# Enable RADIUS and LDAP Support in a DBDS for SR 5.0

# Please Read

## Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

# Notices

## Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

## Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

## Copyright

# Contents

# About This Guide

## Introduction

DBDS systems have traditionally been deployed at sites where authentication of users is performed using locally stored credentials. The benefit of storing user credentials locally is that they are self-contained and do not require an external resource for user authentication. This simple method of local authentication may be appropriate and sufficient for isolated machines/networks, and for a small set of users. However, this method becomes unmanageable and cumbersome when the number of users increases. Also, the local authentication method is inadequate when user login access controls, such as access times and authorized client/network locations, are required.

To address these issues for sites with hundreds of users and network devices to administer and manage across the organization, System Release (SR) 5.0 includes support for the following protocols:

- Remote Authentication Dial In User Service (RADIUS) protocol, which is a client/server protocol that provides centralized Authentication, Authorization and Accounting (AAA) service
- Lightweight Directory Access Protocol (LDAP), which is an application protocol that queries and modifies directory entries in a directory server

  **Note:** In SR 5.0, LDAP includes support for Sudo software. Sudo software permits users to run programs as another user, typically "root" user, and simplifies user logins when LDAP is implemented across heterogeneous platforms, such as Solaris, Linux, and AIX.

This guide provides the configuration changes that must be implemented in a Digital Broadband Operating System (DBDS) to enable support for RADIUS, LDAP, and Sudo software.

## Purpose

This purpose of this guide is to provide system administrators with procedures that allow them to enable RADIUS, LDAP, and Sudo support on a client, such as a Digital Network Control System (DNCS), a Remote Network Control Server (RNCS), or an Application server.

## Scope

This guide provides instructions for enabling basic RADIUS, LDAP, and Sudo support on a client host. This guide does not provide instructions for customizing advanced features of RADIUS, LDAP, and Sudo for use with unique site configurations.

## Audience

This guide is written for experienced system administrators. Administrators should have appropriate background and knowledge to complete the procedures described in this document.

**CAUTION:**

**Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product. Incorrectly configuring the system can lock all users out of the system. Correcting this requires a lengthy process of booting from the OS media and undoing the changes.**

## Read Me

Please read this entire guide before beginning the configuration. If you are uncomfortable with any of the procedures, contact Cisco® Services for assistance. To locate the nearest technical support office, go to ***Customer Support*** (on page 20).

**Important:** Perform all of the procedures in this guide in the order in which they are presented. Failure to follow all of the instructions may lead to undesirable results.

## System Release Compatibility

RADIUS, LDAP, and Sudo support can be enabled on a DNCS, RNCS, or Application server with System Release 5.0 (SR 5.0).

For a complete configuration listing of SR 5.0, please contact Cisco Services as indicated in ***Customer Support*** (on page 20).

## Document Version

This is the first formal release of this document.

# 1

# Overview

This chapter provides an overview of RADIUS and LDAP support.

## In This Chapter

# Overview of RADIUS and LDAP

SR 5.0 provides support for RADIUS by bundling a Pluggable Authentication Module (PAM) to a RADIUS authentication module. Additionally, LDAP support in SR 5.0 allows accessing of data stored in an information directory. Bundled in this way, RADIUS and LDAP support provide a centralized authentication, administration, and management solution to meet the needs of a large-scale network.

## Configuration Process

To configure a client host for RADIUS and LDAP, follow this process.

**CAUTION:**

**Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product. Incorrectly configuring the system can lock all users out of the system. Correcting this requires a lengthy process of booting from the OS media and undoing the changes.**

**CAUTION:**

**Make certain to disable NIS before enabling RADIUS and LDAP support. Running NIS and LDAP at the same time can cause damage to your system.**

1. Verify that the client is not using NIS by opening an xterm window on the client host and typing **svcs -a | grep nis/client** and pressing **Enter**. The host displays output similar to the following.

```
bash-3.00$ svcs -a | grep nis/client
disabled       Jul_15   svc:/network/nis/client:default
bash-3.00$
```

2. Is NIS enabled on your system?
   - If **yes**, disable NIS by entering the following command as root user: **# svcadm -v disable -s nis/client svc:/network/nis/client:default disabled**.

     **Important:** Running NIS and LDAP at the same time can cause damage to your system.
   - If **no**, continue with the next step in this procedure.
3. Configure a RADIUS client for RADIUS support.

4 Configure an LDAP client for LDAP and Sudo support.

**Important:** Sites that use an LDAP server for central administration and management and that require Solaris Role-Based Access Control (RBAC) functionality should add the necessary RBAC objects to their LDAP database scheme or use Sudo software. Adding and configuring RBAC objects to LDAP database scheme is outside the scope of this document. This document only provides instructions to enable Sudo support.

5 Test RADIUS and LDAP support by logging into the system.

# 2

# Configure RADIUS Support

This chapter provides procedures to enable a client for RADIUS support.

## In This Chapter

# Enable a Client for RADIUS Support

To configure a RADIUS client for RADIUS support, you will add the IP address and shared secret key of the RADIUS server to the RADIUS configuration file, **/etc/raddb/server**, and will add the RADIUS authentication module to the PAM configuration file, **/etc/pam.conf**.

## Before You Begin

**CAUTION:**
**Make certain to disable NIS before enabling RADIUS and LDAP support. Running NIS and LDAP at the same time can cause damage to your system.**

Before you begin, make certain that NIS is disabled on the client. Otherwise damage may occur to your system.

Obtain the following information from the site administrator:

- RADIUS server IP address (or addresses)
- RADIUS server port (typically 1812 or 1645)
- Shared secret key

## Enabling a Client for RADIUS Support

Follow these instructions to configure a client for RADIUS support.

1. Open an xterm window on the RADIUS client.
2. At the prompt, type **su -** and press **Enter**. A password prompt appears.
3. Type the root user password and press **Enter**. A prompt for the root user appears.
4. Type **cd /etc/raddb** and press **Enter**. The directory **/etc/raddb** becomes the working directory.
5. Type **ls server.dist** and press **Enter** to verify that the **server.dist** file exists in the **/etc/raddb** directory.
6. Does the **server.dist** file exist?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, refer to the sample RADIUS server configuration file in ***Appendix C*** (on page 33) and use an editor such as **vi** to create the server.dist file in the **/etc/raddb** directory.
7. Type **cp server.dist server** and press **Enter** to copy the **server.dist** to **server**.

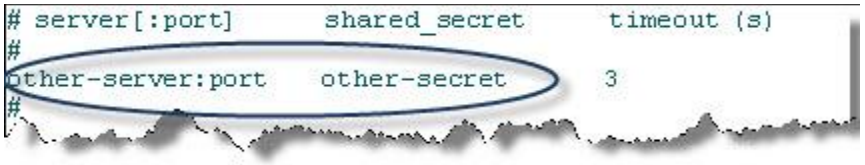
8 Type **chmod 0600 server; chown root:root server** and press **Enter** to set appropriate permissions and ownership.

9 Type **ls -l** and press **Enter** to verify the permissions and ownership.

10 Use an editor such as **vi** to open the **/etc/raddb/server** file and replace the **other-server:port other-secret** line (circled in the following illustration) with the following information.

**Note**: See ***Appendix C*** (on page 33) for an example of the contents of the **/etc/raddb/server** file.

- RADIUS server IP address or IP addresses (from your site administrator)
- RADIUS server port (from your site administrator)
- Shared secret key or keys (from your site administrator)




**Example:** If your site administrator provided you with two pairs of RADIUS server IP addresses/ports and shared secret keys (**192.168.100.1:1812/op3n** and **192.168.100.2:1812/p4sskey**), you would revise the server file as shown in the following illustration:


11 Save and close the **server** file.

12 Type **cd /etc** and press **Enter** to make **/etc** the working directory.

13 Type **ls pam.conf.pam_radius_auth** and press **Enter** to verify that the **pam.conf.pam_radius_auth** file exists.

14 Does the **pam.conf.pam_radius_auth** file exist?

- If **yes**, continue with the next step in this procedure.
- If **no**, refer to the sample PAM configuration file in ***Appendix D*** (on page 35) and use an editor such as **vi** to create the **pam.conf.pam_radius_auth file**.

15 Type **cp -p pam.conf pam.conf.preRADIUS** and press **Enter** to save the current **pam.conf** file.

16 Type **cp pam.conf.pam_radius_auth pam.conf** and press **Enter**. The RADIUS enabled PAM configuration filed is copied to **pam.conf**.

**Note:** A sample **pam.conf** file that supports RADIUS is included in SR 5.0. This file can be further customized to meet the requirements of the site. See the sample PAM configuration file in ***Appendix D*** (on page 35) for details.

17 Type **chmod 0644 pam.conf; chown root:sys pam.conf** and press **Enter** to set appropriate permissions and ownership on pam.conf file.

18 Go to ***Enable the Client for LDAP and Sudo Support*** (on page 10).

# 3

# Configure LDAP and Sudo Support

This chapter provides procedures to enable a client for LDAP and Sudo support.

**Important:** Sites that use an LDAP server for central administration and management and that require Solaris role-based access control (RBAC) functionality should add the necessary RBAC objects to their LDAP database scheme or use Sudo software. Adding and configuring RBAC objects to LDAP database scheme is outside the scope of this document. This chapter only provides instructions to enable LDAP and Sudo support.

## In This Chapter

# Enable the Client for LDAP and Sudo Support

This section describes how to configure a client for LDAP and Sudo support.

To configure an LDAP client for LDAP support, you will use the LDAP client utility called **ldapclient**. This utility binds the client to the specified LDAP server to retrieve configuration information. The **ldapclient** utility can be invoked in multiple ways, but this document describes only the init form. The init form of **ldapclient** uses an existing profile stored on the LDAP server to initialize the LDAP client. All other forms of **ldapclient** invocation are outside the scope of this document. Please refer to Solaris man pages in section 1M for details of using **ldapclient**.

Solaris LDAP clients can be configured to use one of the following authentication methods:

- none
- simple
- sasl/CRAM-MD5
- sasl/DIGEST-MD5
- tls:simple
- tls:sasl/CRAM-MD5
- tls:sasl/DIGEST-MD5

Note that some LDAP servers may not support all of the above authentication methods. This document discusses only "simple" and "tls:simple" authentication methods.

- **Simple Authentication Method** - In "simple" authentication method, the bind password is sent in the clear to the LDAP server. This may be acceptable in some environments where RSA authentication server is used for two-factor authentication and only read access is provided to LDAP objects. Procedures for using the simple authentication method are provided in this chapter.
- **Transport Layer Security (TLS) authentication method** - This authentication method has the ability to encrypt the entire session between the LDAP client and server. However, this requires proper configuration on the LDAP server and appropriate certificates on the client. Procedures for using the TLS authentication method are given in ***Appendix A Enable the LDAP Client with TLS Authentication*** (on page 21).

Manual initialization of LDAP client requires various attributes to be specified on the command line. Obtain the following attributes from the site administrator:

- LDAP server hostname and IP address.
- LDAP server port numbers if not using the default ports of 389 or 636
- Name of existing profile (profileName) that can be used for initializing the LDAP client
- Bind Distinguished Name (DN) for proxy identity (proxyDN)
- Client proxy password (proxyPassword)
- LDAP domain name
- If LDAP server supports Transport Layer Security (TLS) authentication and the client requires TLS, request Root CA and any subordinate CA signing certificates.

Please note that initialization of an LDAP client creates the following files:

- **/var/ldap/ldap_client_cred** - contains the client credentials
- **/var/ldap/ldap_client_file** - contains information about the server to which LDAP client should connect

In addition, **ldapclient** will modify multiple entries in the name service switch file (**/etc/nsswitch.conf**) with **ldap** tag. However, these entries must be modified for optimal performance.

## Enable the LDAP Client with Simple Authentication

These procedures must be executed on a client that requires simple authentication. If the session between the LDAP client and server must be encrypted, then TLS authentication that is described in the next section must be used.

**Important:** When enabling LDAP support for your LDAP client, you must obtain these attributes as they pertain to your system from the site administrator. These instructions use the following sample LDAP client attributes to illustrate the procedures.

- LDAP server hostname = ldapsrvr
- LDAP server IP address = 192.168.1.1
- Default LDAP port = 389
- profileName=simple_profile
- proxyDN = "cn=readonly,dc=example,dc=com"

- proxyPassword = secret
- LDAP domain name (domainName) = example.com

## Before You Begin

Before you begin, gather the following information from the site administrator:

- LDAP server hostname and IP address
- LDAP port number if not using the default of 389
- Existing profile name (profileName)
- Proxy distinguished name (proxyDN)
- Proxy password (proxyPassword)

## Enabling the LDAP Client with Simple Authentication

Follow these instructions to configure the LDAP client with simple authentication for LDAP support.

**CAUTION:**

**Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product. Incorrectly configuring the system can lock all users out of the system. Correcting this requires a lengthy process of booting from the OS media and undoing the changes.**

1. If you have not already done so, open an xterm window on the LDAP client and log in as **root** user.
2. Use a text editor such as vi to open **/etc/hosts** and add the following information to it:
   - LDAP server hostname
   - LDAP server IP address
3. Type **cp -p nsswitch.conf nsswitch.conf.preLDAP** and press **Enter**. The system makes a copy of **nsswitch.conf** and names the copy **nsswitch.conf.preLDAP**.
4. Initialize LDAP client by typing the following and then pressing **Enter**.

   **Note:** This command uses the **line continuation character** (\) to indicate that the command continues on the subsequent line.

```
LDAP_Client# ldapclient -vv init \
-a profileName=simple_profile \
-a proxyDN=cn=readonly,dc=example,dc=com \
-a proxyPassword=secret \
-a domainName=example.com \
-a "defaultServerList=ldapsrvr"
```

5 Did the above command run successfully?
- If **yes**, continue with the next step in this procedure.
- If **no**, contact Cisco Services and provide a screen capture from the above command.

6 Type **cp -p nsswitch.files nsswitch.conf** and press **Enter**. The system copies **nsswitch.files** to **nsswitch.conf**.

7 Use a text editor such as vi to open **/etc/nsswitch.conf** and add the ldap tag only for password, group, and netgroup entries as shown below:

```
passwd:   files ldap
group:    files ldap
netgroup: ldap
```

8 Save and close the **/etc/nsswitch.conf** file.

9 After the above modifications have been made, a file comparison of **/etc/nsswitch.files** and **/etc/nsswitch.conf** should reflect the following differences:

```
LDAP_Client# diff /etc/nsswitch.files /etc/nsswitch.conf
16,17c16,17
< passwd:   files
< group:    files
---
> passwd:   files ldap
> group:    files ldap
29c29
< netgroup: files
---
> netgroup: ldap
```

10 Does the file **/etc/nsswitch.conf** reflect the above changes?
- If **yes**, go to ***Configure Sudo Support*** (on page 14).
- If **no**, go back to step 5 and make the necessary modifications.

## Configure Sudo Support

Sudo (su "do") is a program that allows certain users to run commands with privileges of root or another user. Configuration of **sudo** is contained in the **sudoers** file. This configuration file contains a list of users and the commands they are authorized to run. All permitted commands must be invoked by prefixing the command with **sudo**. Before running a command, a user is forced to enter his password. Once authenticated, sudo verifies the user's authorization by checking the **sudoers** file. SR 5.0 bundles a default sudo configuration in **/usr/local/etc/sudoers** file. Only the **visudo** program must be used to edit the sudoers file because of its built-in syntax checking.

Many factors influence the configuring of the **sudoers** file. Only a simple configuration for administering DNCS is presented here. Application Servers and the RNCS can be also be administered using these procedures. However, sites must contact Cisco services for advanced configurations and other customizations.

Site administrators must define DBDS administrators using LDAP netgroup entries. As shown in the following example, DBDS administrators can be defined using the following LDIF:

```
# DBDSAdmins, Netgroup, example.com
dn: cn=DBDSAdmins,ou=Netgroup,dc=example,dc=com
objectClass: nisNetgroup
objectClass: top
cn: DBDSAdmins
description: All DBDS Admins in the Organization
nisNetgroupTriple: (,dbdsusr1,)
nisNetgroupTriple: (,dbdsusr2,)
nisNetgroupTriple: (,dbdsusr3,)
```

## Before You Begin

Before you begin, gather the following information from the site administrator:

- Userids and/or LDAP netgroup name that defines DBDS administrator.

**Important:** The following procedure assumes that the DBDSADMINS netgroup entry exists in LDAP.

## Configuring Sudo Support

Follow these instructions to configure Sudo support on an LDAP client.

> **CAUTION:**
> **Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product. Incorrectly configuring the system can lock all users out of the system. Correcting this requires a lengthy process of booting from the OS media and undoing the changes.**

1. If you have not already done so, open an xterm window on the LDAP client and log in as **root** user.
2. Type **cp -p /usr/local/etc/sudoers /usr/local/etc/sudoers.preLDAP** and press **Enter**. The system makes a copy of **sudoers** and names the copy **sudoers.preLDAP**.
3. Type **/usr/local/sbin/visudo** and press **Enter**. This opens **/usr/local/etc/sudoers** file using vi editor.
4. Add the following entries in the appropriate sections:
   - User_Alias DBDSADMINS = +DBDSADMINS
   - Cmnd_Alias SUX = /usr/local/bin/sux - dncs
   - Defaults timestamp_timeout = 0
   - DBDSADMINS ALL = (root) SUX
5. Save and close the **/usr/local/etc/sudoers** file.
6. Does the file **/usr/local/etc/sudoers** reflect the above changes?
   - If **yes**, go to ***Test RADIUS, LDAP, and Sudo Configuration*** (on page 17).
   - If **no**, go back to step 4 and make the necessary modifications.

# 4

# Test RADIUS, LDAP, and Sudo Configuration

This chapter provides procedures to verify that a client, for example DNCS, RNCS, or Application server, has been successfully configured for RADIUS, LDAP, and Sudo support. The test involves logging in to a client that has been configured for RADIUS, LDAP, and Sudo.

## In This Chapter

# Log In To a Client Configured for RADIUS and LDAP Support

Follow these instructions to log in to the client you have enabled for RADIUS, LDAP, and Sudo support. A successful login indicates that the client has been configured correctly.

1. Log in to a system that you have enabled for RADIUS, LDAP, and Sudo support with **userID** and **SecurID** code (or password).
2. Were you able to log in successfully?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, refer to ***Appendix F*** (on page 41) for troubleshooting assistance.
3. Test Sudo privileges and access by typing **sudo -l** and pressing **Enter**. The system displays a warning message about privacy and responsibilities, and prompts for the user password.
4. Did the system display the warning message?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, contact Cisco Services for assistance.
5. Enter the user password and press **Enter**. The system displays the list of privileged commands that the user can execute, including **sudo /usr/local/bin/sux - dncs entry**.
6. Did the system display the list of commands, including the **sux** entry?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, contact Cisco Services for assistance and provide the output from the above commands.
7. Assume the DNCS role by typing **sudo /usr/local/bin/sux - dncs** and pressing **Enter**.
8. Did the system allow you to login?
   - If **yes**, you have confirmed that the system is correctly enabled for RADIUS and LDAP support.
   - If **no**, contact Cisco Services for assistance and provide the output from the above commands.

# 5

# Customer Information

## Introduction

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

## In This Chapter

# Customer Support

## If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

# A

# Enable the LDAP Client with TLS Authentication

This appendix provides procedures to enable a client with TLS authentication. Follow the procedures in this appendix only for sites that require TLS authentication between the LDAP client and server. To be successful, the LDAP server must already have been configured for TLS authentication.

**Important:** Sites that use an LDAP server for central administration and management and that require Solaris role-based access control (RBAC) functionality should add the necessary RBAC objects to their LDAP database scheme or use Sudo software. Adding and configuring RBAC objects to the LDAP database scheme is outside the scope of this document. This appendix only provides instructions to enable the LDAP client with TLS authentication.

## In This Appendix

# Enable the LDAP Client with TLS Authentication

This procedure should be followed only at sites that require TLS authentication between LDAP client and server. For this to work, the LDAP server MUST have been configured for TLS authentication.

**Important:** When enabling LDAP support for your LDAP client, you must obtain these attributes as they pertain to your system from the site administrator. These instructions use the following sample LDAP client attributes to illustrate the procedures.

- LDAP server hostname = ldapsrvr
- LDAP server IP address = 192.168.1.1
- LDAP port = 389
- profileName=tls_simple_profile
- proxyDN = "cn=readonly,dc=example,dc=com"
- proxyPassword = secret
- CA certificate file = /var/tmp/cacert.pem

## Before You Begin

Before you begin, gather the following information from the site administrator:

- LDAP server hostname and IP address
- LDAP port number if not using the default of 389
- profileName=tls_simple_profile
- Proxy distinguished name (proxyDN)
- Proxy password (proxyPassword)
- Root CA certificate file (cacert.pem) in PEM format

# Enabling the LDAP Client with TLS Authentication

Follow this procedure to configure the LDAP client with TLS authentication. During this procedure, you will use the certificate database tool **certutil** to create the certificate database in the **/var/ldap** directory.

> **CAUTION:**
> **Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product. Incorrectly configuring the system can lock all users out of the system. Correcting this requires a lengthy process of booting from the OS media and undoing the changes.**

1. If you have not already done so, open an xterm window on the LDAP client and log in as **root** user.
2. Use a text editor such as vi to open the **/etc/hosts** file and add the following information to the file:
   ```
   LDAP server hostname and IP address
   ```
3. Type **/usr/sfw/bin/certutil -N -d /var/ldap** and press **Enter**, as shown in the following example.

   **Example:**
   ```
   LDAP_Client# /usr/sfw/bin/certutil -N -d /var/ldap
   Enter a password which will be used to encrypt your keys.
   The password should be at least 8 characters long,
   and should contain at least one non-alphabetic character.
   ```
4. When the system prompts you to enter a password, press **Enter** twice. The system creates **cert8.db**, **key3.db**, and **secmod.db** in the directory **/var/ldap**.
   ```
   Enter new password:
   Re-enter password:
   ```
5. Type **ls -1 -/var/ldap/*.db** and press **Enter** to check for the presence of these files. The system should display the following output:
   ```
   LDAP_Client# ls -1 /var/ldap/*.db
   /var/ldap/cert8.db
   /var/ldap/key3.db
   /var/ldap/secmod.db
   ```
6. Did the output show all the required files?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, go back to step 5 and re-execute the ls command. If the problem persists, contact Cisco Services and provide a screen capture of the above commands.
7. Copy the Root CA certificate file (**cacert.pem**) that was obtained from the site administrator to the **/var/tmp** directory.

8 Type the following and press **Enter** to import the Root CA certificate into the certificate database.

**Note:** This command uses the **line continuation character** (\) to indicate that the command continues on the subsequent line.

```
LDAP_Client# /usr/sfw/bin/certutil -A -a -i /var/tmp/cacert.pem -n \
"RootCA" -t "CT" -d /var/ldap
```

9 Did the system execute the previous command correctly?

- If **yes**, continue with the next step in this procedure.
- If **no**, contact Cisco Services and provide a screen capture from the above command.

10 Initialize the LDAP client by typing the following and pressing **Enter**.

**Note:** This command uses the **line continuation character** (\) to indicate that the command continues on the subsequent line.

```
LDAP_Client# ldapclient -vv init \
-a profileName=tls_simple_profile \
-a proxyDN=cn=readonly,dc=example,dc=com -a proxyPassword=secret \
-a certificatePath=/var/ldap \
-a domainName=example.com \
-a "defaultServerList=ldapsrvr"
```

11 Did the system execute the previous command correctly?

- If **yes**, continue with the next step in this procedure.
- If **no**, contact Cisco Services and provide a screen capture from the above command.

12 Use a text editor such as vi to open the **/etc/nsswitch.conf** file and add the **ldap** tag only for password, group, and netgroup entries as shown in the following example:

```
passwd:   files ldap
group:    files ldap
netgroup: ldap
```

13 Save and close the **/etc/nsswitch.conf** file.

**14** After the above modifications have been made, a file comparison of **/etc/nsswitch.files** and **/etc/nsswitch.conf** should reflect the following differences:

```
LDAP_Client# diff /etc/nsswitch.files /etc/nsswitch.conf
16,17c16,17
< passwd:   files
< group:    files
---
> passwd:   files ldap
> group:    files ldap
29c29
< netgroup: files
---
> netgroup: ldap
```

**15** Does /etc/nsswitch.conf reflect the above changes?

- If **yes**, go to ***Enable Sudo Support*** (on page 28).
- If **no**, go back to step 6 and make the necessary modifications.

# B

# Enable Centralized Sudo Support

This appendix provides procedures to enable a client for Sudo support. Sudo is a program that allows certain users to execute commands in the super user role.

**Important:** Sites that use an LDAP server for central administration and management and that require Solaris role-based access control (RBAC) functionality should add the necessary RBAC objects to their LDAP database scheme or use Sudo software. Adding and configuring RBAC objects to the LDAP database scheme is outside the scope of this document. This appendix only provides instructions to enable Sudo support.

## In This Appendix

# Enable Sudo Support

Sudo is a program that allows certain users to run commands as super user. The commands a user can run are specified in the sudoers configuration file. Sudo provides a clear audit trail of user actions and when they were performed.

Role Based-Access Control (RBAC) that was introduced in SR 5.0 requires users to be configured on each host, and does not lend itself to a centrally administered solution. Providing the sudoers file via LDAP solves the above issue and supports heterogeneous server environments.

## Before You Begin

Before you begin, gather the following information from the site administrator:

- LDAP server hostname
- Base Distinguished Name (DN) for LDAP operations
- Base Sudoers organization unit
- DNCS Admins netgroup

Also make certain to perform alias and server checks as described in the following sections

### Alias Check

Ensure that the **sux** command alias exists.

### Server Checks

Work with the site administrator to ensure that sudoers objects and related entries exist in the LDAP server. For example, to properly administer a DNCS, RNCS, or Application server, LDAP entries similar to the following must exist:

| LDAP Object | LDIF Entry |
|---|---|
| SUDOers | dn: ou=SUDOers,dc=example,dc=com<br>ou: SUDOers<br>objectClass: top<br>objectClass: organizationalUnit |
| netgroup | dn: ou=Netgroup,dc=example,dc=com<br>ou: netgroup<br>objectclass: top<br>objectClass: organizationalUnit |
| DNCSAdmins | dn: cn=DNCSAdmins,ou=Netgroup,dc=example,dc=com<br>objectClass: nisNetgroup<br>objectClass: top<br>nisNetgroupTriple: (,ldapuser1,)<br>description: All DNCS Administrators on the network<br>cn: DNCSAdmins |
| DNCSHosts* | dn: cn=DNCSHosts,ou=Netgroup,dc=example,dc=com<br>objectClass: nisNetgroup<br>objectClass: top<br>nisNetgroupTriple: (dncshost1,,)<br>description: All DNCS Hosts in the network<br>cn: DNCSHosts |
| defaults | dn: cn=defaults,ou=SUDOers,dc=example,dc=com<br>objectClass: top<br>objectClass: sudoRole<br>description: Default sudo Options<br>sudoOption: ignore_dot<br>sudoOption: ignore_local_sudoers<br>sudoOption: always_set_home<br>sudoOption: !mail_no_user<br>sudoOption: root_sudo<br>sudoOption: log_host<br>sudoOption: logfile=/var/log/sudolog<br>sudoOption: timestamp_timeout=5<br>cn: defaults |

| LDAP Object | LDIF Entry |
|---|---|
| dncsRole | dn: cn=dncsRole,ou=SUDOers,dc=example,dc=com<br>objectClass: top<br>objectClass: sudoRole<br>sudoUser: +DNCSAdmins<br>sudoRunAsUser: root<br>sudoCommand: /usr/local/bin/sux - dncs<br>sudoHost: +DNCSHosts<br>sudoOption: authenticate<br>cn: dncsRole |

*The DNCSHosts nisNetgroup object must contain short hostnames and not fully qualified domain names (FQDN).

## Enabling Sudo Support on the LDAP Client

Follow these instructions to enable Sudo support on the LDAP client.

> **CAUTION:**
> **Only appropriately qualified and skilled personnel should attempt to install, operate, maintain, and service this product. Incorrectly configuring the system can lock all users out of the system. Correcting this requires a lengthy process of booting from the OS media and undoing the changes.**

1. Type **ls /usr/local/etc/sudo.ldap.conf.dist** and press **Enter** to verify that the **sudo.ldap.conf.dist** file exists.
2. Does the **sudo.ldap.conf.dist** file exist?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, refer to the sample LDAP configuration file in ***Appendix E*** (on page 39) and use an editor such as vi to create **/usr/local/etc/sudo.ldap.conf.dist** file.
3. Type **cp -p /usr/local/etc/sudo.ldap.conf.dist /etc/ldap.conf** and press **Enter**. The configuration file is copied into place.
4. Use a text editor such as **vi** to open **/etc/ldap.conf** and press **Enter**. Modify the following entries with appropriate values that you obtained from the site administrator and begin again with step 1 of this procedure.
   - host
   - base
   - sudoers_base
5. Type **ls -l /etc/ldap.conf** and press **Enter** to verify permissions and ownership.
6. Use a text editor such as visudo to open **/usr/local/etc/sudoers** and add the appropriate entries as indicated in Server Checks. Then save and close usr/local/etc/sudoers.
7. Use a text editor such as vi to open **/etc/syslog.conf** and add the **local 2** entry as shown in the following example:
   ```
   local 2: debug /var/log/sudolog
   ```
8. Type **touch /var/log/sudolog** and press **Enter**.
9. Type **svcadm restart svc:/system/system-log:default** and press **Enter** to restart syslogd and activate sudo logging.

# C

# Sample RADIUS Server Configuration File

This appendix contains a sample RADIUS Server configuration file. This file is included with SR 5.0 in **/etc/raddb/sample.server.RADIUS**.

## In This Appendix

# Sample RADIUS Server Configuration File

The following provides an example of the RADIUS server configuration file.

```
#  Sample RADIUS server (/etc/rddb/sample.server.RADIUS) configuration file,
#  copy to: /etc/raddb/server
#
#  For proper security, this file SHOULD have permissions 0600,
#  that is readable by root, and NO ONE else.  If anyone other than
#  root can read this file, then they can spoof responses from the server!
#
#  There are 3 fields per line in this file.  There may be multiple
#  lines.  Blank lines or lines beginning with '#' are treated as
#  comments, and are ignored.  The fields are:
#
#  server[:port] secret [timeout]
#
#  the port name or number is optional.  The default port name is
#  "radius", and is looked up from /etc/services The timeout field is
#  optional.  The default timeout is 3 seconds.
#
#  If multiple RADIUS server lines exist, they are tried in order.  The
#  first server to return success or failure causes the module to return
#  success or failure.  Only if a server fails to response is it skipped,
#  and the next server in turn is used.
#
#  The timeout field controls how many seconds the module waits before
#  deciding that the server has failed to respond.
#
# server[:port] shared_secret      timeout (s)
#
other-server:port    other-secret       3
```

# D

# Sample PAM Configuration File

This appendix contains a sample PAM configuration file with RADIUS support. This file is included with SR 5.0 in /etc/pam.conf.pam_radius_auth.

## In This Appendix

# PAM Configuration File

The following shows a sample of the PAM configuration file.

```
# Sample pam configuration file for pam_radius_auth. Copy this file
# to /etc/pam.conf
#
sshd-password   auth required      /usr/lib/security/pam_radius_auth.so.1 debug localifdown
sshd-password   auth sufficient    pam_unix_cred.so.1
sshd-password   auth sufficient    pam_unix_auth.so.1
#
sshd-kbdint     auth required      /usr/lib/security/pam_radius_auth.so.1 debug localifdown
sshd-kbdint     auth sufficient    pam_unix_cred.so.1
sshd-kbdint     auth sufficient    pam_unix_cred.so.1
#
sshd-none       auth required      /usr/lib/security/pam_radius_auth.so.1 debug localifdown
sshd-none       auth requisite     pam_authtok_get.so.1
sshd-none       auth sufficient    pam_unix_cred.so.1
sshd-none       auth sufficient    pam_unix_auth.so.1
#
login           auth required      /usr/lib/security/pam_radius_auth.so.1 debug localifdown
#login          auth requisite     pam_authtok_get.so.1
login           auth sufficient    pam_unix_cred.so.1
login           auth sufficient    pam_unix_auth.so.1
#
other           auth required      /usr/lib/security/pam_radius_auth.so.1 debug localifdown
#other          auth requisite     pam_authtok_get.so.1
other           auth sufficient    pam_unix_cred.so.1
other           auth sufficient    pam_unix_auth.so.1
#
passwd          auth required      pam_passwd_auth.so.1
cron            account required   pam_unix_account.so.1
```

```
#
other           account requisite     pam_roles.so.1
other           account sufficient    pam_unix_account.so.1
other           account sufficient    pam_ldap.so
#
other           session required      pam_unix_session.so.1
#
other           password requisite    pam_authtok_get.so.1
other           password requisite    pam_authtok_check.so.1
other           password required     pam_authtok_store.so.1
#
```

# E

# Sample LDAP Configuration File

This appendix contains a sample sudoers LDAP configuration file. This file is included with SR 5.0 in **/usr/local/etc/sudo.ldap.dist**.

## In This Appendix

# LDAP Configuration File

The following provides an example of the LDAP configuration file.

```
#
# @(#) %full_filespec: %
#
# Sample ldap configuration file for sudo
#
# 1) Copy this file to /etc/ldap.conf
#
# 2) Edit /etc/ldap.conf to fit your system
#
# 3) Add the following line to /etc/nsswitch.conf
#      sudoers: ldap
#


host ldapsrv
base dc=example,dc=com
sudoers_base ou=SUDOers,dc=example,dc=com
sudoers_debug 0
```

# F

# Troubleshooting RADIUS, LDAP, and Sudo Configuration

This appendix contains information for turning on PAM debugging in order to troubleshoot RADIUS, LDAP, and Sudo configuration.

## In This Appendix

# Troubleshooting the Login Process

This section describes how to enable PAM debugging to troubleshoot login issues. After you have used the utility to capture debugging data, you should return logging to its original level because the large volume of debugging data has the potential to fill up the **/var** file system.

## Activating PAM Debugging

Follow this procedure to turn on PAM debugging. In this procedure, all debugging messages from PAM are logged to **/var/log/pam_log**.

**Important:** Because the large volume of debugging data has the potential to fill up **/var** file system, turn PAM debugging off as soon as you are done troubleshooting the login process.

1. Type **touch /etc/pam_debug** and press **Enter**.
2. Use a text editor such as **vi** to open **/etc/syslog.conf** and change auth.info entry to **auth.debug**.

   **Note:** Multiple **<tab>** characters separate the two fields auth.**debug** and **/var/log/authlog**.
3. Save and close the **/etc/syslog.conf** file.
4. Type the following command and then press **Enter** to restart **syslogd** and activate PAM debugging:

   `LDAP_Client#` **svcadm restart svc:/system/system-log:default**
5. Type **view /var/log/authlog** and press **Enter** to view the PAM log for debugging messages. Contact Cisco Services for assistance interpreting debugging messages.
6. Save and close the **/var/log/authlog** file.
7. As soon as you have captured debugging data, close the **/var/log/authlog** file and turn PAM debugging off. The large volume of debugging data has the potential to fill up **/var** file system. To disable PAM debugging, go to ***Deactivating PAM Debugging*** (on page 43).

## Deactivating PAM Debugging

Follow this procedure to turn PAM debugging off. The large volume of debugging data has the potential to fill up **/var** file system.

1. Use a text editor such as **vi** to open **/etc/syslog.conf** and change the **auth.debug** entry that you added in *Activating PAM Debugging* (on page 42) to **auth.info**.
2. Save and close the **/etc/syslog.conf** file.
3. Type the following command and then press **Enter** to restart **syslogd** and deactivate PAM debugging.

   ```
   LDAP_Client# svcadm restart svc:/system/system-log:default
   ```
4. Type **rm /etc/pam_debug** and press **Enter** to remove the PAM debug file.
5. Type **view /var/log/authlog** and press **Enter** to view the PAM log file and ensure that there are no debugging messages in the file.
6. Close the **/var/log/authlog** file.
7. Does **/var/log/authlog** contain debugging messages?
   - If **yes**, you have successfully deactivated PAM debugging.
   - If **no**, contact Cisco Services for assistance turning off PAM debugging.

# Index

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com



March 2012 Printed in United States of America Part Number 4017610 Rev A