

Watchdog

<https://campus.barracuda.com/doc/41115912/>

The Barracuda NG Firewall watchdog complements the functionality provided by the control daemon. The watchdog daemon ensures that the control daemon remains up and running at all times. You can set limits on critical system resources and monitor additional resources at defined intervals. When system resource limits are exceeded or core processes are unexpectedly terminated, the watchdog triggers preset actions to repair or reboot the system. The watchdog also attempts to correct system errors. For high availability (HA) systems, the watchdog helps ensure swift takeovers take place in case the system freezes, hardware or file system problems.

In this article:

System Tests and Monitoring

The watchdog performs the following tests to monitor the status of your system:

Test	Configurable	Settings	Repair Method
Is the process table full?	No	None	Immediate system reboot
Has a file table overflow occurred?	No	None	Specified by repair mode
Is enough free memory available?	Yes	Percentage of total RAM plus swap	Specified by repair mode
Has the load average exceeded a max value?	Yes	Separately for 1, 5, and 15 min. averages	Specified by repair mode
Is a given process is still running?	Yes	Separate settings for control and SSH daemon	Specified by repair mode

If any of the system tests (except for the process table check) fails, the watchdog will invoke the repair binary at `/usr/sbin/repair`. When the routine returns a zero exit code to the watchdog, the system is considered successfully repaired. Otherwise, the system is soft booted by the watchdog. The watchdog also resets the system if it is not able to correct a system error after a specified number of consecutive attempts. The watchdog uses its own built-in shutdown procedure so that it does not have to rely on the availability of potentially critical system resources. If the shutdown fails, the system is hard reset by the kernel. The reboot is dependent on the hardware state of the system and its interrupts.

If any of the system tests last longer than one minute the NG Firewall is rebooted as well. `/dev/watchdog` must be written to within a minute after being opened or the system will be reset. Each write delays the reboot time for another minute. Watchdog delays this reset by writing to

`/dev/watchdog` at least once every minute when the system is healthy.

Repair Modes

When configuring the watchdog, you can select any of the following repair modes to handle system errors:

- **Ignore_Errors** – Monitoring mode. Errors are only logged.
- **Repair_or_Ignore** – Default mode. Repairs are only attempted for the following error types:
 - ENFILE (23) – Too many open files in system
 - ENOMEM (12) – Cannot allocate memory
 - ESRCH (3) – No such process
 - ENOENT (2) – No such file or directory
 - EINVMEM (-7) – /proc/meminfo contains invalid data
 - EMAXLOAD (-3) – Load average too high
 - ENOLOAD (5) – /proc/loadavg contains no data

If the repair is not successful after a specified number of attempts, the watchdog reboots the system. All other errors are ignored.

- **Repair_or_Reboot** – Strict mode. Repairs are attempted for all errors. If the repair is not successful after a specified number of attempts, the watchdog reboots the system.
- **Always_Reboot** – Paranoid mode. The error condition is logged and the watchdog reboots the system.

Each monitored entity is allotted its own counter for repair attempts. Negative error codes designate special errors generated by the check routines of watchdog. All other errors conform to the standard error coding scheme of Linux. The following error codes are used:

- ENFILE (23) – Out of file descriptors (that is file table overflow)
- ENOMEM (12); EINVMEM (-7) – Low on memory
- EMAXLOAD (-3); ENOLOAD (-5) – Maximum allowed system load average exceeded
- ESRCH (3); ENOENT (2) – Monitored process has died or its pid-file is missing

File Table Overflow

When a file table overflow occurs, the repair binary increases the number of available file descriptors by 10%. If the error condition persists, the number of available file descriptors is increased until the maximum number of repair attempts is exceeded. The number of repair attempts is written to the `/var/run/watchdog.state.fd` file. Increasing the number of available file descriptors also increases kernel memory consumption and may eventually lead to a memory shortage.

Control and SSH Daemons

To monitor the control daemon (`controld`) and the SSH daemon (`sshd`), the watchdog verifies that the processes corresponding to the process ids given in `/var/run/control.pid` and `/var/run/sshd.pid` are still running.

- When `controld` is down, it is stopped (`/opt/phionctrl box stop controld`) and then started (`/opt/phionctrl box start controld`). A check is then performed to verify that the restart attempt was successful. Unsuccessful restart attempts are incremented and written to `/var/run/watchdog.state.pid`. If the maximum number of repair attempts is exceeded, the entire Barracuda NG Firewall subsystem is shut down (`/opt/phionctrl shutdown`) and restarted (`/opt/phionctrl startup`). If the error condition persists, which means `controld` is still not running, a reboot is requested.
- When `sshd` is down, `/etc/rc.d/init.d/ssh condrestart` is invoked to restart it. Attempts to restart `sshd` are not incremented because it is unnecessary to restart the system while the daemon is down.

To facilitate system maintenance, such as software updates which involve a temporary shutdown of either `controld` or `sshd`, the repair binary ignores the `ESRCH` error code if a `/var/run/watchdog.state.service` file exists. The Barracuda NG Firewall software update procedure will automatically create and remove this file. If you interact with the system on the command line, touch and subsequently remove this file when shutting down or blocking `controld`. Alternatively, you may shut down (restart) watchdog by invoking `/etc/rc.d/init.d/watchdog stop [start]`.

System Resources

On the Barracuda NG Firewall, resource problems are most likely caused by overloaded service processes. Memory shortages or excessive loads are thus attributed to the operation of the Barracuda NG Firewall subsystem as a whole.

- Memory shortage – The Barracuda NG Firewall subsystem is shut down (`/opt/phionctrl shutdown`) and subsequently restarted (`/opt/phionctrl startup`). The number of repair attempts is written to `/var/run/watchdog.state.mem`.
- Maximum load exceeded – The Barracuda NG Firewall subsystem is shut down (`/opt/phionctrl shutdown`) and subsequently restarted (`/opt/phionctrl startup`). The number of repair attempts is written `/var/run/watchdog.state.load`.

During a reboot, the repair counters and service indicator file are automatically reset. All contents of `/var/run` are automatically purged by the system. All counter files, but not the service file, are deleted when watchdog is restarted and when the configuration is changed.

- **Operational Events** – Errors that are generated by the repair binary which relate to system information are the 34 [Critical System Condition], 510 [Invalid Argument], and 4202 [System Reboot] events.

If necessary, you can temporarily block the watchdog repair routine. At the command line, enter: `/etc/phion/bin/servicemode` Then, enter the number of minutes for which the watchdog should be blocked.

For a longer term solution, it is recommended that you try to reduce the load on the system by going to the **Control** page (**Config > Full Config > Box > Infrastructure Services**) and deactivating unnecessary services. In the **Monitoring Parameters** section, add the services that you want to deactivate to the **Deactivate Service** table.

The following infrastructure services can be deactivated if they are not needed:

- SMS-Control (bsms) – Used for remote control of Barracuda NG Firewall services via SMS command.
- SNMP-Service (bsnmp) – Used for SNMP monitoring.
- Statistics-Collector (cstat) – Collects statistics to be sent to a Barracuda NG Control Center.
- Statistics-Viewer (qstat) – Used by the Statistics Viewer.
- Authentication-Service (phibs) – Used for authentication.
- Data-Upload (dist) – Used for data upload.
- Event (event) – Used by the eventing service.
- Host-Firewall (boxfw) – Used by the box firewall.
- Log (log) – Used by the log service.
- Log Wrapper (logwrap) – Used by the log service.
- Syslog-Log Converter (psyslog) – Used by the log service.

Configure the Watchdog

Enable the watchdog on the Barracuda NG Firewall, select the applicable repair mode, and configure resource handling and monitoring.

For more information, see [How to Configure the Watchdog](#).

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.