux computers and applications that submit lookup requests directly to a NIS server listening on the NIS port, you can also deploy the Centrify Network Information Service, `adnisd`, to receive

and respond to NIS client requests from the NIS map information stored in Active Directory.

Removing software after an evaluation

The evaluation software can only be used for a limited time. After you complete the evaluation, you should remove the software to free up space on the physical or virtual computers you used for the evaluation. This chapter describes the steps for removing components from the Windows computer you used for the evaluation and the UNIX or Linux computer you added to Active Directory.

Remove DirectManage Access

The most efficient way to remove Centrify DirectManage components from a Windows computer is to rerun the setup program that installed them.

To remove DirectManage Access components

1. On the physical or virtual computer where you downloaded Enterprise Edition software, double-click **autorun.**
2. On the **Getting Started** page, click **Access**.
3. At the **Welcome** page, click **Next**.
4. Select **Uninstall**, then click **Next**.
5. Review the list of software to be removed, then click **Next**.
6. Click **Finish** to exit the wizard.

The DirectManage Access components are now removed from the host Windows computer. You should note, however, that these steps do not remove any of the Active Directory organizational units, users, or groups you used for the evaluation. You should manually remove these objects with Active Directory Users and Computers or ADSI Edit.

Remove DirectManage Audit

The most efficient way to remove Centrify DirectManage components from a Windows computer is to rerun the setup program that installed them.

To remove DirectManage Audit components

1. On the physical or virtual computer where you downloaded Enterprise Edition software, double-click **autorun.**
2. On the **Getting Started** page, click **Audit**.
3. Select **Uninstall**, then click **Next**.
4. Click **Finish** to exit the wizard.

The DirectManage Audit components are now removed from the host Windows computer. You should note, however, that these steps do not remove the installation service connection point, databases, or database instances. You should manually remove these objects with ADSI Edit and Microsoft SQL Server Management Studio.

Remove Centrify agents

There are two ways to remove Centrify UNIX agents and utilities from managed computers:

- Using Deployment Manager to remove software packages
- Running install.sh to remove software packages

Both procedures produce the same results: the agents and command line programs—such as adinfo, adjoin, adquery, dacontrol, and dzinfo—are removed from the computer.

Using Deployment Manager to remove software packages

If you have Deployment Manager installed, you can use it to remove Centrify software packaged from a central location.

To remove the agent and other packages using Deployment Manager

1. Open Deployment Manager from your Windows computer.
2. Select the remote UNIX or Linux computer, right-click, then select **Manage Software.**
3. Select **Remove installed components**.

   Deployment Manager analyzes the selected computer and displays a list of the Centrify software found. If there are package dependencies, dependent packages are removed automatically. If there are no dependencies, you can remove packages independently.
4. Click **Next**.
5. Type the user name and password for an account with Active Directory administrator privileges.

   Deployment Manager does not delete the Active Directory users accounts. They remain in Active Directory and continue to have the roles assigned to them. However, the accounts can no longer be used to log on to the selected UNIX or Linux computer.
6. Click **Finish** to remove the agent software and tools.

Running install.sh to remove software packages

You can also rerun the `install.sh` script interactively or silently using a configuration file to remove Centrify software from a managed computer.

To remove the agent and other packages using the install.sh script

1. Log on and open a terminal on the managed computer.
2. Run the `adleave` command to remove the computer from the domain controller.

   ```
   adleave -u administratorname
   ```

   The user name you specify with the *`administratorname`* argument should be an account with Active Directory administrator privileges.
3. Type the password for the an account name you specified.

4. Change to the directory that contains the extracted agent package.
5. Run the installation script.

   ```
   /bin/sh install.sh
   ```

   The script determines the Centrify software you have installed on the computer and displays the details for you to review.
6. Enter E to proceed.
7. Conform the removal of packages by entering Y to proceed.
8. Enter Y to reboot the computer after removing software packages.

Index