cPHulk Management on the Command Line

Overview

This document describes how to manage the cPHulk service from the command line.

Notes:

- You can also manage the cPHulk service with WHM's *cPHulk Brute Force Protection* interface (*WHM >> Home >> Security Center >> cPHulk Brute Force Protection*).
- In cPanel & WHM version 72 and later, you can use cPanel's *Terminal* interface (*cPanel >> Home >> Advanced >> Terminal*) or WHM's *Terminal* interface (*WHM >> Home >> Advanced >> Terminal*) to access the command line from within the interface.
- This **feature** requires that you log in to the server as the `root` user.

Manage cPHulk

Use the following methods to manage the cPHulk service on your server.

Important:
The system **requires** several configuration changes in order to properly enable the cPHulk service. Therefore, we **strongly** recommend that you do **not** enable it from the command line. Instead, use WHM's *cPHulk Brute Force Protection* interface (*WHM >> Home >> Security Center >> cPHulk Brute Force Protection*) to enable the cPHulk service.

Debug mode

To enable debug mode for the cPHulk service, run the following command:

```
touch /var/cpanel/hulkd/debug
```

Check cPHulk's status

To check the status of the cPHulk service, run the `ps aux | grep -i cphulk` command. The system will return output that resembles the following example:

```
root 1501 0.0 0.4 34816 5076 ? S 07:58 0:00 cPhulkd - processor
```

Note:
In this example, the output indicates that cPHulk is enabled.

Restart the cPHulk daemon (`cphulkd`)

To restart the `cphulkd` daemon, perform one of the following actions:

- Use WHM API 1's `configureservice` function to perform the restart, which also performs the necessary the Dovecot® service rebuild and restart. To do this, run the following commands:

```
whmapi1 configureservice service=cphulkd enabled=0 monitored=0
whmapi1 configureservice service=cphulkd enabled=1 monitored=1
```

- Perform a soft restart, rebuild the Dovecot service, and restart the Dovecot service. To do this, run the following commands:

```
/scripts/restartsrv_cphulkd
/scripts/builddovecotconf
/scripts/restartsrv_dovecot
```

- Perform a hard restart and force the system to flush the daemon's memory, rebuild the Dovecot service, and restart the Dovecot service. To do this, run the following commands:

```
/scripts/restartsrv_cphulkd --stop; /scripts/restartsrv_cphulkd
--start
/scripts/builddovecotconf
/scripts/restartsrv_dovecot
```

Disable cPHulk

To disable the `cphulk` daemon, perform one of the following actions:

- Use WHM API 1's `configureservice` function to disable the cPHulk service:

```
whmapi1 configureservice service=cphulkd enabled=0 monitored=0
```

- Run the following commands:

```
/usr/local/cpanel/etc/init/stopcphulkd
/usr/local/cpanel/bin/cphulk_pam_ctl --disable
```

To disable the cPHulk service so that it remains offline, even after a restart of cPanel & WHM, perform the following steps at the command line:

1. Remove the cPHulk touch file with the following command:

```
rm /var/cpanel/hulkd/enabled
```

2. Edit the `/etc/dovecot/dovecot.conf` file and remove the following line:

```
auth_policy_server_url = http://127.0.0.1:579/dovecot-auth-polic
```

3. Rebuild Dovecot's configuration file and restart it with the following commands:

```
/scripts/builddovecotconf
/scripts/restartsrv_dovecot
```

Log files

cPHulk stores its logs in the following files:

```
/usr/local/cpanel/logs/cphulkd.log
/usr/local/cpanel/logs/cphulkd_errors.log
```

IP address management

Add IP addresses to the whitelist

To add IP addresses to the whitelist from the command line, run the `/scripts/cphulkdwhitelist IP` command, where `IP` represents the IP address or IP address range that you wish to add.

For example, to add the `192.168.0.20` IP address to the whitelist, run the following command:

```
/scripts/cphulkdwhitelist 192.0.2.0
```

Add IP addresses to the blacklist

To add IP addresses to the blacklist from the command line, run the `/scripts/cphulkdblacklist IP` command, where `IP` represents the IP address or IP address range that you wish to add.

For example, to add the `192.0.2.0` IP address to the blacklist, run the following command:

```
/scripts/cphulkdblacklist 192.0.2.0
```

Remove lockouts

If the cPHulk service locks you out of your cPanel account, the `/scripts2/doautofixer?autofix=disable_cphulkd` script in WHM can disable cPHulk and allow you to log in.

For example, log in to WHM and navigate to `https://www.example.com:2087/scripts2/doautofixer?autofix=disable_cphulkd`, where `www.example.com` represents your server's hostname.

If you enabled the *Block IP addresses at the firewall level if they trigger brute force protection* or the *Block IP addresses at the firewall level if they trigger a one-day block* options in WHM's *cPHulk Brute Force Protection* interface (*WHM >> Home >> Security Center >> cPHulk Brute Force Protection*), remove the `iptables` rule that the system created. To do this, run the following command:

```
iptables -F cphulk && mysql -e "Delete from cphulkd.login_track;"
```

Note:
This command removes **all** of the cPHulk service's lockouts. To remove the lockout for a specific IP address, on servers that run cPanel

& WHM version 11.50 or later, call WHM API 1's `flush_cphulk_login_history_for_ips` function.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- cPHulk Management on the Command Line
- How to Configure Your Firewall for cPanel Services
- Basic Security Concepts
- How to Purchase a KernelCare License
- Additional Security Software

- How to Use cPanel API Tokens
- Security
- Man-in-the-Middle Attacks
- How to Configure Microsoft Windows 7 to use TLS Version 1.2
- Important Notices

- cPHulk Management on the Command Line
- How to Configure Your Firewall for cPanel Services
- Basic Security Concepts
- How to Purchase a KernelCare License
- Additional Security Software

- WHM API 1 Functions - flush_cphulk_login_history
- WHM API 1 Functions - get_cphulk_failed_logins
- WHM API 1 Functions - get_cphulk_excessive_brutes
- WHM API 1 Functions - get_cphulk_brutes
- WHM API 1 Functions - save_cphulk_config