PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Table Of Contents

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Introduction:

This document was first conceived in late 2002 as a means to facilitate the installation of Nagios. At that time, Nagios, still in beta release, was being tested at the company where the author works. Since that time, several updates have occurred to the application as well as the operating system on which it resides. As of this writing, Nagios is currently available as version 1.0. The operating system on which the program runs at the author's site is now Red Hat 8.0.

The purpose of this document is similar to that of its predecessor: to provide a step-by-step procedure for new users of the application. It is not an all-encompasing paper that will answer all questions that are asked of it. Rather, it is one person's experience with the installation and various configuration issues associated with the program. What has been documented here, may or may not have occurred in other instances. Continuing the spirit and tradition of its predecessor, this document is available for all to peruse, and critique. If there are errors in what is being described, please feel free to contact the author via the Nagios Users groups to notify him of the error(s).

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Section One: Installation of the Operating System

Note: This section is included simply to provide an example configuration. The description that follows has been successfully installed and tested as a viable platform for running Nagios. At the same time, this method of configuration is only one of a wide variety of setups that can be used, and is therefore NOT exhaustive.

1. Obtain or download onto CD the ISO images for Red Hat 8.0 There will be a total of five CD's, but only three will be used during the installation procedure.

2. Make sure the workstation or server that will be hosting Nagios has at least 256 megabytes of RAM. Hard drive size and type, i.e: IDE or SCSI, can vary, but a good starting point is twenty gigabytes.

3. Obtain, if possible, a static ip address for the Nagios server. Additionally, add the hostname and fully qualified domain name (FQDN) with the associated address to the DNS server of the network. This will allow connection to the server via its hostname rather than having to rely on the ip address for connectivity.

4. Begin the installation of the operating system onto the workstation. Red Hat 8.0 has a utility that will scan the operating system CD's for any defects before proceeding with the loading of the software. It is entirely at the administrator's discretion whether a scan should be done.

5. Select Custom Installation when the appropriate screen appears. Using this method will allow the administrator to have complete control over what is and is not installed onto the computer and how it is configured.

6. The configuration of the mount-points for the server can be accomplished via the Disk Druid utility. One example layout could be the following:

Procedure for the Installation of the Nagios Network Monitoring Program

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/hda8	1004024	278896	674124	30%	/
/dev/hda1	1004024	44036	908984	5%	/boot
/dev/hda7	1004024	191486	761572	21%	/home
/dev/hda2	5036316	32828	4747656	1%	/opt
/dev/hda9	537572	17068	493196	4%	/tmp
/dev/hda5	5036316	2959336	1821116	62%	/usr
/dev/hda3	5036316	122224	4658260	3%	/var

7. The following screens include the various components that can be installed onto the system. Included here are the Gnome and KDE desktop environments as well as the individual packages. Depending on what the needs are, some or all of the files can be slated for installation. Several items that are available on the Red Hat CD's but do not need to be installed are the Apache and MySQL programs. Each of these has a later version that is freely available on the Internet. The various shells, i.e: bash, tcsh, can be installed at the administrator's discretion, although it is a very good rule of thumb to install the bash shell.

8. Configure the static ip address for the soon-to-be Nagios server. Along with the address, implement the hostname that has been assigned to the computer. If the server is to become part of an NIS domain, configure the machine in the appropriate manner.

9. After installation of the operating system is complete, install the appropriate errata packages that coextend with the base operating system.

10. Installation of the base system is complete. The Nagios application can be installed.

Note: It is probably quite apparent the above procedure is, at best, an overview of the installation procedure. There were several important steps not mentioned here. The purpose here was to pro-vide one example configuration that can be used as a reference for whatever configuration the administrator setting up Nagios chooses to use.

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Section Two – Installation of Host Server Programs

1. Obtain Nagios

- Download the Nagios core program from the appropriate website. At this writing, the URL for the website is http://www.nagios.org.
- Obtain the plug-ins that Nagios uses to monitor the network. **This is an important point:** The core program is strictly the engine of the program, and does not have any monitoring functionality of its own. ***The plug-in's are necessary for the network monitoring that will be taking place***.
- The various nodes on the network will need a client program in order for them to be able to communicate with the Nagios application server. There are two such programs: NSClient (Windows) and NRPE (Linux). The homepage of NSClient is http://nsclient.ready2run.nl, while NRPE can be downloaded from the Nagios homepage. Refer to Appendix A for the documentation associated with the client software.
- Periodically, there will be updates to the core program and various addons to the application.
- After installation is complete, regular checks on the Nagios and its associated websites is recommended.

2. Prerequisite Installs

- Download and install the Apache web server from the www.apache.org website. Nagios uses a web interface for the front-end of the program. Additionally, be prepared to make modifications to the httpd.conf file to accommodate Nagios. An additional program that can be downloaded is the Comanche user-interface that serves as a front-end for the Apache program. The program can be downloaded from www.comanche.org. Refer to the documentation that comes with the download for proper installation.
- Download and install the open-source MySQL database program from www.mysql.org. Certain aspects of Nagios use MySQL as a means to better organize data for the program. Refer to the documentation that comes with the download for proper installation.

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

3. Install Nagios

- Unpack the distribution file that was downloaded from the Internet. There are two commands.
  gunzip nagios-*version number*.tar.gz tar *or* –xvf nagios-*version number*.tar

  Note: If the zip version of the program was downloaded, the syntax would be the following.

  Unzip nagios-*version number*.zip

- Create the installation directory for the program. The root or sudo user account should be used when this and future steps are done to insure there are no permissions issues later during the installation. The syntax to use is:

  mkdir /usr/local/nagios

- Create the User and Group associated with the program. Nagios has its own user account and private group. The command shown will accomplish both:

  adduser nagios

- Run the configure script. This shell script will automatically create the necessary directory structure for the program. The generic version of the script is the following

  ./configure --prefix=*prefix* --with-cgiurl=*cgiurl* –with-htmurl=*htmurl* --with-nagios-user=*someuser* –with-nagios-grp=*somegroup*

  - •Replace *prefix* with the installation directory that was created previously.
    (the default is /usr/local/nagios)
  - •Replace *cgiurl* with the actual URL that will be used for accessing the CGI's
    (the default is /cgi-bin/nagios) **Do not append a slash at the end of the URL.**
  - •Replace *htmurl* with the actual URL to be used when accessing the html
    for the main interface and documentation (the default is /nagios)
  - •Replace *someuser* with the name of the user on the system that will be
    used for setting permissions on the installed files. (the default is nagios)
  - •Replace *somegroup* with the name of the group on the system that will
    be used for setting permissions on the installed files. (the default is nagios)

Procedure for the Installation of the Nagios Network Monitoring Program

- Compile the binaries. These are the executable files needed for Nagios' operation. The command syntax is:

<div align="center">make all</div>

- Install the Binaries and HTML Files. After the binaries are compiled (created) the next step is to actually install them in their appropriate directories. This is coupled with doing the same for the html files. The command to accomplish this task is:

<div align="center">make install</div>

- Install the Init Script. This is the startup script used by Nagios to automatically start the program upon system boot. The script is created in /etc/rc.d/init.d/nagios. The script can be modified to reflect the correct paths for the operating system and Nagios installation. The command syntax is:

<div align="center">make install-init</div>

Refer to Appendix B for the complete syntax of the script.

- Verify the directory structure of Nagios is correct. The location of the program, by default, is /usr/local/nagios. Executing the command ls –l will provide a detailed view of the infrastructure. The directory structure for Nagios should be the following:

/usr/local/nagios
        /bin – Nagios core program
        /etc – Main, Resource, Object, and CGI configuration files
        /libexec – Plug-In's
        /sbin - CGI's
        /share – HTML files (for web interface and online documentaion)
        /var – log files

- Install the plug-in's that are associated with Nagios. The procedure to install the plug-ins is similar to that of the core program. Refer to Appendix C for the documentation associated with

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

the plug-ins.

- Set up the Web Interface for Nagios. As mentioned previously, the httpd.conf, main config-uration, file for Apache will need to be modified in order for Nagios to work. It is recommended that an original file be kept intact in the event of a problem with Apache and/or Nagios. The sim-plest way to save and original version of the file is to copy the file with the same name and add an .orig suffix at the end. This can be accomplished by going to the appropriate directory where the conf file is located, for Apache 2 the location is /usr/local/apache2/conf, and make the change there. For example:

  <p style="text-align:center">cp –pr httpd.conf <u>httpd.conf.orig</u></p>

- After an original copy is made an alias for the CGI's needs to be made. The default installation expects to find them accessible at **http://machinename /nagios/cgi-bin/** The following lines should be added to the httpd.conf file for this to happen:

  <pre style="color:red">ScriptAlias /nagios/cgi-bin/ /usr/local/nagios/sbin/
<Directory "/usr/local/nagios/sbin/">
AllowOverride AuthConfig
Options ExecCGI
Order allow,deny
Allow from all
</Directory></pre>

- The following entries should be added to the httpd.conf file in order for the HTML files to be accessible via the web server.

  <pre style="color:red">Alias /nagios/ usr/local/nagios/share/
<Directory "/usr/local/nagios/share">
Options None
AllowOverride AuthConfig
Order allow,deny
Allow from all
</Directory></pre>

Procedure for the Installation of the Nagios Network Monitoring Program

- The entries shown above will allow for the viewing of the HTML web interface and document-ation. The alias should be the same value that was entered for the --with-htmurl argument in the configure script. **The default is /nagios/**.

Important: The Alias directive must come *after* the ScriptAlias directive for the CGI's. If it doesn't users will be confronted with a 404 error when attempting to access the CGI's.

- After the directive entries have been entered, it is necessary for Apache to default to the Nagios CGI's as opposed to its defaults. The httpd.conf file contains a section for Apache's CGI's. Included in the file is the notation that the default setting /usr/local/apache2/cgi-bin should be changed to whatever the ScriptAliased CGI directory is if it is so configured for an application. The simplest way to insure the Nagios CGI's are referenced is to comment out the entire default directive. See below:

    Excerpt from a typical httpd.conf file:

    ```
    # "/usr/local/apache2/cgi-bin" should be changed to whatever your
    # ScriptAliased CGI directory exists, if you have that configured.
    #
    # <Directory "/usr/local/apache2/cgi-bin">
    # AllowOverride None
    # Options None
    # Order allow,deny
    # Allow from all
    # </Directory>
    ```

- The above excerpt shows the default cgi-bin directive commented out. Appendix D provides the entire httpd.conf file with the changes made while Appendix E lists the file in its original format.
- After the changes have been made to the httpd.conf file, the web server will need to be re-booted for the changes to go into effect. There are two commands that can be used to do this:

    /usr/local/apache2/bin/apachectl restart *or* /etc/rc.d/init.d/httpd restart

- Verify the changes that have been made are correct by pointing a web browser at http://yourmachine/nagios. If the web interface is displayed, then the configurations are correct. It is important to note the CGI's will not display information at this point.

Procedure for the Installation of the Nagios Network Monitoring Program

- Configure Web Authentication by enabling access for specific users and/or groups to the CGI's.The first step is to make sure the httpd.conf file contains the AuthOverride AuthConfig statement for the Nagios CGI-BIN directory. If it does not, the following entry should be added and the web server should be subsequently rebooted.

> <Directory /usr/local/nagios/sbin>
> Allow Override AuthConfig
> order allow,deny
> allow from all
> Options ExecCGI
> </Directory>

- If authentication for access to the HTML pages in Nagios is desired, the following should also be added to the httpd.conf file.

> <Directory /usr/local/nagios/share>
> AllowOverride AuthConfig
> order allow,deny
> allow from all
> </Directory>

- The second step is to create a file named .htaccess in the root of the CGI, and optionally to the HTML, directory. The defaults for Nagios is /usr/local/nagios/sbin and /usr/local/nagios/share respectively. The file(s) should have similar to the following:

> AuthName "Nagios Access"
> AuthType Basic
> AuthUserFile /usr/local/nagios/etc/htpasswd.users
> require valid-user

Refer to Appendix F for the complete syntax of the file.

- Set up authenticated users for Nagios. Use the htpasswd command that is bundled with

Procedure for the Installation of the Nagios Network Monitoring Program

Apache. Running the program will create a new file called htpasswd.users in the /usr/local/nagios/etc directory. While running the program, a password will be requested to be associated with users who will be authenticating to the web server. The example below shows the syntax of the command when entering the nagiosadmin user.

<p style="color:red; text-align:center;">htpasswd –c /usr/local./nagios/etc/htpasswd.users nagiosadmin</p>

- The process can be continued to add more users as needed to the list of authenticated users. The syntax used for adding more users is similar to the one shown above except the –c option should not be used. This option actually creates the file, and using it again would overwrite the existing file with another one. Hence, the correct syntax for additional users would be:

<p style="color:red; text-align:center;">htpasswd /usr/local./nagios/etc/htpasswd.users username</p>

- Enable authentication and authorization functionality to the CGI files. This is accomplished by editing the cgi.cfg file. The user_authentication variable should be modified to a non-zero value (typically 1) to activate the basic feature. The correct syntax is the following:

<p style="color:red; text-align:center;">use_authentication=1</p>

- Once this is complete, it is necessary to remove the comment (#) symbol from the author-ized_for_*servicename* lines and add the usernames created in the htpasswd.users file at the end of the lines. Each one of these authorization lines allow the user who is logging into the machine to be able to view from the web browser the information that would be displayed on the screen. If the username is not entered, or if the authorization line was left commented out, the screen in question would display a message indicating the permissions were not valid. Refer to Appendix G for the modified and original versions of the CGI.CFG files for further information.

- Verify Nagios is configured properly. Affectionately known as the sanity check, a shell command is executed to verify that all configuration settings are in order. Nagios automatically runs a "pre-flight" check before it starts monitoring, but the option is also available to run this check manually before starting the program. This is accomplished by adding the –v command line argument as follows:

Procedure for the Installation of the Nagios Network Monitoring Program

<p align="center" style="color:red">/usr/local/nagios/bin/nagios –v <main configuration file></p>

The pathname of the main configuration file typically is:

<p align="center" style="color:red">/usr/local/nagios/etc/nagios.cfg</p>

- There are four methods for starting Nagios:
  - Manually as a foreground process
  - Manually as a background process
  - Manually as a daemon
  - Automatically at system boot

- For the purposes of this installation procedure, the focus will be on items C and D. Further information of the other startup methods can be found in the Nagios Documentation guide.

- Running Nagios in daemon mode requires the inclusion of the –d switch on the command line as follows:

<p align="center" style="color:red">/usr/local/nagios/bin/nagios –d <main configuration file></p>

As mentioned previously, the main configuration file is normally

<p align="center" style="color:red">/usr/local/nagios/etc/nagios.cfg.</p>

- Running Nagios automatically at system boot requires a startup script file and two symbolic links in the appropriate runlevel. The startup script is normally found in the /etc/rc.d/init.d directory, while the symbolic link is located in /etc/rc.d/rc*x*.d. The default is usually /etc/rc.d/rc3.d. The init script for Nagios, known as **Nagios**, can be found in Appendix B. The two symbolic links, Start and Kill, can be created to reference the initialization script. Listed below are the links as they appear in one such configuration:

<p align="center" style="color:red">S96nagios -> /etc/rc.d/nagios <i>and</i> K21nagios -> /etc/rc.d/nagios</p>

- Stopping and restarting Nagios is accomplished via the Init Script that was described

<p align="center">12</p>

Procedure for the Installation of the Nagios Network Monitoring Program

previously, or through the kill command. The focus here will be on using the former. The chart shown below provides the information.

Desired Action	Command	Description
Stop Nagios	/etc/rc.d/init.d/nagios stop	This kills the Nagios process
Restart Nagios	/etc/rc.d/init.d/nagios start	This kills the current Nagios process and then starts Nagios up again
Reload Configuration Data	/etc/rc.d/init.d/nagios reload	Sends a SIGHUP to the Nagios process, causing it to flush its current configuration data, reread the configuration files, and start monitoring again.

- Install the net-snmp utility. The files are freely available for download at www.net-snmp.org. Several plug-in's that Nagios uses, ie: check_hpjd, check_snmp, use the snmp libraries for monitoring nodes on the network. As of this writing, the latest stable version available is 5.0.7. Refer to Appendix I for the installation procedure for the net-snmp utility.

Procedure for the Installation of the Nagios Network Monitoring Program

Section Three – Installation of the Linux Client Software (NRPE)

1. Obtain the NRPE Client Program

- Download the NRPE client program from the appropriate website. At the time of this writing, the URL for the website is http://www.nagios.org.

2. Installing NRPE

- Unpack the distribution file that was downloaded from the Internet. There are two commands:

   gunzip nrpe-*version number*.tar.gz *and* tar –xvf nagios-*version number*.tar

Note: If the zip version of the program was downloaded, the syntax would be the following:

   unzip nagios-*version number*.zip

   Refer to Appendix H for additional documentation on how to compile and install the program.

- Create the installation directory on the remote host for the program. The root or sudo user account should be used when this and future steps are done to insure there are no permissions issues later during the installation. The syntax to use is:

   mkdir /usr/local/nagios

- Create the libexec directory under the nagios directory created in the previous step. The complete path to the directory should read:

   /usr/local/nagios/libexec

- The check_nrpe plugin should be placed on the Nagios **application server** along with the other plugins. The default location is the /usr/local/nagios/libexec directory.

- The nrpe program and the configuration file (nrpe.cfg) should be placed in the directory that was created in the previous steps on the **remote host**. Additional plugins will need to be installed on the remote host in order for the add-on to function properly. The add-ons can be copied from the application server's libexec directory and pasted into the appropriate

directory on the remote host.

- Configure the nrpe client to run under the control of inetd or xinetd. Refer to Appendix H for detailed information on the proper syntax for this operation.

- Configure the proper settings on the Nagios host (application server). Examples for configuring the nrpe daemon are found in the sample nrpe.cfg file included in the distribution. The config file resides on the remote host(s) along with the nrpe daemon. The check_nrpe plugin is installed on the Nagios host (application server). In order to use the check_nrpe plugin from within Nagios, several things in the host configuration (hosts.cfg) file need to be defined. An example command definition for the check_nrpe plugin would look like this:

  define command{
  command_name check_nrpe
  command_line /usr/local/nagios/libexec/check_nrpe $HOSTADDRESS$ -c $ARGI$
  }

- In any service definitions that use the nrpe plugin/daemon to get their results, you would set the service check command portion of the definition to something like this (sample service definition is simplified for this example):

  define service{
      host_name someremotehost
      service_description someremoteservice
      check_command check_nrpe!yourcommand
      .. etc ...
  }

- where "yourcommand" is a name of a command that you define in your nrpe.cfg file on the remote host (see the docs in the sample nrpe.cfg file for more information).

- An example of the correct syntax on the application server for running the check_disk plug-in on the remote host would be the following:

Procedure for the Installation of the Nagios Network Monitoring Program

```
define service{
            use generic-service ; name of service template to use
            host_name bugzilla.mgh.harvard.edu
            service_description Free Space
            is_volatile 0
            check_period 24x7
            max_check_attempts 3
            normal_check_interval 5
            retry_check_interval 1
            contact_groups linux-admins
            notification_interval 120
            notification_period 24x7
            notification_options w,u,c,r
            check_command check_nrpe!check_disk1
            }
```

- The nrpe.cfg file on the remote machine would have something like or similar to the following to allow the application server to run the above plug-in:

    ```
    command[check_disk1]=/usr/local/nagios/libexec/check_disk 80 95 /dev/hda1
    ```

- It is important to remember that whatever services are to be monitored from the application server, the appropriate plug-ins must be installed on the remote host(s) libexec directory. Also, the accurate command syntax must be present in the nrpe.cfg file on the remote host as well as the services.cfg file on the application server.

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Excerpt from posting on the Nagios Users discussion group:
You only have to provide check_command check_nrpe!check_disk1 in yourservices.cfg. The nrpe on the target machine should translate that into   /../check_disk 80 95 …

-----Ursprüngliche Nachricht-----
Von: Kaplan, Andrew H. [mailto:AHKAPLAN@PARTNERS.ORG]
Gesendet: Mittwoch, 2. Oktober 2002 15:24
An: nagios-users@lists.sourceforge.net
Betreff: [Nagios-users] Incorrect command line arguments supplied error message
Hi,
I have installed the nrpe plugin on the nagios host and the daemon on a remote host. However,
when I try to monitor the disk space usage on the remote host, I encounter the following error on the web browser:
INCORRECT COMMAND LINE ARGUMENTS SUPPLIED
The text that I added on the host machine is as follows:
checkcommands.cfg:
# 'check_nrpe' command definition
define command{

       command_name check_nrpe
       command_line /usr/local/nagios/libexec/check_nrpe $HOSTADDRESS$ -c $ARG1$
       }
services.cfg
# Service definition
define service{

       use generic-service ; Name of service template to use
       host_name bugzilla.mgh.harvard.edu
       service_description Free Space
       is_volatile 0
       check_period 24x7
       max_check_attempts 3
       normal_check_interval 1
       contact_groups linux-admins
       notification_interval 120
       notification_period 24x7
       notification_options w,u,c,r
       check_command check_nrpe!command[check_disk1]=/usr/local/nagios/libexec/check_disk 80 95
       /dev/hda5
I installed the nrpe daemon and nrpe.cfg filesonto the remote host at/usr/local/nagios. I created the /usr/local/nagios/libexec directory thereas well. I copied the check_disk, check_load, check_procs, and the check_users plugins from the host machine into thelibexec directory on the remote machine. The nrpe file was created in the /etc/xinetd.d directory. Also, I added the following line to the nrpe.cfg file:

command[check_disk1]=/usr/local/nagios/libexec/check_disk 80 95 /dev/hda5

What arguments did I miss or have the wrong syntax for?

Procedure for the Installation of the Nagios Network Monitoring Program

Section Four – Installation of the Windows Client Software (NSClient)
(based on the documentation for NSClient)

1. Obtain the NSClient Program

- Download the NSClient program from the appropriate website. At the time of this writing, the URL for the website is http://nsclient.ready2run.nl/.

- Unpack the distribution file that was downloaded from the Internet. Any zip utility will do so long as it successfully expands the executable and library files of the program.

2. Installing NSClient

- Log onto the Windows machine as Administrator or as a user that has administrator access to the system.

- On the Windows machine copy pNSClient.exe in any directory on the machine you want to monitor. ie. (c:\nsclient).

- Open a command prompt in the installation directory

- Run the following command : >pNSClient /install

- Start the service 'Netsaint NT Agent' in the services applet of the control panel. The installation will create an entry for the service in the registry and create a new key to store parameters. The created key is the following: HKEY_LOCAL_MACHINE\SOFTWARE\NSClient

- Add the following lines to the checkcommands.cfg file:

```
command[check_nt_disk]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v USEDDISKSPACE -l $ARG1$ -w $ARG2$ -c $ARG3$
command[check_nt_cpuload]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v CPULOAD -l $ARG1$
command[check_nt_uptime]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v UPTIME
command[check_nt_clientversion]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v CLIENTVERSION
command[check_nt_process]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v PROCSTATE -l $ARG1$
command[check_nt_service]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v SERVICESTATE -l $ARG1$
command[check_nt_memuse]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v MEMUSE -w $ARG1$ -c $ARG2$
command[check_nt_pagingfile]=$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v COUNTER -l "\\Paging
                File(_Total)\\% Usage","Paging File usage is %.2f %%" -w $ARG1$ -c $ARG2$
```

3. Uninstallation

- Go to the installation directory and run the following command: >pNSClient /uninstall. All entries in the registry will be removed as well as the definition of the service.

4. Configuration

- There are two parameters you can change: the port (default: 1248) and the password (default: 'None'). These two settings are store in the registry and can only be changed using 'regedit'. Open the following key and change the values if needed :

  HKEY_LOCAL_MACHINE\SOFTWARE\NSClient\Parms

- If you change the password, you will have to use the -s <password> with every request you send to NSClient.

- Refer to Appendix A for the complete documentation for NSClient. Included is the syntax for the plug-in's. Although NSClient was originally written for Netsaint, it has been successfully proven to work with Nagios.

PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Section Five – Using the check_snmp plug-in for non-HP printers

The check_snmp plug-in can be used for printers where one or more of the following conditions apply:

- The printer is not a Hewlett-Packard brand
- The printer does not use a Jet-Direct network card
- The network card the printer uses is not Jet-Direct compatible
- The printer has SNMP capability

The check_snmp plug-in uses standard snmp versions 1 and 2 MIB's (management information blocks) to send out requests to the various clients. It requires the net-snmp package that was mentioned earlier, and it also needs the Net::SNMP perl module. Assuming the net-snmp program has been installed on the Nagios server, what follows is a listing of the steps to install the perl module and also the correct syntax for the check_snmp command itself. ***Note: The Nagios application should be disabled before proceeding.***

1. While logged onto the Nagios server, access the CPAN website for the Net::SNMP module. The url for the package is the following:

   http://search.cpan.org/author/DTOWN/

2. Click on the download link to copy the file onto the server.

3. Unpack the file using the gunzip (if necessary) and tar utilities. A directory called Net-SNMP-4.0.3 will be created. Change to the directory.

4. There are two approaches for installing the perl module. The first has the installation conducted on-line with all the necessary configurations being automatically completed. The second has the administrator doing a manual installation. The former will be discussed here. Refer to Appendix J for more detailed information concerning the manual installation.

   To install the Net::SNMP module and all of it's dependencies directly from the Comprehensive Perl Archive Network (CPAN) execute the command:

Procedure for the Installation of the Nagios Network Monitoring Program

perl -MCPAN -e "install Net::SNMP"

5. The check_snmp plug-in should be tested prior to configuring the remote printers to be monitored by Nagios. The root or sudo account can be used to accomplish this task. While in a terminal command shell, go to the appropriate directory where the plug-in is located, which for argument can be the default /usr/local/nagios/libexec, and type the following:

./check_snmp -H *ip address* -C public -o sysDescr.0

The printer should return some SNMP information string which describes its current status as well as various information about its firmware and other components. If an error message similar to "**SNMP problem – No data returned from host.**" is returned one of several issues may be occurring:

- The command syntax is wrong
- The printer does not have an SNMP stack

If the printer does not have an SNMP stack, the vendor can be contacted to determine if SNMP is either not configured on the system or can be installed onto the printer. However, if the vendor does not have any SNMP solution available, then the printer can not be monitored via the check_snmp plug-in. The only recourse available in that case would be to use the check_ping utility to verify the printer being available on the network.

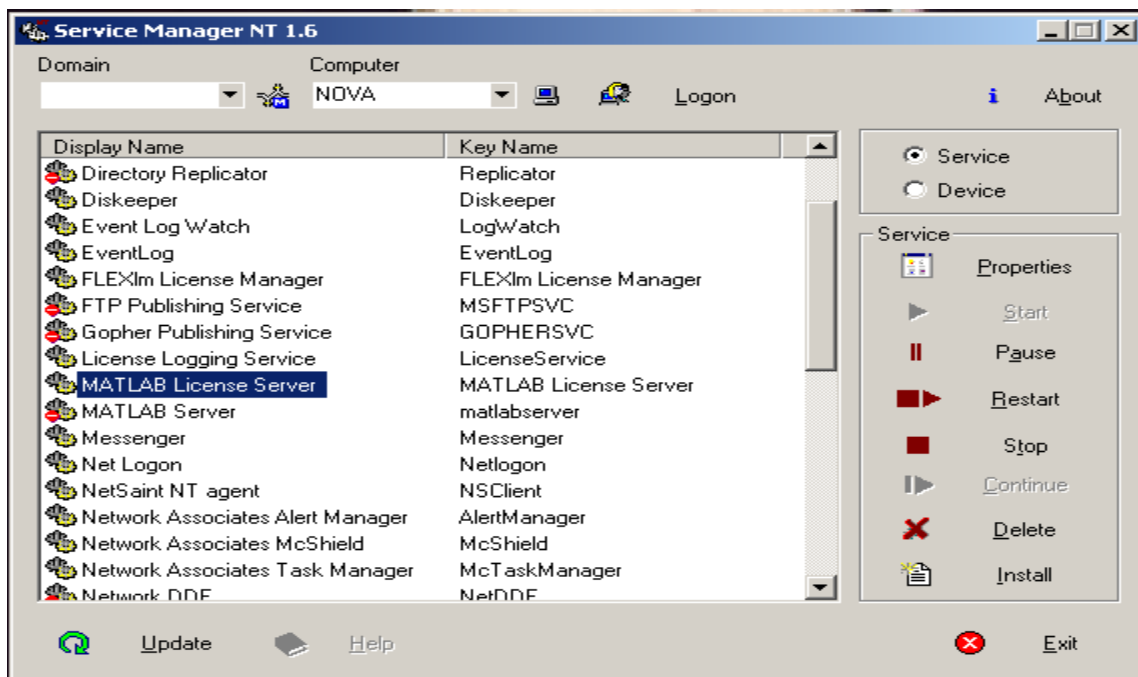# PROCEDURE FOR THE INSTALLATION OF THE NAGIOS NETWORK MONITORING PROGRAM

Section Six – Configuration of the check_flexlm plug-in

The check_flexlm plug-in is used to monitor the flexlm license server common to various mathematical applications. Several such programs include Matlab and IDL. The license server is available for Windows, Linux, and several other platforms. Monitoring the flexlm service can be accomplished using methods specific to the platform. The Windows approach will be briefly discussed and will be followed by the Linux analysis.

Windows:

The Windows version of flexlm is monitored via the NSClient or Ntray utility. For the purposes of this document, the NSClient utility and Matlab license server will be used as references. After installing the NSClient program on the license server, the administrator can configure the service to be monitored from the Nagios application server. A tool that provides access to the list of services running on the Windows machine is Service Manager NT. This utility is freely downloadable from the Internet.

After connecting to the remote Windows server, locate the application's license server. The figure below is a screenshot of one example:

Procedure for the Installation of the Nagios Network Monitoring Program

To configure the license server to be monitored, modify the services.cfg file on the Nagios server. One such example follows:

```
# Service definition
define service{
        use                             generic-service         ; Name of service template to use

        host_name                 nova
        service_description       MATLAB License Server
        is_volatile               0
        check_period              24x7
        max_check_attempts        3
        normal_check_interval     5
        retry_check_interval      1
        contact_groups            nt-admins
        notification_interval     120
        notification_period       24x7
        notification_options      w,u,c,r
        check_command             check_nt_service!'MATLAB License Server'
        }
```

The check_command line defines the executable for monitoring the license server. Special note should be given to the quotation marks. The Service Manager program advertised the Display Name of the service which happened to be comprised of several words. The inclusion of the quotation marks tells the Linux operating system, where the Nagios application resides, the text that is included within is part of one filename rather than several. This allows the administrator have user-friendly names represent the services on the remote system.[1]

Linux:

The configuration for check_flexlm involves three files on the license server, and the services.cfg file on the Nagios server. The three files are the utils.pm, check_flexlm.pl, and nrpe.cfg files.

The utils.pm file is the utility drawer or resource file the Nagios plug-ins use for referencing the locations of various daemons that are to be monitored on the client. If the file is not on the license server, it should be copied to the same directory on the client where the plug-in's are located. Once the file has been copied and/or located, it should be modified to accommodate the location of the lmstat file, which is the license server daemon. The line in the file that is modified is

---

[1]   If there were serveral dependencies associated with a particular service that needed to be monitored. Th e above example would apply with addition of commas separating each dependency. For example: check_nt_service!'OTG DiskXtender','OTG License Server','OTG MediaStor'

Procedure for the Installation of the Nagios Network Monitoring Program

$PATH_TO_LMSTAT = *"path to the lmstat file"*

The check_flexlm.pl file, written by Subhendu Ghosh, is a perl script that will conduct the actual inquiry to the lmstat file. It relies on the utils.pm file for the correct path to the flexlm license daemon. The modification needed in this file occurs on the first line of the file. It is here the lo-cation of Perl on the client computer is designated for the script. To find the location of Perl, run the following command:

which perl

The output of the command should be incorporated into the script for proper functionality.

The nrpe.cfg file should have a line similar to the one shown below added to have the nrpe client program check on the status of the flexlm daemon.

```
command[check_flexlm.pl]=/usr/local/nagios/libexec/check_flexlm.pl -F /exports/apps/matlab/etc/license.dat
```

The -F option specifies the location of the license.dat file. The full pathname to the file should be provided.

After the changes have been made to the client system, restart the xinetd.d services on the client with the following:

/etc/rc.d/init.d/xinetd restart

Prior to making changes the services.cfg file on the Nagios application server, disable the application. After that has been done, the services.cfg file should subsequently have a similar entry to the following added to the configuration:

Procedure for the Installation of the Nagios Network Monitoring Program

```
# Service definition
define service{
        use                             generic-service         ; Name of service template to use

        host_name                       oneofxeon
        service_description             Matlab License Server
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              3
        normal_check_interval           5
        retry_check_interval            1
        contact_groups                  linux-admins
        notification_interval           120
        notification_period             24x7
        notification_options            w,u,c,r
        check_command                   check_nrpe!check_flexlm.pl
        }
```

The Nagios server should be restarted. After several minutes, the status of the flexlm license server should appear on Services Detail screen.

Procedure for the Installation of the Nagios Network Monitoring Program

Section Seven – Configuration of the 2D and 3D Status Maps