Integrating Novell eDirectory with FreeRADIUS

forge.novell.com

ADMINISTRATION GUIDE

February 14, 2005

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.

www.novell.com

Integrating Novell eDirectory with FreeRADIUS Administration Guide
February 14, 2005

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

Novell is a registered trademark of Novell, Inc. in the United States and other countries.
SUSE is a registered trademark of SUSE AG, a Novell business.
eDirectory is a trademark of Novell, Inc.
NMAS is a trademark of Novell.Inc.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

About This Guide

This guide describes how to integrate Novell® eDirectory™ with FreeRADIUS and configure eDirectory users for RADIUS authentication. This guide is intended for eDirectory or RADIUS administrators and is divided into the following chapters:

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX* or Linux*, should use forward slashes as required by your software.

User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Integrating Novell eDirectory with FreeRADIUS Administration Guide*, see the Novell Forge site (http://forge.novell.com/modules/xfmod/docman/?group_id=1623).

Additional Documentation

For documentation on getting started with the integration of eDirectory with FreeRADIUS, refer to the *Integrating Novell eDirectory with FreeRADIUS Quick Start Guide* on the Novell Documentation site (http://www.novell.com/documentation/edir_radius/index.html).

1 Overview

You can integrate Novell® eDirectory™ 8.7.1 or later with FreeRADIUS 1.0.2 onwards to allow wireless authentication for eDirectory users.

If you are new to FreeRADIUS, refer to the FreeRADIUS site (http://www.freeradius.org) for more information.

For more information on eDirectory, refer to the *Novell eDirectory 8.7.1 Administration Guide* (http://www.novell.com/documentation/edir871/index.html)

By integrating eDirectory with FreeRADIUS, you can do the following:

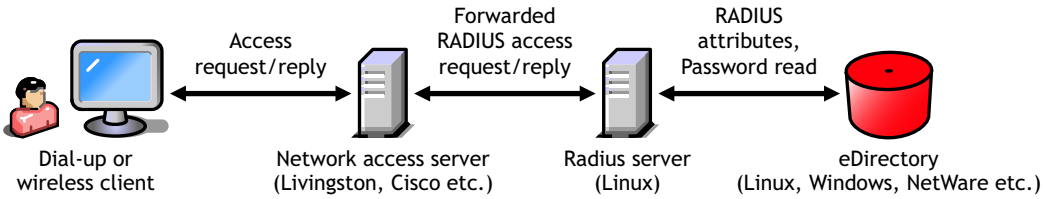
- Use universal password for RADIUS authentication

  Universal password provides single login and authentication for eDirectory users. Therefore, the users need not have a separate password for RADIUS and eDirectory authentication.

- Enforce eDirectory account policies for users

  The existing eDirectory policies on the user accounts can still be applied even after integrating with RADIUS. Also, you can make use of the intruder lockout facility of eDirectory by logging the failed logins into eDirectory.

Figure 1 Wireless Authentication to FreeRADIUS integrated eDirectory



FreeRADIUS and eDirectory can be on two different machines. For example, you can have an eDirectory LDAP server with NMAS running on Netware, but run FreeRADIUS on Linux without eDirectory on it.

eDirectory users can use any of the following protocols for RADIUS authentication:

- CHAP
- EAP-MSCHAP v1 and v2
- EAP-TLS
- LEAP
- MS-CHAP v1 and v2
- PEAP

For a complete list of protocols and information on them, refer to the IETF web site (http://ietf.org/rfc).

IMPORTANT: We recommend that you use SHA-1 or SHA-2 based algorithms and not MD5-based authentication protocols for better security.

To integrate eDirectory with FreeRADIUS, you need to

- Install and configure FreeRADIUS server.
- Enable RADIUS authentication for eDirectory users by configuring them using the iManager plug-in for RADIUS.

The information on the above topics are covered in the subsequent chapters.

2 Installing FreeRADIUS

This chapter explains how to install FreeRADIUS.

Supported Platforms

The eDirectory integration with FreeRADIUS is supported on the following Linux platforms:

- Red Hat* 8.0
- Red Hat* 9.0
- SLES 8
- SLES 9

Prerequisites for Installing FreeRADIUS

- ❑ Linux: Red Hat* 8.0, Red Hat* 9.0, SLES 8 or SLES 9 installed.
  - OpenLDAP libraries: Refer to the OpenLDAP site (http://www.openldap.org/) for more information.
  - OpenSSL libraries: Refer to the OpenSSL site (http://www.openssl.org/) for more information.
- ❑ On SLES: You need to install the following pakages before you install the RPMs. For more information on installing RPMs, refer to “Installing FreeRADIUS on SLES” on page 8.
  - cyrus-sasl-devel
  - db-devel
  - heimdal-devel
  - heimdal-lib
  - libiodbc
  - libiodbc-devel
  - mysql-devel
  - mysql-shared
  - openldap2
  - openldap2-client
  - openldap2-devel
  - openssl
  - openssl-devel

- postgresql
- postgresql-devel
- postgresql-libs
- python
- python-devel

Installing FreeRADIUS on Red Hat

1. Download the source code of FreeRADIUS version 1.0.2 or later.

   Currently, the FreeRADIUS site does not offer precompiled binaries. You need to download the latest source code from FreeRADIUS Web site (http://www.freeradius.org./getting.html).

2. Uncompress and untar the tar file.

   ```
   tar -xvzf downloaded_compressed_tar_file
   ```

   For example:

   ```
   tar -xvzf freeradius-1.0.2.tar.gz
   ```

   The freeradius-1.0.2 directory is created in the current directory.

3. Go to freeradius-1.0.2 directory.

4. Enter the following command:

   ```
   ./configure --with-edir
   ```

5. Enter the following command to compile the source code:

   ```
   make
   ```

6. Enter the following command in to install the binaries:

   ```
   make install
   ```

NOTE: For more information on the above commands, refer to FreeRADIUS Install (http://www.freeradius.org/radiusd/INSTALL).

Installing FreeRADIUS on SLES

To install eDirectory integrated FreeRADIUS on SLES 8 and SLES 9 platforms, you need to install and download the RPMs from the Novell Forge site (http://forge.novell.com/modules/xfcontent/downloads.php/edirfreeradius).

- Installing FreeRADIUS on SLES 8
- Installing FreeRADIUS on SLES 9

  IMPORTANT: You need to set up a Novell Login account to access Forge, at this site (ttps://secure-www.novell.com/selfreg/jsp/createAccount.jsp?target=http%3A//www.novell.com/nps/).

Installing FreeRADIUS on SLES 8

To install eDirectory integrated FreeRADIUS on SLES 8 platform, you need to download the following RPMs:

- freeradius-1.0.2-0.i386.rpm

- freeradius-devel-1.0.2-0.i386.rpm

Installing FreeRADIUS on SLES 9

To install eDirectory integrated FreeRADIUS on SLES 9 platform, you need to download the following RPMs:

- freeradius-1.0.2-0.i586.rpm
- freeradius-devel-1.0.2-0.i586.rpm

What's Next?

After downloading and compiling FreeRADIUS, you need to configure the FreeRADIUS server and eDirectory users. For more information, refer to Chapter 3, "Configuring the FreeRADIUS Server to Integrate with eDirectory," on page 11 and Chapter 4, "Configuring eDirectory Users for RADIUS Authentication Using iManager Plug-in," on page 17.

3 Configuring the FreeRADIUS Server to Integrate with eDirectory

This chapter helps you configure the FreeRADIUS server to integrate with Novell® eDirectory™ and discusses the following information:

Prerequisites for Configuring the FreeRADIUS Server

- ❑ Linux: Red Hat 8.0, Red Hat 9.0, SLES 8 or SLES 9 installed.
- ❑ Download and install the following:
  - FreeRADIUS 1.0.2: Install FreeRADIUS 1.0.2. For installation instructions, refer to Chapter 2, "Installing FreeRADIUS," on page 7.
  - Novell eDirectory 8.7.1 or later: For installation instructions, refer to the *Novell eDirectory 8.7.1 Administration Guide* (http://www.novell.com/documentation/edir871/edir871/data/a2uci7d.html).

    After installing eDirectory, you need to configure it using iManager. Refer to "Configuring eDirectory Using iManager" on page 11 for more information.

    You also need to extract the self-signed certificate of the Certificate Authority (CA). For more information, refer to "Extracting the Self-Signed Certificate of the Certificate Authority" on page 12.
  - Novell iManager 2.0.*x*: For installation instructions, refer to the *Novell iManager 2.0.x Administration Guide* (http://www.novell.com/documentation/imanager20/imanager20/data/alw39eb.html#alw39eb).

    You need to download the RADIUS iManager plug-in from the Novell Forge site (http://forge.novell.com/modules/xfcontent/file.php/edirfreeradius/radius_npm.tar.gz).
- ❑ Security considerations: Ensure that you meet the security considerations as discussed in Chapter 5, "Security Considerations," on page 23.

Configuring eDirectory Using iManager

You need to configure the following in eDirectory using iManager:

- Universal password
- RADIUS administrator object in eDirectory

- Administration rights for the RADIUS administrator
- Administration rights to retrieve password

Enabling Universal Password for eDirectory Users

Ensure that you enable universal password for the users in eDirectory. After enabling, you need to set the universal password either manually or by logging in. For more information, refer to the *Novell Modular Authentication Services 2.3.x Administration Guide* (http://www.novell.com/documentation/nmas23/admin/data/allq21t.html).

Creating the RADIUS Administrator Object

A User object is same as an Administrator object.

For information on creating an RADIUS Administrator object in eDirectory, refer to the Creating an Object section in the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a4jgpgc.html#a3olp4k).

You need to mention the FDN of the RADIUS Administrator object while modifying the attributes in the LDAP module.

Granting Administration Rights for the RADIUS Administrator

Grant the RADIUS administrator the write right over the ACL attribute of the user object whose universal password has to be read. By granting this right, the RADIUS administrator will gain the administrative rights over that user object.

The eDirectory administrator can also be the RADIUS administrator. For more information on eDirectory rights, refer to the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/fbachifb.html#fbachifb).

Granting Rights to RADIUS Administrator to Retrieve Password

By default, the administrator do not have the right to read universal password. The password policy has to be modified to explicitly give the RADIUS Administrator right to read Universal Password. To do this, complete the following steps:

1. In iManager, click the Roles and Tasks button 
2. Click eDirectory Administration >Modify Object.
   - **2a** Select Universal Password On from password policies in the Security Container.
   - **2b** Click OK.
3. Click General tab.
   - **3a** Edit the nspmConfigurationOptions attribute and add 32 to the value already shown.

Extracting the Self-Signed Certificate of the Certificate Authority

You need to extract the self-signed certificate of the Certificate Authority in base 64 format. For information on extracting the certificate, refer to the *Novell Certificate Server 2.7.x Administration Guide* (http://www.novell.com/documentation/crt27/index.html?page=/documentation/crt27/crtadmin/data/a2ebopb.html#a2ebopd).

You need to mention the extracted path and the certificate filename while modifying the attributes in the LDAP module of the radiusd.conf configuration file. The two configuration parameters are:

- tls_cacertfile: Specifies the full path of a certificate file in the UNIX file system.
- tls_cacertdir: Specifies the full path of a directory containing certificates.

  NOTE: If either of the parameter is specified, then the RADIUS server administrator has to make sure that the (UNIX) user having RADIUS server rights also has right to read the certificate files.

Modifying the LDAP Module

You need to modify the following attributes in the ldap module in the *install_path*/etc/raddb/radiusd.conf file:

- server = "*hostname (not IP address)*"
- identity = "*FDN of the RADIUS Server object in eDirectory*"
- password = *password of the RADIUS Server object in eDirectory*
- basedn = "*The DN of the container that stores the RADIUS users and profile objects*"

  NOTE: The RADIUS server looks for objects in the subtree under this basedn. If you want multiple search bases, you can create multiple LDAP modules. For example, refer to "Example for Creating Multiple Instances of LDAP Module" on page 15.
- filter = "(cn=%{Stripped-User-Name:-%{User-Name}})"
- start_tls = yes
- tls_cacertfile = *Path of the self-signed certificate of the CA who has issued certificate to the eDirectory server*
- tls_require_cert = "demand"
- dictionary_mapping = ${raddbdir}/ldap.attrmap
- password_attribute=nspmPassword

  By setting the value of this attribute to nspmPassword, you configure FreeRADIUS to enable users to use their universal passwords for RADIUS authentication.

  NOTE: nspmPassword is not case sensitive. For example, you can use either nspmPassword or nspmpassword.

  IMPORTANT: Ensure that you have enabled universal password for eDirectory. For more information, refer to "Prerequisites for Configuring the FreeRADIUS Server" on page 11.
- edir_account_policy_check=yes

  eDirectory account policy check is enabled by default. By setting the value of this attribute to no, you disable the eDirectory account policy check and intruder detection in eDirectory.

  NOTE: If a user has grace logins, they are used up when the user authenticates through RADIUS. This might lock the user's account without warning.

  The advantages of eDirectory account policy check are:

  - The existing eDirectory policies on the user accounts can still be applied after integrating with RADIUS.
  - eDirectory intruder detection is enabled.

  IMPORTANT: If you find the performance of the RADIUS servers low, you can disable the eDirectory account policy check at the cost of security risks.

For more detailed explanation of the above attributes, refer to the *install_path*/doc/rlm_ldap file.

After modifying the LDAP module, you need to enable the module in the authorization section and specify ‘ldap’ in the post-authentication section of the radiusd.conf file. Refer to “Enabling the LDAP Module in the Authorization Section” on page 15 and “Specifying the LDAP Module in the Post-Authentication Section” on page 15 for more information.

Example of the Modified LDAP Module

```
ldap {

server = "eDir.test.com"
identity = "cn=admin,o=org"
password = secret
basedn = "o=org"
filter = "(cn=%{Stripped-User-Name:-%{User-Name}})"
base_filter = "(objectclass=radiusprofile)"
# set this to 'yes' to use TLS encrypted connections
# to the LDAP database by using the StartTLS extended
# operation.
# The StartTLS operation is supposed to be used with normal
# ldap connections instead of using ldaps (port 689) connections
start_tls = yes
tls_cacertfile= /opt/etc/raddb/certs/cacert.b64
# tls_cacertdir= /path/to/ca/dir/
# tls_certfile= /path/to/radius.crt
# tls_keyfile= /path/to/radius.key
# tls_randfile= /path/to/rnd
tls_require_cert= "demand"
# default_profile = "cn=radprofile,ou=dialup,o=My Org,c=UA"
# profile_attribute = "radiusProfileDn"
access_attr = "dialupAccess"
# Mapping of RADIUS dictionary attributes to LDAP
# directory attributes.
dictionary_mapping = ${raddbdir}/ldap.attrmap
ldap_connections_number = 5
#
# NOTICE: The password_header directive is NOT case insensitive
#
# password_header = "{clear}"
#
#  The server can usually figure this out on its own, and pull
#  the correct User-Password or NT-Password from the database.
#
#  Note that NT-Passwords MUST be stored as a 32-digit hex
#  string, and MUST start off with "0x", such as:
#
#0x000102030405060708090a0b0c0d0e0f
#
#  Without the leading "0x", NT-Passwords will not work.
#  This goes for NT-Passwords stored in SQL, too.
#
password_attribute = nspmPassword
# groupname_attribute = cn
# groupmembership_filter = "(|(&(objectClass=GroupOfNames)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{Ldap-UserDn})))"
# groupmembership_attribute = radiusGroupName
timeout = 4
timelimit = 3
net_timeout = 1
# compare_check_items = yes
```

```
# do_xlat = yes
# access_attr_used_for_allow = yes
edir_account_policy_check = yes
}
```

Example for Creating Multiple Instances of LDAP Module

If you want multiple search bases, you can create multiple LDAP modules, by using the following syntax in the module section of the radiusd.conf.

```
modules {
        ..........
        ..........

        ldap ldap1 {
         attribute = value
         attribute = value
         ..............
         ..............
        }
        ldap ldap2 {
         attribute = value
         attribute = value
         ..............
         ..............
        }
        ldap ldap3 {
         attribute = value
         attribute = value
         ..............
         ..............
        }
}
```

You can use the configured modules in authorize, authenticate and post-authenticate sections by specifying the module name and instance name. For example:

```
authorize{
        .....
        .....
        ldap ldap1
        ldap ldap2
        .....
        .....
}
```

Enabling the LDAP Module in the Authorization Section

To enable the LDAP module, you need to comment out the LDAP module in the authorize section of the *install_path*/etc/raddb/radiusd.conf file. For information on setting up LDAP with FreeRADIUS, refer to the /doc/ldap_howto.txt file.

Specifying the LDAP Module in the Post-Authentication Section

You need to add ‘ldap’ in the post-authentication section of the *install_path*/etc/raddb/radiusd.conf file as shown below:

```
post-auth {
         #  Get an address from the IP Pool.

ldap
#       main_pool
         #
         #  If you want to have a log of authentication replies,
         #  un-comment the following line, and the 'detail reply_log'
         #  section, above.
#       reply_log
         #
         #  After authenticating the user, do another SQL qeury.
         #
         #  See "Authentication Logging Queries" in sql.conf
#       sql
         #
         #  Access-Reject packets are sent through the REJECT sub-section
         #  of the post-auth section.
         #
       Post-Auth-Type REJECT {
             ldap
            }
```

4 Configuring eDirectory Users for RADIUS Authentication Using iManager Plug-in

Using the iManager plug-in for RADIUS, you can configure Novell® eDirectory™ users to authenticate through FreeRADIUS. You can convert the existing eDirectory users to RADIUS users by adding the RADIUS attributes. If you want to add new FreeRADIUS users, you need to first add a corresponding eDirectory user and then add RADIUS attributes to the user objects.

This chapter provides the following information:

Prerequisites to Configure eDirectory Users for RADIUS Authentication

- ❑ Novell iManager plug-in for RADIUS: Download the iManager plug-in from the Novell Forge site (http://forge.novell.com/modules/xfcontent/file.php/edirfreeradius/radius_npm.tar.gz).

  For installation instructions, refer to the *Novell iManager 2.0.x Administration Guide* (http://www.novell.com/documentation/imanager20/imanager20/data/alw39eb.html#alw39eb).

  You need to configure iManager plug-in with SSL/TLS connection to eDirectory for RADIUS to work with iManager plug-in. For more information, refer to the Configuring iManager Plug-in for RADIUS section below.
- ❑ Extension of eDirectory schema: You need to extend the eDirectory schema with the FreeRADIUS schema. For more information, refer to the Extending the eDirectory Schema for RADIUS section below.
- ❑ eDirectory User: To add new eDirectory User objects, refer to the *Novell eDirectory 8.7.3 Administration Guide* (http://www.novell.com/documentation/edir873/edir873/data/a4jgpgc.html#a3olp4k).

Configuring iManager Plug-in for RADIUS

You need to configure iManager plug-in with SSL/TLS connection to eDirectory for RADIUS to work with iManager plug-in. You can have RADIUS iManager plug-in and iManager on same machine or on two different machines.

- If you configure RADIUS iManager plug-in and iManager on same machine, then by default, iManager is configured for SSL/TLS connection to eDirectory.

- If you want to configure RADIUS iManager plug-in and iManager on different machines, you need to configure iManager for SSL/TLS connection to eDirectory manually. For more information on Configuring iManager for SSL/TLS connection to eDirectory, refer to *iManager 2.0 Administration Guide* (http://www.novell.com/documentation/lg/imanager20/index.html?page=/documentation/lg/imanager20/imanager20/data/am4ajce.html#bow4dv4).

Extending the eDirectory Schema for RADIUS

There are three possible scenarios of extending the eDirectory schema for RADIUS.

Scenario 1

If mapping already exists between RADIUS:Profile to rADIUSProfile, then follow the below steps:

1. In iManager, click the Roles and Tasks button  .
2. Click LDAP > LDAP Overview
   - 2a. Select View LDAP Groups.
   - 2b. Select Class Map from the drop down list.
   - 2c. Select the RADIUS:Profile to rADIUSProfile mapping.
   - 2d. Click Edit.
   - 2e. Change the primary LDAP class name to anything other than rADIUSProfile, for example, novellradiusprofile.
   - 2f. Click Apply.
3. Refresh LDAP server.
4. Click RADIUS > Extend schema for RADIUS.
   - 4a. Click OK.

   Help is available on the screens.

Scenario 2:

If mapping does not exist between RADIUS:Profile to rADIUSProfile, then follow the below steps:

1. In iManager, click the Roles and Tasks button  .
2. Click LDAP > LDAP Overview
   - 2a. Select View LDAP Groups.
   - 2b. Select Class Map from the drop down list.
   - 2c. Click Add mapping button.
   - 2d. In the eDirectory class drop down list, select RADIUS:Profile.
   - 2e. Change the primary LDAP class name to anything other than rADIUSProfile, for example, novellradiusprofile.
   - 2f. Click OK.
3. Refresh LDAP server.
4. Click RADIUS > Extend schema for RADIUS.

4a Click OK.

Help is available on the screens.

Scenario 3:

If mapping already exists between RADIUS:Profile to any name other than radiusprofile, then follow the below steps:

1. In iManager, click the Roles and Tasks button  .
2. Click LDAP > LDAP Overview
   - **2a** Select View LDAP Groups.
   - **2b** Select Class Map from the drop down list.
   - **2c** Select the RADIUS:Profile to any name other than rADIUSProfile mapping.
3. Refresh LDAP server.
4. Click RADIUS > Extend schema for RADIUS.
   - **4a** Click OK.

   Help is available on the screens.

   TIP: You can extend the schema using ldif files, in case you are not able to extend through the iManager plug-in. Refer "Extending the eDirectory Schema Using LDIF Files" on page 31 for more information.

Adding RADIUS Attributes to eDirectory Users

You can add the RADIUS attributes to the following:

- Users
- Profiles that can be associated with the users.

You can also add the RADIUS attributes when you are modifying users or the eDirectory objects.

Profile Objects

You can create Profile objects in eDirectory to store a set of RADIUS attributes. Profile objects help in associating a User object collectively with the RADIUS attributes. For example, a set of RADIUS attributes, Auth-Type, NAS-IP-Address, and Framed-IPX-Network is to be assigned to users Jack, Tom, and Jane. You can create a Profile object PR1 containing these RADIUS attributes and then assign PR1 to all the three users.

Managing RADIUS Objects

You can manage RADIUS objects using the iManager plug-in for RADIUS management. Ensure that you meet all the prerequisites before proceeding further.

This section provides information on

- "Managing RADIUS Users" on page 20
- "Managing RADIUS Profiles" on page 20

Managing RADIUS Users

This section provides information on

- Creating RADIUS Users (page 20)
- Modifying RADIUS Users (page 20)
- Deleting RADIUS Users (page 20)

Creating RADIUS Users

1. In iManager, click the Roles and Tasks button  .
2. Click RADIUS > Create RADIUS User.
3. Specify the User object to create either by typing in the object name or using the object selector.
4. (Optional) Specify the Profile object you want to associate with the user by typing in its name or using the object selector.
5. Click OK.

Modifying RADIUS Users

1. In iManager, click the Roles and Tasks button  .
2. Click RADIUS > Modify RADIUS User.
3. Specify the User object to modify either by typing in the object name or using the object selector.
4. (Optional) Specify or modify the RADIUS attributes for the User object.
5. Click OK.

Deleting RADIUS Users

1. In iManager, click the Roles and Tasks button  .
2. Click RADIUS > Delete RADIUS User.
3. Specify the User object to delete either by typing in the object name or using the object selector.
4. Click OK.

Managing RADIUS Profiles

This section provides information on

- Creating RADIUS Profiles (page 20)
- Modifying RADIUS Profiles (page 21)
- Deleting RADIUS Profiles (page 21)

Creating RADIUS Profiles

1. In iManager, click the Roles and Tasks button  .
2. Click RADIUS > Create RADIUS Profile.

3 Specify the context for the Profile object to create either by typing in the object name or using the object selector.

4 Click OK.

Modifying RADIUS Profiles

1 In iManager, click the Roles and Tasks button  .

2 Click RADIUS > Modify RADIUS Profile.

3 Specify the RADIUS Profile object to modify either by typing in the object name or using the object selector.

4 (Optional) Specify or modify the RADIUS attributes for the Profile object.

5 Click OK.

Deleting RADIUS Profiles

1 In iManager, click the Roles and Tasks button  .

2 Click RADIUS > Delete RADIUS Profile.

3 Specify the RADIUS Profile object to delete either by typing in the object name or using the object selector.

4 Click OK.

5 Security Considerations

Integration of Novell® eDirectory™ with FreeRADIUS requires that the passwords be read in clear text. So, deploying a RADIUS server affects the security of eDirectory and user passwords. Ensure that the following security considerations are met before integrating eDirectory with FreeRADIUS:

Protecting the RADIUS Server

In order to support several RADIUS protocols, the RADIUS server must have access to users' eDirectory passwords.

Therefore, you need to

- Take precautions to protect the RADIUS server from any attack or subversion. Have a strong eDirectory password for the RADIUS server.
- Always protect the RADIUS server with local and network-edge firewalls, so that it is not directly accessible to the Internet.
- Avoid the exploitation of the vulnerabilities in the software running on the host with root privileges by restricting host login.
- Apply the latest security patches to the networked services running on the host and strictly control access to these services by using a good firewall configuration.
- Regularly monitor and review the log files for any evidence of attack. You need to enable the logging of critical information such as username and passwords in case of authentication or password failures.

  To enable logging of usernames, authentication failures, and passwords, set the value of the following parameters to yes in the *install_path*/etc/raddb/radiusd.conf file:

  - **`log_stripped_names=yes`**

    Logs the User-Name attribute as it was found in the request.

  - **`log_auth=yes`**

    Logs authentication requests to the log file.

- **log_auth_badpass=yes**

  log_auth_goodpass=yes

  Log passwords with the authentication requests.

  Enabling log_auth_badpass logs password when it is rejected and enabling log_auth_goodpass logs password when the password is correct

NOTE: Protect the log file using file system rights. For more information, refer to "Protecting the Configuration Files" on page 24.

Risks of Enabling PAP

RADIUS supports protocols that are generally recognized to be unsafe to use in a security-sensitive area, such as, PAP.

Be aware of the serious security risks that the use of PAP can present to your user and the systems to which they connect. We strongly recommend that you disable PAP.

Protecting the Configuration Files

Because the radiusd.conf, proxy.conf, and clients.conf configuration files contain passwords in plain text, they must not be readable by anyone other than the FreeRADIUS administrator ('root'). These are protected by file system rights.

You need to protect the following configuration files in /usr/local/etc/raddb/

- clients
- clients.conf
- naspasswd
- proxy.conf
- radiusd.conf
- realms
- snmp.conf
- users

You need to give read/write rights to the above files to 'root' users only. To give these rights, do the following:

1. Log in as 'root'.
2. Execute the following command for each of the files mentioned above:

   chmod go-rwx *filename*

Defining Roles and Granting Rights to Administrators

There are three major roles in eDirectory that you need to clearly define:

- **eDirectory administrator:** Complete access rights to the tree.
- **RADIUS administrator:** Complete access only to the RADIUS container and users.

The eDirectory administrator can grant the RADIUS administrator rights to read the universal password of all users under a container C by granting the administrator inheritable write rights to the ACL attribute of C.

After integrating eDirectory with FreeRADIUS, the RADIUS administrator needs to be given rights to read the login details of the RADIUS users. So, the RADIUS administrator has to be trusted with such rights.

- **RADIUS and eDirectory users:** Access rights as defined by the eDirectory administrator to all of their own attributes. Access to RADIUS attributes is not required.

Risks of Enabling Universal Password

The risks of enabling universal password are documented by NMAS™. Refer to the Deploying Universal Password section in the *Novell Modular Authentication Service 2.3.x Administration Guide* (http://www.novell.com/documentation/nmas23/admin/data/allq21t.html).

Risks of Disabling eDirectory Account Policy Checking

With eDirectory integration, the RADIUS server can read the universal password from eDirectory. Therefore, if the account of the user is disabled or closed in eDirectory, the RADIUS server can still read the universal password and authorize the user. Also, the intruder detection facility of eDirectory will be bypassed.

To avoid the above risks, we strongly recommend that you enable the eDirectory account policy check so that the authorization fails if either the RADIUS server or the eDirectory server does not authorize the user.

Figure 2 eDirectory Account Policy Check Disabled

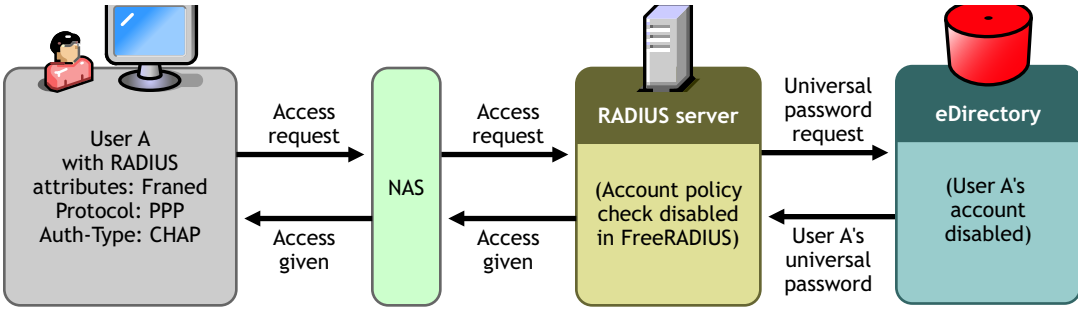
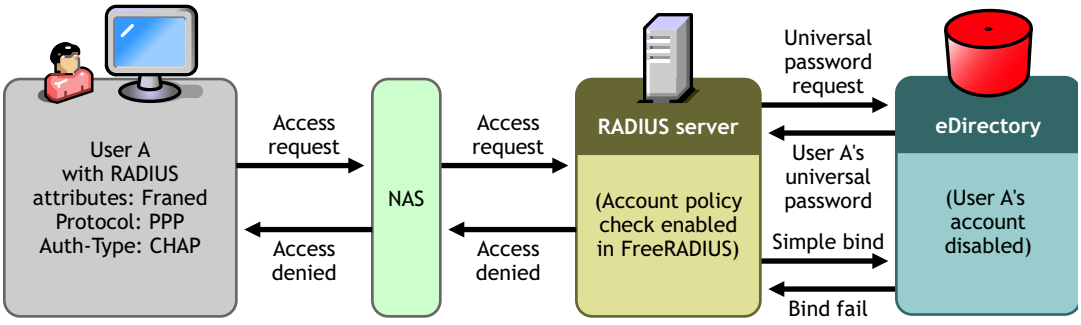


Figure 3 eDirectory Account Policy Check Enabled



6 Novell Technical Support for eDirectory Integrated FreeRADIUS

This chapter provides information on reporting bugs through bugzilla. Novell Technical Support (NTS) will be available to customers only if they use these RPMs and integrate FreeRADIUS with eDirectory. NTS will be unable to support the customers who download and use the FreeRADIUS source code directly.

Reporting Bugs

You can report eDirectory Integrated FreeRADIUS related bugs through bugzilla.

Check (http://bugs.freeradius.org/query.cgi) to find out if the bug you intend to file is already filed by someone else.

To file a new bug:

1. Create a new account at http://bugs.freeradius.org/createaccount.cgi (http://bugs.freeradius.org/createaccount.cgi).

   A password is sent to you from this site.

2. Log in with the password.

3. Click New to file new bugs after a successful login.

   You need to give information such as version, component, OS, and severity. The maintainer or the component owner is notified after you save your changes.

For information on writing bugs, refer to the bug writing guidelines (http://www.freedos.org/bugs/bugzilla/bugwritinghelp.html).

7 Troubleshooting

This chapter provides information on error codes and solutions for commonly faced problems you might encounter while using Novell® eDirectory™ integrated with FreeRADIUS.

Error Codes

-603 fffffda5 NO SUCH ATTRIBUTE

Source

eDirectory.

Explanation

The requested attribute could not be found. In eDirectory or NDS, if an attribute does not contain a value, then the attribute does not exist for the specific object.

The request might be

- Read an eDirectory or NDS schema attribute definition
- Remove an eDirectory or NDS schema attribute definition
- Update an eDirectory or NDS schema attribute definition

WARNING: Applying all solutions mentioned in this topic could make the problem worse if the actual cause of the problem is not known. Before following a course of action, make sure that you understand the cause of the error and the consequences for the actions suggested.

Possible Cause

The definition for the specified schema attribute does not exist on the server replying to the request.

Action

Look at what type of object the error is occurring on.

If the object is a simple object, such as a single user that is not a critical user, delete and recreate the problem object.

If it is the source server that is missing the attribute, then use DSREPAIR to perform a Receive All Updates from the Master to This Replica operation on the source server.

WARNING: The Receive All Updates from the Master to This Replica operation in DSREPAIR removes the replica and then places the replica back on the server. This operation cannot be performed on the server that holds the master replica. If this operation needs to be performed on the server holding the master replica, reassign the master replica to another replica ring using DSREPAIR before starting this operation.

Possible Cause

The specified object does not have the specified attribute.

Action

Perform a Send All Objects to Every Replica in the Ring operation from DSREPAIR.

WARNING: When a Send All Objects to Every Replica in the Ring operation is performed on large partitions or partitions with numerous replicas, considerable traffic on the network can result.

Possible Cause

The requester does not have sufficient rights to the attributes for the specified object.

Action

If appropriate, assign the requester the necessary rights.

-1659 fffff985 E ACCESS NOT ALLOWED

Source

Novell® Modular Authentication Services (NMAS™).

Explanation

You do not have sufficient rights to read the universal passwords of the users.

Possible Cause

The "Allow password retrieval by admin" option is not enabled in the password policy.

Action

Enable the "Allow password retrieval by admin" option in the password policy.

-1697 Oxfffff95f NMAS_E_INVALID_SPM_REQUEST

Source

Novell® Modular Authentication Services (NMAS™).

Explanation

The requested password operation is invalid.

Possible Cause

Universal password is not enabled for the container in which the object exists.

Action

Enable Universal Password for the container containing the objects.

Solutions for Commonly Faced Problems

This section lists some scenarios for extending the eDirectory schema.

- **Scenario 1:** If the object class by FreeRADIUS radiusprofile is already existing in eDirectory.

  Solution: You need not extend the schema.

- **Scenario 2:** If the object class by FreeRADIUS radiusprofile is visible in iManager.

  Solution: You can edit it through iManager.

- **Scenario 3:** If the object class by FreeRADIUS radiusprofile is not visible in iManager.
  - **Scenario 1:** If schema mapping is absent.

    Solution: You need to map the schema through iManager.

  - **Scenario 2:** If schema mapping is present but not visible.

    Solution: You need to extend the schema by using LDIF files. Refer "Extending the eDirectory Schema Using LDIF Files" on page 31 for more information.

Extending the eDirectory Schema Using LDIF Files

You can extend the eDirectory schema using ldif files, in case you are not able to extend through the iManager plug-in. The iManager plug-in package contains the following ldif files which can be used to extend the schema:

- addclassmap.ldif
- RADIUS-LDAPv3.ldif

The addclassmap.ldif file is used to change the mapping, as eDirectory already has the rADIUSProfile object class which is a part of the Novell RADIUS server. The objectclass required by FreeRADIUS is also called radiusprofile and hence the schema extension will not fail unless the mapping is changed.

NOTE: This ldif file should not be used, if schema mapping is already done through iManager. classes.

The RADIUS-LDAPv3.ldif is the LDAPv3 schema for FreeRADIUS.

A RADIUS Attribute Definitions

This section describes the RADIUS attributes and possible values of an attributes in the base schema.

Attribute Name	Description	Values
radiusArapFeatures	Specifies the password information that the NAS should send to the user in an ARAP "feature flags" packet.	
radiusArapSecurity	Specifies an ARAP security module to be used in an access-challenge packet.	
radiusArapZoneAccess	Describes the use of the ARAP zone list for the user.	1=Only allow access to default zone 2=Use zone filter inclusively 4=Use zone filter exclusively
radiusCallbackId	Specifies a name of a place to be called which is interpreted by the NAS.	
radiusCallbackNumber	Specifies a dialing string to be used for callback.	
radiusCalledStationId	Allows the NAS to send in the Access-Request packet the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology.	
radiusCallingStationId	Allows the NAS to send in the access-request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology.	
radiusClass	Contains a multivalued attribute sent by the RADIUS server to the client to be forwarded to the RADIUS accounting server.	
radiusFilterId	Specifies the name of the filter list for the user.	
radiusFramedAppleTalkLink	Contains the AppleTalk network number which should be used for the serial link to the user, which is another AppleTalk router.	

Attribute Name	Description	Values
radiusFramedAppleTalkNetwork	Contains the AppleTalk Network number which the NAS should probe to allocate an AppleTalk node for the user.	
radiusFramedAppleTalkZone	Specifies the AppleTalk Default Zone to be used for this user.	
radiusFramedCompression	Defines a compression protocol to be used for the link.	0=None 1=VJ TCP/IP header compression [10] 2=IPX header compression 3=Stac-LZS compression
radiusFramedIPAddress	Defines an address to be configured for the user.	IP address.
radiusFramedIPNetmask	Defines an IP netmask to be configured for the user.	IP address.
radiusFramedIPXNetwork	Defines an PX Network number to be configured for the user.	
radiusFramedMTU	Specifies the Maximum Transmission Unit to be configured for the user.	
radiusFramedProtocol	Indicates the framing to be used for framed access.	1=PPP 2=SLIP 3=AppleTalk Remote Access Protocol (ARAP) 4=Gandalf proprietary SingleLink/ MultiLink protocol 5=Xylogics proprietary IPX/SLIP 6=X.75 Synchronous
radiusFramedRoute	Contains a multivalued attribute for routing information to be configured for the user on the NAS.	
radiusFramedRouting	Specifies the routing method for the user, when the user is a router to a network.	0=None 1=Send routing packets 2=Listen for routing packets 3=Send and Listen
radiusIdleTimeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.	
radiusLoginIPHost	Decides on the system with which to connect the user.	

Attribute Name	Description	Values
radiusLoginLATGroup	Describes a LAT group codes which the user is authorized to use.	
radiusLoginLATNode	Defines the node with which the user is to be automatically connected by LAT.	
radiusLoginLATPort	Defines the port with which the user is to be connected by LAT.	
radiusLoginLATService	Defines the system with which the user is to be connected by LAT.	
radiusLoginService	Defines the service to use to connect the user to the login host.	0=Telnet 1=Rlogin 2=TCP Clear 3=PortMaster (proprietary) 4=LAT 5= X25-PAD 6= X25-T3POS 8=TCP Clear Quiet (suppresses any NAS-generated connect string)
radiusLoginTCPPort	Specifies the TCP port with which the user is to be connected.	An integer *i (0 < i < 65536).*
radiusPasswordRetry	Specifies the number of authentication attempts a user may be allowed to attempt before being disconnected.	Integer.
radiusPortLimit	Specifies the maximum number of ports to be provided to the user by the NAS.	Integer.
radiusPrompt	Decides whether the NAS should echo the user's response (to a challenge) as it is entered.	0=No Echo 1=Echo

Attribute Name	Description	Values
radiusServiceType	Specifies the type of service the user has requested or the type of service to be provided.	1=Login 2=Framed 3=Callback Login 4=Callback Framed 5=Outbound 6=Administrative 7=NAS Prompt 8=Authenticate Only 9=Callback NAS Prompt 10=Call Check 11=Callback Administrative
radiusSessionTimeout	Specifies the maximum number of seconds of service to be provided to the user before termination of the session or prompt.	Integer.
radiusTerminationAction	Decides on kind of action the NAS should take when the specified service is completed.	0=Default 1=RADIUS-Request
radiusTunnelAssignmentId	Contains a multivalued attribute which is used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned.	

Attribute Name	Description	Values
radiusTunnelMediumType	Contains a multilevel attribute used to indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.	1 IPv4 (IP version 4) 2 IPv6 (IP version 6) 3 NSAP 4 HDLC (8-bit multidrop) 5 BBN 1822 6 802 (includes all 802 media plus Ethernet “canonical format”) 7 E.163 (POTS) 8 E.164 (SMDS, Frame Relay, ATM) 9 F.69 (Telex) 10 X.121 (X.25, Frame Relay) 11 IPX 12 Platelike 13 Decant IV 14 Banyan Vines 15 E.164 with NSAP format subduers
radius Tunnel Password	Contain a password to be used to authenticate to a remote server.	
radius Tunnel Preference	Contains a multilevel attribute which should be included in each set to indicate the relative preference assigned to each tunnel, when more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator.	
radius Tunnel Private Group Id	Contain a multilevel attribute which indicates the group ID for a particular tunneled session.	
radius Tunnel Server Endpoint	Contains a multilevel attribute which indicates the address of the server end of the tunnel.	

Attribute Name	Description	Values
radius Tunnel Type	Contains a multivalued attribute which indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	1 Point-to-Point Tunneling Protocol (PPTP) [1] 2 Layer Two Forwarding (L2F) [2] 3 Layer Two Tunneling Protocol (L2TP) [3] 4 Ascend Tunnel Management Protocol (ATMP) [4] 5 Virtual Tunneling Protocol (VTP) 6 IP Authentication Header in the Tunnel-mode (AH) [5] 7 IP-in-IP Encapsulation (IP-IP) [6] 8 Minimal IP-in-IP Encapsulation (MIN-IP-IP) [7] 9 IP Encapsulating Security Payload in the Tunnel-mode (ESP) [8] 10 Generic Route Encapsulation (GRE) [9] 11 Bay Dial Virtual Services (DVS) 12 IP-in-IP Tunneling [10]
radiusVSA	Contains a multivalued RADIUS vendor specific attributes.	
radiusTunnelClientEndpoint	Contains a multivalued attribute which has the address of the initiator end of the tunnel.	
radiusAuthType	Specifies authentication types like MS-CHAP, NS-MTA-MD5 etc.	
radiusClientIPAddress	Defines the client through which the user requests must be sent.	IP address.
radiusGroupName	Contains a multivalued attribute which is a list of groups the user belongs to.	
radiusHint	Provides a hint for the user.	
radiusHuntgroupName	Contains a multivalued attribute of Huntgroup for the user.	
radiusProfileDn	Specifies the DN of radiusProfile object for this user.	
radiusProxyToRealm	Specifies the FreeRadius (non-protocol) attribute used to forward RADIUS requests.	
radiusReplicateToRealm	Describes a depricated freeRadius attribute.	

Attribute Name	Description	Values
radiusRealm	Describes a FreeRadius (non-protocol) attribute.	
radiusSimultaneousUse	Limits the number of times one user account can login.	
radiusLoginTime	Specifies the FreeRadius (non-protocol) attribute used to define the time span a user may login to the system.	
radiusUserCategory	Specifies the FreeRadius (non-protocol) attribute. Refers to the definition of a group to which the user belongs.	
radiusStripUserName		
dialupAccess	Used for access control.	
radiusExpiration	Specifies the date of expiration of RADIUS account.	
radiusCheckItem	Contains a multivalued attribute which stores the generic radius check-items.	
radiusReplyItem	Contains a multivalued attribute which stores generic radius reply-items.	