RADIUS RETURNED ATTRIBUTES

Radius Returned Attributes

radius

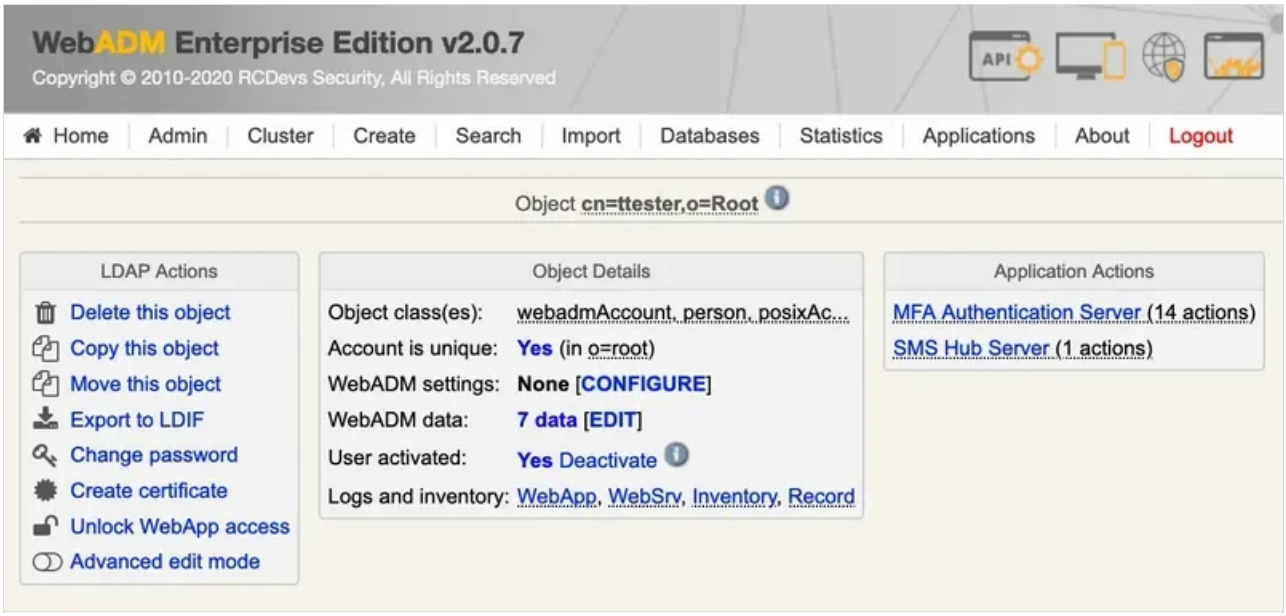
1. Overview

In that documentation, we will explain how to return Radius Attributes to a Radius client in order to provide extra information after a successfull authentication.

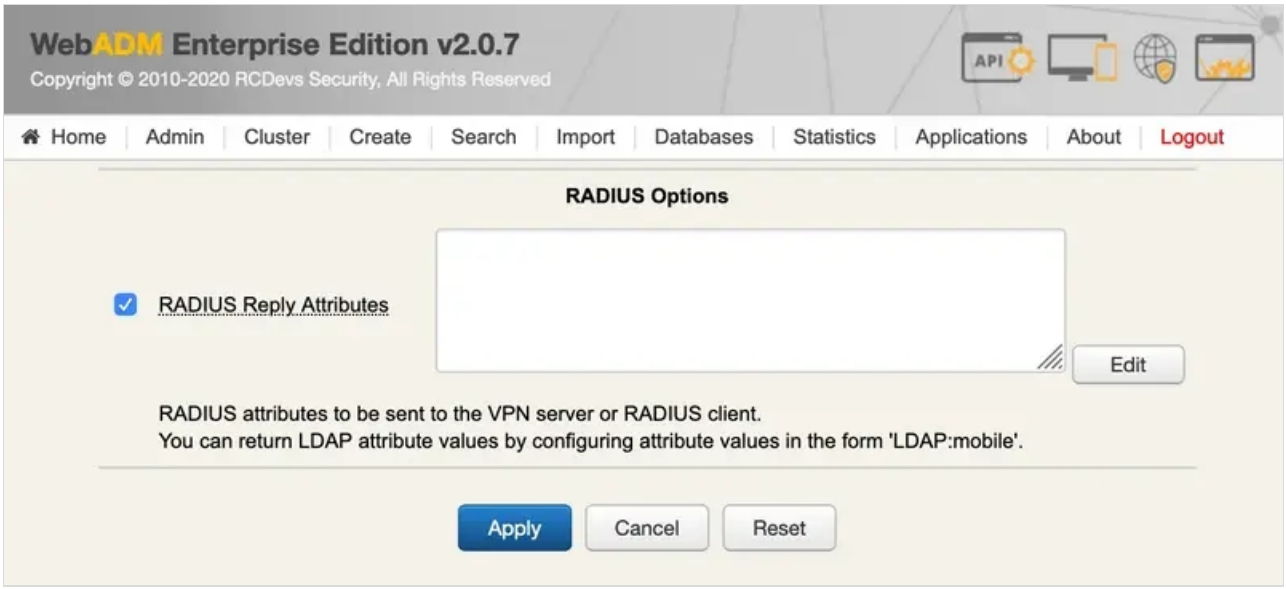
For this recipe, you will need to have a WebADM, OpenOTP and Radius Bridge installed and configured. Please refer to WebADM Installation Guide, WebADM Manual and Radius Bridge Manual for instructions on these.

2. Send an LDAP Value

We select the user in WebADM and we click on `WebADM settings: None [CONFIGURE]`:



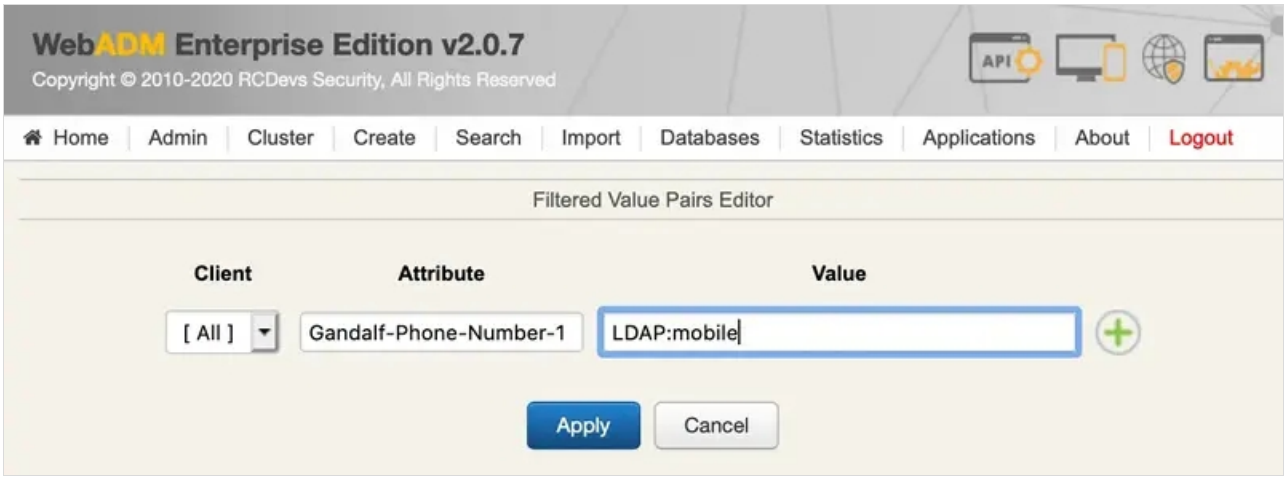
We select `OpenOTP` and scroll down to `RADIUS Options`, we check the box and click on `Edit`:



We select an attribute from a dictionary. We check that `Gandalf-Phone-Number-1` attribute is present in Radius Bridge:

```
[root@localhost ~]# grep -r "Gandalf-Phone-Number-1" /opt/radiusd/lib/dictionaries/
/opt/radiusd/lib/dictionaries/dictionary.gandalf:ATTRIBUTE Gandalf-Phone-Number-1   17 string
```

We add the attribute name and the value from the `mobile` LDAP attribute:



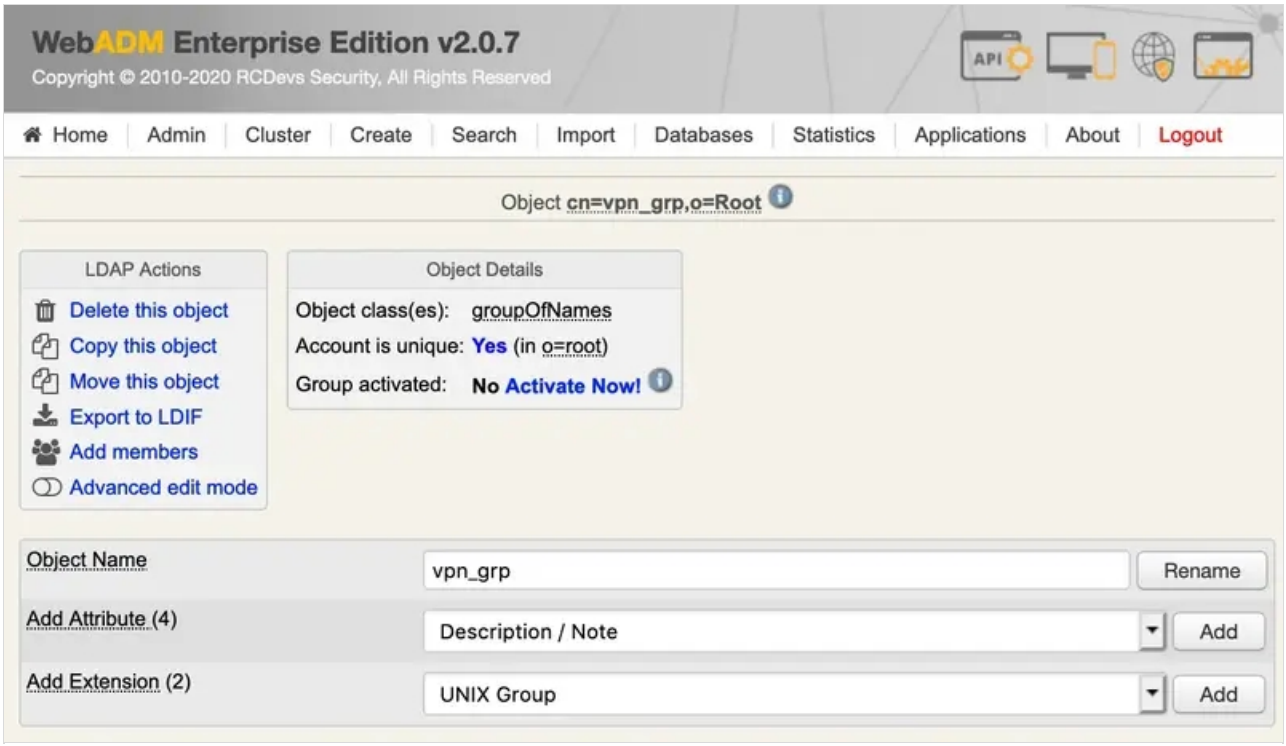
We apply twice and we try with radtest:

```
[root@localhost ~]# /opt/radiusd/bin/radtest john
Enter password: ******
(0) -: Expected Access-Accept got Access-Challenge
Result: Challenge
Session: 32773731486f443674624f393349416a
Enter your TOKEN password: 381469
Result: Success
Sent Access-Request Id 177 from 0.0.0.0:51646 to 127.0.0.1:1812 length 71 User-Name: "john"
User-Password: "381469"
State: 0x32773731486f443674624f393349416a NAS-Identifier: "RadTest"
Cleartext-Password: "381469"
Received Access-Accept Id 177 from 127.0.0.1:1812 to 0.0.0.0:0 length 63 Reply-Message:
"Authentication success"
Gandalf-Phone-Number-1: "123 456 789"
```

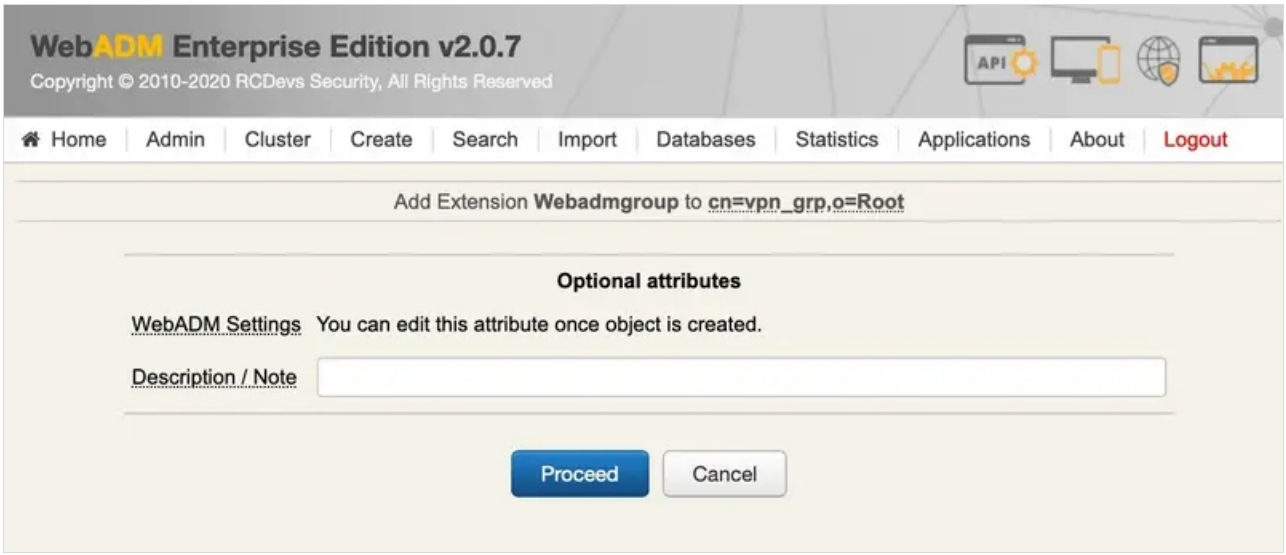
We can see `Gandalf-Phone-Number-1` radius attribute at the end with the value from `mobile` LDAP attribute.

3. Send a Value To All Members of a Group

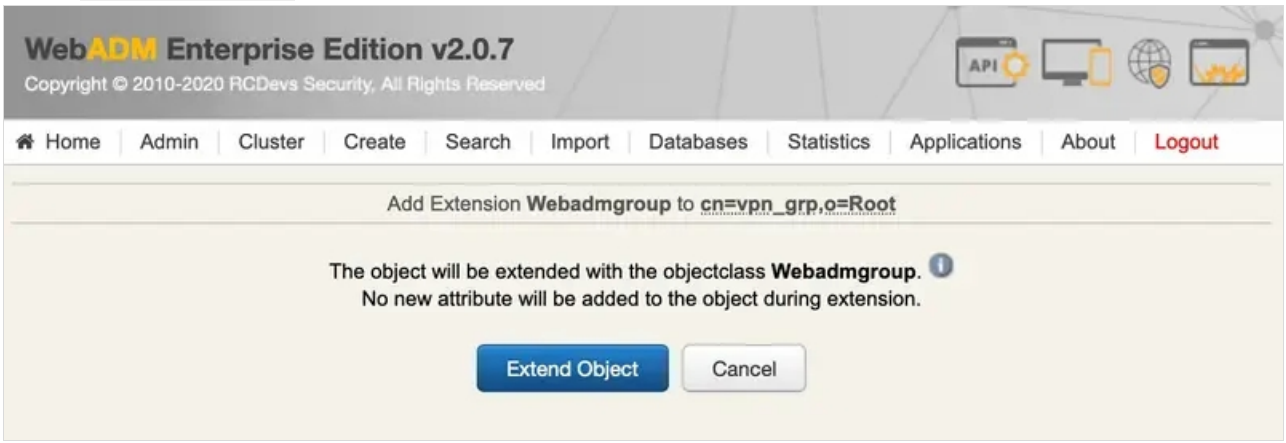
We select the group in WebADM:



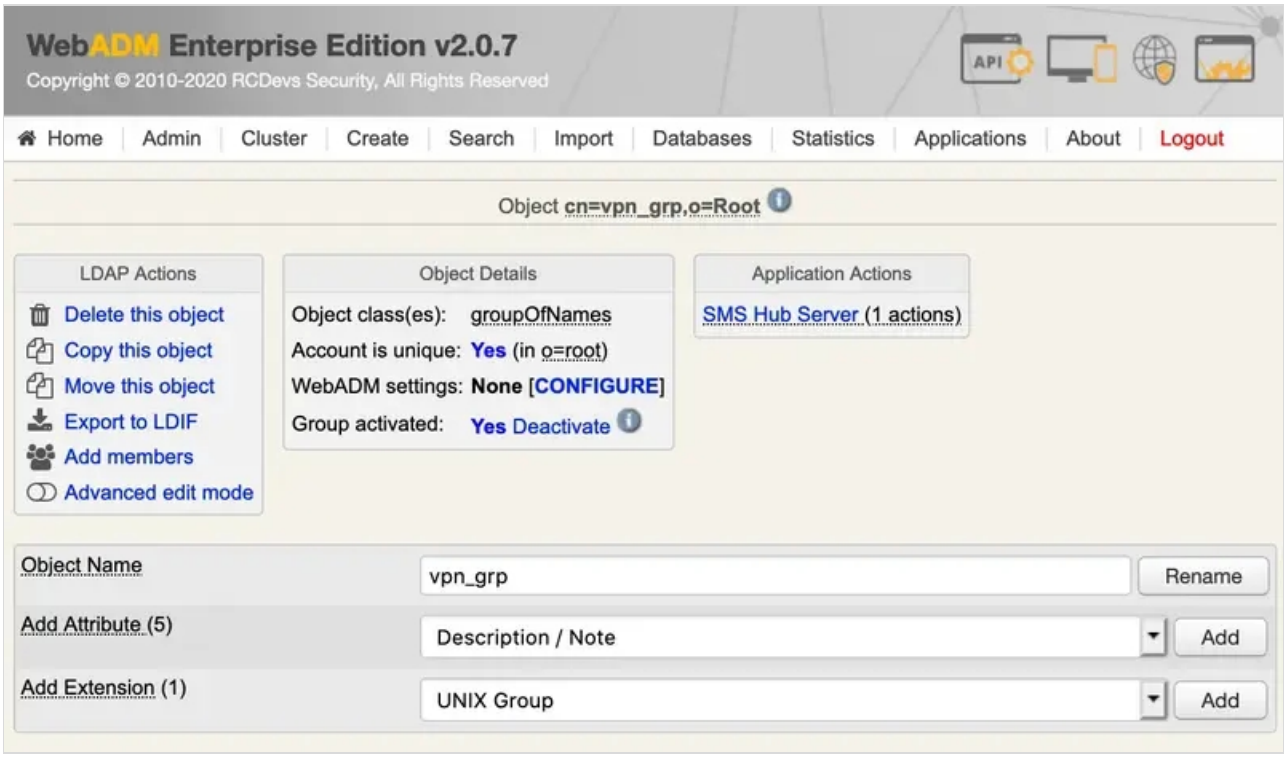
We click on `Activate Now!` and `Proceed`:



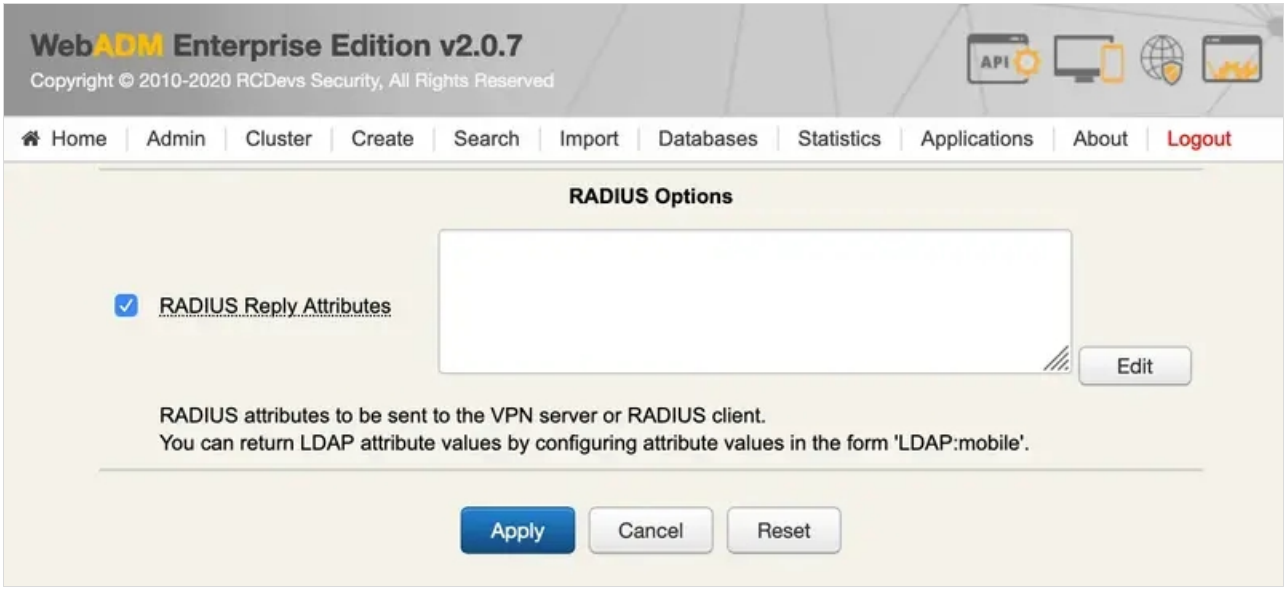
We click on `Extend Object`:



We click on `WebADM settings: None [CONFIGURE]`:



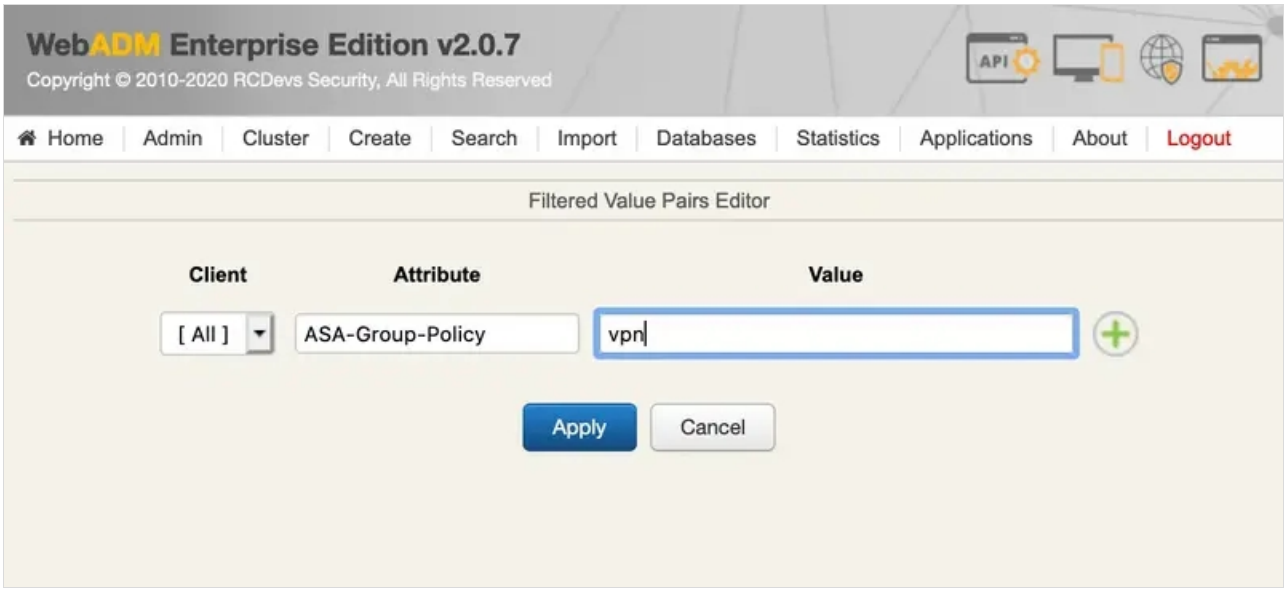
We select `OpenOTP` and scroll down to `RADIUS Options`, we check the box and click on `Edit`:



We select an attribute from a dictionary. We check that `ASA-Group-Policy` attribute is present in Radius Bridge:

```
[root@localhost ~]# grep -r "ASA-Group-Policy" /opt/radiusd/lib/dictionaries/
/opt/radiusd/lib/dictionaries/dictionary.cisco.asa:ATTRIBUTE ASA-Group-Policy   25 string
```

We add the attribute name and a value:



We apply twice and we try with radtest:

```
[root@localhost ~]# /opt/radiusd/bin/radtest john
Enter password: ******
(0) -: Expected Access-Accept got Access-Challenge
Result: Challenge
Session: 705179694d59693771534a6b536e4f65
Enter your TOKEN password: 090807
Result: Success
Sent Access-Request Id 32 from 0.0.0.0:57454 to 127.0.0.1:1812 length 71 User-Name: "john"
User-Password: "090807"
State: 0x705179694d59693771534a6b536e4f65 NAS-Identifier: "RadTest"
Cleartext-Password: "090807"
Received Access-Accept Id 32 from 127.0.0.1:1812 to 0.0.0.0:0 length 55 Reply-Message: "Authentication
success"
ASA-Group-Policy: "vpn"
```

We can see `ASA-Group-Policy` radius attribute at the end with `vpn` value.

4. Troubleshooting of Radius returned attributes

4.1 Invalid RADIUS return attributes

It's possible to configure radius returned attributes through WebADM GUI for specific users, groups or clients applications. Please refer to Radius Attributes documentation for how to configure them. RADIUS return attributes must comply with the RADIUS dictionaries stored in `/opt/radiusd/lib/dictionaries/`. If they do not, the authentication will fail. In the example below, RADIUS Bridge receives return attribute `ASA-VLAN="string"`, which is not correct as the attribute is defined as integer.

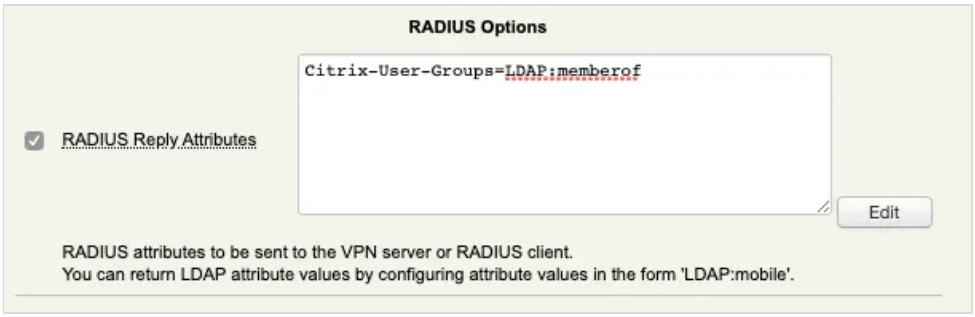
```
[root@rcvm8 ~]# /opt/radiusd/bin/radiusd debug
...
rlm_openotp: OpenOTP authentication succeeded

rlm_openotp: Reply Data: ASA-VLAN="string"
rlm_openotp: Invalid Reply Data (invalid value-pairs format or attribute not in dictionary)
NOTE <<<<

(3)     [openotp] = fail
(3)   } # Auth-Type OTP = fail
(3) Failed to authenticate the user
(3) Using Post-Auth-Type Reject
(3) Post-Auth-Type sub-section not found.  Ignoring.
(3) Login incorrect: [test] (from client any port 0)
(3) Sent Access-Reject Id 52 from 127.0.0.1:1812 to 127.0.0.1:34295 length 0
(3) Finished request
```

4.2 Check Radius Returned Attributes

For this test, I configured `Citrix-User-Groups` as Radius returned attribute with a mapping to `memberof` attribute of my Administrator account.



Radius Client output :

```
[root@radius_cli ~]# /opt/radiusd/bin/radtest Administrator 192.168.3.64:1812 'testing123$!'
Enter password: ********
Result: Success
Sent Access-Request Id 55 from 0.0.0.0:60026 to 192.168.3.64:1812 length 62 User-Name:
"Administrator"
User-Password: "password"
NAS-Identifier: "RadTest"
Cleartext-Password: "password"
Received Access-Accept Id 55 from 192.168.3.64:1812 to 192.168.3.54:60026 length 410 Citrix-User-
Groups: "CN=Organization Management,OU=Microsoft Exchange Security Groups,DC=yorcdevs,DC=eu"
Citrix-User-Groups: "CN=Group Policy Creator Owners,CN=Users,DC=yorcdevs,DC=eu"
Citrix-User-Groups: "CN=Domain Admins,CN=Users,DC=yorcdevs,DC=eu"
Citrix-User-Groups: "CN=Enterprise Admins,CN=Users,DC=yorcdevs,DC=eu"
Citrix-User-Groups: "CN=Schema Admins,CN=Users,DC=yorcdevs,DC=eu"
Citrix-User-Groups: "CN=Administrators,CN=Builtin,DC=yorcdevs,DC=eu"
Reply-Message: "Authentication success"
```

As you can see, groups of my Administrator account are well returned.

Radius Bridge output :

```
(2) Received Access-Request Id 55 from 192.168.3.54:60026 to 192.168.3.64:1812 length 62
(2)   User-Name = "Administrator"
(2)   User-Password = "password"
(2)   NAS-Identifier = "RadTest"
(2) # Executing section authorize from file /opt/radiusd/lib/radiusd.ini
(2)   authorize {
(2) eap: No EAP-Message, not doing EAP
(2)     [eap] = noop
(2) pap: WARNING: No "known good" password found for the user.  Not setting Auth-Type
(2) pap: WARNING: Authentication will fail unless a "known good" password is available
(2)     [pap] = noop
(2)     [openotp] = ok
(2)   } # authorize = ok
(2) Found Auth-Type = OTP
(2) # Executing group from file /opt/radiusd/lib/radiusd.ini
(2)   Auth-Type OTP {
rlm_openotp: Found client ID attribute with value "RadTest"
rlm_openotp: Found source IP attribute with value ""
rlm_openotp: Found device ID attribute with value ""
rlm_openotp: Found client IP attribute with value ""
rlm_openotp: Sending openotpSimpleLogin request
rlm_openotp: OpenOTP authentication succeeded
rlm_openotp: Reply Data: Citrix-User-Groups="CN=Organization Management,OU=Microsoft Exchange
Security Groups,DC=yorcdevs,DC=eu",Citrix-User-Groups="CN=Group Policy Creator
Owners,CN=Users,DC=yorcdevs,DC=eu",Citrix-User-Groups="CN=Domain
Admins,CN=Users,DC=yorcdevs,DC=eu",Citrix-User-Groups="CN=Enterprise
Admins,CN=Users,DC=yorcdevs,DC=eu",Citrix-User-Groups="CN=Schema
Admins,CN=Users,DC=yorcdevs,DC=eu",Citrix-User-
Groups="CN=Administrators,CN=Builtin,DC=yorcdevs,DC=eu"
rlm_openotp: Reply message: Authentication success
rlm_openotp: Sending Access-Accept
(2)     [openotp] = ok
(2)   } # Auth-Type OTP = ok
(2) Login OK: [Administrator] (from client any port 0)
(2) Sent Access-Accept Id 55 from 192.168.3.64:1812 to 192.168.3.54:60026 length 0
(2)   Citrix-User-Groups = "CN=Organization Management,OU=Microsoft Exchange Security
Groups,DC=yorcdevs,DC=eu"
(2)   Citrix-User-Groups = "CN=Group Policy Creator Owners,CN=Users,DC=yorcdevs,DC=eu"
(2)   Citrix-User-Groups = "CN=Domain Admins,CN=Users,DC=yorcdevs,DC=eu"
(2)   Citrix-User-Groups = "CN=Enterprise Admins,CN=Users,DC=yorcdevs,DC=eu"
(2)   Citrix-User-Groups = "CN=Schema Admins,CN=Users,DC=yorcdevs,DC=eu"
(2)   Citrix-User-Groups = "CN=Administrators,CN=Builtin,DC=yorcdevs,DC=eu"
(2)   Reply-Message := "Authentication success"
(2) Finished request
```

Below, the OpenOTP logs for the previous authentication. You can see once the authentication factors are validated by OpenOTP, OpenOTP return the attribute configured on my Administrator account and then the log regarding radius returned attribute

appears : `Returning 6 RADIUS reply attributes`.

```
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] New openotpSimpleLogin SOAP request
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] > Username: Administrator
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] > Password: xxxxxxxx
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] > Client ID: RadTest
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] > Options: RADIUS,-U2F
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Registered openotpSimpleLogin request
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Ignoring 2 memberof values for user
'CN=Administrator,CN=Users,DC=yorcdevs,DC=eu' (out of domain group search base)
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Resolved LDAP user:
CN=Administrator,CN=Users,DC=yorcdevs,DC=eu
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Resolved LDAP groups: group policy creator
owners,domain admins,enterprise admins,schema admins,denied rodc password replication group
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Started transaction lock for user
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Found user fullname: Administrator
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Found 1 user emails:
Administrator@yorcdevs.eu
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Found 47 user settings:
LoginMode=LDAPOTP,OTPType=TOKEN,PushLogin=Yes,LockTimer=0,MaxTries=3,BlockTime=0,ChallengeMo
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExpire=10,
[1 Items]
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Found 10 user data:
LastOTP,TokenType,TokenKey,TokenState,TokenID,TokenSerial,Device1Type,Device1Name,Device1Data,Dev

[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Last OTP expired 2020-04-17 18:29:43
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Found 1 registered OTP token (TOTP)
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Requested login factors: LDAP & OTP
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] LDAP password Ok
[2020-04-17 18:50:45] [192.168.3.64] [OpenOTP:4JKBFJ4C] Authentication challenge required
[2020-04-17 18:50:46] [192.168.3.64] [OpenOTP:4JKBFJ4C] Sent push notification for token #1
[2020-04-17 18:50:46] [192.168.3.64] [OpenOTP:4JKBFJ4C] Waiting 27 seconds for mobile response
[2020-04-17 18:50:56] [192.168.3.56] [OpenOTP:4JKBFJ4C] Received mobile authentication response from
192.168.3.1
[2020-04-17 18:50:56] [192.168.3.56] [OpenOTP:4JKBFJ4C] > Session: cupcbM2KWdmcAxjF
[2020-04-17 18:50:56] [192.168.3.56] [OpenOTP:4JKBFJ4C] > Password: 16 Bytes
[2020-04-17 18:50:56] [192.168.3.56] [OpenOTP:4JKBFJ4C] Found authentication session started 2020-04-
17 18:50:45
[2020-04-17 18:50:56] [192.168.3.56] [OpenOTP:4JKBFJ4C] PUSH password Ok (token #1)
[2020-04-17 18:50:56] [192.168.3.64] [OpenOTP:4JKBFJ4C] Returning 6 RADIUS reply attributes
[2020-04-17 18:50:56] [192.168.3.64] [OpenOTP:4JKBFJ4C] Updated user data
[2020-04-17 18:50:56] [192.168.3.64] [OpenOTP:4JKBFJ4C] Sent login success response
```