Enable RADIUS and LDAP Support Configuration Guide

for EC 9.0 and DTACS 5.2

Please Read

Important

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. To view a list of Cisco trademarks, go to this URL: **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. (1110R)

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

Digital Broadband Delivery System (DBDS) systems have traditionally been deployed at sites where authentication of users is performed using credentials that are stored locally. 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, Explorer Controller (EC) System Release (SR) 9.0 and Digital Transport Adapter Control System (DTACS) SR 5.2 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) services.
- Lightweight Directory Access Protocol (LDAP), which is an application protocol that queries and modifies directory entries in a directory server.

  Note: In EC SR 9.0 and DTACS SR 5.2, LDAP includes support for sudo. sudo permits users to run programs as another user, typically the "root" user.

This guide provides the configuration changes that must be implemented in a DBDS to enable support for RADIUS, LDAP, and sudo.

Purpose

The 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 an EC or DTACS.

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.

System Release Compatibility

RADIUS, LDAP, and sudo support can be enabled on an EC SR 9.0 and DTACS SR 5.2 system.

For a complete configuration listing of EC SR 9.0 and DTACS SR 5.2, please contact Cisco Services.

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

An EC or DTACS system provides support for RADIUS and LDAP features. These features are used for authenticating Linux and Web UI logins to an EC or a DTACS system.

RADIUS

RADIUS support for the EC and DTACS shell login is provided by bundling a Pluggable Authentication Module (PAM) with a RADIUS authentication module. If all users and their authentication exist on the RADIUS server then you only need RADIUS for authentication. If user authorization information is stored remotely, then LDAP is required to store that information. LDAP for the EC and DTACS shell login is required to provide user profile attributes such as UID, GID, and the home directory after a user is successfully authenticated through RADIUS. This is the reason LDAP is coupled with RADIUS for the EC and DTACS shell login.

RADIUS support for the EC and DTACS Web UI login is provided by an xRADIUS module that is bundled with the Apache server.

LDAP

LDAP support for the EC and DTACS shell login is provided by openldap client software, which in turn is provided by the operating system. Currently, for the EC and DTACS shell login, LDAP support is available only with simple authentication (cleartext), as well as LDAP-over-TLS (encrypted), with client certificate verification disabled.

RADIUS and LDAP support, bundled in this way, provide a centralized authentication, administrative, 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. Open a terminal window on the client host and enter the following command to verify that the client is not using NIS.

   ```
   authconfig --test | grep nis
   ```

   Result: The host displays output similar to the following.

   ```
   authconfig --test | grep nis
   nss_nis is disabled
   nss_nisplus is disabled
   ```

2. Is NIS enabled on your system?
   - If **yes**, disable NIS by entering the following command as **root** user: **authconfig --disablenis --update**
   - 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.
5. Test RADIUS and LDAP support by logging into the system.

2

Configure LDAP Support

This chapter provides procedures to set up a standalone EC or DTACS server to use LDAP authentication for the shell login.

Note: The setup steps provided in this chapter assume that the LDAP server is an OpenLDAP server running server software version 2.4 or higher.

In This Chapter

Overview of LDAP Support for the EC or DTACS Shell Login

This section provides steps to enable LDAP authentication for a shell login on an EC or DTACS system. Here, you are configuring your EC or DTACS system as an LDAP client for an existing LDAP server infrastructure.

To configure an LDAP client for LDAP support, CentOS uses ldapsearch. ldapsearch is part of the openldap-clients package that is installed by default on the system.

OpenLDAP 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 the "simple" authentication method, the bind password is sent in the clear to the LDAP server. This may be acceptable in some environments where the 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.

Manual initialization of the 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 the LDAP server supports Transport Layer Security (TLS) authentication and if the client requires TLS, request Root CA and any subordinate CA signing certificates

Enable LDAP Support for the EC or DTACS Shell Login with Simple Authentication

These procedures must be executed on a client that requires simple authentication. This means that passwords and communication between the LDAP server and clients will be in the clear. If the session between the LDAP client and server must be encrypted, then TLS authentication, 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) = dc=example,dc=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 a terminal window on the LDAP client and log in as **admin** user.
2. Type **sudo -i** to change to root user.
3. Use a text editor to open the **/etc/hosts** file and add the following information to it:

   Command syntax:

   ```
   [LDAP IP Address]   [LDAP server hostname]
   ```

   Example:

   ```
   192.168.1.1   LdapServer_Lab1
   ```
4. Save and close the **/etc/hosts** file.
5. Type the following command and press **Enter** to change to the **/etc** directory.

   ```
   cd /etc
   ```
6. Type the following commands and press **Enter** to make backups of configuration files.

   ```
   cp -p nsswitch.conf nsswitch.conf.preLDAP
   cp -p nslcd.conf nslcd.conf.preLDAP
   ```
7. Initialize the LDAP client by typing the following and then pressing **Enter**.

   Notes:

   - This command uses the line continuation character (\) to indicate that the command continues on the subsequent line.
   - Substitute the appropriate entries for the terms shown in brackets. Do not include the brackets.

   ```
   authconfig --enableldap \
   --enableldapauth \
   --ldapserver=[your-ldap-server].com \
   --ldapbasedn="dc=[your-base]-dn,dc=com" \
   --enablemkhomedir \
   --update
   ```

8 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.

9 Type `less /etc/nsswitch.conf` and press **Enter** to verify that the following entries are present.

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

10 Enter the following command to test the connection to the LDAP server.

```
ldapwhoami -vv -H ldap://ldapsrv.dvsg-ldap.com -x
```

Example output:

```
ldap_initialize( ldap://ldapsrv.dvsg-ldap.com:389/??base )
anonymous
Result: Success (0)
```

Enable LDAP Support Over TLS

In Transport Layer Security (TLS) authentication, a TLS (encrypted) session is established between an LDAP client and server before any data is sent to the LDAP server. This TLS session between server and client can be established on an LDAP server by enabling root CA and client certificate verification for the incoming client request, or by just enabling verification of the root CA certificate for the incoming client request. The enabling of the client certificate verification on the LDAP server is done through an attribute setting on the LDAP server. This setting on the LDAP server is site-specific and must be confirmed by the site administrator.

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.

LDAP Support for the EC or DTACS Shell Login with TLS Authentication

This section provides steps to enable LDAP support for the EC or DTACS shell login with TLS authentication. Two types of TLS authentication pertain:

- LDAP Support Over TLS *without* Client Certificate Verification
- LDAP Support Over TLS *with* Client Certificate Verification

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
- LDAP Root CA certificate file = /etc/httpd/user-conf/cacert.pem (example filename)
- LDAP Server Cert file = /etc/httpd/user-conf/ldapsrv-cert.pem (example filename)

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
- LDAP Server certificate file (ldapsrv-cert.pem) in PEM format

Is client certificate verification enabled on the LDAP server?

- If **no** (it is disabled), go to the next section.
- If **yes**, go to ***Enable LDAP Support Over TLS with Client Certificate Verification*** (on page 15).

Enable LDAP Support Over TLS without Client Certificate Verification

Complete this procedure on the EC or DTACS server to configure LDAP support over TLS *without* client certificate verification for shell logins.

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 a terminal window on the LDAP client and log in as **admin** user.
2. Enter **sudo -i** to change to **root** user.
3. Is DNS enabled on your system?
   - If **no**, go to the next step.
   - If **yes**, go to step 6.
4. Use a text editor to open the **/etc/hosts** file and add the following information to the file:

   Command syntax:

   ```
   [LDAP IP Address]   [LDAP server hostname]
   ```

   Example:

   ```
   192.168.1.1         LdapServer_Lab1
   ```
5. Save and close the **/etc/hosts** file.

6 Type the following command to change to the **/etc** directory.

```
cd /etc
```

7 Type the following commands and press **Enter** to make a backup of the following configuration files.

```
cp -p nsswitch.conf nsswitch.conf.preLDAP
cp -p nslcd.conf nslcd.conf.preLDAP
```

8 Type `/usr/bin/certutil -N -d /etc/openldap/certs`

9 Copy the root CA certificate file (**cacert.pem**) that was obtained from the site administrator to the **/etc/httpd/user-conf** directory.

10 Type the following command 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.

```
/usr/bin/certutil -A -a -i /etc/httpd/user-conf/cacert.pem -n
\ "RootCA" -t "CT" -d /etc/openldap/certs
```

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 command.

12 Copy the LDAP server certificate file (for example, ldapsrv-cert.pem) that was obtained from the site administrator to the **/etc/httpd/user-conf** directory.

13 Type the following command and press **Enter** to import the LDAP server certificate file (ldapsrv-cert.pem) into the certificate database.

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

```
/usr/bin/certutil -A -a -i /etc/httpd/user-conf/ldapsrv-
cert.pem -n \
"LDAP-Srv-Cert-Peer" -t "P" -d /etc/openldap/certs
```

14 Did the system execute the previous command correctly?

- If **yes**, continue with the next step.
- If **no**, contact Cisco Services and provide a screen capture of the output of the command.

15 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.

```
authconfig --disablefingerprint --disablecache --update

authconfig --enableldap \
--enableldapauth \
--ldapserver=ldap://your-ldap-server.com \
--ldapbasedn=dc=you-base,dc=com \
--enablemkhomedir \
--enableldaptls \
--disableldapstarttls \
--disablesssd \
--disablesssdauth \
--updateall
```

16 Did the system execute the previous command correctly?

- If **yes**, the following output should display. Continue with the next step in this procedure.

  ```
  Starting nslcd:
  [OK]
  ```

- If **no**, contact Cisco Services and provide a screen capture from the above command.

17 Is the LDAP server certificate a self-signed certificate?

- If **no**, go to the next step.
- If **yes**, execute the following commands and then go to the next step.

  ```
  echo TLS_REQCERT allow >> /etc/openldap/ldap.conf
  echo tls_reqcert allow >> /etc/nslcd.conf
  echo tls_reqcert allow >> /etc/pam_ldap.conf
  ```

18 Enter the following command to test the connection to the LDAP server.

Note: Substitute the appropriate entry for the term in brackets. Do not include the brackets.

```
ldapwhoami -v -H ldap://[your-ldap-server].com -x -Z
```

Example command:

```
ldapwhoami -vv -H ldap://ldapsrv.dvsg-ldap.com -x -Z
```

Example output:

```
ldap_initialize( ldap://ldapsrv.dvsg-ldap.com:389/??base )
anonymous
Result: Success (0)
```

Enable LDAP Support Over TLS with Client Certificate Verification

LDAP support over TLS with Client Verification has not been tested and is not supported.

LDAP Authentication Over TLS for Application Web UI Login

Important: This procedure was not tested. Only the procedure without client verification was tested.

This section provides the steps to configure the application Web UI on the EC, DTACS or LDAP server to use LDAP authentication over TLS for user logins.

These procedures should be followed only at sites that require LDAP authentication over TLS for a Web UI login between an LDAP client and server. The LDAP server must support authentication over TLS.

Important: The steps provided in this section assume that the LDAP server is an OpenLDAP server running server software version 2.4 or higher.

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.

Configure LDAP over TLS with Client Certificate Verification Enabled

Enable Client Certificate Verification is a setting on the LDAP server that is used while establishing a TLS session between a client and server. This TLS session can be established with or without enabling client certificate verification. This section provides you with steps to set up your application Web UI on the EC or DTACS to use LDAP authentication over TLS with client certificate verification enabled.

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

Before You Begin

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

Note: These are all sample file names.

- LDAP Root CA certificate file in .PEM format — /etc/httpd/user-conf/cacert.pem
- LDAP Client Cert file in .PEM format — /etc/httpd/user-conf/dncsec1-cert.pem
- LDAP Client key file in .PEM format — /etc/httpd/user-conf/dncsec1-key.pem

LDAP Authentication Over TLS with Client Certificate Verification Enabled

These instructions assume that all EC or DTACS application processes are already running and that web access is working as expected. After configuring LDAP authentication for the EC Web UI, only LDAP users can log into the Web UI. Locally-added htdigest or RADIUS (using two-factor authentication) users cannot log in to the Web UI console.

Important: The Apache service and processes will be down momentarily on the EC or DTACS while performing these steps.

1. Copy the LDAP root CA certificate file (for example, cacert.pem), that was obtained from the site administrator, to the **/etc/httpd/user-conf** directory.
2. Copy the LDAP client certificate file (for example, dncsec1-cert.pem) and client key file (for example, dncsec1-key.pem), that were obtained from the site administrator, to the **/etc/httpd/user-conf** directory.
3. If you have not already done so, open a terminal window on the LDAP client and log in as **root** user.
4. Use a text editor to open the **/etc/hosts** file and add the following information to it. Then, save and close the file.
   - LDAP server IP address
   - LDAP server IP hostname
5. Type the following command and then press **Enter** to stop Apache services.
   ```
   systemctl stop httpd
   ```
6. Type the following command and then press **Enter** to make sure that associated httpd process are down. The command output should be blank.
   ```
   ps -aef | grep -i httpd | egrep -v "httpd-dncsws|grep"
   ```

7 Uncomment the following entries in the **/etc/httpd/user-conf/httpd.conf.extension** file and update the location path for the certificate files to **/etc/httpd/user-conf**.

```
#LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/user-conf
/<Filename for Root CA Certificate>
#LDAPTrustedMode STARTTLS
```

Example input: When you are finished, the entries should look similar to the following example:

```
LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/user-conf/cacert.pem
LDAPTrustedMode STARTTLS
```

8 Open the **/etc/httpd/user-conf/CSCOec.auth_ldap** or **etc/httpd/user-conf/CSCOdtacs.auth_ldap** file using a text editor. Modify the hostname value in the "AuthLDAPURL" directive to an appropriate LDAP server hostname with FQDN.

```
AuthLDAPURL "ldap://[your-ldap-server].com:389/your-ldap-
query-string"
```

Example input: The finished entry should look similar to this example:

```
AuthLDAPURL "ldap://ldapsrv.dvsg-ldap.com:389/ou=People,dc=dvsg-
ldap,dc=com?uid"
```

9 If present, remove the following line ***above*** the AuthLDAPURL entry.

```
AuthzLDAPAuthoritative on
```

10 Add the following lines below the AuthLDAPURL entry:

```
LDAPTrustedClientCert CERT_BASE64 /etc/httpd/user-conf/dncsec1-cert.pem
LDAPTrustedClientCert KEY_BASE64 /etc/httpd/user-conf/dncsec1-key.pem
```

11 Save and close the file.

12 Type the following command and press **Enter** to note the symbolic link for the **/etc/httpd/conf/CSCOec.auth** or the **/etc/httpd/conf/CSCOdtacs.auth** file.

Example for an EC:

```
ls -ltr /etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
ls -ltr /etc/httpd/conf.cisco/CSCOdtacs.auth
```

13 Type the following command and press **Enter** to remove the **/etc/httpd/conf.cisco/CSCOec.auth** or the **/etc/httpd/conf/CSCOdtacs.auth** file.

Example for an EC:

```
rm /etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
rm /etc/httpd/conf.cisco/CSCOdtacs.auth
```

14 When prompted to confirm the deletion of the file, type **y** and press **Enter**.

15 Type the following command and press **Enter** to symbolically link the **/etc/httpd/conf.cisco/CSCOec.auth** file to the **/etc/httpd/conf.cisco/CSCOec.auth_ldap**; or to link the **/etc/httpd/conf/CSCOdtacs.auth** file to the **/etc/httpd/conf.cisco/CSCOec.auth_ldap** file.

Example for an EC:

```
ln -s /etc/httpd/user-conf/CSCOec.auth_ldap
/etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
ln -s /etc/httpd/user-conf/CSCOdtacs.auth_ldap
/etc/httpd/conf.cisco/CSCOdtacs.auth
```

Note: The auth_ldap files require AuthLDAPBindDN and AuthLDAPBindPassword entries if the user and password are required for bind.

16 Type the following command and press **Enter** to verify that the proper link is created for CSCOec.auth and the CSCOdtacs.auth files.

Example for an EC:

```
ls -ltr /etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
ls -ltr /etc/httpd/conf.cisco/CSCOdtacs.auth
```

Example output:

```
lrwxrwxrwx  1 root   root 35 Jan 23 10:30 /etc/httpd/conf.cisco/CSCOec.auth -
> /etc/httpd/user-conf/CSCOec.auth_ldap
lrwxrwxrwx  1 root   root 35 Jan 23 10:30
/etc/httpd/conf.cisco/CSCOdtacs.auth -> /etc/httpd/user-
conf/CSCOdtacs.auth_ldap
```

17 Type the following command and press **Enter** to start the Apache services.

```
systemctl start httpd
```

18 Type the following command and press **Enter** to ensure that the associated httpd process are running.

```
ps -aef | grep -i httpd | egrep -v "httpd-dncsws|grep"
```

Example output:

```
root      4735     1  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4737  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4738  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4739  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4740  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4741  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
```

```
dncs      4742  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4743  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
dncs      4744  4735  0 17:11 ?        00:00:00 /usr/sbin/httpd -D EC -f
/etc/httpd/conf/httpd-dncs.conf
```

19 Access the EC or DTACS Web UI to test the LDAP authentication.

Note: In the EC or DTACS login window, look for "Cisco DNCS LDAP" to verify web access using LDAP authentication.

20 Were you able to log in successfully?

- If **yes**, you have successfully configured LDAP authentication for the EC or DTACS Web UI.
- If **no**, contact Cisco Services for assistance.

Configure LDAP Over TLS with Client Certificate Verification Disabled

This section provides you with steps to set up your application Web UI on the EC or DTACS to use LDAP authentication over TLS with client certificate verification disabled.

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

Before You Begin

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

- LDAP root CA certificate file in .PEM format — /etc/httpd/user-conf/cacert.pem (sample file name)

LDAP Authentication Over TLS with Client Certificate Verification Disabled

These instructions assume that all EC or DTACS application processes are already running and web access is working as expected. After configuring LDAP authentication for the EC or DTACS Web UI, only LDAP users can log into the Web UI. Locally-added htdigest or RADIUS (using two-factor authentication) users cannot log into the Web UI console.

Important: Apache services and processes will be down momentarily on the EC or DTACS while performing these steps.

1. As **root** user, open the **/etc/hosts** file in a text editor.

   ```
   vi /etc/hosts
   ```

2. Add the following information to the /etc/hosts file.

   Command syntax:

   ```
   [LDAP server IP address]  [LDAP server hostname]
   ```

   Example input:

   ```
   192.168.1.2                    LdapServer_Lab1
   ```

3. Copy the LDAP root CA certificate file (for example, cacert.pem) that was obtained from the site administrator to the **/etc/httpd/user-conf** directory.

4. Type the following command and then press **Enter** to stop the Apache services.

   ```
   systemctl stop httpd
   ```

5. Type the following command and then press **Enter** to make sure the associated httpd process are down. The command output should be blank.

   ```
   ps -aef | grep -i httpd | egrep -v "httpd-dncsws|grep"
   ```

6. Uncomment the following entries in the **/etc/httpd/user-conf/httpd.conf-extension** file and update the location path for the certificate files to **/etc/httpd/user-conf**.

   ```
   #LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/user-conf
   /<Filename for root CA Certificate>
   ```

   ```
   #LDAPTrustedMode STARTTLS
   ```

   Example input: When you are finished, the directives should look similar to the following example:

   ```
   LDAPTrustedGlobalCert CA_BASE64 /etc/httpd/user-conf/cacert.pem
   ```

   ```
   LDAPTrustedMode STARTTLS
   ```

7. Open the **/etc/httpd/conf.cisco/CSCOec.auth_ldap** or the **/etc/httpd/conf.cisco/CSCOdtacs.auth_ldap** file using a text editor. Modify the hostname value in the "AuthLDAPURL" directive to an appropriate LDAP server hostname with FQDN.

   Example: The line you are looking for looks similar to this:

   ```
   AuthLDAPURL "ldap://< server hostname with
   FQDN>:389/ou=People,dc=dvsg-ldap,dc=com?uid"
   ```

   Example input: After modification, the line should look similar to this:

   ```
   AuthLDAPURL "ldap://ldapsrv.dvsg-ldap.com:389/ou=People,dc=dvsg-
   ldap,dc=com?uid"
   ```

8. If present, remove the following line *above* the AuthLDAPURL entry.

   ```
   AuthzLDAPAuthoritative on
   ```

9 Type the following command and press **Enter** to note the symbolic link for the **/etc/httpd/conf.cisco/CSCOec.auth** or the **/etc/httpd/conf.cisco/CSCOdtacs.auth** file.

Example for an EC:

```
ls -ltr /etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
ls -ltr /etc/httpd/conf.cisco/CSCOdtacs.auth
```

10 Type the following command and press **Enter** to remove the **/etc/httpd/conf.cisco/CSCOec.auth** or the **/etc/httpd/conf.cisco/CSCOdtacs.auth** file.

Example for an EC:

```
rm /etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
rm /etc/httpd/conf.cisco/CSCOdtacs.auth
```

11 Type the following command and press **Enter** to symbolically link the **/etc/httpd/conf.cisco/CSCOec.auth** file to **/etc/httpd/user-conf/CSCOec.auth_ldap** or to link **/etc/httpd/conf.cisco/CSCOdtacs.auth** file to **/etc/httpd/user-conf/CSCOdtacs.auth_ldap**.

Example for an EC:

```
ln -s /etc/httpd/user-conf/CSCOec.auth_ldap \
/etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
ln -s /etc/httpd/user-conf/CSCOdtacs.auth_ldap \
/etc/httpd/conf.cisco/CSCOdtacs.auth
```

12 Type the following command and press **Enter** to verify that the proper links were created.

Example for an EC:

```
ls -ltr /etc/httpd/conf.cisco/CSCOec.auth
```

Example for a DTACS:

```
ls -ltr /etc/httpd/conf.cisco/CSCOdtacs.auth
```

Example output:

```
lrwxrwxrwx   1 root     root          35 Jan 23 10:30
/etc/httpd/conf.cisco/CSCOec.auth -> /etc/httpd/user-conf/CSCOec.auth_ldap
lrwxrwxrwx   1 root     root          35 Jan 23 10:30
/etc/httpd/conf.cisco/CSCOdtacs.auth -> /etc/httpd/user-
conf/CSCOdtacs.auth_ldap
```

13 Type the following command and press **Enter** to start the Apache services.

```
systemctl start httpd
```

14 Type the following command and press **Enter** to ensure that the associated httpd process are running.

```
ps -aef | grep -i httpd | egrep -v "httpd-dncsws|grep"
```

Example output:

```
nobody 6819 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
nobody 6820 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
nobody 6821 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
nobody 6822 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
nobody 6823 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
nobody 6824 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
nobody 6825 6816 0 08:37 ? 00:00:00 /usr/sbin/httpd-dncsws -D SSL -D EC -f /etc/httpd/httpd-dncsws/ht
tpd-dncsws.conf
root 19367 1 0 13:30 ? 00:00:00 /usr/sbin/httpd -D SSL -D EC -f /etc/httpd/conf/httpd-dncs.conf
dncs 19369 19367 0 13:30 ? 00:00:00 /usr/sbin/httpd -D SSL -D EC -f /etc/httpd/conf/httpd-dncs.conf
dncs 19370 19367 0 13:30 ? 00:00:00 /usr/sbin/httpd -D SSL -D EC -f /etc/httpd/conf/httpd-dncs.conf
dncs 19371 19367 0 13:30 ? 00:00:00 /usr/sbin/httpd -D SSL -D EC -f /etc/httpd/conf/httpd-dncs.conf
dncs 19372 19367 0 13:30 ? 00:00:00 /usr/sbin/httpd -D SSL -D EC -f /etc/httpd/conf/httpd-dncs.conf
```

15 Access the EC or DTACS Web UI to test the LDAP authentication.

Note: In the EC or DTACS login window, look for "Cisco DNCS LDAP" to verify web access using LDAP authentication.

16 Were you able to log in successfully?

- If **yes**, you have successfully configured LDAP authentication for the EC or DTACS Web UI.
- If **no**, contact Cisco Services for assistance.

3

Configure RADIUS Support

This chapter provides procedures to enable RADIUS support for the Linux and Web UI logins on an EC or DTACS system.

In This Chapter

Enable RADIUS Support for the EC or DTACS Shell Login

This section provides steps to enable RADIUS authentication (two-factor authentication) for a shell login to an EC or DTACS system. Here, you are configuring your EC or DTACS system as a RADIUS client to an existing RADIUS server infrastructure.

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/pam_radius.conf,** and will add the RADIUS authentication module to the sshd PAM configuration file, **/etc/pam.d/sshd**.

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.

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 RADIUS Support for EC or DTACS Shell Login

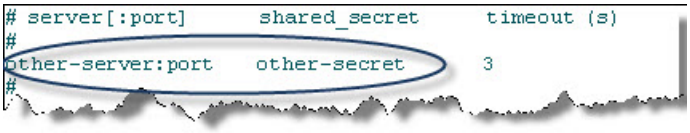
Follow these instructions to configure a client for RADIUS support.

1. Open a terminal window on the RADIUS client and log in as **admin** user.
2. At the prompt, type **sudo -i** and press **Enter** to change to **root** user.
3. Type `cd /etc` and press **Enter**. The directory **/etc** becomes the working directory.
4. Type `cp -p pam_radius.conf pam_radius.orig` and press **Enter** to copy the **pam_radius.conf** file to **pam_radius.orig**.
5. Type `chmod 0600 server ; chown root:root pam_radius.conf` and then press **Enter** to set appropriate the permissions and ownership.
6. Type `ls -l` and press **Enter** to verify the permissions and ownership.

7 Use a text editor to open the **/etc/pam_radius.conf** file and replace the **other-server: other-secret** line (circled in the following illustration) with the following information:

Note: See *Sample RADIUS Server Configuration File* (on page 49) for an example of the contents of the **/etc/pam_radius.conf** file.

- When replacing this entry, make sure you add **:[port]** to the end of the IP entry.
- 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:

Important: If the following entry is present in the file, comment it out as shown.

```
#127.0.0.1  secret  1
```

8 Save and close the **pam_radius.conf** file.

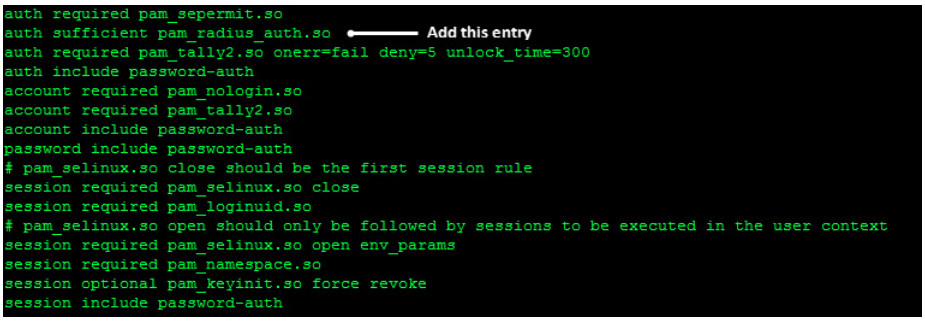
Note: You can now enable LDAP support for the EC or DTACS shell login on the EC system. This enables user attributes, such as UID and GID, to be available.

9 Open the **/etc/pam.d/sshd** file in a text editor.

10 Add the following line to the file.

```
auth sufficient pam_radius_auth.so
```

Example:



11 Save and close the file.

12 For sites that require sudo support for shell users, go to ***Configure Sudo Support*** (on page 33).

Enable RADIUS Support for the EC or DTACS Web UI Login

This section provides steps to enable RADIUS authentication (two-factor authentication) for the application Web UI login running on an EC or DTACS system.

These instructions assume that all EC or DTACS application processes are already running and web access is working as expected.

Important: After configuring RADIUS authentication (two-factor authentication) for the EC or DTACS Web UI, locally added *htdigest* users cannot log into the EC or DTACS Web UI console.

Requirements and Prerequisites

Make certain that the following prerequisites are in place before you configure RADIUS authentication for the Web UI.

Before beginning this procedure, verify the following:

- Web access is working as expected
- You have a RADIUS user account (an RSA security key fob, for example)
- You know the following information:
  - RADIUS server IP address
  - RADIUS authentication port number
  - RADIUS password
- You have verified the following:
  - Network connectivity exists between the RADIUS server and the EC that you are configuring

Configure RADIUS Authentication for the EC or DTACS Web UI

To complete this procedure, log in to the EC or DTACS host as **root** user.

1. Type the following command and press **Enter** to stop Apache services.

   ```
   systemctl stop httpd
   ```

2. Type the following command and press **Enter** to delete this file on an EC host.

   Example for an EC:

   ```
   rm /etc/httpd/conf.cisco/CSCOec.auth
   ```

   Example for a DTACS:

   ```
   rm /etc/httpd/conf.cisco/CSCOdtacs.auth
   ```

3. Type the following command and press **Enter** to create a soft link to **/etc/httpd/user-conf/CSCOec.auth_radius** with the name **/etc/httpd/conf.cisco/CSCOec.auth;** or to link the **/etc/httpd/user-conf/CSCOdtacs.auth_radius** to the **/etc/httpd/conf.cisco/CSCOdtacs.auth** file**.**

   Example for an EC:

   ```
   ln -s /etc/httpd/user-conf/CSCOec.auth_radius \
   /etc/httpd/conf.cisco/CSCOec.auth
   ```

   Example for a DTACS:

   ```
   ln -s /etc/httpd/user-conf/CSCOdtacs.auth_radius \
   /etc/httpd/conf.cisco/CSCOdtacs.auth
   ```

4. Type the following command and press **Enter** to copy the file CSCOec.radius.template to **CSCOec.radius** or the CSCOdtacs.radius.template to **CSCOdtacs.radius**.

   Example for an EC:

   ```
   cp /etc/httpd/user-conf/CSCOec.radius.template
   /etc/httpd/user-conf/CSCOec.radius
   ```

   Example for a DTACS:

   ```
   cp /etc/httpd/user-conf/CSCOdtacs.radius.template
   /etc/httpd/user-conf/CSCOdtacs.radius
   ```

5. Use a text editor to add the following line to the **/etc/httpd/user-conf/CSCOec.radius** or the **/etc/httpd/user-conf/CSCOdtacs.radius** file:

   ```
   AuthXRadiusAddServer <RADIUS server IP address>:<listening TCP
   port> <RADIUS password>
   ```

   Example input:

   ```
   AuthXRadiusAddServer 10.90.177.31:1812 testing123
   ```

6. Enter the following command to enable **memcached**.

   ```
   systemctl enable -now memcached
   ```

7. Type the following command and press **Enter** to start the Apache service.

   ```
   systemctl start httpd
   ```

8 Go to the EC or DTACS Web UI to test RADIUS authentication.

Note: In the EC or DTACS login window, look for **Cisco DNCS RADIUS** to verify web access using RADIUS authentication.

9 Enter your RADIUS authentication credentials for the EC or DTACS Web UI.

Example: If your PIN is **111** and the six-digit number on the token card is **234567**, you would use **111234567**.

10 Were you able to log in successfully?

- If **yes**, you have successfully configured RADIUS support for the EC or DTACS Web UI.
- If **no**, contact Cisco Service for assistance.

4

Configure sudo Support

Introduction

This chapter provides procedures to set up sudo support on a standalone EC or DTACS server.

In This Chapter

Configure sudo Support

sudo 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 the password. Once authenticated, sudo verifies the user's authorization by checking the sudoers file. EC SR 9.0 and DTACS SR 5.2 bundles a default sudo configuration in the **/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 the EC is presented here. However, sites must contact Cisco Services for advanced configurations and other customizations.

Site administrators can 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

Gather the following information from the site administrator:

- Userids and/or the LDAP netgroup name that defines the 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.

Note: If different users require sudo rights, create a unique file based on other files in the /etc/sudoers.d directory (e.g. 90-[username]-privileges). Do not use the visudo command as it may compromise sudo access for other users.

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. Login to the LDAP client as **admin** user and then enter the following command to change to **root** user.

   ```
   sudo -i
   ```

2. Type the following command and press **Enter**. The system makes a copy of **sudoers** and names the copy **sudoers.preLDAP**.

   ```
   cp -p /etc/sudoers /etc/sudoers.preLDAP
   ```

3. Type the following command and press **Enter** to open the **/etc/sudoers** file in a vi editor.

   ```
   /usr/sbin/visudo
   ```

4. Update the file for your system needs.

   Example: This example indicates what the dncs user may have access to

   ```
   ## Define status commands for critical EC system services.
   Cmnd_Alias EC_SYS_SVC_STATUS_CMDS = /sbin/service tomcat status, \
   /sbin/service httpd status, \
   /sbin/service httpd-dncsws status, \
   /sbin/service informix status, \
   /sbin/service oammgrctrl status

   ## Allow dncs user to manage dncsInitd service and check status.
   dncs ALL=(root) NOPASSWD: /sbin/service dncsInitd *, \
   EC_SYS_SVC_STATUS_CMDS

   # Don't require tty to allow execution from scripts.
   Defaults: dncs !requiretty

   ## Allow users in dncsadmin group to becomes dncs
   %dncsadmin ALL=(root) /bin/su - dncs

   ## Define EC Administration Commands
   Cmnd_Alias DNCS_START = /dvs/dncs/bin/dncsStart
   Cmnd_Alias DNCS_STOP = /dvs/dncs/bin/dncsStop
   Cmnd_Alias DNCS_KILL = /dvs/dncs/bin/dncsKill
   Cmnd_Alias DNCS_CTRL = /dvs/dncs/bin/dncsControl, /dvs/dncs/bin/dncsControl.pl
   Cmnd_Alias SHOW_DB_SESS = /dvs/dncs/bin/showActiveSessions
   Cmnd_Alias KILL_DB_SESS = /dvs/dncs/bin/killActiveSessions
   Cmnd_Alias START_WEB_SRV = /dvs/dncs/bin/startWebServers
   Cmnd_Alias STOP_WEB_SRV = /dvs/dncs/bin/stopWebServers
   Cmnd_Alias DNCS_LOGLVL = /dvs/dncs/bin/logLvl
   ```

5. Save and close the **/etc/sudoers** file.

6. Does the file **/etc/sudoers** reflect the above changes?

   - If **yes**, go to the next chapter.
   - If **no**, go back to step 4 and make the necessary modifications.

5

Test RADIUS, LDAP and sudo Configuration

Introduction

This chapter provides procedures to verify that a client, for example, an EC, has been successfully configured for RADIUS, LDAP with simple authentication, and sudo support for the shell login. The test involves logging into a client that has been configured for RADIUS, LDAP with simple authentication, and sudo.

In This Chapter

Log In To a Client Configured for RADIUS and LDAP Support

Follow these instructions to log into the client you have enabled for RADIUS, LDAP with simple authentication, 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 your **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 A, Troubleshooting RADIUS, LDAP, and sudo Configuration*** (on page 41) for troubleshooting assistance.
3. Test sudo privileges and access by typing **sudo -i** 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.
6. Did the system display the list of commands?
   - 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. Switch to the **dncs** user account by typing the following command and pressing **Enter**.

   ```
   su dncs
   ```
8. Did the system allow you to login?
   - If **yes**, you have confirmed that the system is correctly enabled for RADIUS and LDAP with simple authentication for the Linux login.
   - If **no**, contact Cisco Services for assistance and provide the output from the previous commands.

6

Customer Information

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

Troubleshooting RADIUS, LDAP, and sudo Configuration

This appendix contains information for turning on PAM debugging in order to troubleshoot RADIUS, LDAP with simple authentication, and sudo configuration.

In This Appendix

Troubleshooting the Login Process

To troubleshoot login issues, review the **/var/log/secure** file.

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.

In This Appendix

Enable sudo Support Draco

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.

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
- EC or DTACS Admins netgroup

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

Alias Check

Ensure that the **su** 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 an EC or DTACS, LDAP entries similar to the following must exist:

LDAP Object	LDIF Entry
SUDOers	dn: ou=SUDOers,dc=example,dc=com ou: SUDOers objectClass: top objectClass: organizationalUnit
netgroup	dn: ou=Netgroup,dc=example,dc=com ou: netgroup objectclass: top objectClass: organizationalUnit

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

LDAP Object	LDIF Entry
dncsRole	dn: cn=dncsRole,ou=SUDOers,dc=example,dc=com
	objectClass: top
	objectClass: sudoRole
	sudoUser: +DNCSAdmins
	sudoRunAsUser: root
	sudoCommand: /bin/su dncs
	sudoHost: +DNCSHosts
	sudoOption: authenticate
	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 the following command and press **Enter** to verify that the **sudo.ldap.conf** file exists.

   ```
   ls /etc/sudo-ldap.conf
   ```

2. Does the **sudo.ldap.conf** file exist?
   - If **yes**, continue with the next step in this procedure.
   - If **no**, refer to the sample LDAP configuration file in ***Sample LDAP Configuration File*** (on page 53) and use an editor to create the **/etc/sudo-ldap.conf** file.
3. Type the following command and press **Enter**. The configuration file is copied into place.

   ```
   cp -p /etc/sudo-ldap.conf /etc/sudo-ldap.conf.orig
   ```

4. Use a text editor to open the **/etc/ldap-sudo.conf** file. Modify the following entries with appropriate values that you obtained from the site administrator.
   - host
   - base
   - sudoers_base

5 Type the following command and press **Enter** to verify permissions and ownership.

```
ls -l /etc/sudo-ldap.conf
```

6 Use the visudo editor to open the **/etc/sudoers** file and add the appropriate entries as indicated in **Server Checks**. Then save and close the file.

7 To debug sudo, open the **/etc/sudo-ldap.conf** file in a text editor and add the following line to the end of the file.

```
Debug sudo /var/log/sudo_debug all@warn,plugin@info
```

8 Save and close the **/etc/sudo-ldap.conf** file.

C

Sample RADIUS Server Configuration File

This appendix contains a sample RADIUS server configuration file. This file, /etc/httpd/user-conf/CSCOec.radius.template, is included with EC SR 9.0 and DTACS SR 5.2.

In This Appendix

Sample RADIUS Server Configuration File

The following provides an example of the RADIUS server configuration file, **/etc/httpd/user-conf/CSCOec.radius.template**.

```
#------------------------------------------------------------------------
#----------------------------- CISCO CONFIDENTIAL -----------------------
#------------------ Copyright (c) 2009, Cisco Systems, Inc.--------------
#------------------------------------------------------------------------
#------------------------------------------------------------------------
#                 Objectname: %full_filespec: CSCOec.radius.template,4:ascii:Da=1 %
#             Original Author: %created_by: teymoub %
#         Last changed Author: %derived_by: teymoub %
#                     Version: %version: 4 %
#         Last check-out date: %date_created: Tue Jan 26 10:40:18 2016 %
#------------------------------------------------------------------------
#/
#ident "@(#) %full_filespec: CSCOec.radius.template,4:ascii:Da=1 %"
AuthXRadiusAddServer <Radius Server IP>:<Port No> <password>
AuthXRadiusTimeout 3
AuthXRadiusRetries 1
```

D

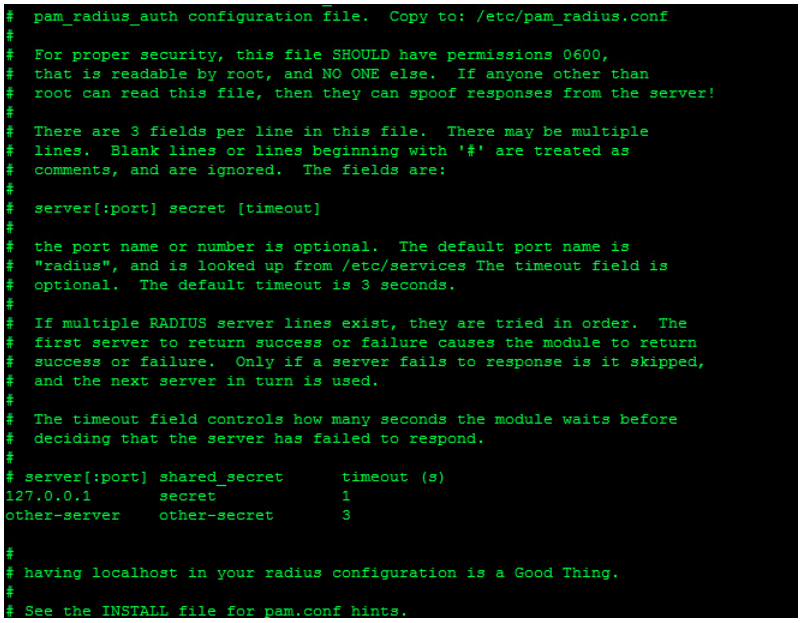
Sample PAM Configuration File

This appendix contains a sample PAM configuration file with RADIUS support. This file, /etc/pam_radius.conf, is included in EC 9.0 and DTACS 5.2.

In This Appendix

PAM Configuration File

The following graphic displays the **/etc/pam_radius.conf** file.



```
#  pam_radius_auth configuration file.  Copy to: /etc/pam_radius.conf
#
#  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)
127.0.0.1       secret             1
other-server    other-secret       3

#
# having localhost in your radius configuration is a Good Thing.
#
# See the INSTALL file for pam.conf hints.
```

E

Sample LDAP Configuration File

This appendix contains a sample sudoers LDAP configuration file. This file, /etc/sudo-ldap.conf, is included with EC 9.0 and DTACS 5.2.

In This Appendix

LDAP Configuration File

The following graphic displays the **/etc/sudo-ldap.conf** file.

```
##  ates an opportunity for man-in-the-middle attacks since the
##  server's identity will not be authenticated.  If possible, the CA's
##  certificate should be installed locally so it can be verified.
##  This option is not supported by the Tivoli Directory Server LDAP
##  libraries.
#tls_checkpeer yes

##
## URI ldap[s]://[hostname[:port]] ...
##  Specifies a whitespace-delimited list of one or more
##  URIs describing the LDAP server(s) to connect to.
##
#uri ldap://ldapserver

##
## SUDOERS_BASE base
##  The base DN to use when performing sudo LDAP queries.
##  Multiple SUDOERS_BASE lines may be specified, in which
##  case they are queried in the order specified.
##
#sudoers_base ou=SUDOers,dc=example,dc=com

##
## BIND_TIMELIMIT seconds
##  The BIND_TIMELIMIT parameter specifies the amount of
##  time to wait while trying to connect to an LDAP server.
##
#bind_timelimit 30

##
## TIMELIMIT seconds
##  The TIMELIMIT parameter specifies the amount of time
##  to wait for a response to an LDAP query.
##
#timelimit 30

##
## SUDOERS_DEBUG debug_level
##  This sets the debug level for sudo LDAP queries. Debugging
##  information is printed to the standard error. A value of 1
##  results in a moderate amount of debugging information.
##  A value of 2 shows the results of the matches themselves.
##
#sudoers_debug 1
```

Index

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

May 2019