Antivirus Plugin

Bacula Systems Documentation

Contents

Contents

Distinction between Antivirus Plugin and Malware

In an Antivirus Check, Bacula will transmit the files to the ClamAV Antivirus Socket, which will perform the scan and report to Bacula if any viruses are discovered. In the instance of Malware, Bacula will retrieve the Malware database signatures from https://abuse.ch/ and then do a file verification with those signatures. If a Backup job finds malware in the backup content, an error message is generated and the Job status is changed.

- *Overview*
- *ClamAV Installation*
  - *Debian / Ubuntu*
  - *Fedora / Redhat / Centos*
- *Bacula Enterprise Antivirus Plugin Installation*
- *Bacula Enterprise Verify Job Configuration*
  - *Parameters*
  - *Plugin Options*
- *Bacula Enterprise Antivirus Plugin Behavior*

1 Overview

The Bacula Enterprise Antivirus Plugin provides integration between the ClamAV Antivirus daemon and Bacula verify jobs, allowing post-backup virus detection within Bacula Enterprise.

2 ClamAV Installation

ClamAV is an open source (GPLv2) anti-virus toolkit. It provides a flexible and scalable multi-threaded daemon. For more information on ClamAV architecture, best practices and options, please refer to https://docs.clamav.net/

2.1 Debian / Ubuntu

Installation:

Use the existing Debian packages:

```
sudo apt-get update
sudo apt-get install clamav clamav-daemon
```

TCP Configuration:

The ClamAV 'clamd' daemon is configured with the clamav.conf file (located in /etc/clamav/). By default, the ClamAV daemon listens on a Unix LocalSocket:

```
LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
```

In order for Bacula to interact correctly with ClamAV, it is essential to reconfigure the ClamAV daemon so it allows TCP connections instead.

On Debian you can do so automatically by running:

```
sudo dpkg-reconfigure clamav-daemon
```

Answer "yes" to reconfigure automatically Make sure to change the socket type to "TCP". Choose the TCP port clamd will listen on (The default port 3310 will be assumed in the rest of the documentation). Continue the reconfiguration according to your needs (press enter to keep the default settings) At the end of the reconfiguration process, the ClamAV daemon restarts. You can verify that the clamav.conf file now contains:

```
TCPSocket 3310
```

Alternatively, you can reconfigure manually, by editing clamav.conf. Replace:

```
LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
```

with:


```
TCPSocket 3310
```

and restart the ClamAV daemon:

```
sudo systemctl restart clamav-daemon
```

2.2 Fedora / Redhat / Centos

Installation:

EPEL creates ClamAV packages for Fedora. To enable the EPEL repository for CentOS:

```
sudo dnf install -y epel-release
```

EPEL offers a selection of packages to install ClamAV:

```
clamd - The ClamAV Daemon
clamav - End-user tools for the ClamAV scanner
clamav-data - Virus signature data for the ClamAV scanner
clamav-devel - Header files and libraries for the ClamAV scanner
clamav-lib - Dynamic libraries for the ClamAV scanner
clamav-milter - Milter module for the ClamAV scanner
clamav-update - Auto-updater for the ClamAV scanner data-files
```

Bacula minimally requires clamav, clamd, and clamav-update to run:

```
sudo dnf install -y clamav clamd clamav-update
```

TCP Configuration:

The ClamAV daemon is configured with the clamav.conf file (located in /etc/clamav/).

Edit the configuration file:

```
sudo dnf install nano -y
sudo nano /etc/clamd.d/scan.conf
```

Make sure the Example line is commented out:

```
#Example
```

By default, the ClamAV daemon connects over Unix LocalSocket. In order for Bacula to interact correctly with ClamAV, it is essential to reconfigure the ClamAV daemon so it allows TCP connections instead. enable TCP connection instead by uncommenting the following line:

```
TCPSocket 3310
```

Optionally, you can also restrain the TCP binding (by default the ClamAV daemon binds to INADDR_ANY):

```
TCPAddr 127.0.0.1
```

Once that's done, you can run the virus definition database update:


```
sudo freshclam
```

Lastly, start the clamd service and run it on boot:

```
sudo systemctl enable clamd@scan
sudo systemctl start clamd@scan
```

3 Bacula Enterprise Antivirus Plugin Installation

Installation of the Bacula Enterprise Antivirus Plugin is most easily done by adding the repository file suitable for the existing subscription and the distributions package manager configuration. An example would be `/etc/apt/sources.list.d/bacula.list` for Debian based Linux distributions with the following content:

```
# Bacula Enterprise
deb https://www.baculasystems.com/dl/@customer-string@/debs/bin/@version@/bullseye-64/␣
↪stretch main
```

After that, a run of `apt-get update` is needed. Then, the plugin can be installed using `apt-get install bacula-enterprise-antivirus-plugin`

On Redhat/CentOS 7 extend the repository file for your package manager to contain a section for the plugin - `/etc/yum.repos.d/bacula.repo`:

```
[Bacula]
name=Bacula Enterprise
baseurl=https://www.baculasystems.com/dl/@customer@/rpms/bin/@version@/rhel7-64/
enabled=1
protect=0
gpgcheck=0
```

Then perform a `yum update` and after that the package `bacula-enterprise-antivirus-plugin` can be installed with `yum install bacula-enterprise-antivirus-plugin`.

Manual installation of the packages can be done after downloading the right files from the Bacula Systems provided download area, and then using the low-level package manager (`rpm` or `dpkg`) to do the plugin installation.

4 Bacula Enterprise Verify Job Configuration

4.1 Parameters

The Bacula Enterprise Antivirus Plugin accepts two parameters:

- **hostname:** The binding address of the ClamAV daemon (specified in clamav.conf as TCPAddr). Can be any IP4 TCP address. Default is 'localhost'
- **port:** The ClamAV daemon port number (specified in clamav.conf as TCPSocket). Default port is 3310.

4.2 Plugin Options

Contrary to “classical” Bacula FD plugins, these parameters are configured in the Verify Job as PluginOptions rather than a “Plugin =” in a FileSet.

There are three possible ways to instruct a Bacula Verify Job to run the antivirus plugin:

Add a PluginOptions directive to the Verify Job configuration (recommended):

```
Job {
  Name = Verify_and_AV_Scan
  Type = Verify
  Level = Data
  Client = localhost-fd
  FileSet = LinuxHome
  Storage = File
  Pool = Default
  Messages = Standard
  PluginOptions = "antivirus: hostname=127.0.0.1 port=3310"   # <---- Add this line here
}
```

Specify the `pluginoptions` as a parameter to the ‘run’ command in bconsole:

```
*run job=Verify_and_AV_Scan jobid=1 storage=File1 pluginoptions="antivirus:␣
↪hostname=localhost port=3310"
```

Dynamically modify the verify job within bconsole

```
*run job=Verify_and_AV_Scan jobid=1 storage=File1

JobName:        Verify_and_AV_Scan
Level:          Data
Client:         localhost-fd
FileSet:        LinuxHome
Pool:           Default (From Job resource)
Storage:        File1 (From Command input)
Verify Job:     LinuxHome.2021-10-12_05.31.58_03
Verify List:
When:           2021-10-12 05:40:12
Priority:       10
OK to run? (yes/mod/no): m
Parameters to modify:
    1: Level
    2: Storage
    3: Job
    4: FileSet
    5: Client
    6: When
    7: Priority
    8: Pool
    9: Verify Job
    10: Plugin Options
Select parameter to modify (1-10): 10
Please Plugin Options string: antivirus: hostname=127.0.0.1 port=3310
Run Verify Job
```

(continues on next page)

(continued from previous page)

```
JobName:         Verify_and_AV_Scan
Level:           Data
Client:          localhost-fd
FileSet:         LinuxHome
Pool:            Default (From Job resource)
Storage:         File1 (From Command input)
Verify Job:      LinuxHome.2021-10-12_05.31.58_03
Verify List:
When:            2021-10-12 05:40:12
Priority:        10
Plugin Options: antivirus: hostname=127.0.0.1 port=3310
OK to run? (yes/mod/no): yes
```

5 Bacula Enterprise Antivirus Plugin Behavior

Under normal conditions, the Verify Job will silently scan existing files from the specified backup and should terminate with a "Verify OK" Job status:

```
run job=Verify_and_AV_Scan jobid=1 storage=File1

JobName:         Verify_and_AV_Scan
Level:           Data
Client:          localhost-fd
FileSet:         LinuxHome
Pool:            Default (From Job resource)
Storage:         File1 (From Command input)
Verify Job:      LinuxHome.2021-10-12_06.04.11_03
Verify List:
When:            2021-10-12 06:04:17
Priority:        10
Plugin Options: antivirus: hostname=localhost port=3310
OK to run? (yes/mod/no): yes

12-Oct 06:04 localhost-dir JobId 2: Verifying against JobId=1 Job=LinuxHome.2021-10-12_
↪06.04.11_03
12-Oct 06:04 localhost-dir JobId 2: Start Verify JobId=2 Level=Data Job=Verify_and_AV_
↪Scan.2021-10-12_06.04.17_05
12-Oct 06:04 localhost-dir JobId 2: Connected to Storage "File1" at localhost:8103 with␣
↪TLS
12-Oct 06:04 localhost-dir JobId 2: Using Device "FileStorage1" to read.
12-Oct 06:04 localhost-dir JobId 2: Connected to Client "localhost-fd" at localhost:8102␣
↪with TLS
12-Oct 06:04 localhost-fd JobId 2: Connected to Storage at localhost:8103 with TLS
12-Oct 06:04 localhost-sd JobId 2: Ready to read from volume "TestVolume001" on File␣
↪device "FileStorage1" (/mnt/archive).
12-Oct 06:04 localhost-fd JobId 2: Got plugin command = antivirus: hostname=localhost␣
↪port=3310
12-Oct 06:04 localhost-sd JobId 2: Forward spacing Volume "TestVolume001" to addr=228
12-Oct 06:05 localhost-sd JobId 2: End of Volume "TestVolume001" at addr=98844823 on␣
↪device "FileStorage1" (/mnt/archive).
```

(continues on next page)

(continued from previous page)

```
12-Oct 06:05 localhost-sd JobId 2: Elapsed time=00:00:51, Transfer rate=1.935 M Bytes/
↪second
12-Oct 06:05 localhost-dir JobId 2: Bacula localhost-dir 12.9.2 (11Oct21):
Build OS:               x86_64-pc-linux-gnu ubuntu 9.12
JobId:                  2
Job:                    Verify_and_AV_Scan.2021-10-12_06.04.17_05
FileSet:                LinuxHome
Verify Level:           Data
Client:                 localhost-fd
Verify JobId:           1
Verify Job:
Start time:             12-Oct-2021 06:04:19
End time:               12-Oct-2021 06:05:21
Elapsed time:           1 min 2 secs
Accurate:               no
Files Expected:         2,238
Files Examined:         2,238
Non-fatal FD errors:    0
SD Errors:              0
FD termination status:  OK
SD termination status:  OK
Termination:            **Verify OK**
```

When a virus is detected by ClamAV, an error is reported in the Bacula job log and the Job will continue to verify the rest of the files, but it will terminate with a "Verify OK – with warnings" Job status.

Within the job output, the antivirus plugin specifies the infected file(s) and the virus name(s) detected.

```
run job=Verify_and_AV_Scan jobid=3 storage=File1

JobName:        Verify_and_AV_Scan
Level:          Data
Client:         localhost-fd
FileSet:        LinuxHome
Pool:           Default (From Job resource)
Storage:        File1 (From Command input)
Verify Job:     LinuxHome.2021-10-12_06.05.22_07
Verify List:
When:           2021-10-12 06:05:27
Priority:       10
Plugin Options: antivirus: hostname=localhost port=3310
OK to run? (yes/mod/no): yes

12-Oct 06:05 localhost-dir JobId 4: Verifying against JobId=3 Job=LinuxHome.2021-10-12_
↪06.05.22_07
12-Oct 06:05 localhost-dir JobId 4: Start Verify JobId=4 Level=Data Job=Verify_and_AV_
↪Scan.2021-10-12_06.05.27_09
12-Oct 06:05 localhost-dir JobId 4: Connected to Storage "File1" at localhost:8103 with␣
↪TLS
12-Oct 06:05 localhost-dir JobId 4: Using Device "FileStorage1" to read.
12-Oct 06:05 localhost-dir JobId 4: Connected to Client "localhost-fd" at localhost:8102␣
↪with TLS
12-Oct 06:05 localhost-fd JobId 4: Connected to Storage at localhost:8103 with TLS
```

(continues on next page)

(continued from previous page)

```
12-Oct 06:05 localhost-sd JobId 4: Ready to read from volume "TestVolume001" on File␣
↪device "FileStorage1" (/mnt/archive).
12-Oct 06:05 localhost-fd JobId 4: Got plugin command = antivirus: hostname=localhost␣
↪port=3310
12-Oct 06:05 localhost-sd JobId 4: Forward spacing Volume "TestVolume001" to␣
↪addr=98844823
12-Oct 06:05 localhost-sd JobId 4: End of Volume "TestVolume001" at addr=98845442 on␣
↪device "FileStorage1" (/mnt/archive).
12-Oct 06:05 localhost-sd JobId 4: Elapsed time=00:00:01, Transfer rate=197  Bytes/second
12-Oct 06:05 localhost-fd JobId 4: **Error: /home/nbizet/src/bacula-bee/regress/tmp/
↪eicar Virus detected stream: Eicar-Signature FOUND**
12-Oct 06:05 localhost-dir JobId 4: Bacula localhost-dir 12.9.2 (11Oct21):
Build OS:               x86_64-pc-linux-gnu ubuntu 9.12
JobId:                  4
Job:                    Verify_and_AV_Scan.2021-10-12_06.05.27_09
FileSet:                LinuxHome
Verify Level:           Data
Client:                 localhost-fd
Verify JobId:           3
Verify Job:
Start time:             12-Oct-2021 06:05:29
End time:               12-Oct-2021 06:05:29
Elapsed time:           1 sec
Accurate:               no
Files Expected:         1
Files Examined:         1
Non-fatal FD errors:    1
SD Errors:              0
FD termination status:  OK
SD termination status:  OK
Termination:            **Verify OK -- with warnings**
```

