NAME

send_nsca.cfg – NSCA–ng client configuration file

SYNOPSIS

/etc/send_nsca.cfg

DESCRIPTION

The **send_nsca**(8) process reads configuration data from the file specified with **–c** on the command line or from */etc/send_nsca.cfg*.

File Format

Configuration settings are defined by specifying a variable name followed by an equals sign (“=”) and a value, one setting per line. Values can be strings or integers. Strings have to be enclosed in single or double quotes if they contain whitespace characters, hash mark characters, or literal quotation marks. Otherwise, quoting is optional. To specify a literal single or double quote in a string, either escape it by preceding it with a backslash (“\”) or quote the string using the other quote character. A literal backslash must be preceded with a second backslash.

Any whitespace surrounding tokens is ignored. Empty lines and comments are also ignored. Comments are introduced with a hash mark character (“#”) and span to the end of the line. If the last character of a line is a backslash (“\”), the subsequent line is treated as a continuation of the current line (and the backslash is otherwise ignored).

Settings

The **send_nsca**(8) client recognizes the following variables. They may appear in arbitrary order. The type of each value is denoted after an equals sign in angle brackets.

delay = <*integer*>

Wait for a random number of seconds between 0 and the specified delay before contacting the server. This might be useful to reduce the server load if many **send_nsca**(8) clients are invoked simultaneously. The default setting is 0, which tells **send_nsca**(8) to connect to the server immediately. The specified value will be ignored if **send_nsca**(8) is called with the **–D** option.

encryption_method = <*string*>

This setting is ignored. It is accepted for compatibility with NSCA 2.x.

identity = <*string*>

Send the specified client identity to the server. The client identity is used for authentication and authorization. The same identity may be provided by multiple clients. By default, the local host name will be used.

password = <*string*>

Use the specified passphrase for authentication and encryption. The default password is “change-me”. Change it!

port = <*string*>

Connect to the specified service name or port number on the server instead of using the default port (5668). The specified value will be ignored if **send_nsca**(8) is called with the **–p** option.

server = <*string*>

Connect and talk to the specified server address or host name. The default server is “localhost”. The specified value will be ignored if **send_nsca**(8) is called with the **–H** option.

timeout = <*integer*>

Close the connection if the server didn’t respond for the specified number of seconds. If the timeout is set to 0, **send_nsca**(8) won’t enforce connection timeouts. The default timeout is 15 seconds. The specified value will be ignored if **send_nsca**(8) is called with the **–o** option.

tls_ciphers = <*string*>

Limit the cipher suites offered during the TLS negotiation to the specified list of ciphers. The format of the string is described in the **ciphers**(1) manual. By default, the ciphers in the list `PSK-AES256-CBC-SHA:PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:PSK-RC4-SHA` will be offered.

EXAMPLES

The **/etc/send_nsca.cfg** file might look similar to the following example.

```
identity = "web-checker"
password = "djMKCIcurJJLSQGT5qIhCfqCHQLTcvp9"
server = "monitoring.example.com"
tls_ciphers = "PSK-AES256-CBC-SHA"
delay = 2
port = 5668
timeout = 10
```

CAVEATS

Please set the permissions appropriately to make sure that only authorized users can access the **/etc/send_nsca.cfg** file.

SEE ALSO

send_nsca(8), **nsca–ng**(8), **nsca–ng.cfg**(5),

http://www.nagios.org/developerinfo/externalcommands/

AUTHOR

Holger Weiss <holger@weiss.in-berlin.de>