NAME

      nsca–ng – monitoring command acceptor

SYNOPSIS

      nsca–ng [–**FSs**] [–**b** *listen*] [–**C** *file*] [–**c** *file*] [–**l** *level*] [–**P** *file*]

      nsca–ng –h | –V

DESCRIPTION

      The **nsca–ng** server makes the Nagios command file accessible from remote systems. This allows for submitting passive check results, downtimes, and many other commands to Nagios (or compatible monitoring solutions). The communication with clients is TLS encrypted and authenticated using pre-shared keys (as per RFC 4279). The **nsca–ng** server supports per-client passwords and fine-grained authorization control.

      The server process rereads its configuration file when it receives a hangup signal (SIGHUP) by executing itself with the name and arguments it was started with.

      When compiled with **systemd**(1) support, the **nsca–ng** server auto-detects whether it was socket activated. If so, it behaves as if the **–F** option was specified, while it ignores the **–b** option and the **listen** setting in the **nsca–ng.cfg**(5) file. The **nsca–ng** server supports **systemd**(1)'s **notify** process startup type as well as the **WatchdogSec** feature (see the **systemd.service(5)** manual).

OPTIONS

      –b *listen*

            Bind to the specified *listen* address or host name. The default setting is "*", which tells **nsca–ng** to listen on all available interfaces. A colon (":") followed by a service name or port number may be appended in order to override the default port (5668) used by **nsca–ng**. If this option is specified, the **listen** setting in the **nsca–ng.cfg**(5) file is ignored.

      –C *file* Submit monitoring commands into the specified *file*. This should be the named pipe (FIFO) that Nagios checks for external commands to process. By default, **nsca–ng** submits commands into */var/nagios/rw/nagios.cmd*. This option takes precedence over the **command_file** setting in the **nsca–ng.cfg**(5) file.

      –c *file* Read the configuration from the specified *file* instead of using the default configuration file */etc/nsca–ng.cfg*. If a directory is specified instead of a *file*, the configuration will be read from all files with a *.cfg* or *.conf* extension in this directory and all subdirectories. Symbolic links are followed.

      –F   Don't detach from the controlling terminal, and write all messages to the standard error output (unless the **–s** option is specified).

      –h   Print usage information to the standard output and exit.

      –l *level* Use the specified log *level*, which must be an integer value between 0 and 5 inclusive. A value of 0 tells **nsca–ng** to generate only fatal error messages, 1 adds non-fatal error messages, 2 adds warnings, 3 additionally spits out every submitted monitoring command (plus startup and shutdown notices), 4 also logs each message sent or received at the protocol level, and 5 generates additional debug output. The default log *level* is 3. If this option is specified, the **log_level** setting in the **nsca–ng.cfg**(5) file is ignored.

      –P *file* During startup, try to create and lock the specified *file* and write the process ID of the **nsca–ng** daemon into it. Bail out if another process holds a lock on the *file*. By default, no such PID *file* is written. This option takes precedence over the **pid_file** setting in the **nsca–ng.cfg**(5) file.

      –S   Write all messages to the standard error output and (with the exception of startup messages) to the system logger. This option may only be specified together with the **–F** option.

      –s   Send all messages to the system logger, except for startup messages. This is the default behaviour (unless the **–F** option is specified).

–V Print version information to the standard output and exit.

FILES

/etc/nsca–ng.cfg
The **nsca–ng.cfg**(5) configuration file.

SEE ALSO

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

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

AUTHOR

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