

# Web Hosting

## Installation and configuration of clamscan Installation and configuration of clamscan

1. Install epel repo if not available already.

```
yum install epel-release
```

2. Install clamav.

```
yum install clamav
```

This will install clamav. You should update the virus definitions before doing your first scan. To do this, issue the following command.

```
freshclam
```

3. scan the server using clamscan command

```
clamscan -irl /folder/to/scan
```

Eg:

```
clamscan -irl /var/www/vhosts/example.com
```

The above command will scan the root folder and scan report(only infected files) will saved in cscanreport file.

use clamscan -help to find more options.

Unique solution ID: #1278

Author: Bytehouse Technical Support

Last update: 2015-10-13 04:27