RADIUS Plugin for pGina | Admin Manual

Provided by Holger Weiß <holger@ZEDAT.FU-Berlin.DE>
ZEDAT | Freie Universität Berlin | http://www.ZEDAT.FU-Berlin.DE/

Code contributions by Kostas Kalevras <kkalev@noc.ntua.gr>

Overview

The RADIUS Plugin for pGina provides RADIUS authentication and (optionally) RADIUS accounting for Microsoft® Windows™ clients. It can be configured to either allow any of your users to do RADIUS authentication requests in order to log in to the Windows PC, or to permit only those users who already have an account on the local Windows PC to authenticate against your RADIUS server. As an example, this distinction enables us to use RADIUS authentication not only for pool PCs, to which all students of our university have access, but also for staff PCs, to which students should *not* have access. The RADIUS Plugin for pGina is Free Software (that is, it's GPL'd).

Requirements

A working installation of pGina is of course required in order to use the RADIUS plugin. pGina can be found on http://pgina.xpasystems.com/. The RADIUS plugin requires much less than 1 MB of disk space. So far, it is tested with pGina 1.7.x on Windows 2000 and Windows XP clients only; I don't know (and I'm sceptical) about Windows NT. In any case, please let me know if you have tested the RADIUS plugin with newer and/or older versions of pGina and/or Windows.

Downloading and Installing the Plugin

After downloading the Windows installer file provided on the RADIUS plugin website (http://pgina.xpasystems.com/plugins/radius.php), run the executable. This will install, but *not* configure the plugin.

Configuring the Plugin

Configuration of the RADIUS plugin is performed just as any other plugin – run the configuration utility that was provided with pGina 1.6.2 or higher, select the "General" tab, click on the "Browse" button below the "Plugin Path" field and then choose the RADIUSplugin.dll from the location to which you installed it in the previous step. Once selected, you can configure the plugin by using the "Configure" button. This will invoke the configuration dialog shown in Figure 1.

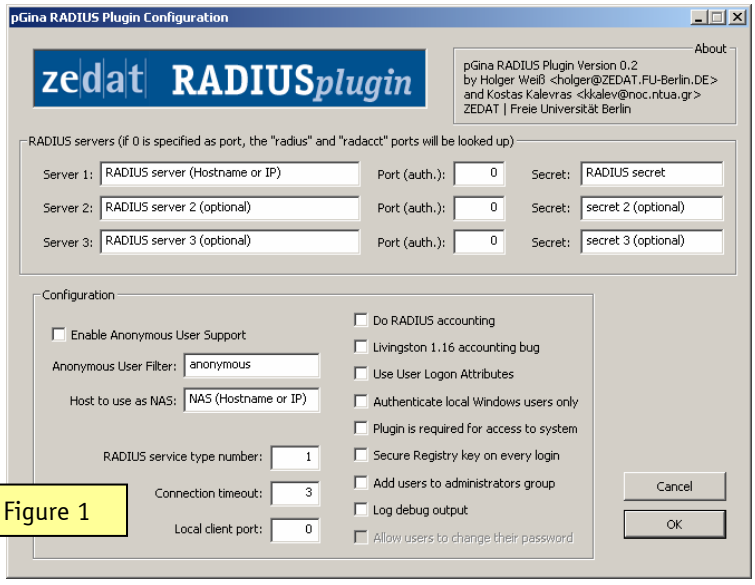

Figure 1

RADIUS servers section

Within this section, the RADIUS server(s) to use for authentication (and accounting) are specified. If you specify multiple RADIUS servers, they are tried in order. The first server to return success or failure causes the RADIUS plugin to return success or failure. Only if a server fails to respond it is skipped, and the next server in turn is used. Specifying more than one server is of course fully optional. For each server to use, there are three fields:

SERVER

This is the hostname or IP address of the RADIUS server to use for authentication and (optionally) accounting. If the DNS server returns multiple IP addresses for a given hostname, one of them will be chosen randomly. If the plugin was configured to do accounting, the same IP address will be used for authentication and the corresponding accounting requests.

PORT (AUTH.)

This is the UDP port number used for RADIUS authentication. RADIUS accounting will be done one port higher. The port name for authentication is "`radius`"; the port name for accounting is "`radacct`". Those will be used if `0` is specified as port number; they will be looked up from `%SystemRoot%\system32\drivers\etc\services`.

SECRET

This is your RADIUS password. Please note that the *secret will be saved plaintext to the Windows Registry*, which means that *anybody who is in the "administrators" group* on the Windows PC will be able to read it. See also the option "Secure Registry key on every login".

Configuration section

Within this section, various options that influence the operation of the RADIUS plugin may be specified.

ENABLE ANONYMOUS USER SUPPORT

This option enables anonymous user support. This just adds a UserLogon-Restriction attribute with a value of Anonymous-User to the RADIUS authentication request (see the section on user logon attributes below). The RADIUS server is responsible for performing any special operations in this case.

ANONYMOUS USER FILTER

If set, this filter will be used for selecting usernames which will be considered anonymous users (as long as anonymous user support is enabled in the first place). All usernames *beginning* with (and equal to) the specified filter string will be matched.

HOST TO USE AS NAS

If set, specifies the host to be used as NAS in RADIUS packets sent to the RADIUS server. If the host corresponds to an IP address, all packets sent to the RADIUS server will carry a NAS-IP-Address attribute with that address, otherwise they will carry a NAS-Identifier attribute with the value set in this option. This can be handy for grouping requests from multiple workstations, based on a common NAS-IP-Address attribute.

RADIUS SERVICE TYPE NUMBER

This field allows you to specify the numerical value of the service type attribute sent to the RADIUS server. For possible values see RFC 2865, 5.6 (although you can of course use a custom value instead). The default value used by the plugin is `1` ("Login").

CONNECTION TIMEOUT

Here, the number of seconds the RADIUS plugin will wait for a response from the server before retrying (and then giving up) is specified. The default, `3` seconds, should be more than enough in most cases.

NUMBER OF RETRIES

Specifies how often the RADIUS plugin will retry to connect to the RADIUS server if it doesn't get a response.

LOCAL CLIENT PORT

This field allows you to specify the local port number used by the RADIUS plugin. This feature was requested in order to allow using the RADIUS plugin together with some paranoid packet filter setup. However, normally it makes sense to leave this set to `0`, in which case the plugin will choose a port number itself.

DO RADIUS ACCOUNTING (NOT ONLY AUTHENTICATION)

If this option is set, the RADIUS plugin will not only provide RADIUS authentication, but also send an accounting start request when the user logs in and an appropriate stop request when the user logs out.

LIVINGSTON 1.16 ACCOUNTING BUG

When used, the accounting response vector is *not* validated. This option will probably only be necessary on *really* old (i.e. Livingston 1.16) servers.

USE USER LOGON ATTRIBUTES

This option enables special user logon attributes. UserLogon attributes are vendor specific attributes which can be used to carry information for the user in RADIUS authentication and accounting packets. Administrators can add the accompanied dictionary file 'dictionary.ntua' to their RADIUS servers in order to support such attributes. Below is a list of available attributes in the dictionary file and their usage:

- UserLogon-Homedir: The user's home directory. Returned in RADIUS Access-Accept packets and used by pGina on user creation.
- UserLogon-Restriction: Specifies any user restrictions. Can take one of the Anonymous-User,Admin-User values. The Anonymous-User value is added by the RADIUS plugin itself as described above in the anonymous user configuration options. The Admin-User can be present in RADIUS Access-Accept packets and can be used to instruct the RADIUS plugin to add the corresponding user to the administrators group.
- UserLogon-GroupNames: Specifies the group names the user belongs to. Returned in RADIUS Access-Accept packets.

- UserLogon-DriveNames: Specifies the drives to map for the user. Returned in RADIUS Access-Accept packets.
- UserLogon-UserDescription: Specifies the user description. Returned in RADIUS Access-Accept packets and used by pGina on user creation.
- UserLogon-UserFullName: Specifies the user full name. Returned in RADIUS Access-Accept packets and used by pGina on user creation.
- UserLogon-UserDomain: Specifies the domain to be used for that user by pGina if domain management is enabled.
- UserLogon-LogonTask: Currently not implemented
- UserLogon-LogoffTask: Currently not implemented
- UserLogon-Expiration: Currently not implemented
- UserLogon-UserProfile: Specifies the path to load the user profile from. Returned in RADIUS Access-Accept packets and used by pGina on user creation.

AUTHENTICATE LOCAL WINDOWS USERS ONLY

If this option is set, only those users who already have an account on the local Windows PC will be allowed to do RADIUS authentication requests. For users that don't exist locally, the RADIUS server won't be asked, but the plugin will report an appropriate error instead. If this option is not set, any user (except for "administrator") may do RADIUS authentication requests.

PLUGIN IS REQUIRED FOR ACCESS TO SYSTEM

This option dictates the actions of pGina upon a failed authentication attempt. If the plugin is required, then only a local administrator account can login via the local SAM. If the plugin is not required, then pGina will check to see if a local account and password exist which match the attempted login.

SECURE REGISTRY KEY ON EVERY LOGIN

No matter whether or not this option is set: The RADIUS plugin will *always* set an access control list (ACL) on the Registry key `HKLM\Software\pGina\RADIUSplugin` (which includes the password of your RADIUS server). This ACL gives only the "administrators" group read and write access to the key. Any users not in this group won't have any access to that key, but *all users in the "administrators" group will have full access* to it. This ACL will be *(re)set every time you close the RADIUS plugin configuration dialog* by clicking "Ok". Moreover, if you set this option, the ACL will also be set *every* time a user logs in.

ADD USERS TO ADMINISTRATORS GROUP

Setting this option would add *all* users that authenticate via RADIUS to the "administrators" group. This might be useful for debugging purposes, but it should of course never be set for production use. Instead, the UserLogon-Restriction attribute could be used for adding *selected* users to the administrators group, see the section on user logon attributes above.

LOG DEBUG OUTPUT

If set, the RADIUS plugin will write some output to the Windows event log, this should be useful for debugging. However, if this option is not set, no log output will be produced at all, since the pGina logs should normally suffice.

ALLOW USERS TO CHANGE THEIR PASSWORD

The option to allow users to change their RADIUS password is *not* implemented yet.

RADIUS Server Setup

You will need to allow access to all workstations using the corresponding secret configured on each workstation.

Each incoming RADIUS request will always include the following RADIUS attributes (apart from those configured in the above sections):

- NAS-Port-Type = Virtual
- Calling-Station-Id with the IP address of the workstation pGina is running on.
- NAS-Port-Id with the PID of pGina.

In the case of accounting packets, every packet will also include the following attributes:

- Acct-Status-Type with a value of Start in case of accounting-start packets (sent on user logon) and a value of Stop in case of accounting-stop packets (sent on user logoff).
- Acct-Session-Id with a random string, unique (as much as possible) for each user session.
- Acct-Authentic = RADIUS
- Acct-Session-Time with the user's online time on accounting-stop packets.
- Acct-Terminate-Cause = User-Request
- Class attribute if the attribute was available in the Access-Accept received from the RADIUS server containing the value received in the Access-Accept.

The RADIUS server can include (apart from the attributes already discussed in the previous sections) the following attributes in it's response to the plugin authentication requests:

- Class attribute. It's value will be copied in corresponding Class attributes in the accounting packets sent by the plugin.
- Reply-Message which can be included in Access-Reject packets containing the rejection cause of the user.
- Session-Timeout containing the maximum allowed user session time in seconds.

Uninstalling the Plugin

If the RADIUS plugin is still in use, pGina must first be configured to use another plugin. After logging in with the new plugin, use the uninstaller provided with the RADIUS plugin in order to remove it. This will delete all RADIUS plugin files and the Registry key.

Contact

The RADIUS Plugin for pGina is written by Holger Weiß <holger@ZEDAT.FU-Berlin.DE> and Kostas Kalevras <kkalev@noc.ntua.gr>. Feel free to drop us an e-mail if you have any questions, bug reports or comments on the RADIUS plugin.