Using LDAP to Connect to a Directory

FreeRADIUS supports multiple methods of using LDAP to connect to a local directory. This page details these options, and how to configure them.

1. Introduction

FreeRADIUS has support for LDAP, which is enabled by installing the `freeradius-ldap` module on both Debian- and RedHat-based platforms.

Using LDAP requires the use of a low-privileged user with permissions to search the directory and retrieve attributes from it, if necessary.

> For Moonshot, it is recommended that LDAP lookups and authentications are limited to the `/etc/raddb/sites-available/inner-tunnel` (or `/etc/freeradius/sites-available/inner-tunnel`) file, as Moonshot uses EAP-TTLS and the real username is only exposed in the tunnel itself.

2. Using the LDAP protocol itself

Because LDAP is a directory access protocol, FreeRADIUS support relies on the directory it connects to to provide the password in a format it understands. The LDAP module will use a defined user to connect to the directory and search for the specified username, before it retrieves the appropriate password attribute.

The password can be in different formats, but the administrator implementing the FreeRADIUS connection to the directory must specify in the LDAP configuration which password attribute will be required. For more information, see http://wiki.freeradius.org/modules/Rlm_ldap.

Current implementations of Moonshot have been tested with OpenLDAP and eDirectory by following the standard instructions for deploying FreeRADIUS with LDAP.

3. Using the LDAP "bind as user" method

FreeRADIUS also supports the so-called bind-as-user method of authentication, in which FreeRADIUS attempts to use the username and password provided to connect to the directory. If the bind with the provided combination is successful, FreeRADIUS considers this a successful authentication attempt. For more information on this method, please read http://deployingradius.com/documents/protocols/oracles.html

For directories that defer authentication to another mechanism, such as Kerberos or SASL, or for those unable to install SAMBA to enable access to Active Directory, this method is recommended.

To use this method in your Moonshot implementation, read FreeRADIUS + OpenLDAP with SASL, courtesy of the University of Edinburgh and the Diamond Light Source.