

Virus Scan Curation Task

Virus Scan Bitstreams in DSpace

Clam AntiVirus is an open source (GPL) anti-virus toolkit for UNIX. The virus scanning curation task interacts with the ClamAV virus scanning service to scan the bitstreams contained in items, reporting on infection(s). Like other curation tasks, it can be run against a container or item, in the GUI or from the command line. It should be installed according to the documentation at <http://www.clamav.net>. It should not be installed in the dspace installation directory. You may install it on the same machine as your dspace installation, or on another machine which has been configured properly.

Setup the service from the ClamAV documentation

This plugin requires a ClamAV daemon installed and configured for TCP sockets. Instructions for installing ClamAV (<http://www.clamav.net/doc/latest/clamdoc.pdf>)

NOTICE: The following directions assume there is a properly installed and configured clamav daemon. Refer to links above for more information about ClamAV.

The Clam anti-virus database must be updated regularly to maintain the most current level of anti-virus protection. Please refer to the ClamAV documentation for instructions about maintaining the anti-virus database.

DSpace Configuration

In [dspace]/config/modules/, edit the configuration file curate.cfg:

- Add the plugin to the comma separated list of curation tasks.

```
### Task Class implementations
plugin.named.org.dspace.curate.CurationTask = \
org.dspace.curate.ProfileFormats = profileformats, \
org.dspace.curate.RequiredMetadata = requiredmetadata, \
org.dspace.curate.ClamScan = vscan
```

- Optionally, add the vscan friendly name to the configuration to enable it in the administrative user interface.

```
ui.tasknames = \
profileformats = Profile Bitstream Formats, \
requiredmetadata = Check for Required Metadata, \
vscan = Scan for Viruses
```

In <dspace install>/config/modules, edit configuration file clamav.cfg:

```
service.host = 127.0.0.1
Change if not running on the same host as your DSpace installation.
service.port = 3310
Change if not using standard ClamAV port
socket.timeout = 120
Change if longer timeout needed
scan.failfast = false
Change only if items have large numbers of bitstreams
```

Task Operation from the GUI

Curation tasks can be run against container and item dspace objects by e-persons with administrative privileges. A curation tab will appear in the administrative ui after logging into DSpace:

1. Click on the curation tab.
2. Select the option configured in ui.tasknames above.
3. Select Perform.

Task Operation from the curation command line client

To output the results to the console:

```
[dspace]/bin/dspace curate -t vscan -i <handle of container or item dso> -r -
```

Or capture the results in a file:

```
[dspace]/bin/dspace curate -t vscan -i <handle of container or item dso> -r - > /<path...>/<name>
```

Table 1 – Virus Scan Results Table

GUI (Interactive Mode)	FailFast	Expectation
Container	T	Stop on 1 st Infected Bitstream
Container	F	Stop on 1 st Infected Item
Item	T	Stop on 1 st Infected Bitstream
Item	F	Scan all bitstreams
Command Line		
Container	T	Report on 1 st infected bitstream within an item/Scan all contained Items
Container	F	Report on all infected bitstreams/Scan all contained Items
Item	T	Report on 1 st infected bitstream
Item	F	Report on all infected bitstreams