Linux Deployment Guide

How to deploy Network Shutdown Module for Linux

1 Contents

2 Introduction

This document discusses how to install the Schneider Electric Network Shutdown Module, version 3.06 on to modern Linux operating systems. It also discusses known issues and how to address them.

3 To Prepare your System for Install

Network Shutdown Module requires a few pre-requisites before installation can be attempted; these are given in Table 1. These packages are available to install through your operating system package manager. In order to ensure these packages are available to you, you may need to register your system with your OS vendor. See your Operating System documentation for details on receiving updated packages.

Depending on your system configuration, your package manager may install additional packages to satisfy the dependencies of these packages. Once these packages have been installed, Network Shutdown Module can be installed using the procedure documented in the User Guide.

Table 1 - Prerequisite Packages

Operating System	Architecture	Required Packages
RedHat 5.9	i386	compat-libstdc++-33
RedHat 5.9	x86_64	compat-libstdc++-33.i386
RedHat 6.4	i386	glibc gtk2 compat-libstdc++-33 libxml2 nss-softokn-freebl
RedHat 6.4	x86_64	glibc.i686 gtk2.i686 compat-libstdc++-33.i686 libxml2.i686 nss-softokn-freebl.i686
SUSE 11 SP3	i386	None
SUSE 11 SP3	x86_64	libstdc++33-32bit

3.1 RedHat 5.9 i386 Command

From the console as root, issue the following:

```
yum install compat-libstdc++-33
```

3.2 RedHat 5.9 x86_64 Command

From the console as root, issue the following:

```
yum install compat-libstdc++-33.i386
```

3.3 RedHat 6.4 i686 Command

From the console as root, issue the following:

```
yum install glibc gtk2 compat-libstdc++-33 libxml2 nss-softokn-freebl
```

3.4 RedHat 6.4 x86_64 Command

From the console as root, issue the following:

```
yum install glibc.i686 gtk2.i686 compat-libstdc++-33.i686 libxml2.i686 nss-softokn-freebl.i686
```

3.5 SuSE 11 SP3 x86_64 Command

From the console as root, issue the following:

```
zipper install libstdc++33-32bit
```

4 Known Issues

4.1 Installation and Removal Issues

4.1.1 Kdesu not found on path

Problem: When running the installer or uninstaller as a user, the following output is produced:

```
which: no kdesu in
(/home/bunsen/bin:/usr/local/bin:/usr/bin:/bin:/usr/bin/X11:/usr/X11R6/bin:/usr/games:/usr/
lib/mit/bin:/usr/lib/mit/sbin)

which: invalid option -- 'c'
```

Fix: These warnings can be safely ignored.

Problem: Running the uninstaller on SUSE Linux as a regular user prompts for the administrator password. Then the uninstaller fails to execute.

Fix: Run the uninstaller as the root user. Use “sudo su” or log in as root before attempting to execute the “nsmInstaller –uninstall” command.

4.1.2 Glib Errors/ Warnings

Problem: When running the installer or uninstaller as the root user, output similar to the following is produced:

```
(nsm_linux_3_06_04.run:26443): GLib-GObject-WARNING **: instance of invalid non-
instantiatable type `(null)'

(nsm_linux_3_06_04.run:26443): GLib-GObject-CRITICAL **:
g_signal_handlers_disconnect_matched: assertion `G_TYPE_CHECK_INSTANCE (instance)' failed

... other lines omitted.
```

Fix: These warnings can be safely ignored.

4.1.3 Close and Cancel buttons remain enabled during file installation.

Problem: The Close (x) and Cancel buttons remain enabled during the installation wizard as it copies files to the install path. Clicking on either of these will result in the installer aborting, before all files have been installed. This can result in failures of the uninstall process in cleanly removing all Network Shutdown Module related files.

Fix: Avoid clicking either the close or cancel button as files are being copied. Allow the installer to complete before attempting software removal.

4.1.4 Installer accepts a blank or root folder path.

Problem: The Network Shutdown Module will accept a blank install path, or a path consisting of the root directory. In both cases the installation path will be set to the root folder. Installation will proceed successfully. On uninstall, there is a risk of deleting system files unrelated to Network Shutdown Module, as the uninstaller attempts to delete all files and subdirectories under the installation path.

Fix: Ensure a subdirectory path is specified for Network Shutdown Module.

4.2 PHP Issues

Network Shutdown Module 3.06 uses PHP 5.2.8.

4.2.1 PHP 5.2.8 Multiple Vulnerabilities

Network Shutdown Module uses a version of PHP that is affected by multiple flaws:

- PHP 5.2.8 is no longer actively supported by the PHP project.
- PHP versions earlier than 5.2.11 are affected by multiple flaws.
- Multiple Cross Site Scripting Vulnerabilities.
- Multiple Cookie Injection Scripting Vulnerabilities.
- Multiple HTML Injection Vulnerabilities
- Multiple Cross Site Request Forgery Vulnerabilities.

Fix: Restrict access to the application. Once configuration has been completed, turn off the web server, as outlined in section 5.1.

4.2.2 Phpinfo.php Information Disclosure

Problem: The following file calls the function phpinfo() which discloses potentially sensitive information to a remote attacker:

../MGE/NetworkShutdownModule/www/phpinfo.php

Fix: This file can safely be deleted.

4.3 Lighttpd Issues

Network Shutdown Module 3.06 uses Lighttpd 1.4.11 as its web server.

4.3.1 Lighttpd 1.4.11 Multiple Vulnerabilities

Network Shutdown Module uses a version of Lighttpd that is affected by multiple flaws:

- Lighttpd 'mod_userdir' case sensitive comparison security bypass vulnerability.
- Lighttpd trailing slash information disclosure.
- Lighttpd slow request handling remote denial of service vulnerability.

Fix: Once configuration has been completed, turn off the web server, as outlined in section 5.1.

4.4 Secure Socket Layer (SSL) Issues

Network Shutdown Module 3.06 uses OpenSSL 0.9.7e to provide encryption services.

4.4.1 SSL Certificate Cannot Be Trusted

Problem: Network Shutdown Module installs a self-signed certificate. Self signed certificates can provide encryption for HTTPS traffic, but cannot be used to verify the authenticity of the remote host, so are open to man in the middle attacks.

Fix: Replace the default certificate with a trusted certificate, as outlined in section 5.2.

4.4.2 Check for SSL Weak Ciphers

Problem: Network Shutdown Module supports the following relatively weak ciphers:

- SSL2_RC4_128_EXPORT40_WITH_MD5 : SSL_EXPORT
- SSL2_RC2_CBC_128_CBC_EXPORT40_WITH_MD5 : SSL_EXPORT
- SSL3_RSA_EXPORT1024_WITH_RC4_56_MD5 : SSL_EXPORT
- SSL3_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 : SSL_EXPORT
- SSL3_RSA_EXPORT1024_WITH_DES_CBC_SHA : SSL_EXPORT
- TLS1_RSA_EXPORT1024_WITH_RC4_56_MD5 : SSL_EXPORT
- TLS1_RSA_EXPORT1024_WITH_RC2_CBC_56_MD5 : SSL_EXPORT
- TLS1_RSA_EXPORT1024_WITH_DES_CBC_SHA : SSL_EXPORT

Fix: Once configuration has been completed, turn off the web server, as outlined in section 5.1.

4.5 Application Issues

4.5.1 The Upgrade Check reports that the Upgrade URL is Unreachable.

Problem: The Network Shutdown Module upgrade check page reports that the "Upgrade URL is unreachable".

Fix: Edit the <install path>/www/libs/upgrade.inc PHP file, and replace line 26 with:

```
$autoUpgradeCheckVersionURL =
"http://soft.apc.com/download/soft/install/$osType/nsm/nsmUpgradeVersion";
```

Refreshing the Upgrade Check page should show if an upgrade is available.

4.5.2 Shutdown Delays are not respected.

Problem: The "Shutdown After" and "Shutdown Duration" values specified in the Central Shutdown Configuration of the Network Management Card are not respected by the Network Shutdown Module. For example, specifying a Shutdown After value of 3 minutes, one would expect when Utility Failure occurs, it must persist for at least 3 minutes before the attached Network Shutdown Module would begin the shutdown procedure. For Network Shutdown Module 3.06, an issue exists where these values are not respected, and shutdown will occur immediately after the UPS event occurs.

There is no fix or workaround available at this time.

5 Workarounds

5.1 Turn Off the Web Server

To allow the Network Shutdown Module Web Server to be enabled or disabled separately, use the procedure documented in the following subsections.

Please Note: When the web server is stopped, the system tray icon will not receive updates, and will show the status, "localhost: unreachable". This can safely be ignored. The system tray icon will begin receiving updates the next time the web server is enabled.

5.1.1 Stop Network Shutdown Module

As the root user, issue the following command:

```
# service mge-nsm stop
```

5.1.2 Create a Service Configuration File

Create a configuration file called /etc/NSM3.conf with the following contents:

```
# Service Configuration for Network Shutdown Module 3.06


# The Network Shutdown Module Web Server is responsible for presenting the user
# interface.  Disabling the web server will prevent configuration changes to
# Network Shutdown Module.
#
# To disable the web server, comment this line, or set to false.
ENABLE_WEBSERVER=true


# !!! WARNING !!!
# The Data Acquisition Engine (DAE) monitors the UPS status and initiates shut
# down based on the events configured at the user interface.  Disabling the DAE
```

```
# will leave your server unprotected.
#
# To disable the Data Acquisition Engine, comment this line, or set to false.
ENABLE_DAE=true
```

This configuration enables both the Web Server and the Data Acquisition Engine. To disable a service, comment the line by placing a hash ('#') in front of it, or set the value from true to false.

5.1.3 Replace the Service Startup Script.

Replace the /etc/init.d/mge-nsm script, with the following contents:

```
#! /bin/sh
#############################################################################
# LSB compatible init script for the MGE UPS SYSTEMS - Network Shutdown Module #
#############################################################################

### BEGIN INIT INFO
# Provides:          mge-nsm
# Required-Start:    $network
# Should-Start:
# Required-Stop:
# Should-Stop:
# Default-Start:     3 5
# Default-Stop:      0 1 6
# Short-Description: MGE UPS Systems - Network Shutdown Module
# Description:       Network Shutdown Module provide power
# protection to your computer
### END INIT INFO

set -e

source /etc/NSM3.conf

DESC="Network Shutdown Module"
MGE_NSM_HOME="`cat /etc/NSM3_path`"
```

```
WEBSVR_PID_PATH="${MGE_NSM_HOME}/bin/webserver/logs/lighttpd.pid"
DAE_PID_PATH="${MGE_NSM_HOME}/bin/dae/mgeDAE.pid"

# Update the needed environment variables
LD_LIBRARY_PATH=$MGE_NSM_HOME/lib:$MGE_NSM_HOME/bin/webserver/bin:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH MGE_NSM_HOME

daemon_start() {
  if [ ! -z ${MGE_NSM_HOME} ];
  then
    if [ "$ENABLE_WEBSERVER" = "true" ]; then
           # Start the webserver
           cd ${MGE_NSM_HOME}/bin/webserver/bin
           ./lighttpd -f ../conf/lighttpd.conf -m ./
    fi

    if [ "$ENABLE_DAE" = "true" ]; then
           # Start the Data Acquisition Engine
           cd ${MGE_NSM_HOME}/bin/dae
           ./mgeDAE -start
    fi
  fi
}

daemon_stop() {
  # Stop the webserver
  [ -f ${WEBSVR_PID_PATH} ] && kill `cat ${WEBSVR_PID_PATH}` 2>/dev/null

  # Stop the Data Acquisition Engine
  cd ${MGE_NSM_HOME}/bin/dae
  ./mgeDAE -stop
```

```
  # workaround for hard stop
#  sleep 2 && killall -9 mgeDAE  2>&1 1>/dev/null
}


case "$1" in
  start)
#    echo "Starting $DESC."
    daemon_start
    ;;
  stop)
#    echo "Stopping $DESC."
    daemon_stop
    ;;
  restart)
#    echo "Restarting $DESC."
    daemon_stop
    sleep 2
    daemon_start
    ;;
  *)
    echo "$DESC:"
    echo "Usage: $0 {start|stop|restart}" >&2
    exit 3
    ;;
esac


exit 0
```

5.1.4 Restart the NSM Service(s)

Issue the following command:

```
# service mge-nsm start
```

Depending on the configuration given in the /etc/NSM3.conf, the new startup script will selectively start the enabled services.

5.2 Replace the HTTPS Certificate

To replace the self-signed certificate with one signed by a trusted Certificate Authority, use the following procedure.

In this process we will use the following file names for the various files needed (you may change these as you wish):

- server.key: A private key file.
- server.csr: A certificate signing request file.
- server.crt: The web server certificate file.
- intermediate.crt: The CA provided intermediate certificate trust path.

5.2.1 Generate a Private Key.

Begin by creating a private key file, using openssl as shown here:

```
# openssl genrsa -out server.key 2048

 Generating RSA private key, 2048 bit long modulus

 ..................................++++++

 ..................................................++++++

 e is 73547 (0x01001)
```

5.2.2 Create an OpenSSL configuration file.

Save the following to a file called openssl.cnf. Replace values in braces with values appropriate to your location and server.

```
[req]

default_bits=2048

default_keyfile=server.key

distinguished_name=req_distinguished_name

prompt=no


[req_distinguished_name]

C={ISO3166 two character country code}

ST={state or province}

L={Locality; generally – city}

O={Organisation – Company Name}

OU={Organisation Unit – typically certificate type or brand}

CN={Common Name – typically the fully qualified local host name}
```

```
emailAddress={optional email address, remove this line if unused}
```

5.2.3 Generate a Certificate Signing Request.

Create a certificate Signing Request (server.csr) file using openssl as shown here:

```
# openssl req -new -key server.key -out server.csr -config openssl.cnf
```

No output is given unless an error occurs. All going well, the server.csr file will be created based on the values given in the openssl.cnf file.

5.2.4 Purchase a Valid SSL Certificate

Details may vary here as you interact with your trusted Certificate Authority and how they produce certificates. Typically they will ask for the contents of the server.csr file and using this they will produce a server certificate (server.crt) file for you. Save this file to the server host.

When asked which type of certificate to produce, choose that which is appropriate for ApacheSSL/mod_ssl, which Network Shutdown Module is compatible with.

Your Certificate Authority will also make available an intermediate CA bundle, which contains any root and intermediate certificates needed to authenticate your new certificate. Save this file also to the server host, (e.g. intermediate.crt).

5.2.5 Configure Lighttpd to use the new Certificate.

Copy the server.key, server.crt, and intermediate.crt files to /usr/local/MGE/NetworkShutdownModule/bin/webserver/bin, or to your custom install path.

Concatenate the server.key and newly created server.crt file together (the order is not important).

```
# cat server.key server.crt > server.pem
```

For added security, change the owner and permissions for these files to root:

```
# chown root:root *.pem *.key *.csr *.crt

# chmod 600 *.pem *.key *.csr *.crt
```

Edit /usr/local/MGE/NetworkShutdownModule/bin/webserver/conf/lighttpd.conf and modify the HTTPS configuration as follows:

```
$SERVER["socket"] == ":4680" {

       ssl.engine = "enable"

       ssl.pemfile = "server.pem"

       ssl.ca-file = "intermediate.crt"

}
```

Save this file and restart the web server for settings to take effect:

```
# /etc/init.d/mge-nsm restart
```

Using a browser to connect to the Network Shutdown Module user interface over https on port 4680, will present the new Certificate Authority signed SSL certificate.

*** End of Document ***