pfSense - Bug #6086

RADIUS WebUI login does not work with attribute class (25) when the server returns multiple attribute entries with different data

04/07/2016 02:20 AM - Phillip Hernandez

Status:	Resolved	**Start date:**	04/07/2016
Priority:	Normal	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Web Interface	**Estimated time:**	0.00 hour
Target version:	2.3.1		
Affected Version:	All	**Affected Architecture:**	All

Description

After doing several packet capture and reviewing RFC 4372. It seems to be a normal operation to include the class 25 attrib in a response back to the client. This causes 2 of the same type of attribs in the same response. Since this a part of the radius standard to include a class AVP. I suggest that this be changed to filter-id since it is already a string, can be used in this specific use case, and abides by the RFC.

Code that would need to be changed.

/etc/inc/auth.inc

```
/*
$attributes must contain a "filter_id" key containing the groups and local
groups must exist to match.
*/
function radius_get_groups($attributes) {
$groups = array();
if (!empty($attributes) && is_array($attributes) && !empty($attributes['filter_id'])) {
$groups = explode(";", $attributes['filter_id']);
foreach ($groups as & $grp) {
$grp = trim($grp);
if (strtolower(substr($grp, 0, 3)) == "ou=") {
$grp = substr($grp, 3);
}
}
}
return $groups;
}
```

Associated revisions

Revision 461bae6b - 04/07/2016 09:58 AM - Jim Pingle

Respect all Class attributes returned by the RADIUS server, not only the last one received. Fixes #6086

Revision 1dd07051 - 04/07/2016 09:59 AM - Jim Pingle

Respect all Class attributes returned by the RADIUS server, not only the last one received. Fixes #6086

History

#1 - 04/07/2016 08:08 AM - Jim Pingle

- Status changed from New to Needs Patch

- Priority changed from High to Normal

- Target version set to Future

Class does work when returned properly by the RADIUS server. If it doesn't work, the RADIUS server isn't returning it properly. While support could be added for an additional attribute for groups, changing it outright to something else would break everyone that is currently working.

It works when used against FreeRADIUS when the user has a reply attribute set similar to:

```
Class := "admins;VPNUsers"
```

#2 - 04/07/2016 09:57 AM - Jim Pingle

- Subject changed from RADIUS WebUI login does not work with attribute class (25) to RADIUS WebUI login does not work with attribute class (25) when the server returns multiple attribute entries with different data

- Status changed from Needs Patch to Assigned

- Assignee set to Jim Pingle

- Target version changed from Future to 2.3.1

- Affected Version set to All

I was able to reproduce your original issue against an AD server but the fix is not correct. The correct fix is not to use a different attribute, but to check all of the Class responses and not just the last one.

I'll push a fix shortly that will be in 2.3.1, you can apply it to a 2.3 system as a patch if needed. It may also apply to a 2.2.x box but might need some manual adjustment.

#3 - 04/07/2016 10:10 AM - Jim Pingle

- Status changed from Assigned to Feedback

- % Done changed from 0 to 100

Applied in changeset 461bae6b08d883d232db853a21337e688c1defee.

#4 - 04/07/2016 10:27 AM - Phillip Hernandez

Can you please add support for another AVP as well? In working systems where the Class AVP is not a string changing its type could cause other adverse affects. In several enterprise radius products this is not a string but an octet array by default.

Changing things outright from what was working is exactly what happen to me when this feature was introduced in the first place :)

Thanks for your help

#5 - 04/07/2016 10:45 AM - Jim Pingle

If an additional suitable attribute/AVP is available for this purpose, it would not be difficult to support. "filter_id" as suggested is not for this purpose, it is for ACLs (like firewall rules). That would belong in a separate ticket, however.

With this fix in place it works against FreeRADIUS and AD+NPS (On 2012) without making any fundamental changes to either.

#6 - 04/07/2016 11:03 AM - Phillip Hernandez

Ok thanks for your help. I will investigate further and open a separate ticket for adding another AVP.

Thanks

#7 - 04/07/2016 11:34 AM - Phillip Hernandez

I wanted to confirm that this works. I created a custom patch to apply to my pfsense boxes that are running 2.2.6 and I am now able to log in without the page error.

Thanks

#8 - 04/07/2016 12:16 PM - Jim Pingle

- Status changed from Feedback to Resolved

Thanks for the additional testing