WP fail2ban Blocklist

Charles Lecklider

Aug 23, 2022

CONTENTS

WP fail2ban Blocklist is a collaborative preemptive blocklist for ClassicPress and WordPress.

CHAPTER

ONE

CONFIGURATION

1.1 fail2ban

1.1.1 Standard Filters

The filter files included should not be edited; there are no user-serviceable parts inside.

Typical Settings

If you are using the typical settings for *WPf2b* the Blocklist add-on will work without further configuration.

Creating a Custom Jail

1. Copy `wpf2b-blocklist-hard.conf` to your `fail2ban/filters.d` directory
2. Create a new file in `fail2ban/jail.d` called `wpf2b-blocklist.conf`

```
[wpf2b-blocklist-hard]
enabled = true
filter = wpf2b-blocklist-hard
logpath = /var/log/auth.log
maxretry = 1
port = http,https
```

Note: Make sure you change `logpath` to the correct log for your OS. If your OS uses *systemd* it may be simpler and/or easier to install a real syslog service first.

Tip: It is *strongly* recommended that you also use a different `syslog` facility with a custom jail.

See also:

Using a local0..7 Facility

3. Add the following to `wp-config.php`

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_CUSTOM_JAIL', true);
```

See also:

WP_FAIL2BAN_ADDON_BLOCKLIST_CUSTOM_JAIL

4. Reload or restart `fail2ban`

1.2 Syslog

If you are using a custom jail is it *strongly* recommended that you also use one of the `local0..7` facilities.

1.2.1 Using a local0..7 Facility

The BNS sends the list of IPs to block as a single batch, and each IP address results in one line written to `syslog`. With some plans sending as many as 1000 IPs the default log (`/var/log/auth.log`) can be swamped with BNS entries, making it difficult to use for its usual purposes.

To prevent this you should configure the Blocklist to use one of the local facilities, for example, `local3`.

Configuring `syslogd`

It is assumed that you have configured the `syslogd` variant you use to write `local3` to `/var/log/wpf2b-block.log`.

1.2.2 Configuring WP fail2ban

Add the following to your `wp-config.php` file:

```
/**
 * The blocklist messages use the "block" class
 */
define('WP_FAIL2BAN_PLUGIN_LOG_BLOCK', true);

/**
 * Use the custom facility we configured earlier for the block messages.
 *
 * Be sure to change this to match the syslog facility you're using.
 */
define('WP_FAIL2BAN_PLUGIN_BLOCK_LOG', LOG_LOCAL3);
```

Update your Blocklist jail to use the new log file:

```
[wpf2b-blocklist-hard]
enabled = true
filter = wpf2b-blocklist-hard
logpath = /var/log/wpf2b-block.log
maxretry = 1
bantime = 86400
```

Reload or restart `fail2ban` and check everything is working after the next BNS update.

1.3 Site Health Tool

New in version 2.1.0.

WP fail2ban Blocklist uses the standard WordPress Site Health tool to check that the Secret Key is available for communication with the BNS, and if possible, that `fail2ban` has been configured correctly.

See also:

WP fail2ban - Site Health Tool

CHAPTER

TWO

DEFINE() CONSTANTS

2.1 All

2.1.1 WP_FAIL2BAN_ADDON_BLOCKLIST_CUSTOM_JAIL

New in version 1.0.0.

Changes the log format to match entries in `wpf2b-blocklist-hard.conf` instead of `wordpress-hard.conf`.

If you cannot set `maxretry = 1` in your `wordpress-hard` jail you must set this and create a custom jail.

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_CUSTOM_JAIL', true);
```

Default: `false`

See also:

Creating a Custom Jail

2.1.2 WP_FAIL2BAN_ADDON_BLOCKLIST_IGNORE_IPS

New in version 1.0.0.

Changed in version 2.0.0: Entries can include IPv6 addresses.

A list of IP addresses to ignore if they appear in a Blocklist update.

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_IGNORE_IPS', [
   '1.2.3.4',
   '2.3.4.5/24'
]);
```

Default: `[]` *(empty list)*

Commonly used when accessing a site via shared access (e.g. Campus proxy, 3rd-party VPN, etc.).

Note: IPv6 addresses require *WP fail2ban* version 5 or later.

Tip: If you have whitelisted IPs in `fail2ban` because of shared access you should also add them here.

See also:

WP_FAIL2BAN_PROXIES has the same syntax.

2.1.3 WP_FAIL2BAN_ADDON_BLOCKLIST_LOG

New in version 1.0.0.

The syslog facility to use for a custom jail.

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_LOG', LOG_LOCAL7);
```

Default: `LOG_AUTH` *or* `LOG_AUTHPRIV`

See also:

- *WP_FAIL2BAN_ADDON_BLOCKLIST_CUSTOM_JAIL*
- WP_FAIL2BAN_USE_AUTHPRIV

2.2 Logging

2.3 Miscellaneous

2.4 Remote IPs

2.5 WP fail2ban

- WP_FAIL2BAN_SITE_HEALTH_SKIP_FILTERS
- WP_FAIL2BAN_INSTALL_PATH