NRPE - v3 Enhanced Security

Article Number: 519 | Rating: 3.7/5 from 6 votes | Last Updated: Wed, Mar 31, 2021 at 11:17 AM

Overview

This KB article discusses NRPE v3 and the new security features implemented in that version.

- A 2048-bit DH key is used instead of a 512-bit key
- The `ssl_version` directive lets you set which versions of SSL/TLS you want to allow (`TLSv2+` by default)
- The `ssl_cipher_list` directive lets you specify which ciphers you want to allow (`ALL:!MD5:@STRENGTH` by default)
- Certificates can be used for security
  - NRPE client can use a certificate for encryption
  - The NRPE client can request the `check_nrpe` plugin provide a valid certificate

Nomenclature

The following explains the terms used in this document.

- Client / Agent
  - This is what is listening for NRPE requests
  - "NRPE Client" refers to the Unix/Linux based client, provided by Nagios Enterprises
  - NSClient++ is the Windows client that has an NRPE listening module, developed externally by a third party
- Plugin
  - This is what sends the request off to the client / agent
  - `check_nrpe` is the name of the binary
  - This is what is installed on the Nagios server, but is also installed on the NRPE client by default (not NSClient++)

Certificates

Why would you want to use certificates? It provides extra layers of security.

On the NRPE client a certificate can be used for encryption.

On the NRPE client, the `ssl_client_certs` directive specifies whether or not a certificate will be requested when the `check_nrpe` plugin tries to connect. A value of `2` for this direct

Certificates need to be issued by a certificate authority (CA), so it can be assumed that the certificate is from a trusted source because you have that CA in your configs.

What does **supply a valid certificate** mean? A certificate is valid if the certificate is within it's period of validity and it is from a trusted CA.

NOTE: When using `ssl_client_certs=2` in `nrpe.cfg` on the NRPE client, it is required that the `ssl_cacert_file=` , `ssl_cert_file=` and `ssl_privatekey_file=` are define

How many certificates are required?

- NRPE Client
  - There should be a separate certificate for each NRPE client
  - In the instructions below the files are created as `client_cert.xxx`, this is to make the instructions clear and concise
- `check_nrpe` Plugin
  - There is only one certificate required for the `check_nrpe` plugin

Following is an example of how to create the certificates and implement them.

Creating Certificates Using OpenSSL

The following example does not follow best practice for creating and running a CA or creating certificates. It is for testing or possibly for use in a small environment. Sloppy se

In reality your environment would have a dedicated CA server and you would request the certificates from your security team.

Create Certificate Authority

To provide a working example the first step will be to create a Certificate Authority to issue the certificates. In this example:

- The CA will be created on the Nagios server
- It is assumed that the `openssl` package is already installed on the server
- We are going to put everything in the `/usr/local/nagios/etc/ssl` directory

Execute the following commands in an SSH session on your Nagios server.

Setup Directories

```
mkdir -p -m 750 /usr/local/nagios/etc/ssl
chown root.nagios /usr/local/nagios/etc/ssl
cd /usr/local/nagios/etc/ssl/
mkdir -m 750 ca nagios_server_certs client_certs
chown root.root ca
chown root.nagios nagios_server_certs client_certs
touch /etc/pki/CA/index.txt
echo '1000' > /etc/pki/CA/serial
```

Create Certificate Authority

```
cd /usr/local/nagios/etc/ssl/ca/
openssl req -x509 -newkey rsa:4096 -keyout ca_key.pem -out ca_cert.pem -utf8 -days 3650
```

You will be prompted to type a PEM pass phrase, make sure to keep a note of this as you will need it in the future.

You will be prompted to provide information, see the following example:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Minnesota
Locality Name (eg, city) [Default City]:Saint Paul
Organization Name (eg, company) [Default Company Ltd]:Nagios
Organizational Unit Name (eg, section) []:Monitoring
Common Name (eg, your name or your server's hostname) []:CA
Email Address []:email@domain.local
```

Now that the CA has been created you can proceed to create the NRPE client certificate and the `check_npre` plugin certificate.

NRPE Client Certificate

Create The Certificate

These commands are to be executed on the Nagios server as that is where the certificate authority was created earlier.

```
cd /usr/local/nagios/etc/ssl/client_certs/
openssl req -new -newkey rsa:2048 -keyout client_cert.key -out client_cert.csr -nodes
```

You will be prompted to type "A challenge password", do not type anything, just press **Enter**. The example also did not provide anything for **"An optional company name"**. See the

```
Generating a 2048 bit RSA private key
..............+++
.................+++
writing new private key to 'client_cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Minnesota
Locality Name (eg, city) [Default City]:Saint Paul
Organization Name (eg, company) [Default Company Ltd]:Nagios
Organizational Unit Name (eg, section) []:Monitoring
Common Name (eg, your name or your server's hostname) []:NRPE_Client
Email Address []:email@domain.local

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Next we have to sign this certificate request by our CA.

```
cd /usr/local/nagios/etc/ssl/
openssl ca -days 365 -notext -md sha256 -keyfile ca/ca_key.pem -cert ca/ca_cert.pem -in client_certs/client_cert.csr -out client_certs/
```

You will be prompted for the CA PEM pass phrase that you provided before when creating the Certificate Authority.

You will then be prompted to sign new certificate, answer **y** twice:

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ca/ca_key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Jul  6 03:59:02 2016 GMT
            Not After : Jul  6 03:59:02 2017 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Minnesota
            organizationName          = Nagios
            organizationalUnitName    = Monitoring
            commonName                = NRPE_Client
            emailAddress              = email@domain.local
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                3D:0D:FE:51:6E:1C:16:5F:21:05:46:4D:76:C6:2E:5B:1F:12:14:5C
            X509v3 Authority Key Identifier:
                keyid:5A:81:97:96:99:47:19:76:70:24:AB:EC:3B:BE:07:0C:E8:AD:4B:E7

Certificate is to be certified until Jul  6 03:59:02 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

The two files `client_certs/client_cert.pem` and `client_certs/client_cert.key` need to be copied to the server running the NRPE client along with the `ca/ca_cert.pem`

Implement NRPE Client Certificate

On the NRPE client, execute the following commands to copy the certificates from the Nagios server (10.25.5.60 in this example):

```
mkdir -p /usr/local/nagios/etc/ssl
scp root@10.25.5.60:/usr/local/nagios/etc/ssl/ca/ca_cert.pem /usr/local/nagios/etc/ssl/
scp root@10.25.5.60:/usr/local/nagios/etc/ssl/client_certs/client_cert.key /usr/local/nagios/etc/ssl/
scp root@10.25.5.60:/usr/local/nagios/etc/ssl/client_certs/client_cert.pem /usr/local/nagios/etc/ssl/
```

If you don't have scp installed *(openssh-clients)* on both machines, then you will need to use another method to transfer the certificates from the Nagios server to the NRPE client.

Next the NRPE client config file needs updating so it knows to use the new certificate. In the file `/usr/local/nagios/etc/nrpe.cfg` you will need the following three entries:

```
ssl_cacert_file=/usr/local/nagios/etc/ssl/ca/ca_cert.pem
ssl_cert_file=/usr/local/nagios/etc/ssl/client_cert.pem
ssl_privatekey_file=/usr/local/nagios/etc/ssl/client_cert.key
```

You should put them in the SSL section of the file (around line 220).

Then you need to restart the NRPE client, this will vary depending on the operating system you are on, some examples of the restart command are:

```
restart nrpe
service nrpe restart
systemctl restart nrpe.service
```

This completes creating and implementing the NPRE client certificate. If you would like to confirm if the certificate is being used, you will need to enable additional logging. In the file `/`

```
ssl_logging=0x01
```

Then restart the NRPE service. Once restarted you can observe the following log entries in the syslog `/var/log/messages` file (may vary on your operating system):

```
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Certificate File: /usr/local/nagios/etc/ssl/client_cert.pem
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Private Key File: /usr/local/nagios/etc/ssl/client_cert.key
Jul  6 14:29:11 centos16 nrpe[1744]: SSL CA Certificate File: /usr/local/nagios/etc/ssl/ca_cert.pem
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Cipher List: ALL:!MD5:@STRENGTH
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Allow ADH: Allow
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Client Certs: Don't Ask
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Log Options: 0x01
Jul  6 14:29:11 centos16 nrpe[1744]: SSL Version: TLSv1 And Above
Jul  6 14:29:11 centos16 nrpe[1744]: Starting up daemon
Jul  6 14:29:11 centos16 nrpe[1744]: Server listening on 0.0.0.0 port 5666.
Jul  6 14:29:11 centos16 nrpe[1744]: Server listening on :: port 5666.
Jul  6 14:29:11 centos16 nrpe[1744]: Warning: Daemon is configured to accept command arguments from clients!
```

```
Jul  6 14:29:11 centos16 nrpe[1744]: Listening for connections on port 5666
Jul  6 14:29:11 centos16 nrpe[1744]: Allowing connections from: 127.0.0.1,10.25.5.2
```

check_nrpe Plugin Certificate

Create The Certificate

This certificate is to be used on the Nagios server by the `check_nrpe` plugin. These commands are to be executed on the Nagios server because this is where the certificate author

```
cd /usr/local/nagios/etc/ssl/nagios_server_certs/
openssl req -new -newkey rsa:2048 -keyout nagios_server.key -out nagios_server.csr -nodes
```

You will be prompted to type "A challenge password", do not type anything, just press **Enter**. The example also did not provide anything for **"An optional company name"**. See the

```
Generating a 2048 bit RSA private key
.....................................+++
..................+++
writing new private key to 'nagios_server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Minnesota
Locality Name (eg, city) [Default City]:Saint Paul
Organization Name (eg, company) [Default Company Ltd]:Nagios
Organizational Unit Name (eg, section) []:Monitoring
Common Name (eg, your name or your server's hostname) []:Nagios_Server
Email Address []:email@domain.local

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Next we have to sign this certificate request by our CA.

```
cd /usr/local/nagios/etc/ssl/
openssl ca -days 365 -notext -md sha256 -keyfile ca/ca_key.pem -cert ca/ca_cert.pem -in nagios_server_certs/nagios_server.csr -out nagi
```

You will be prompted for the CA PEM pass phrase that you provided before when creating the Certificate Authority.

You will then be prompted to sign new certificate, answer **y** twice:

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ca/ca_key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Jul  6 06:58:34 2016 GMT
            Not After : Jul  6 06:58:34 2017 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = Minnesota
            organizationName          = Nagios
            organizationalUnitName    = Monitoring
            commonName                = Nagios_Server
            emailAddress              = email@domain.local
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F5:3C:09:60:EC:18:65:9A:E7:61:FB:39:60:E7:20:59:F9:E4:41:9B
            X509v3 Authority Key Identifier:
                keyid:5A:81:97:96:99:47:19:76:70:24:AB:EC:3B:BE:07:0C:E8:AD:4B:E7

Certificate is to be certified until Jul  6 06:58:34 2017 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

The files `ca/ca_cert.pem` , `nagios_server_certs/nagios_server.pem` and `nagios_server_certs/nagios_server.key` will be referenced in the `check_nrpe` command (

Using Certificates With check_nrpe Plugin

On the nagios server the `check_nrpe` command needs to reference the certificates in the command line. The remote NRPE client in this example is 10.25.13.34:

```
/usr/local/nagios/libexec/check_nrpe -A /usr/local/nagios/etc/ssl/ca/ca_cert.pem -C /usr/local/nagios/etc/ssl/nagios_server_certs/nagio
```

If it all was OK then the result will be something like:

```
NRPE v3.0
```

You will need to configure your Nagios command / service definitions to use the certificates. Alternatively you can create a `check_nrpe` config file and reference that in the command article:

Documentation - NRPE - v3 check_nrpe Config File

Configure NRPE Client To Require Certificates

While the `check_nrpe` plugin is sending a certificate, NRPE v3 does not require a certificate unless you update the NRPE configuration file. At this point the NRPE Client is not enforcing

The NRPE client has the following configuration directive in the `nagios.cfg` file:

```
ssl_client_certs=
```

The options available are:

```
Values: 0 = Don't ask for or require client certificates (default)
          1 = Ask for client certificates
          2 = Require client certificates
```

Option **2** will require the `check_nrpe` plugin to supply a certificate (adding an extra layer of security). Option **1** means that it will ask `check_nrpe` to supply a certificate, but if it does

On the NRPE client, edit the file `/usr/local/nagios/etc/nrpe.cfg` and define the following:

```
ssl_client_certs=2
```

You should put them in the SSL section of the file (around line 230).

Then you need to restart the NRPE client, this will vary depending on the operating system you are on, some examples of the restart command are:

```
restart nrpe
service nrpe restart
systemctl restart nrpe.service
```

Going back to the nagios server execute the `check_nrpe` command again:

```
/usr/local/nagios/libexec/check_nrpe -A /usr/local/nagios/etc/ssl/ca/ca_cert.pem -C /usr/local/nagios/etc/ssl/nagios_server_certs/nagio
```

If it all was OK then the result will be something like:

```
NRPE v3.0
```

Here's what happens if you don't supply the certificate:

```
/usr/local/nagios/libexec/check_nrpe -H 10.25.13.34
```

The result will be something like:

```
CHECK_NRPE: Error - Could not complete SSL handshake with 10.25.13.34: 1
```

If you would like to confirm if the certificate is being used, you will need to enable additional logging. In the file `/usr/local/nagios/etc/nrpe.cfg` you will need to add the followi

```
ssl_logging=0xff
```

Then restart the NRPE service. Once restarted you can observe the following log entries in the syslog `/var/log/messages` file (may vary on your operating system).

When a certificate was used:

```
Jul  6 17:40:27 centos16 nrpe[1951]: Remote 10.25.5.60 - SSL Version: TLSv1.2
Jul  6 17:40:27 centos16 nrpe[1951]: Remote 10.25.5.60 - TLSv1/SSLv3, Cipher is DHE-RSA-AES256-GCM-SHA384
Jul  6 17:40:27 centos16 nrpe[1951]: SSL Client 10.25.5.60 has a valid certificate
Jul  6 17:40:27 centos16 nrpe[1951]: SSL Client 10.25.5.60 Cert Name: /C=US/ST=Minnesota/O=Nagios/OU=Monitoring/CN=Nagios_Server/emailA
Jul  6 17:40:27 centos16 nrpe[1951]: SSL Client 10.25.5.60 Cert Issuer: /C=US/ST=Minnesota/L=Saint Paul/O=Nagios/OU=Monitoring/CN=CA/em
```

When a certificate was not used:

```
Jul  6 17:39:17 centos16 nrpe[1949]: Error: Could not complete SSL handshake with 10.25.5.60: peer did not return a certificate
```

Certificate Arguments Explained

In the examples above you were walked through the process of creating certificates, defining them in `nrpe.cfg` and the `check_nrpe` command line arguments. A clear explanation o

NRPE Client

Directive	Explanation
`ssl_cert_file=`	The certificate that the NRPE Client uses to provide encryption
`ssl_privatekey_file=`	The corresponding key file for `ssl_cert_file=`
`ssl_cacert_file=`	The certificate authority file that the NRPE Client uses to validate the certificate provided by the `check_nrpe` plugin

check_nrpe Plugin

Directive	Explanation
`-C <clientcert>`	The certificate that the `check_nrpe` plugin submits to the NRPE Client to prove it's validity
`-K <key>`	The corresponding key file for `-C <clientcert>`
`-A <ca-certificate>`	The certificate authority file that the `check_nrpe` plugin uses to validate the certificate provided by the NRPE Client for encryption

When you are using the same CA to issue the `check_nrpe` plugin and NRPE client certificates it is very straight forward to configure and use.

However when you use separate CA's to issue the `check_nrpe` plugin and NRPE client certificates, the CA certificates must be placed in the following manner:

- `check_nrpe` plugin
  - The CA certificate referenced by `-A <ca-certificate>` must the CA certificate that issued the NRPE client certificate
- NRPE Client
  - The CA certificate referenced by `ssl_cacert_file=` must the CA certificate that issued the `check_nrpe` plugin certificate

SSL/TLS Version and Ciphers

There are arguments that allow the `check_npre` plugin *(command line arguments)* and the NRPE client *(nrpe.cfg)* to define what SSL/TLS version and ciphers are allowed to be used.

check_npre Plugin	NRPE Client	Default Used
`-S <ssl version>`	`ssl_version=`	`TLSv1+`
`-L <cipherlist>`	`ssl_cipher_list=`	`ALL:!MD5:@STRENGTH`

This is quite a complicated topic, if you would like to understand more about this please refer to the OpenSSL documentation:

Documentation - SSL / TLS

Documentation - OpenSSL ciphers

Final Thoughts

For any support related questions please visit the Nagios Support Forums at:

http://support.nagios.com/forum/