APPLICATION NOTE

Centralized User Management using Open Source Protocols: RADIUS and LDAP Deployment

INTRODUCTION

Centralized management of users and authentication information offers great benefit when implementing and managing security policies and compliance requirements. It implements a single system for managing the creation and deletion of users, their roles, and the rules for their authentication (e.g. password rules, 2-factor authentication requirements, etc.).

A centralized system for user management is considered a best practice by industry security standards such as IEC 62443, which has in its Part 4-2:

> Technical security requirements for IACS components - 5.5 CR 1.3 – Account management: “Devices must have the ability to support the administration of all accounts directly or integrated into a centralized system that manages those accounts, in accordance with 62443-3-3”.

This paper will discuss the implementation of such a system, based on widely used open-source components. The example uses the iS5Com RAPTOR as the client device, but this could (and should) be extended to all devices supporting LDAP and/or RADIUS.

LDAP

LDAP stands for Lightweight Directory Access Protocol. This is a lightweight protocol for accessing directory services, which runs over TCP/IP. LDAP is an IETF Standard protocol specified by RFC4510.

LDAP operates using a client-server model. One or more LDAP servers contain the data comprising the directory information tree (DIT). The client connects to servers and issues queries, to which the server responds based on information in the DIT.

In general, a directory service is needed when central management of data, such as user information, is required. LDAP facilitates storing and accessing the data from a central location.

A common use of LDAP is to provide a central store for usernames and their associated password information. Many different applications and services may then connect to this LDAP server to validate users.

Some common examples found throughout the industry include:

- Machine Authentication
- User Authentication
- User/System Group membership
- Asset Tracking
- Telephony Information Store
- User resource management

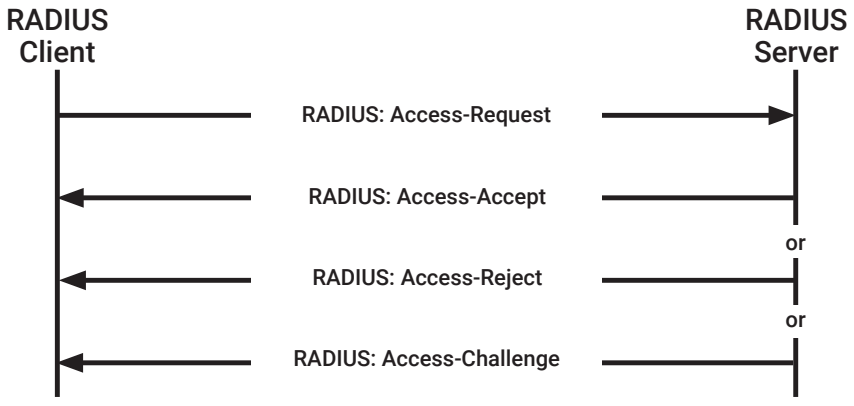
RADIUS

Remote Authentication Dial-In User Service (RADIUS) provides centralized Authentication, Authorization, and Accounting (AAA or Triple-A) management of users who connect to and use a network service. It operates on port 1812.

The RADIUS protocol serves three main functions:

- Authentication of users or devices before allowing them access to a network
- Authorization of those users or devices for specific network services
- Accounting for and tracking of the usage of those services

RADIUS uses a client-server model. A RADIUS client (also called a Network Access Server, or NAS) sends requests to a RADIUS server. The RADIUS server then processes the request and sends back a response.



Why do we need both LDAP and RADIUS?

In an industrial network, a variety of devices need to be connected. Devices such as IEDs, RTUs, SCADA servers, PLCs, network devices (switch, router, firewall) build the automation system for an industrial process.

These devices support either LDAP or RADIUS but rarely both. For example, most industrial network devices support only RADIUS.

Although LDAP and RADIUS are both protocols used for authentication and authorization, they have been created for different use cases. LDAP was created primarily for the authentication of systems and applications. RADIUS, on the other hand, was created to authenticate dial-up users via modems. They do have significant differences in how they perform authentication and the functionalities supported by each protocol.

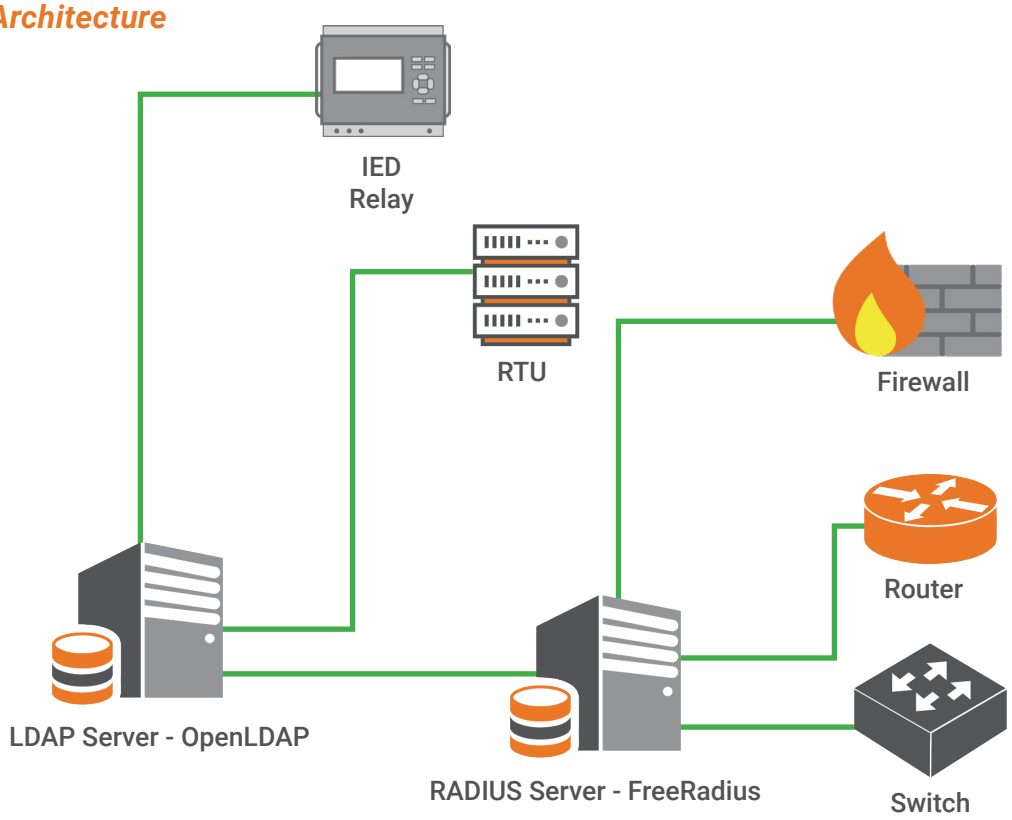
LDAP is used to implement a directory service. A directory service is like a database where all user attributes will be stored. User attributes can be user IDs and password, privilege level, telephone number, email, etc.

Using a directory service will allow users to use one user ID and password to access all the devices on the network. User access management is facilitated by having all the access credentials stored in one location rather than having access credentials spread over the systems within the network.

RADIUS will be used for two major reasons apart from the fact that some devices support only RADIUS.

1. RADIUS supports authentication and authorization like LDAP. In addition, RADIUS also supports accounting. Accounting is the recording of resources a user consumes during the time they are on the network. This can include system time used, the amount of data sent, and the quantity of data received by the user during a session.
2. RADIUS also supports multi-factor authentication. LDAP does not.

Figure 1.0 - Architecture



Both the RADIUS and LDAP servers can run on the same machine since they use different layer four ports. Devices that support LDAP will authenticate directly to the LDAP server.
The devices that support only RADIUS or require accounting or multi-factor authentication service will need to authenticate to the RADIUS server. The RADIUS server will communicate with the LDAP server to verify the access credential and the privilege level. Once the LDAP server performs verification, the RADIUS server will allow access to the user and assign it to the appropriate role.
If multi-factor authentication is needed, the RADIUS server will send a challenge message to the user after being authenticated on the LDAP server. The RADIUS server will proxy the authentication to a one-time password, for example.

Open-source software

OpenLDAP and FreeRADIUS have been used to implement the LDAP and RADIUS server.

OpenLDAP is a free, open-source implementation of the Lightweight Directory Access Protocol (LDAP) developed by the OpenLDAP Project. Several common Linux distributions include OpenLDAP Software for LDAP support.

FreeRADIUS is the world's most popular and the most widely deployed open source RADIUS server. It serves as the basis for many commercial offerings, and it supplies the authentication, authorization, and accounting) needs of many Fortune 500 companies and Tier 1 ISPs. It is also widely used by the academic community.

FreeRADIUS module rlm_LDAP enables authentication via LDAP. With this module, the FreeRADIUS server can connect to an LDAP server, authenticate, and query the directory to verify user information such as privilege level and user ID and password.

FreeRADIUS also provide an LDAP schema file. Schema files are used by LDAP to describe the structure of the database and the entries. For example, a schema file for a person would contain the first and last name, phone number, email address, position, user ID, Authentication information, etc.

The schema file provided by FreeRADIUS needs to be added to OpenLDAP. Once added, RADIUS users can be created in the LDAP directory.

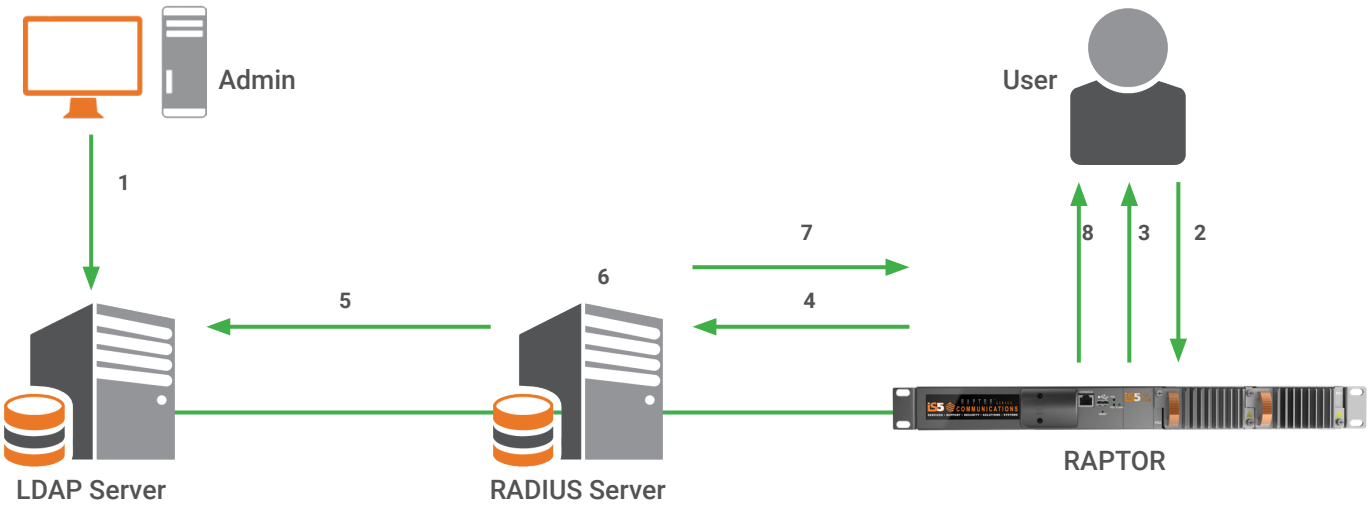
Flow of authentication

The flow of the authentication process is described below:

1. The system administrator must create users in the LDAP directory and assign user IDs and passwords
2. A user attempts to connect to a client device (e.g. the RAPTOR)
3. The client device prompts the user for username and login credentials (e.g. password)
4. The client device will send an access request to the RADIUS server, incuding the username and credentials

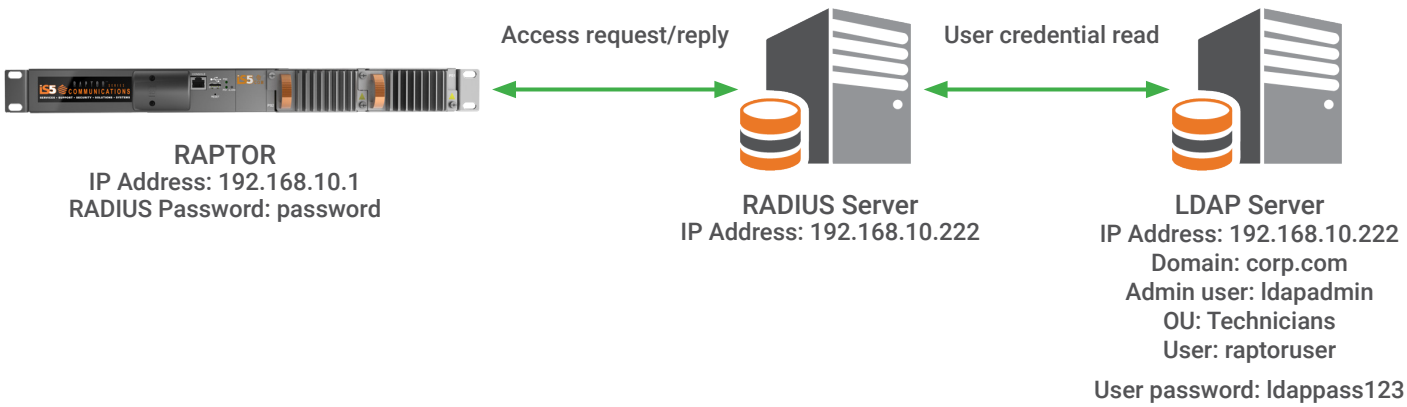
5. The RADIUS server will query the LDAP directory to verify the ID and password
6. The RADIUS server performs the authentication
7. The RADIUS server replies to the network device with the access accept
8. The client device allows access to the user, with the appropriate privileges for their role

Figure 2.0



CONFIGURATION STEPS

Figure 3.0 - Configuration details



RAPTOR configuration

The RAPTOR configuration requires two steps:

1. Set the RADIUS server IP address and password with the radius-server host command.

```
RAPTOR# configure terminal
RAPTOR(config)# radius-server host 192.168.10.222 key password
```

2. Select RADIUS as the main authentication mechanism and a local authentication as back-up

```
RAPTOR(config)# login authentication radius local
```

Verify that the RAPTOR is receiving RADIUS access-accept or access-reject messages with the command “show radius statistics”.

```
RAPTOR(config)# login authentication radius local

RAPTOR# show radius statistics

Radius Server Statistics
-------------------------
Index                          : 1
Server address                 : 192.168.10.222
UDP port number                : 1812
Round trip time                : 0
No of request packets          : 2
No of retransmitted packets    : 0
No of access-accept packets    : 1
No of access-reject packets    : 1
No of access-challenge packets : 0
No of malformed access responses : 0
No of bad authenticators       : 0
No of pending requests         : 2
No of time outs                : 0
No of unknown types            : 0
----------------------------------------
```

FreeRADIUS server installation and configuration

Install the required packages with the following command

 # yum install FreeRADIUS FreeRADIUS-utils FreeRADIUS-ldap FreeRADIUS-mysql FreeRADIUS-perl –y

After a few minutes, all the packages will be installed, and you will receive an installation complete message.

1. Start the FreeRADIUS server with the following command

 # systemctl start radiusd

RADIUSd is FreeRADIUS daemon in CentOS Linux distribution

We use the following command to ensure that the FreeRADIUS server will run when the system starts

 # systemctl enable radiusd

2. Allow the UDP ports used by the RADIUS server

The FreeRADIUS server uses UDP port 1812 to listen to authentication requests and port 1813 for accounting requests. These ports should be allowed in the firewall.

To allow ports 1812 and 1813 on the CentOS firewall, use the following commands

 # firewall-cmd –zone=public –add-port=1812/udp
 # firewall-cmd –zone=public –add-port=1813/udp

We make these changes permanent with the following commands

 # firewall-cmd –zone=public –permanent –add-port=1812/udp
 # firewall-cmd –zone=public –permanent –add-port=1813/udp

FreeRADIUS is configured in CentOS by modifying the configuration files located in /etc/raddb

3. Client creation

Use the text editor vim to modify the file “client.conf”. This file defines RADIUS clients.

Add the RAPTOR in the client definition.

```
client RAPTOR{
        ipaddr = 192.168.10.1
        secret = password

}
```

4. Configure and activate the LDAP module

Configure the LDAP module with the appropriate parameters to query the LDAP directory

You need to modify the following attributes in the ldap file located at /etc/raddb/mods-available

A. Set the address of the OpenLDAP server. You can use either the hostname or the IP address of the LDAP server.

Since the LDAP server runs on the same machine as the FreeRADIUS server, the default configuration “localhost” is kept.

```
ldap {
        #  Note that this needs to match the name(s) in the LDAP server
        #  certificate, if you're using ldaps.  See OpenLDAP documentation
        #  for the behavioral semantics of specifying more than one host.
        #
        #  Depending on the libldap in use, server may be an LDAP URI.
        #  In the case of OpenLDAP this allows additional the following
        #  additional schemes:
        #  - ldaps:// (LDAP over SSL)
        #  - ldapi:// (LDAP over Unix socket)
        #  - ldapc:// (Connectionless LDAP)
        server = 'localhost'
#       server = 'ldap.rrdns.example.org'
#       server = 'ldap.rrdns.example.org'
```

B. Set the user account used by the RADIUS server to search the LDAP directory.

```
#  Administrator account for searching and possibly modifying.
#  If using SASL + KRB5 these should be commented out.
identity = 'cn=ldapadm,dc=corp,dc=com'
password = root
```

C. Set the base_dn from which the RADIUS server starts the research.

```
#  Unless overridden in another section, the dn from which all
#  searches will start from.
base_dn = 'dc=corp,dc=com'
```

D. In the directory /etc/raddb/mods-enabled/ create a soft link to the ldap file located in mods-available using the following commands.

 # ln -s ../mods-available/ldap ldap

E. Enable the LDAP module in the configuration file.

The LDAP module is enabled by uncommenting the LDAP authorize section in the file “default” located in /etc/raddb/sites-available/default.

```
#  The ldap module reads passwords from the LDAP database.
ldap
```

FreeRADIUS server installation and configuration

1. Install all OpenLDAP components with the following command

 # yum -y install openldap*

2. Start the OpenLDAP service

 # systemctl start slapd

Ensure that the OpenLDAP server auto-start when the system starts.

 # systemctl enable slapd

Allow requests to the LDAP server in the firewall if the RADIUS server is installed on a different machine.

3. Use the command slappasswd to generate a hashed value of the password used to create the admin user

```
[root@localhost anis]# slappasswd
New password:
Re-enter new password:
{SSHA}gea19Md+YRFUFQmZEKHYeoelRK5J3e6m
```

Store this value; it will be used later during the configuration steps.

4. Configure OpenLDAP

OpenLDAP is configured by the ldapadd and ldapmodify commands. To change the parameters in the config file of the server, create an LDIF file with all the required parameters and use the ldapadd or ldapmodify commands to add them to the OpenLDAP database.

A. Create an LDIF file ldaprootpasswd.ldif and add the parameters below. Use the hashed password generated by the slappasswd command.

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=corp,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=ldapadm,dc=corp,dc=com

dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SHAA}nHnbvHHW7qjOQiziu7ur1Ub4Q36YN7oP
```

Use the command ldapmodify.

 # ldapmodify -Y EXTERNAL -H ldapi:/// -f ldaprootpasswd.ldif

B. Create an LDIF file monitor.ldif and add the parameters below.

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,
 cn=auth" read by dn.base="cn=ldapadm,dc=corp,dc=com" read by * none
```

Use the command ldapmodify.

 # ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif

C. Copy the sample database configuration file for slapd into the /var/lib/ldap directory and set the correct permissions on the file.

 # cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
 # chown ldap:ldap /var/lib/ldap/*

D. Import basic LDAP schemas from the /etc/openldap/schema directory as follows.

 # ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
 # ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
 # ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

E. Add your domain in the LDAP database by creating a file called base.ldif and add the parameters as follows.

```
dn: dc=corp,dc=com
dc: corp
objectClass: top
objectClass: domain

dn: cn=ldapadm,dc=corp,dc=com
objectClass: organizationalRole
cn: ldapadm
description: LDAP Manager

dn: ou=Technicians, dc=corp,dc=com
objectClass: organizationalUnit
ou: People
```

Use the ldapadd command to add the above configuration

 # Ldapadd -x -W -D "cn=ldapadm,dc=corp,dc=com" -f base.ldif

Enter the LDAP root password when requested.

F. Create a user entry. Create an LDIF file called raptoruser.ldif.

```
dn: cn=raptoruser,ou=Technicians,dc=corp,dc=com
objectClass: person
cn: raptoruser
sn: raptoruser
userPassword: {crypt}x
```

Use the ldapadd command to add the above configuration

 # ldapadd -x -W -D "cn=ldapadm,dc=corp,dc=com" -f raptoruser.ldif

```
[root@localhost ~]# ldapadd -x -W -D "cn=ldapadm,dc=corp,dc=com" -f raptoruser.ldif
Enter LDAP Password:
```

G. Create a password for the new user "raptoruser"

 # ldappasswd -s ldappass123 -W -D "cn=ldapadm,dc=corp,dc=com" -x "cn=raptoruser,ou=Technicians,dc=corp,dc=com"

The Password of the user raptoruser is ldappass123 in the command above.

CONCLUSION

Centralized user management is a valuable service to simplify user access management and improve security by having better control over users' credentials and privileges. There are various user management solutions in the market which offer a large variety of functionality and increased security. However, all these solutions come with a price. They are usually license based and tend to be very expensive to deploy. In this document we analyzed one of the solutions for centralized user management based on open-source software. OpenLDAP and FreeRADIUS are well known and used open-source software. FreeRADIUS provides an LDAP module and an LDAP schema file that simplifies an LDAP directory integration. This solution leverages the advantages of both LDAP and RADIUS. User information will be centrally managed by the OpenLDAP directory, while accounting and multifactor authentication can be performed by the FreeRADIUS server.

ABOUT iS5 COMMUNICATIONS INC.

iS5 Communications Inc. ("iS5Com") is a global provider of integrated services and solutions, and manufacturer of intelligent Industrial Ethernet products. Our products are designed to meet the stringent demand requirements of utility sub-stations, roadside transportation, rail, and industrial applications. iS5Com's services and products are key enablers of advanced technology implementation such as the Smart Grid, Intelligent Transportation Systems, Intelligent Oil Field, and Internet of Things. All products have the ability to transmit data efficiently without the loss of any packets under harsh environments and EMI conditions.

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

For more information, visit: is5com.com

toll free: +1-844-520-0588 | fax: +1-289-401-5206 | info@is5com.com
technical support: +1-844-475-8324 | support@is5com.com
Address: 5895 Ambler Dr, Mississauga, ON L4W 5B7