How to install NetIQ Identity Manager 4.8 / eDirectory 9.2.2 in RHEL 8 / CentOS 8

15.02.25

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

How to install NetIQ Identity Manager 4.8 / eDirectory 9.2.2 in RHEL 8 / CentOS 8

Overview

This is a step by step checklist on how to install your eDirectory 9.2.2 and IDM 4.8 to a freshly installed RHEL 8. With CentOS 8 the drill is the same but with added install customization.

Remove firewalld and replace with iptables

I like to do this for better control.

```
dnf install iptables-services
dnf erase firewalld
systemctl enable iptables
vim /etc/sysconfig/iptables
```

Add your iptables rules such as

```
-A INPUT -m tcp -m multiport -p TCP --dports 22,80,389,524,636,443,8440 -s
<your IDM admin network> -j ACCEPT
```

Install required packages

```
dnf install libgcc*.i686 libnsl* libnsl*.i686 libncurses*
dnf install dnf-utils ksh gettext.x86_64 libXrender.i686 libXau.i686
libxcb.i686 libX11.i686 libXext.i686 libXi.i686 libXtst.i686 glibc-*.i686
libstdc++.x86_64 libgcc-*.i686 unzip bc lsof net-tools createrepo_c libXtst
```

Set other stuff

Network. Replace “ens123” with your interface name.

```
ip route add 224.0.0.0/4 dev ens123
```

Add following contents to the route file: /etc/sysconfig/network-scripts/route-ens123 :

```
ADDRESS0=224.0.0.0
NETMASK0=240.0.0.0
```

Add the right selinux context if you decide to try and go with it.

```
chcon --reference /etc/sysconfig/network-scripts/ifcfg-ens123
/etc/sysconfig/network-scripts/route-ens123
```

Set /etc/hosts

```
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
1.2.3.4     myidm1.domain.com
1.2.3.5     myidm2.domain.com
1.2.3.6     myidm3.domain.com
```

Set SELinux permissive and reboot. You may be able to make it work with SELinux set to enforcing but did not try with the latest versions of IDM/eDir. It did work with eDirectory 8.8.

Mount IDM iso and check the pre-requisites

```
mount -o loop Identity_Manager_4.8.1_Linux.iso /mnt/
/mnt/RHEL-Prerequisite.sh
```

Ignore the compat-libsrdc++-33 messages, they are no longer needed.

Install eDirectory

Unpack the latest full install eDirectory package. You will usually find the latest in dl.netiq.com patches but you need to check from the release notes if the package is a full install version or a patch only. Locate the latest full installer.

CentOS 8 install notes

Skip this topic if using RHEL.

CentOS custom RHEL server rpm

CentOS is an exact replica of RHEL with difference only in branding and support. You can use IDM /

eDirectory with CentOS 8 but your support options will be limited.

Install is using dnf repository with dependencies which look for a specific redhat-release-server package to identify RHEL system. With CentOS 8 you need to create an empty RPM package called redhat-release to indicate we're dealing with a redhat server. Create a file “redhat-release.spec” with following contents

```
Name:           redhat-release-server
Version:        8.1.1911
Release:        1%{?dist}
Summary:        RedHat Release Dummy Package

Group:          Networking/Daemons
License:        No Licence
URL:            http://www.mysite.com

%description
This is an empty dummy package to satisfy a dependency.

%files

%changelog
* Tue Jun 30 2020 Pekka K
- Initial release
```

Install rpmbuild, create package and install it.

```
dnf install rpm-build
rpmbuild -bb redhat-release.spec
dnf localinstall /root/rpmbuild/RPMS/x86_64/redhat-
release-8.1.1911-1.el8.x86_64.rpm
```

CentOS install script customization

Edit nds-install script and copy-paste line

```
"Red Hat Enterprise Linux Server") os=rhel;;
```

to line

```
"CentOS Linux") os=rhel;;
```

eDirectory install

Continue straight here without previous CentOS customizations if you are using RHEL.

Install eDirectory with command

```
./nds-install
```

In the first server configure a new tree with command (with dot notation)

```
ndsconfig new -t <treename> -n <ou=servers.ou=path> -a <cn=admin.ou=path>
```

In the replicas add the edirectory to the tree with command:

```
ndsconfig add -t <treename> -n <ou=servers.ou=path> -a <cn=admin.ou=path> -p
<server1 ip address>
```

Add eDirectory paths to your working environment at /etc/profile.d/edirectory.sh:

```
export PATH=/opt/novell/eDirectory/bin:/opt/novell/eDirectory/sbin:$PATH
export MANPATH=/opt/novell/man:/opt/novell/eDirectory/man:$MANPATH
export TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale
```

Activate the paths

```
. /etc/profile.d/edirectory.sh
```

Set /etc/opt/novell/eDirectory/conf/hosts.nds

```
TREENAME.
idm1    1.2.3.4
idm2    1.2.3.5
idm3    1.2.3.6
```

Link to /etc

```
ln -s /etc/opt/novell/eDirectory/conf/hosts.nds /etc/
```

Identity manager installation

If not mounted anymore do mount Identity Manager image and install with command

```
./install.sh
```

Select identity engine and iManager.

Configure IDM with command

```
./configure.sh
```

Select

- custom configuration
- configure identity manager engine
- set common password
- add to existing local machine identity vault
- install new driverset

At the slave servers go to install image mount directory and execute

```
./configure.sh
```

- custom configuration
- configure identity manager engine
- set common password
- add to existing local machine identity vault
- DO NOT install new driverset

Configure iManager

Create certificate for Apache. You can do better than this as this is just a self signer certificate.

```
openssl req -x509 -nodes -newkey rsa:4096 -keyout
/etc/pki/tls/private/idm1.domain.key -out /etc/pki/tls/certs/idm1.domain.crt
-days 3650
```

Install apache with ssl

```
dnf install httpd mod_ssl apr-util apr
```

Create AJP proxying to /etc/httpd/conf.d/imanager.conf

```
ServerName idm1.domain

SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite ALL:!aNULL:!eNULL:!SSLv2:!LOW:!EXP:!MD5:@STRENGTH
```

```
SSLCertificateFile /etc/pki/tls/certs/idm1.domain.crt
SSLCertificateKeyFile /etc/pki/tls/private/idm1.domain.key

ProxyPass /nps ajp://localhost:9009/nps
ProxyPassReverse /nps ajp://localhost:9009/nps

<Location "/nps>
    Options +FollowSymLinks
</Location>

<Location "/nps">
    Options MultiViews FollowSymLinks
    Order allow,deny
    Allow from all
</Location>

<Location "/nps/WEB-INF/">
    deny from all
</Location>

<Location "/nps/META-INF/">
    deny from all
</Location>
```

Fix certificate paths also to /etc/httpd/conf.d/ssl.conf

Check config and enable / start Apache

```
systemctl enable httpd
apachectl configtest
systemctl start httpd
```

Now log in to the tree with iManager and add all servers to the driver set.

Import to Designer

Now import the identity vault and driver set to Designer, add all the servers and start doing actual IDM work :)

Comments

All comments and corrections are welcome.