Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

NetIQ

Radius

1. WebADM/OpenOTP/Radius Bridge

For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to WebADM Installation Guide and WebADM Manual to do it.

2. NetIQ Installation and Initial Configuration

- We used the NetIQ appliance version 4.3 downloaded from the Microfocus website (trial version).
- ISO file name: `AM_43_AccessManagerAppliance_Eval-0831.iso`
- It's SUSE Linux:

```
netiqam:~ # cat /etc/SuSE-release
SUSE Linux Enterprise Server 11 (x86_64)
VERSION = 11
PATCHLEVEL = 4
NetIQ Access Manager Appliance 4.3.0.0-391 (x86_64)
```

- NetIQ is a resource-hungry application, we used the following setup:
  - 2 Cores VM
  - 8 GB RAM
  - 50GB HD

  Even with this configuration, we received one warning about disk size (the minimum requirement is 100GB). *Lack of resources, especially RAM, can cause erratic behavior and failures to start.*
- NetIQ is configured during the initial boot of the VM, using all default values when possible.
- *Remember to take note of all configuration details.*
- The admin account DN for WebADM is: `cn=admin,o=novell`
- Our settings for the WebADM mount point:

Mount DN:	ou=netiq
Host Name(s):	192.168.3.221
Port Number:	636
Encryption Type:	SSL
Tree Base:	o=novell
Login DN:	cn=admin,o=novell
Login Password:	It's set during the inital setup.

3. Mount eDirectory on WebADM

- Create a container (e.g. an OU) - our one is called `netiq`.
- Create the mount point using:
  - The container as `Mount DN`.
  - `Login DN` set to “cn=admin,o=novell” (in our case).
  - The NetIQ specific details (see above table as an example).

- Extend the eDirectory schema (You must have write access to the LDAP schema to complete the operation).

- In the end, you should have the eDirectory mounted on WebADM.

4. Create a Local Domain

- Select the container used for the eDirectory mount point - in our case `netiq`.

5. Configure the User for Testing (in WebADM)

- Create a new user in WebADM within the eDirectory domain (in our case `netiq`).
- Activate the user in WebADM (this add WebADM attributes to the user in eDirectory).

- Setup the OTP features for the user.

- This is an example setup that can be customized based on specific needs.

- Register a soft token (we used RCDevs own mobile application).

6. Create the Radius Class in NetIQ

From the Dashboard, go to Devices -> Identity Servers and select the entry (in our case there is only one, IDP-Cluster).

Under the tab Local, perform all of the following subtab configurations:

- “Classes”
- “Methods”
- “Contracts”
- “Defaults”

Classes

Use the “Radius Class” Java class with the following Java classpath:

“com.novell.nidp.authentication.local.RadiusClass”

In the second page, add details of the server running the Radius Bridge daemon (normally the same server running WebADM). Here we used the default values that you can find in `/opt/radiusd/conf/client.conf` (port and `Shared secret`).

Make sure the port (in this case 3001, the default), it's open between the NetIQ AM server and the WebADM/Radius server.

Methods

Create a new entry using the Radius class from the list in `Class`.

"Contracts"

Create a new entry adding the method for Radius in the bottom box from the list on the right.

Defaults

Create new entry selecting the Radius contract.

7. Update the NetIQ Configuration and Make Sure The Server Is Operational

Once you have created all the above entries, you need to update the server configuration in Server Health -> Health tab.

The update can take several minutes depending on your VM configuration and in our limited experience sometimes it might be necessary to restart the entire system.

Login as root to the VM and execute:

```
netiq:/etc/init.d # ./novell-appliance restart
```

Repeat the "Update from server" and "Refresh" until it gets green or investigates what went wrong.

8. Test User Login

- To test the user login I used the default NetIQ portal app. In our case, that's `https://netiq.test.com/portal/` (netiq.test.com resolves to the local IP address of the NetIQ VM).
- Please keep in mind that the password is authenticated by NetIQ/eDirectory, while the token is authenticated by OpenOTP via Radius.

9. WebADM Log Entries

This is the log entry of a failed login where I provided the wrong OTP.

```
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] New openotpSimpleLogin SOAP
request
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Username: test02
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Password: xxxxxxx
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Client ID: 192.168.3.221
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Options: RADIUS,-U2F
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Enforcing client policy: netiq
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Registered openotpSimpleLogin
request
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Resolved LDAP user:
cn=test02,ou=netiq
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Started transaction lock for
user
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found user language: EN
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found 37 user settings:
LoginMode=OTP,OTPType=TOKEN,OTPFallback=DISABLED,OTPLength=6,ChallengeMode=Yes,Challenge1
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=S

[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found 5 user data:
LoginCount,LastOTP,TokenType,TokenKey,TokenState
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Last OTP expired 2017-06-13
14:48:21
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found 1 registered OTP token
(TOTP)
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Requested login factors: OTP
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Wrong TOTP password (token #1)
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Updated user data
[2017-06-13 14:48:36] [192.168.3.108] [OpenOTP:UJM5WOBB] Sent failure response
```

This is the log of a successful login:

```
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] New openotpSimpleLogin SOAP
request
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Username: test02
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Password: xxxxxx
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Client ID: 192.168.3.221
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Options: RADIUS,-U2F
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Enforcing client policy: netiq
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Registered openotpSimpleLogin
request
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Resolved LDAP user:
cn=test02,ou=netiq
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Started transaction lock for
user
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found user language: EN
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found 37 user settings:
LoginMode=OTP,OTPType=TOKEN,OTPFallback=DISABLED,OTPLength=6,ChallengeMode=Yes,Challenge1
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=S

[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found 7 user data:
LoginCount,RejectCount,LastOTP,TokenType,TokenKey,TokenState,TokenOffset
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Last OTP expired 2017-06-13
11:59:12
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found 1 registered OTP token
(TOTP)
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Requested login factors: OTP
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] TOTP password Ok (token #1)
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Updated user data
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Sent success response
```

› Example of a failed login - notice the token value (from the Radius bridge log). Please note that “User-Password” is actually the content of the token field, as the actual password is authenticated directly by NetIQ and unknown to OpenOTP.

```
rad_recv: Access-Request packet from host 192.168.3.221 port 34761, id=6, length=48
User-Name = "susanred"
User-Password = "wrong"
# Executing section authorize from file /opt/radiusd/conf/radiusd.conf
+group authorize {
[pap] WARNING! No "known good" password found for the user.  Authentication may fail
because of this.
++[pap] = noop
++[openotp] = ok
+} # group authorize = ok
Found Auth-Type = openotp
# Executing group from file /opt/radiusd/conf/radiusd.conf
+group authenticate {
rlm_openotp: Sending openotpSimpleLogin request
rlm_openotp: OpenOTP Authentication failed
rlm_openotp: Reply message: Invalid username or password
rlm_openotp: Sending Access-Reject
++[openotp] = reject
+} # group authenticate = reject
Failed to authenticate the user.
Login incorrect: [susanred] (from client any port 0)
Using Post-Auth-Type Reject
WARNING: Unknown value specified for Post-Auth-Type.  Cannot perform requested action.
Sending Access-Reject of id 6 to 192.168.3.221 port 34761
Reply-Message = "Invalid username or password"
Finished request 2.
Going to the next request
Waking up in 9.9 seconds.
Cleaning up request 2 ID 6 with timestamp +686
```