

OneFS: How to lock (chroot jail) FTP users into a specific directory

Article Number:000089716 Version:4

Key Information

Audience: Level 30 = Customers	Original Create Date: Sat May 25 21:16:23 GMT 2013	Article Type: Break Fix
Channels:	First Published: Wed May 29 20:33:13 GMT 2013	Validation Status: Final Approved
Originally Created By: Isilon Published	Last Modified: Tue Jul 23 22:31:20 GMT 2013	Last Published: Tue Jul 23 22:31:20 GMT 2013
Summary:		

Article Content

Issue: **Introduction**

This article describes how to use the `isi ftp` command to configure access to directories on the cluster for users connecting using FTP.

The following procedures are covered:

- List the current ftp settings.
- Restrict all ftp users to their home directory.
- Restrict all users to a specific directory other than their home directory.
- Restrict some users to their home directory while granting exceptions to other users.
- Restrict users to a specific directory using a configuration file.

Resolution: **Procedures**

List the current FTP settings

1. Open an SSH connection on any node in the cluster and log on using the "root" account.
2. Run the following command to list the current ftp settings:

```
isi ftp ls
```

Output similar to the following is displayed:

```
accept-timeout 60
allow-anon-access NO
allow-anon-upload YES
allow-dirlists YES
allow-downloads YES
allow-local-access YES
```

```
allow-writes YES
always-chdir-homedir YES
anon-chown-username root
anon-root-path /ifs/home/ftp
anon-umask 077
ascii-mode off
connect-timeout 60
data-timeout 300
dirlist-localtime NO
dirlist-names hide
file-create-perm 0666
local-root-path local user home directory
local-umask 077
server-to-server NO
session-timeout 300
user-config-dir
denied-user-list (none)
limit-anon-passwords NO
anon-password-list (disabled)
chroot-local-mode No local users chrooted; exception list inactive
chroot-exception-list (none)
```

In the above output, the `local-root-path` is the local user's home directory, the `user-config-dir` has not been defined, `chroot-local-mode` is disabled, and the `chroot-exception-list` is empty. This is the default FTP configuration. These options will be configured in the procedures below.

NOTE

For additional information on FTP configuration commands, see the [Isilon OneFS 7.0.2 Command Reference](#).

Restrict all FTP users to their home directory

Run the following command to restrict (chroot jail) all FTP users to their home directory after they login:

```
isi ftp chroot-local-mode all
```

When any FTP user logs in, they will be restricted to their home directory, typically `/ifs/home/<user name>`.

Restrict all FTP users to a directory other than their home directory

To restrict all users to a specified directory after they log in , run the following commands:

1. Enable `chroot-local-mode` for all users:

```
isi ftp chroot-local-mode all
```

2. Specify the directory that FTP users will log in to, where `<path>` is the absolute path to the directory:

```
isi ftp local-root-path -v <path>
```

For example, to direct all users to the `/ifs/ftp` directory, run the following command:

```
isi ftp local-root-path -v /ifs/ftp
```

Restrict some users to their home directory while granting exceptions to other users

You can set up an exception list so that specified users are allowed to navigate outside of their home directory. To restrict most users, but allow specified user exceptions, run the following commands:

1. Run the following command to set `chroot-local-mode` to `all-with-exceptions`:

```
isi ftp chroot-local-mode all-with-exceptions
```

Output similar to the following is displayed:

```
chroot-local-mode: all -> all-with-exceptions
chroot-exception-list is active.
```

Restrict users to a specific directory using a configuration file

To restrict some users to their home directory, but restrict other users to different directories, do the following:

- To configure the exception list, run the following command, where `<user>` is the user who is being granted the exception:

```
isi ftp chroot-exception-list add <user>
```

Output similar to the following is displayed:

```
chroot-exception-list: added user '<user>' to list
```

NOTE

Repeat Step 2 for each user that you need to add to the exception list.

1. Run the following command to enable FTP chroot for all users:

```
isi ftp chroot-local-mode all
```

2. Create a per-user configuration file directory, where `<path>` is the absolute path to the directory:

```
mkdir -p <path>
```

For example :

```
mkdir -p /ifs/vsftpd/user_config
```

3. Create a configuration override file for the user who will be restricted to a different directory, where `<username>` is the name of the user and `<path>` is the directory to which the user will be restricted after they login:

```
echo local_root=<path> >> /ifs/vsftpd/user_config/<username>
```

```
echo chroot_local_user=yes >> /ifs/vsftpd/user_config/<username>
```

For example, to create a configuration file for the user "sam" so that they are restricted to the */ifs/ftp_users* directory, run the following commands:

```
echo local_root=/ifs/ftp_users >> /ifs/vsftpd/user_config/sam
```

```
echo chroot_local_user=yes >> /ifs/vsftpd/user_config/sam
```

4. Verify that the file was created correctly:

```
cat /ifs/vsftpd/user_config/sam
```

Output similar to the following is displayed:

```
local_root=/ifs/ftp_users  
chroot_local_user=yes
```

- Specify the directory in which the per-user configuration overrides are stored, where *<path>* is the absolute path to the directory:

```
isi ftp user-config-dir -v <path>
```

For example:

```
isi ftp user-config-dir -v /ifs/vsftpd/user_config
```

Article Metadata

Product: Isilon, Isilon OneFS5.5, Isilon OneFS6.0, Isilon OneFS6.5, Isilon OneFS7.0, Isilon OneFS

External Source: Primus

Primus/Webtop solution ID: emc14000584

Originally Created By: Isilon Published