

VirtFS - Jailed Shell

Overview

- [The /home/virtfs/ directory](#)
- [Enable a jailed shell environment](#)
 - [Exim and VirtFS](#)
 - [CSF or LFD alerts](#)
- [Disable or remove a jailed shell environment](#)
 - [Disable the jailed shell environment](#)
 - [Remove a user's jailed shell environment](#)
 - [The /scripts/clear_orphaned_virtfs_mounts script](#)
- [Additional documentation](#)

Overview

cPanel & WHM uses VirtFS to provide a jailed shell environment for users who connect to a server via SSH. The jailed shell acts as a container for the user, and does **not** allow the user to access other users' home directories on the server.

- Unlike a normal shell environment, a jailed shell environment increases security for a server's other users.
- Users in a jailed shell environment can run otherwise-unavailable commands (for example, `crontab` and `passwd`).

The /home/virtfs/ directory

Warning:

Do **not** use the `rm` command to remove any mounted file or directory within the `/home/virtfs/` directory.

- If you run the `rm` command on any mounted file or directory within the `/home/virtfs/` directory, you will also delete all of the files in the directory to which it is mounted.
- This action **will** render your server **nonfunctional**.

When a user logs in to a jailed shell environment via SSH or SFTP for the first time, the system creates the `/home/virtfs/` directory. This directory contains configuration files, utilities, and BIND mounts.

- You **cannot** prevent the creation of this directory or disable it.
- This directory does **not** use any disk space. However, because it is a virtual mount point, some commands (for example, `du`) report that the directory uses disk space.
- BIND mounts create a virtual link between two locations on the file system.
 - For example, if a user views the contents of the `/home/virtfs/username/usr/bin/` directory, the user actually sees the contents of the `/usr/bin/` directory.
 - For more information about BIND mounts, run the `man 8 mount` command.

Notes:

- Servers that run CentOS 7, CloudLinux™ 7, or Red Hat® Enterprise Linux (RHEL) 7 may use additional mount points for common system paths (for example, `/usr/bin`). Do **not** dismount these mount points.
- On servers that run CentOS 7, CloudLinux 7, or RHEL 7, the `/etc/mtab` symlink points to the `/proc/self/mounts` file.

Enable a jailed shell environment

WHM includes two options to activate a jailed shell environment. The option that you use depends on the type of users for whom you wish to enable jailed shells.

To enable a jailed shell environment for all new and modified users, use the *Use cPanel® jailshell by default* option in WHM's [Tweak Settings](#) interface (*WHM >> Home >> Server Configuration >> Tweak Settings*).

- This option allows you to force the use of a jailed shell for new accounts and accounts that you subsequently edit in the following interfaces:
 - WHM's [Modify an Account](#) interface (*WHM >> Home >> Account Functions >> Modify An Account*).
 - WHM's [Upgrade/Downgrade an Account](#) interface (*WHM >> Home >> Account Functions >> Upgrade/Downgrade An Account*).
- This option does **not** affect accounts that already exist on the server but that you have not edited in these interfaces.

To enable a jailed shell environment for a specific user, use WHM's [Manage Shell Access](#) interface (*WHM >> Home >> Account Functions >>*

Manage Shell Access).

Note:

When you enable jailed shell access for a user, the system sets the user's shell to the `/usr/local/cpanel/bin/jailshell` location.

Exim and VirtFS

When a user's shell location is `/usr/local/cpanel/bin/jailshell` (jailed shell is enabled) or `/usr/local/cpanel/bin/noshell` (all shells are disabled), Exim runs any process from alias or filter files inside VirtFS. This action provides extra security because Exim commands run in a jailed shell and do not affect other users.

CSF or LFD alerts

If you use a utility that monitors system changes (for example, CFS or LFD), you may see an alert that resembles the following example after you upgrade:

```
The following list of files have FAILED the md5sum comparison test. This means that the file has been changed in some way. This could be a result of an OS update or application upgrade. If the change is unexpected it should be investigated:
```

```
/bin/crontab: FAILED
/bin/passwd: FAILED
```

This is a false positive warning. cPanel & WHM uses the `/bin/crontab` and `/bin/passwd` symlinks to link to files in the `/usr/bin` directory. These symlinks allow jailed shell environments to access the `crontab` and `passwd` commands.

Disable or remove a jailed shell environment

Warning:

You **cannot** completely remove the jailed shell system (VirtFS). The directions below remove a jailed shell environment, but **cannot** prevent the recreation of the jailed shell environment.

The following processes may recreate the jailed shell environment:

- Exim processing filters.
- Piped email addresses.
- Cron jobs.
- Jailed Apache virtual hosts that use the `mod_ruid2` module via the *EXPERIMENTAL: Jail Apache Virtual Hosts using mod_ruid2 and cPanel® jailshell* option in WHM's [Tweak Settings](#) interface (*WHM >> Home >> Server Configuration >> Tweak Settings*).

Disable the jailed shell environment

Warning:

You **cannot** disable the `/home/virtfs/` directory for your users, even if you disable jailed shell access. For more information about the `/home/virtfs/` directory, read the [The /home/virtfs/ directory](#) section above.

To disable the jailed shell environment for a specific user, use WHM's *Manage Shell Access* interface (*Home >> Account Functions >> Manage Shell Access*).

To disable the jailed shell environment for all of the users on your server, perform the following steps:

1. Disable the *Use cPanel® jailshell by default* option in WHM's [Tweak Settings](#) interface (*WHM >> Home >> Server Configuration >> Tweak Settings*).
2. Select *Disabled Shell* for all of the server's accounts in WHM's *Manage Shell Access* interface (*Home >> Account Functions >> Manage*

Shell Access).

Note:

When you disable jailed shell access, the system sets the users' shells to the `/usr/local/cpanel/bin/noshell` location. With this location, the user retains access to SFTP in a non-jailed environment.

Remove a user's jailed shell environment

To remove a jailed shell environment, perform the following steps:

1. Disable the jailed shell environment for the user in WHM's *Manage Shell Access* interface (*WHM >> Home >> Account Functions >> Manage Shell Access*).
2. To unmount the VirtFS BIND mounts, run the following command, where `username` is the desired account username:

```
umount /home/virtfs/username/usr/bin
```

The `/scripts/clear_orphaned_virtfs_mounts` script

You can run the `/scripts/clear_orphaned_virtfs_mounts` script to unmount the BIND mounts for users who no longer exist or who no longer use a jailed shell environment.

- This script removes the `/home/virtfs/username/` directory and its contents, where `username` is an affected account's username.
- To force the removal of all VirtFS mount points, run the following command:

```
/scripts/clear_orphaned_virtfs_mounts --clearall
```

To check your system for VirtFS mount points, run the following command, where `username` is the desired account username:

```
grep -i username /proc/mounts
```

Additional documentation

Suggested documentation [For cPanel users](#) [For WHM users](#) [For developers](#)

- [VirtFS - Jailed Shell](#)
- [Manage Shell Access](#)
- [SSH Password Authorization Tweak](#)
- [Terminal in WHM](#)
- [Manage root's SSH Keys](#)

- [SSH Access](#)
- [Terminal in cPanel](#)

- [VirtFS - Jailed Shell](#)
- [How to Troubleshoot Jailshell Problems on a Virtuozzo or OpenVZ VPS](#)
- [How to Create Custom Jailed Shell Mounts](#)
- [Manage Shell Access](#)
- [SSH Password Authorization Tweak](#)

- cPanel API 2 Functions - SSH::genkey_legacy
- cPanel API 2 Functions - SSH::delkey
- cPanel API 2 Functions - SSH::fetchkey
- cPanel API 1 Modules - SSH
- cPanel API 2 Functions - SSH::authkey