

LOCAL WEB SERVER FOR IN-MEMORY HOST CLI ACTIONS

For Host CLI Actions that use in-memory execution, you can upload zip files to the Director that, when detected, get served to the Actor as part of the Host CLI Action being run. One example of a Host CLI Action that uses in-memory execution is A104-844: Host CLI - In-Memory Download, Execution with Rundll32, Javascript, Powershell.

Prerequisites

When uploading zip files to run with a Host CLI Action that uses in-memory execution, follow these guidelines:

- Only HTTP is supported.
- The server listens on localhost only (in other words, on the current system that is attempting to access the file).
- All files to be served must be included in a single-level (no subdirectories) zip file.
- The zip file must either be password free or use a default password (`0p3nZ!p`).
- The zip filename must be in the format `vserver_files*.zip`
 - Examples of valid zip filenames:
 - `vserver_files.zip`
 - `vserver_files_A-200-004.zip`
- The default server port is 3344. If needed, you can override this port by adding `_port_<portnum>` immediately before the `.zip` extension. For example, both of the following zip filenames would cause the server to listen on port 443:
 - `vserver_files_port_443.zip`
 - `vserver_files_A-200-004_port_443.zip`

Start the Local Web Server

When a Host CLI Action that uses in-memory execution is run, a temporary web server starts on the Actor itself to receive the zipped files. The following is an outline of that process:

1. If a file dependency is found whose destination name matches **vserver_files*.zip**, the Actor automatically starts the local HTTP server. This step is done as a separate process when file dependencies are processed.
2. The default port is **3344**.
3. All files in the zip file are made available for download.
4. The server operates on the obfuscated zip file (`*.fta`). This file is deobfuscated in memory, so neither the deobfuscated zip nor the files included in it are written to disk.



The server shuts down automatically. This step happens after all commands are run or after the timeout (120 seconds) has elapsed, whichever happens first.