

DISICO

Instalación y Configuración RADIUS

Manual

¿Que es Radius?

Remote Authentication Dial In User Service. Es un protocolo AAA (Autenticación, Autorización y Administración) para aplicaciones como acceso a redes o movilidad IP.

- **Autenticación**
 - La confirmación de que el usuario es quien dice ser. La autenticación se realiza mediante la presentación de credenciales.
- **Autorización**
 - Permitir el acceso a determinados tipos de servicio o recursos.
- **Administración**
 - El seguimiento del consumo de recursos.

Como funciona RADIUS

Muchos ISP (proveedores de acceso a internet por dial up, DSL, cable módem, Ethernet, WiFi, etc.) requieren que se ingrese un nombre de usuario y contraseña para conectarse a la red. Antes de que el acceso a la red sea concedido, los datos de acceso son pasados por un dispositivo NAS (Network Access Server) sobre un protocolo de capa de enlace (como PPP, para muchos dialups y DSL), luego hacia un servidor RADIUS sobre un protocolo RADIUS. El servidor RADIUS chequea que esa información sea correcta usando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptada, el servidor autorizará el acceso al sistema del ISP y seleccionará una dirección IP, parámetros L2TP, etc.

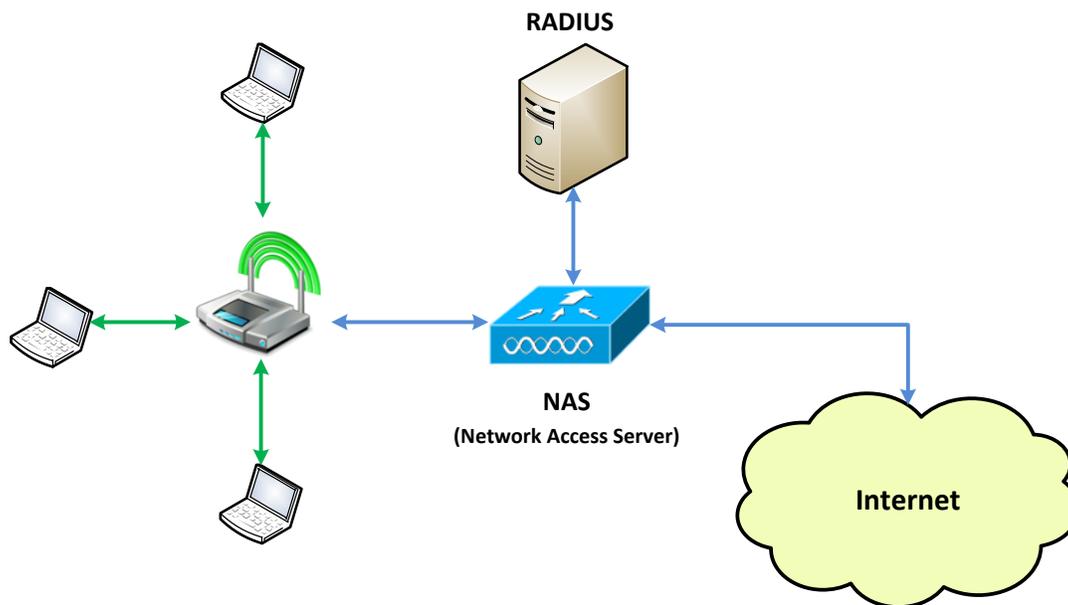


Ilustración 1: Esquema de funcionamiento

Esquema de Implementación

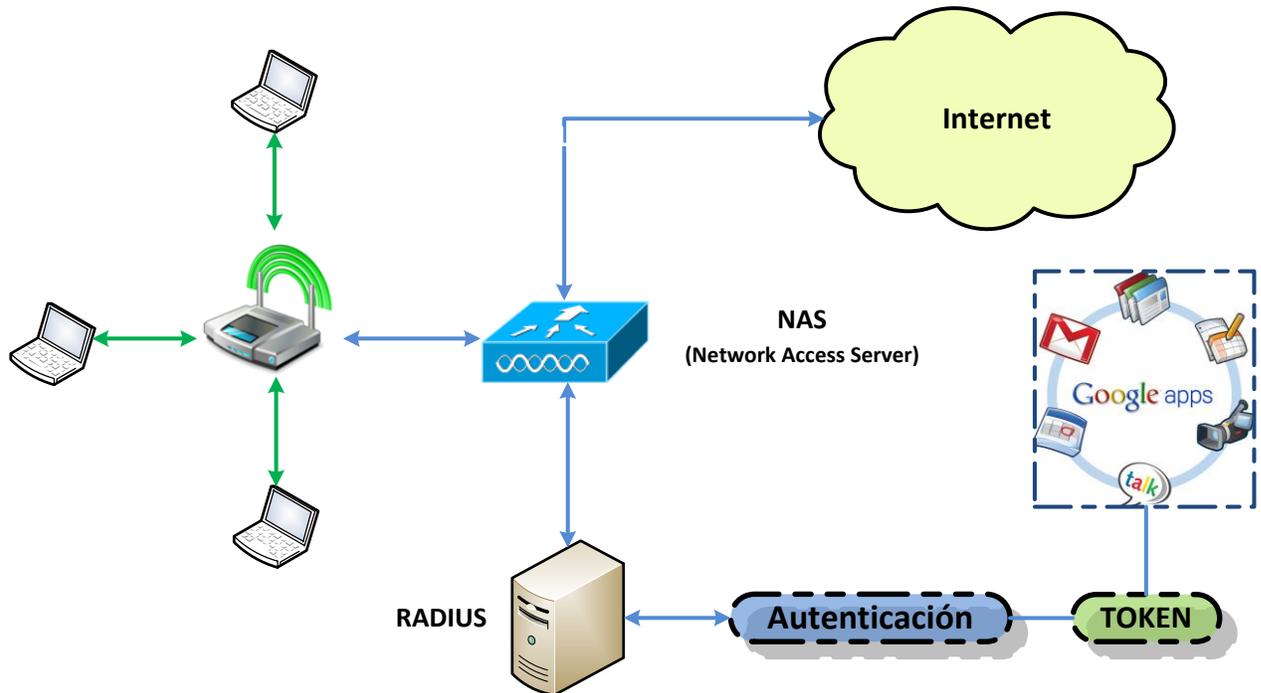


Ilustración 2: Esquema implementación

Instalación y configuración de FreeRADIUS

- **Instalación:**
 - Para instalar FreeRADIUS deberá de dirigirse a la siguiente dirección:
 - **# cd /usr/ports/net/freeradius2/**
 - Luego deberá de ejecutar el siguiente comando:
 - **# make config**
 - *enable-LDAP*
 - *enable-MySQL*
 - Finalmente se procede a instalar la aplicación
 - **# make && make install && make clean**

- **Configuración Test:**

- Posterior a la instalación de FreeRadius deberá de configurar el archivo **users** como se muestra a continuación:

- Hacer una copia del archivo original
 - **# cp /usr/local/etc/raddb/users /usr/local/etc/raddb/users_original**
- Ingresar usuario de prueba para FreeRADIUS
 - **#ee /usr/local/etc/raddb/users**
 - **jnnader Cleartext-Password := "jn_javac"**
 - **#ee /etc/rc.conf**
 - **radiusd_enable="YES"**
 - **#radiusd -X**
 - **#radtest jnnader jn_javac 127.0.0.1 0 testing123**
 - **Access-Accept**

- **Configuración Script Perl**

- Posterior a las pruebas de usuario se deberá de editar el archivo **example.pl** para permitir la autenticación por cuentas Google Apps

- Hacer una copia del archivo original
 - **# cp /usr/local/etc/raddb/example.pl /usr/local/etc/raddb/example.pl.resp_original**
- Agregar código de autenticación, para ello deberá reemplazar el bloque de la función **authenticate** como se muestra a continuación.
 - **#ee /usr/local/etc/raddb/example.pl**
 - **sub authenticate {**
 -
 - **my \$response = \$lwp_object->post(\$url,**
 - **['accountType' => 'HOSTED',**
 - **'Email' => \$RAD_REQUEST{'User-**
 - **Name'}. '@uv.cl',**
 - **'Passwd' => \$RAD_REQUEST{'User-**
 - **Password'},**
 - **'service' => 'apps'**
 - **]**
 - **);**
 -
 - **if(\$response->is_success)**
 - **{**

- `$RAD_REPLY{'h323-credit-amount'} = "100";`
- `return RLM_MODULE_OK;`
- `}`
- `else`
- `{`
- `$RAD_REPLY{'Reply-Message'} = "Denied access`
`by rlm_perl function".$RAD_REQUEST{'User-`
`Name'};`
- `return RLM_MODULE_REJECT;`
- `}`
- `}`
- Para permitir la autenticación de los usuarios mediante perl editar el archivo de configuración user
 - `#ee /usr/local/etc/raddb/users`
 - **DEFAULT Auth-Type = Perl**
- Habilitar perl en default y inner-tunnel
 - `#ee /usr/local/etc/raddb/site_enable/default`
 - **authorize {**
 - **#preprocess**
 - **#chap**
 - **#mschap**
 - **#digest**
 - **#suffix**
 - **eap**
 - **files**
 - **perl**
 - **expiration**
 - **logintime**
 - **pap**
 - **}**
 -
 - **authenticate {**
 - **Auth-Type PAP {**
 - **pap**
 - **}**
 - **Auth-Type CHAP {**
 - **chap**
 - **}**

- perl
- Auth-Type MS-CHAP {
- mschap
- }
- digest
- unix
- eap
- }
-
- accounting {
- detail
- unix
- radutmp
- perl
- exec
- }
- ee /usr/local/etc/raddb/site_enable/inner-tunneling
 - authorize {
 -
 - #chap
 - #mschap
 - #suffix
 - update control {
 - Proxy-To-Realm := LOCAL
 - }
 - eap
 - files
 - perl
 - expiration
 - logintime
 - pap
 - }
 -
 - authenticate {
 - Auth-Type PAP {
 - pap
 - }
 -

- **Auth-Type CHAP {**
- **chap**
- **}**
- **Auth-Type Perl {**
- **perl**
- **}**
-
-
- **Auth-Type MS-CHAP {**
- **mschap**
- **}**
- **unix**
- **eap**
- **}**
- Instalar modulos perl mediante cpan
 - #cpan> Install LWP::UserAgent
 - #cpan> Install LWP::Protocol::https
- Pruebas mediante radius con googleapps
 - /usr/local/bin/radtest nader128 mypassword
127.0.0.1 0 testing123
- Verificar la carga del script
 - #ee /usr/local/etc/raddb/modules/perl
 - perl {
 - #
 - # The Perl script to execute on authorize,
authenticate,
 - # accounting, xlat, etc. This is very
similar to using
 - # 'rlm_exec' module, but it is persistent,
and therefore
 - # faster.
 - #
 - module = \${confdir}/example.pl

Instalación y Configuración de Radlogin from IE

- **Qué es**
- **Instalación**
 - Deberá descargar el paquete de radlogin desde http://www.iea-software.com/ftp/radiusv5/freebsd/radlogin4_freebsd.tar.gz, una vez descargado el archivo se procederá con su instalación
 - #tar -xvf radlogin4_freebsd.tar.gz
 - # cd /usr/ports/misc/compat4x
 - #make install clean
 - # cd /usr/ports/misc/compat5x
 - #make install clean
 - #cd /usr/local/etc/radiuslogin
 - #./install.pl
 - Teclar C y luego enter
 - Iniciar el servicio radlogin
 - #/usr/local/radius/radlogin
 - Ingresar al navegador web para ver el servicio
 - Ip_maquina:8020

- Configuración
 - Ingresar a <http://10.50.1.43:8020>
 - Configurar Settings

Settings

10.50.1.43:8020/configure

Esta página está escrita en inglés ¿Quieres ... Traducir No No traducir nunca del inglés Configuración

RADIUS test client

version 4.0.12

[Settings | RADIUS servers (Add) | Request profiles (Add) | Server monitoring (Add) | Radlogin | RADIUS packet decoder | Change password | Write config]

Settings	
HTTP bind IP Address	<input type="text" value="localhost"/>
HTTP port	<input type="text" value="8020"/>
Server threads	<input type="text" value="10"/>
Default server	<input type="text" value="localhost"/>
Default profile	<input type="text" value="Authentication"/>
Default Acct Start profile	<input type="text" value="Authentication"/>
Default Acct Stop profile	<input type="text" value="Authentication"/>
Monitor refresh interval (secs)	<input type="text" value="3"/>
Date format	<input type="text" value="MMDDCCYY"/>
Date separator	<input type="text" value="/"/>
SMTP server	<input type="text" value="mail"/>
Notify email FROM: address	<input type="text"/>
Notify email Subject	<input type="text" value="[RADLOGIN] \$name is \$status"/>

>> Continue

© 1994-2005 IEA Software, Inc. All rights reserved, world wide.

▪ **Radius Server**

The screenshot shows a web browser window with the URL `10.50.1.43:8020/servers_edit`. The page title is "Edit server" and the main heading is "RADIUS test client" with version "4.0.12". A navigation menu includes links for Settings, RADIUS servers (Add), Request profiles (Add), Server monitoring (Add), Radlogin, RADIUS packet decoder, Change password, and Write config. The main content area is titled "Edit server" and contains a table with the following configuration fields:

Server address	<input type="text" value="localhost"/>
Shared secret	<input type="text" value="testing123"/>
Auth port	<input type="text" value="1812"/>
Acct port	<input type="text" value="1813"/>
Timeout (secs)	<input type="text" value="3"/>
Retries	<input type="text" value="2"/>

At the bottom right of the form is a button labeled ">> Continue". Below the form, the footer text reads: "© 1994-2005 IEA Software, Inc. All rights reserved, world wide."

▪ **Server monitoring**

RADIUS test client version 4.0.12

[Settings | RADIUS servers (Add) | Request profiles (Add) | Server monitoring (Add) | Radlogin | RADIUS packet decoder | Change password | Write config]

Edit scoreboard

Monitor name	localhost
RADIUS Server	localhost
Auth Username	jyanac
Auth Password	jn_javac
Down notify E-Mail	juan.yanac@uv.cl
Profile	[Disabled]
Normal check interval (secs)	15
Down check interval (secs)	15
Response handling	NAK is OK
RADIUS timeout Down (secs)	60
RADIUS timeout Notify (secs)	120

>> Continue

© 1994-2005 IEA Software, Inc. All rights reserved, world wide.

Server monitoring

10.50.1.43:8020/scoreboards

Esta página está escrita en **inglés** ¿Quieres ... Traducir No No traducir nunca del inglés Configuración

RADIUS test client

version 4.0.12

[Settings | RADIUS servers (Add) | Request profiles (Add) | Server monitoring (Add) | Radlogin | RADIUS packet decoder | Change password | Write config]

Server monitoring

Name	Server	Profile	Status	Resp Last	Resp Avg	Uptime	Msg	Age
X Monitor Cuenta Google Apps	localhost	Authentication	OK	536 ms	535 ms	100.000%		13
X Monitor usuario local	localhost	Authentication	OK	0 ms	0 ms	100.000%		8

© 1994-2005 IEA Software, Inc. All rights reserved, world wide.

▪ Radlogin

The screenshot shows a web browser window titled "Radlogin" with the address bar displaying "10.50.1.43:8020/radlogin". The page content includes a navigation menu with links like "Settings", "RADIUS servers (Add)", "Request profiles (Add)", "Server monitoring (Add)", "Radlogin", "RADIUS packet decoder", "Change password", and "Write config".

The main configuration area is titled "Radlogin" and contains the following fields:

- RADIUS Server: localhost
- Profile: Authentication
- Iterations: Single request
- Login: jnnader
- Password: jn_javac

Below the configuration is a section for test results, divided into "Request" and "Response".

Attribute		Data
Standard	NAS-IP-Address	127.0.0.1
Standard	NAS-Identifier	"Localhost"
Standard	NAS-Port	0
Standard	Caller-Id	"1115551212"

Additional test results shown are:

- Status: Good
- Resp Time: 0 ms

At the bottom of the test results section, there is a button labeled ">> Continue".

© 1994-2005 IEA Software, Inc. All rights reserved, world wide.

Para monitorear otro freeradius, se deberá de habilitar el cliente en el server que se quiere monitorear

A – B

Donde A es el server

Donde B es el cliente

En B deberá editar el archivo clients.conf y agregar las siguiente línea

```
client 10.50.1.43{ //ip del server – Permite conexión
    secret      = testing123
    shortname    = localhost
}
```

Para monitorear con la ip del equipo agregar client localhost {

```
# Allowed values are:
# dotted quad (1.2.3.4)
# hostname (radius.example.com)
#ipaddr = 127.0.0.1
ipaddr = 10.50.1.43
```

Para habilitar el correo instalar snmp en el equipo