

NETIQ

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security. WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

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

Limited Warranty - Copyright (c) 2010-2024 RCDevs Security SA. All Rights Reserved.

Mountpoints Multi-Domain Novell

1. Overview

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).

A DeerLDAP (E)	Web Enterprise Edition v1.5.11-1				APIC
11 () chites(2)	# Home Admin Create Search Import Databases Applications	About Logout			
H 🚳 dor-UnixUsers H 🚳 dor-WebADM		05	ect Settings for cn=netle_dc=MountPoints_dc=WebADM		
H () do-myDomainLDAP		Disable Mount Point	🔿 Yes 🕤 No (default)		
H 🕑 onmyOrganization		Mount ON	ou=netiq	Select	
H ar outfractosAD		The LDAP tree node whe	re to mount the remote LDAP.		
Create / Search		2 Host Name(s)	192.160.3.221		
Provide / Check		LDAP server name(s) or You can set a comma-se	IP address(es) paraled list of servers. The next servers are used for fallover.		
		2 Part Number	636		
		LDAP server port.			
		2 Encruption Type	551. 1		
		7 Tree Base	o-novel		
		Mounted LDAP tree base			
		D Login DN	on-admin,o-novel		
		Mounted LDAP bind DN.	WebADM will bind anonymously if not set.		
		Login Password			
		Trusted CA Certificate		68	
		Client Certificate File		6.01	
		Client Certificate Key File		0.00	
			Asso: Reset		

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

DAP Server (OpenLDAP)	Web Enter	prise Edition v1.5.11-1					mo ma
nLDAP (8)	Dopyright © 2010-2017 Rd	CDeve SA, Al Rights Researed				$= \sqrt{\lambda}$	The sea
dc+UnixUsers	# Home Admin 0	zreate Search Import Databases	Apprecisions About Logout				
do-WebADM			Object o	o piteneus			
do-myDomainLDAP	LDAP Actions	Object Details					
ormyOrganization	Delete this object O1 Copy this object	Object class(es): Organization Mountpoint object: eDirectory					
ou-FrancoisAD	LExport to LDIF	Server type: Novell (SSL)					
ournelig (20)	Add permissions	Server infos: [Details] [Schema] Schema extended: No [Extend]					
cn=DNS AG resig test com	C Standard edit mode	1					
cn=IP AG 192.168.3.221	 Crease child object View child objects 						
an=LDAP Group - netig	± Export subtree						
an=LDAP Server - netig	Object Name	/			antia		
cn+NAM-RP-Certificate - n	Add Amily to (115)				netig		He
CT=SAS Service - netic	200 Aut 000 (110)				Accountbalance		1
cn=SSL CertificateONS - n	Permissions				2#entry#o=novel#login	Script	
an-admin	face varies! foesers struc	pune]			RO Entry on loginScript fo	r pinovel)	
cn=admin-console - netig					2#entry#o=novel#print	JobConfiguration	
cnitation					32#subtree#on=netio,o	-novell#[All Attributes Right	15]
🙀 cn=devman - netig					RW Subtree on All Attribu	tes Rights for cometiq.onnove	
on=netia					16#subtree#cn=netio.o	-novel#(Entry Rights)	
chanetic-PS	Detectintruder				The of	IN AN CONTRACTOR OF	
cn-netia test.com - netia	[delete attribute]				TRUE		
our-accessManagerContainer	[delete attribute]	2010			1800		
ou=policyviewusers	Loginintzuderlimit [delete attribute]				7		
reate / Search etails / Check	Organization				novell		
a / Search	[add values] Objectclass						
	Jan Jan Barrison Ba				organization		
					ndsloginproperties		
					ndscontainerioginprope	rties	
					top		
DAP Server (OpenLDAP)	2 Wet	Contraction	v1.5.11-1				
DAP Server (OpenLDAP) enLDAP (8)	C Wet	1996 Enterprise Edition Ight © 2010-2017 RCDuve DA, Al Rights	1 v1.5.11-1				
DAP Server (OpenLDAP) enLDAP (8) on=test01	Copyrt Wet	Mill Enterprise Edition	v1.5.11-1 Reserved	cations About	Logout		
DAP Server (OpenLDAP) enLDAP (8) cn=156801 2 dc=UntAppen	Copyr Web	o 2014 Enterprise Edition gir 0 2010-2017 RODws DA, All Rufes me Admin Create Search	v1.5.11-1 Import Databases Applic	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) entest01 declutikUsers decWebADM	C Wet	ne Admin Create Search	v1.5.11-1 Reserved Import Databases Applic	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) on=test01 des:UnixUsers des:WebADM des:myDomainLDAP	Cover Wet Her Adding	attribute 'webedmeetings' Success	v VI.5.11-1 Reserved Import Databases Applic	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) cnitest01 de=UnixUsers de=UnixUsers de=WebADM de=myDomainLDAP c=Root (3)	Correct Correct Correct Adding Adding Adding	Admin Create Search Admin Create Search artribute Webdamsettings' Success artribute Webdamdate' Success artribute Webdamdate'	VI.5.11-1 Newrod Import Databases Applic	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) dc=UnixUsens dc=UnixUsens dc=WebADM dc=myDomainLDAP peRost (3) ensemin	Correct Correct Correct Correct Adding Addin	Admin Create Search Admin Create Search artribute webadmsettings" Success artribute webadmsettings" Success objectclass webadmsecourf Success	ess	cations About	Lagout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) gn=test01 dc=UnixUsens dc=WebADM dc=myDomainLDAP seRoot (3) gc=somin gc=sopolicy	Correct Correc	attribute webadmsettings' Success attribute webadmsettings' Success attribute webadmsettings' Success attribute webadmsettings' Success objectclass webadmspet' Success objectclass webadmsproup' Success	ess	cations About	Lagout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) cn=test01 dc=UnixUsens dc=WebADM dc=myDomainLDAP peRoof (3) cn=soffic	Corr Re Hor Adding Adding Adding	attribute webadmaettings" Success attribute webadmaettings" Success attribute webadmaettings" Success attribute webadmaeton" Success objectclass webadmaecourf Success objectclass webadmaecourf Success objectclass webadmaecourf Success	ess s	cations About	Lagout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) on:test01 do:UnixUsers do:WebADM dc:myDomainLDAP gc:myDomainLDAP gc:seradmin compositor cnost of Search Dostals / Search Dostals / Search	Com Adding Adding Adding Adding	attribute (vebadmsettings' Success attribute (vebadmsettings' Success attribute (vebadmsettings' Success attribute (vebadmsettings' Success objectclass (vebadmscourf Success objectclass (vebadmscourf Success objectclass (vebadmscourf Success)	v v1.5.11-1 Reserved Import Databases Applic ess is is	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) on-test01 doc-UnixUsers doc-WebADM docmyDomainLDAP enRost (3) enropolicy crost of Search Details / Check enryOrganization	Com Adding Adding Adding Adding	attribute (vebadmsettings' Success attribute (vebadmsettings' Success attribute (vebadmsettings' Success attribute (vebadmdetta' Success objectclass (vebadmcourf Success objectclass (vebadmgroup' Success objectclass (vebadmgroup' Success	v v1.5.11-1 Reserved Import Databases Applic ess is is	cations About	Logout		LDAP Schema Setup
DAP Server.(OpenLDAP) enLDAP (8) smitest01 dcs:Unkulsers dcs:WebADM dcs:myDomainLDAP serRed:(3) ser	Copyr R Hor Adding Adding Adding	attribute webadmsettings" Success attribute webadmsettings" Success attribute webadmsettings" Success objectclass webadmccourt" Success objectclass webadmorouf" Success objectclass webadmorouf" Success	ess s	cations About	Logout		LDAP Schema Setup Ok
DAP Server (OpenLDAP) anLDAP (8) smitest01 d deutricklaers d deutricklaers d deutricklaers d deutricklaers d deutricklaers d deutricklaers d deutricklaers smitest01 d d d d d d d d d d d d d d d d d d d	Copyring Adding Adding Adding Adding	Admin Create Search Admin Create Search Admin Create Search attribute webadmsettings" Success attribute webadmsettings" Success attribute webadmsettings" Success objectclass webadmsetting" Success objectclass webadmgroup" Success objectclass webadmgroup" Success	vv1.5.11-1 Reserved Import Databases Applic	cations About	Logout		LDAP Schema Setup Ok
DAP Server.(OpenLDAP) InLDAP (8) onsteat01 decUnixUsers dedWebADM decmyOpenainLDAP orBoot (3) setSoot	Copyr R Hor Adding Adding Adding	Create Edition Create Search Admin Create Search artribute webadmsettings"Success artribute webadmsettings"Success objectclass webadmsecourfSuccess objectclass webadmgroup'Success	ess	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) onitest01 de=UnixUsers de=WebADM de=WybADM de=myDemainLDAP o=Root (3) for endomin for endomin	Copyring Adding Adding Adding	Admin Create Search Admin Create Search artribute veobadmaettings"Success artribute veobadmatrings"Success objectclass veobadmaccourfSuccess objectclass veobadmgroup"Success objectclass veobadmgroup"Success	ess	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) omiten01, de=UnixUsers de=WebADM de=myDomainLDAP oeRoot (3) cneeRoot (3)	Copy Adding Adding Adding	attribute (vebadmaetilings) Success attribute (vebadmaetilings) Success attribute (vebadmaetilings) Success attribute (vebadmgre) Success objectclass (vebadmgroup) Success objectclass (vebadmgroup) Success objectclass (vebadmgroup) Success	v v1.5.11-1 Reserved Import Databases Apple	cations About	Lagout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) onitee01 deciUnitUsers deciWebADM decimyDomainLDAP oeRoot (3) conspolicy	Copy Re Hor Adding Adding Adding	attribute webadmsettings" Success attribute webadmsettings" Success attribute webadmsettings" Success attribute webadmsettings" Success objectclass webadmsecourf Success objectclass webadmgroup" Success objectclass webadmgroup" Success	vv1.5.11-1 Reserved Import Databases Applic ess is	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) on=test01 de=UnixUsers de=WebADM de=myDemainLDAP or:Root (3) creation / Create / Search Details / Check or:myOrganization ou:=nelss (20) created / Search Details / Check ou:=nelss (20) created / Search ou:=nelss (20) created / Defa Search ou:	Copyring Adding Adding Adding Adding	Control Contro Control Control Control Control Control Control Control Control Co	v v1.5.11-1 Received Import Databases Applie ess is is	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) onstess01 dc=UnixUsers dc=WebADM dc=UnixUsers dc=WebADM dc=UnixUsers dc=WebADM dc=UnixUsers dc=WebADM dc=UnixUsers dc=WebADM dc=UnixUsers compOrt serson gc=nedmin gc=nedmin gc=nedmin create / Search Details / Check our=PrancoisAD our=nedig (20) gc=nelty_Server - netig gc=neltp_Server - netig gc=neltp_Server - netig gc=netigADP Server - netig gc=netigADP Server - netig gc=netigADP Server - netig	Copyring Adding Adding Adding	Create Edition Admin Create Search Admin Create Search artribute webadmsettings"Success artribute webadmsettings"Success artribute webadmsettings"Success objectclass webadmsetting"Success objectclass webadmgroup"Success objectclass webadmgroup"Success	ess	cations About	Legout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) onstest01 dc=UnixUsers dc=WebADM dc=WebADM dc=myOpensinLDAP o=Root (3) sensotian onspoticy create / Search Details / Check o=myOrganization ou=FrancoisAD ou=InKS AG netig test.com onsIP AG 192.1863.3221 cn=IDAP Group - netig cn=IDAP Server - netig	Copyring Adding Adding Adding	Create Edition Admin Create Search Admin Create Search artribute webadmsettings" Success artribute webadmdate" Success artribute webadmdate" Success objectclass webadmsettings" Success objectclass webadmgroup" Success objectclass webadmgroup" Success	ess s	cations About	Logout		LDAP Schema Setup
DAP. Server. (OpenLDAP) InLDAP. (8) onstest01 dc=UnixUsens dc=WebADM dc=myOpenainLDAP o=Boot. (3) setting onsetti	Copyring Adding Adding Adding	Create Edition Galactic Create Search Admin Create Search antribute webadmsettings"Success antribute webadmsettings"Success objectclass webadmsettingSuccess objectclass webadmsettingSuccess objectclass webadmsettingSuccess	ess s	cations About	Logout		LDAP Schema Setup
DAP. Server. (OpenLDAP) InLDAP. (8) on:teorol. dc:UnixUsers dc:WebADM dc:myDomainLDAP oeRoot.(3) created ormotic create / Search Details / Check oermyOrganization ou=FrancoisAQ ou=netis. on:ENS.AG.netig.test.com om:PAG.192.188.3.221 on:EDAP. Group - netig on:EDAP. Group - netig on:EAS. Service - netig	Copy Adding Adding Adding	Admin Create Search Admin Create Search artribute veobadmaettings" Success artribute veobadmaettings" Success objectclass veobadmgtor" Success objectclass veobadmgroup" Success objectclass veobadmgroup" Success	v v1.5.11-1 Reserved Import Databases Apple	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) InLDAP (8) onitem01 desUnixUsers desWebADM desmyDomainLDAP oeReot (3) consection con	Copy Adding Adding Adding	attribute (vebadmsettings" Success attribute (vebadmsettings" Success attribute (vebadmsettings" Success attribute (vebadmsettings" Success objectclass (vebadmsettings" Success objectclass (vebadmsettings" Success objectclass (vebadmsettings" Success objectclass (vebadmsettings" Success objectclass (vebadmsettings" Success	v v1.5.11-1 Reserved Import Databases Apple	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) anLDAP (8) cnitee01 desUnitVisers desWebADM desWebADM desmyDomainLDAP seRoot (3) cnitee01 create / Search Destis / Check semyOrganization ourFrancoisAD ournetig (20) cnito AG resig Jest.com cnitDAP Group - netig cnitDAP Group - netig cnitSAS Service - netig cnitSAS Service - netig cnitSAS Service - netig cnitSAS Service - netig conitSAS Service - netig	Copyr R Hor Adding Adding Adding	attribute (vebadmaettings) Success attribute (vebadmaettings) Success attribute (vebadmaettings) Success attribute (vebadmaettings) Success attribute (vebadmaettings) Success objectclass (vebadmaecour) Success objectclass (vebadmgroup) Success objectclass (vebadmgroup) Success	v v1.5.11-1 Reserved Import Databases Apple ess s	cations About	Logout		LDAP Schema Setup
DAP Server. (OpenLDAP) anLDAP (8) cn=test01 de=UnixUsers de=WebADM de=myDomainLDAP oreRoot (3) cn=stort create / Search Details / Check ormyOrganization ou=FrancoisAD outlins / Check ormyOrganization outlins / Check outlins / Check ormyOrganization outlins / Check outlins / Check	Copy R Hor Adding Adding Adding	Create Search Create Search Admin Create Search artribute webadmsettings"Success artribute webadmsettings"Success artribute webadmsettings"Success objectclass webadmsetting"Success objectclass webadmsetting"Success objectclass webadmsettings"Success objectclass webadmsettings"Success objectclass webadmsettings"Success objectclass webadmsettings"Success	vv1.5.11-1 Reserved Import Databases Apple ees s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) anLDAP (8) cnitest01 declinicklases declinicklases declinicklases declinicklases declinicklases declinicklases declinicklases declinicklases cnitest01 cnitest01 cnitest01 cnitest01 cnitest01 declinicklases declinicklases declinicklas	Copy R Hor Adding Adding Adding	Create Search Create Search Admin Create Search artribute webadmsettings Success artribute webadmdatar Success artribute webadmdatar Success objectclass webadmdarg Success objectclass webadmgroup' Success objectclass webadmgroup' Success	ess s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) anLDAP (8) cmitest01 decUnixUsers decWebADM decmyDomainLDAP serBot (3) cmisof created (3) created (3) cr	Copy R Hor Adding Adding Adding	Create Edition Galactic Create Search Admin Create Search artribute webadmsettings"Success artribute webadmsettings"Success artribute webadmsettings"Success objectclass webadmsettings"Success objectclass webadmsettings"Success	s v1.5.11-1 Reserved Import Databases Apple s s s s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) anLDAP (8) cmiten01 decUnixUsers decimyDomainLDAP decomyDomainLDAP de	Copy If Hor Adding Adding Adding	Admin Create Search Admin Create Search artribute \webadmsettings'Success artribute \webadmsettings'Success artribute \webadmsettings'Success objectclass \webadmsettings'Success objectclass \webadmgroup'Success	v v1.5.11-1 Records Import Databases Apple ess is is	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) anLDAP (8) cmitest01 desUniteUsers desWebADM desmyDomainLDAP geneyOpenainLDAP geneyOpenainLDAP geneyOrganization gen	Copy Adding Adding Adding	attribute (vebadmaetlings" Success attribute (vebadmaetlings" Success attribute (vebadmaetlings" Success attribute (vebadmaetlings" Success attribute (vebadmaetlings" Success attribute (vebadmaetlings" Success attribute (vebadmaetlings" Success objectclass (vebadmaetlings" Success objectclass (vebadmaetlings" Success objectclass (vebadmaetlings" Success objectclass (vebadmaetlings) Success objectclass (vebadma	v v1.5.11-1 Received Import Databases Apple ess is is	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) cnitest01 desUnidusers desWebADM desmyDomainLDAP serRed (3) composity create / Search Details / Check semyOrganization cuenting (20) create / Search Details / Check semyOrganization cuenting (20) create / Search Details / Check semyOrganization cuenting (20) comeDNS AG netig test.com comENS AG netig test.com com comENS AG netig test.com com	Copy Adding Adding Adding Adding	Admin Create Search Admin Create Search arribute webadmsettings"Success arribute webadmsettings"Success arribute webadmsettings"Success arribute webadmgtor"Success arribute webadmgtorSuccess arribute webadmgtoreSuccess arribute webadmgtoreSu	vv1.5.11-1 Reserved Import Databases Apple ess s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) cnitest01 desUnidusers desWebADM desmyDomainLDAP serRod (3) genodin constant constan	Copy Adding Adding Adding Adding	Create Search Create Search Admin Create Search artribute webadmsettings"Success artribute webadmdata"Success artribute webadmdata"Success artrbute webadmgater"Success objectclass webadmgaroup"Success objectclass webadmgroup"Success objectclass webadmgroup"Success	ess s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) snitest01 desUnixUsers desWebADM desmyDomainLDAP seRed (3) genedic sered	Copy Rel Hor Adding Adding Adding	Create Search Create Search Admin Create Search artribute webadmsettings Success artribute webadmsettings Success artribute webadmsettings Success objectclass webadmsetting Success objectclass webadmsetting Success objectclass webadmsetting Success	ess s	cations About	Legout		LDAP Schema Setup
DAP Server.(OpenLDAP) enLDAP (8) cn=test01 dc=UnkUters dc=WebADM dc=myDomainLDAP geRoot (3) cnesdmin cnesdmin creater / Search Details / Check emyOrganization guErrancoisAD putnets (20) coniP AG 192.186.3.221 coniP AG 192.186.3.21 coniP AG 192.186.	Copy Ref. Hor Adding Adding Adding	Create Edition Galactic Create Search artribute webadmsettings"Success artribute webadmsettings"Success artribute webadmsettings"Success objectclass webadmsettings"Success objectclass webadmsettings"Success	ess s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) on:test1 de:UnivUsers de:WebADM de:myDomainLDAP de:myDomainLDAP de:myDomainLDAP eRGost (3) create / Search Details / Check emyQrganization du=FrancoisAD ou:netig (20) create / Search create / Sea	Copy If Hor Adding Adding Adding	Create Edition Create Search artribute \webadmsettings'Success artribute \webadmsettings'Success artribute \webadmsettings'Success objectclass \webadmsettings'Success objectclass \webadmgroup'Success	v v1.5.11-1 Records Import Databases Apple s s s s	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (8) on:test11 de:UnixUters de:WebADM de:myDomainLDAP de:myDomainLDAP de:myOpmainLDAP ensor(3) creater on:ppolicy cre	Copy If Hor Adding Adding Adding	Admin Create Search Admin Create Search artribute (vebadmsettings", Success artribute (vebadmsettings", Success artribute (vebadmsettings", Success objectclass (vebadmgtor), Success objectclass vebadmgtor), Succes objectclass vebadmgtor), Succes	v v1.5.11-1 Received Import Databases Apple ess is is	cations About	Logout		LDAP Schema Setup
DAP Server (OpenLDAP) enLDAP (6) entest11 destUnkUsers destwahDM destwahDM destwahDM destwahDM destwahDM destwahDM destwahChAP endest entest1 destwahChAP entest1 destwahChAP entest entesta entesta entesta destwahChAP entest entesta	Copy R Hor Adding Adding Adding	Admin Create Search Admin Create Search artribute webadmseetlings"Success artribute webadmseetlings"Success artribute webadmseetlings"Success artribute webadmseetlings"Success artribute webadmgroup"Success objectclass webadmseetlings"Success objectclass webadmseetlings"Success objectclass webadmgroup"Success objectclass webadmgroup"Success objectclass webadmseetlings"Success objectclass webadmseetlings	v v1.5.11-1 Received Import Databases Apple ess is is	cations About	Logout		LDAP Schema Setup

> 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 netig.

		Object Settings for cn=netig,dc=Domains,dc=WebADM	
	Disable Domain	🔿 Yes 💿 No (default)	
V	User Search Base	ou=netiq	Select
	The LDAP user searc	h base corresponding to the domain.	
0	Group Search Base		Select
	The LDAP group sear This setting is ignored Note: Defaults to the I	ch base corresponding to the domain. if WebADM uses only direct group_mode. User Search Base if not set.	
	Domain Name Aliase	9	
	Comma-separated lis	t of alternative domain names.	
		User Access Policy	
0	Allowed Groups		

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).



> Set up 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 the following sub tab configurations:

- * "Classes"
- > "Methods"
- * "Contracts"
- > "Defaults"

					- 11		_
NetIQ Acce from Micro Focus	ess Mar	nager					
Dashboard De	vices ~	Policies \sim	Security ~				
Identity Servers							
IDP-Cluster							
General Local	Liberty	SAML 1.1 SA	ML 2.0 WS Federation Bro	kering WS-Trust 0	Auth & OpenID Con	inect	
User Stores Class	es Methods	Contracts [efaults				
New Delete 1 Iter	n(s)						
Name	Type	Default					
SingleBoxUserStore	eDirectory	\mathbf{V}					

Classes

Use the "Radius Class" Java class with the following Java classpath:

``com.novell.nidp.authentication.local.RadiusClass"

III uhha 🚵 ou 🛆 ui	
NetIQ Access from Micro Focus	Manager
Dashboard Device	es v Policies v Security v
Identity Servers IDP-Cluster	•
Create Authenticati	on Class
Step 1 of 2: Specify na	me and java class.
Note: To enable Advan Display name: Java class:	ced Authentication classes, you must configure the Advanced Authentication server. myRadiusClass Radius Class
Java class path:	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).

← → C ▲ Not Secur	re https://n	etiqam.test.com:8443	/nps/servle	t/webacc		
👯 Apps 🔞 Git 🧕 AWS	Wiki 💧	support-questions	my_env	CHECK_THIS_OUT	Support	RumpUP
NetIQ Access N from Micro Focus	lanager					
Dashboard Devices ~	Policies	✓ Security ✓				
Identity Servers IDP-Cluster						
radius						
General Properties						
Servers						
New Delete 👔 🐺 1	Item(s)					
Server						
<u>192.168.3.108</u>						
Port:	3001 💌					
Shared secret:	•••••		- 4			
Reply time:	7000 💌	milliseconds				
Resend time:	2000 💌	milliseconds				
Failed server retry:	5	minutes				
JSP:						
User Lookup Attribute Name:	cn					
	🕗 Require pa	assword				

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.

NetIQ Acc from Micro Focus	cess Manager
Dashboard	Devices V Policies V Security V
Identity Servers IDF	P-Cluster 🕨
myRadiusMe	thod
Display name:	myRadiusMethod
Class:	myRadiusClass
	Identifies User
	Overwrite Temporary User
	Overwrite Real User
User stores:	Available user stores:
SingleBoxUserStor	e <default store="" user=""></default>
Properties	
New Delete 0	ltem(s)
Name Value	
No items	_

"Contracts"

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

NetIQ Access I	Manager
Dashboard Devices	✓ Policies ✓ Security ✓
Identity Servers IDP-Cluster	
Croste Authentication	Contract
Step 1 of 2: Configuration	
Display name:	myRadiusContract
URI:	ootn
Password expiration servlet:	
	Allow user interaction
Login Redirect URL:	https://www.google.com
	Allow user interaction
Authentication Level:	0
Authentication Timeout:	60 Minutes
Activity Realm(s):	
Satisfiable by a contract	of equal or higher level
Satisfiable by External Pr	rovider
Requested By	Do not specify
Allowable Class	
If you add more than one X5 Methods:	09 method, only the first one will be used and it will automatically be moved to the top of the list. Available methods:
myRadiusMethod	Name/Password - Basic Name/Password - Form Secure Name/Password - Basic Secure Name/Password - Form
1	

Net from M	IQ Access Manager
Dashb	ooard Devices V Policies V Security V
Identity Se	ervers 🕨 IDP-Cluster 🕨
Create	e Trusted Identity Provider
Step 2	of 2: Enter authentication card values
ID:	OTPRadius
Text:	OTP Radius:
Image:	Novell
	Show Card
	Passive Authentication Only

Defaults

Create new entry selecting the Radius contract.

	https://patigam.tast.com.0442/	lana laan dat	hushasa			
C - C A NOLS	ecure https://netigam.test.com.o443/	rips/servie	I/webacc	-		-
Apps 🞯 Git 🧃 AN	WS 🔮 Wiki 🦀 🗎 support-questions	my_env	CHECK_THIS_OUT	Support	RumpUP	AWS
NetIQ Access from Micro Focus	s Manager					
Dashboard Device	es v Policies v Security v					
Identity Servers						
IDP-Cluster						
General Local Li	harty SAMI 1 1 SAMI 2 0 WS Endorst	Inn Broker	ing WS Truct OAuth	& OpenID Cor	anort	
Liser Stores Classes Me	thods Contracts Defaults	IOIT (DIOKEI	ing (HS-HOSE (OAULI	a openio coi	meet (
Defaults						
User Store:	SingleBoxUserStore	0				
Authentication Contract:	radius	0				
Authentication Type	Default Contract					
Name Password:	<none></none>	0				
Secure Name Password:	<none></none>	0				
X509:	<none></none>	0				
Smart Card:	<none></none>	0				
Smart Card PKI:	<none></none>	0				
Token:	<none></none>	×.				

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.

Apps 🧔 Git 🚨 AWS 🌊 Wiki	📥 E	support-questions	my_env	CHECK_THIS_OUT	E Support	RumpUP	AWS4RCDEVS	demo_sw	1 t
NetIQ Access Manag	er								
Dashboard Devices v Poli	icies 🗸	Security V							
Servers 🕨 Health									
Server Health: 192.168.3.2	21								
General Health Alerts Comma	and Stat	us Statistics							
Refresh Update from Server									
Status Description									
Server is operational (Passed)									
Services Detail									
Туре	Status	Message							
Services	0	Identity Server Configurat	tion 🔻						
Identity Server Configuration	0	Fully applied							
Configuration Datastore	0	Operating properly							
User Datastores	0	Operating property							
	0	Signing key available ,Cer	tificate Subject	t Name = CN=netigam.test.c	om ,Validity in D	ays = 3649 🔻			
Signing, Encryption and SSL Connector Keys	0	This evaluation version w	ill expire on Th	nu, Aug 31, 2017.					
Signing, Encryption and SSL Connector Keys Evaluation Version									
Signing, Encryption and SSL Connector Keys Evaluation Version									
Signing, Encryption and SSL Connector Keys Evaluation Version									
Signing, Encryption and SSL Connector Keys Evaluation Version									
Signing, Encryption and SSL Connector Keys Evaluation Version									
Signing, Encryption and SSL Connector Keys Evaluation Version									
Signing, Encryption and SSL Connector Keys Evaluation Version									

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.

← → C A Not Secure https://netiqam.test.com/portal/users/main.jsp									
🔢 Apps 🔞 Git 🤱 AWS 🕵 Wiki 🝐 🗎 support-questions	my_env	CHECK_THIS_OUT	E Support	RumpUP	AWS4RCDEVS	🗎 demo_sw	🗎 tools	🗎 AWS	E pe

Application Overview

This is a sample application that demonstrates the basic functionalities of a NetlQ Access Manager.

The functionalities demonstrated are

- Role based access control policies.
 Automatically filling forms with authenticated user's attributes.

Roles & Users

This is a simple application which demonstrates key aspects of the Access Manager.

The NetlQ Access Manager default installation creates the following two users:

- Alice with username as alice and depicts both Manager and Employee role.
 Bob with username as bob and depicts Employee role.

You can login in this application with either of the users. The passwords of these users is "netiq".

You can view the demo by pressing the "login" in this page and follow the instructions. You can remove the portal before moving to production. Refer NetIQ Access Manager documentation on how to remove this portal.

		Access	s Manager			
	\equiv	Sign in to us	se available applic	ations		
			OpenOTPLogin			
		susanred				
		•••••				
		•••••		Ÿ ~		
		Sign in				
Access Manager			W metrog best point			evenue e
Your session has been sufferiticated.						

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: netig [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=netig [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,ChallengeTim 1:HOTP-SHA1-6:QN06-T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode= [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: netig [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=netig [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,ChallengeTim 1:HOTP-SHA1-6:QN06-T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode= [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

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved