opSLA Installation

Installation Prerequisites

- The individual performing this installation has some Linux experience.
- NMIS8 is installed on the same server where opSLA will be installed
- NMIS8 is installed in /usr/local/nmis8
- opSLA will be installed into /usr/local/nmis8
- Root access is available (not always needed but much easier)

Installation Steps

- NMIS8 should be patched or updated to the correct level.
- Install mySQL
  - RedHat and CentOS, very brief steps:
    - yum install mysql
    - yum install mysql-server (this should install DBI and DBD::mysql for Perl as well)
    - chkconfig mysqld on
    - service mysqld start
    - /usr/bin/mysql_secure_installation
    - service mysqld start
  - Debian/Ubuntu, very brief steps:
    - apt-get install mysql-server
    - apt-get install libmysqlclient-dev
    - sysv-rc-conf mysql on
    - service mysql start
    - /usr/bin/mysql_secure_installation
    - service mysql restart
- If not already installed, install the Perl CPAN package DBD::mysql (which may require you to install DBI first)
  - For Debian/Ubuntu, just run:
    - cpan
    - install DBD::mysql
- Copy the opSLA tarball to the server (a tarball is a GZIP'd tar file, e.g. opSLA-2.6.tar.gz)
  1. You may need to use SCP or FTP to get the file onto the server.
- Change into the directory where the tarball was copied (the file will now likely be in the users home directory)
- Untar the file and copy the contents to NMIS8

```
unalias cp (not required for Debian/Ubuntu)
cd ~
tar xvf ~/opsla-<version>.tar.gz
cd opsla/
cp -r * /usr/local/nmis8/
/usr/local/nmis8/admin/fixperms.pl
```

Basic opSLA Configuration

There are many configuration options in opSLA, but the following are essential to make it work correctly.

Edit the NMIS Config in /usr/local/nmis8/conf/Config.nmis.

ipsla

This is the name of the IPSLA GUI which NMIS8 will use, change this to opsla.pl

'ipsla' => '<cgi_url_base>/opsla.pl',

daemon_ipsla_filename

This is the name of the IPSLA daemon which NMIS8 will use, change this to opslad.pl

'daemon_ipsla_filename' => 'opslad.pl',

daemon_ipsla_active

This configuration option enables the ipSLA daemon in NMIS8, change it to true if it is not already set.

'daemon_ipsla_active' => 'true',

NMIS8 Database Setup

The following settings are the defaults and will suffice for running mySQL on the same server as NMIS8 is installed, and using the default password of nmis. If you do not want to use these settings you will need to change them accordingly.

'nmisdb' => 'nmisdb',
'db_server' => 'localhost',
'db_port' => '3306',
'db_user' => 'nmis',
'db_password' => 'nmis'

Setting Up mySQL

To setup mySQL you should run /usr/bin/mysql_secure_installation and following the instructions.

If you are using the Opmantek Virtual Appliance, we have already done this and you will find the passwords you need in this article, Default Credentials (Passwords) for NMIS8 VM.

Create NMIS Database

When setting up mySQL

Access mysql from the command line and login as the root user

```
mysql -u root -p
```

When prompted, use the password you setup when you ran /usr/bin/mysql_secure_installation or from Default Credentials (Passwords) for NMIS8 VM

Enter the following SQL commands to create the database.

```
CREATE DATABASE nmisdb character set utf8;
CREATE USER 'nmis'@'localhost' IDENTIFIED BY 'nmis';
GRANT ALL PRIVILEGES ON nmisdb.* TO 'nmis'@'localhost' WITH GRANT OPTION;
```

Initialiase the NMIS Database for opSLA

Run the command /usr/local/nmis8/admin/opsla_setup.pl, which will create the database tables ready for opSLA to use.

Upgrading opSLA

If upgrading from a previous version of opSLA, you will need to update the database tables:

```
/usr/local/nmis8/bin/opslad.pl type=alter
```

Configuration Options

Handling of rttMonEchoAdminControlEnable

A configuration has been added to NMIS in /usr/local/nmis8/conf/Config.nmis. to support the enabling or disabling of the rttMonEchoAdminControlEnable SNMP MIB for an IPSLA Probe.

When using the TCP Connect or UDP Echo probes the IPSLA probe will need to communicate with the IPSLA Responder router, which is done out of band from the IPSLA Probe. If rttMonEchoAdminControlEnable is set to false, the IPSLA Probe device will not try to communicate with the IPSLA Responder. If using the IPSLA Responders which are NOT managed by opSLA, and you do not want opSLA to control them, set an NMIS configuration option for "ipsla_control_enable_other" set to "false", otherwise leave un-configured or set to true.