

ClamAV Add-on for PCF[®]

Version 1.2

User's Guide

© 2018 Pivotal Software, Inc.


Table of Contents

Table of Contents	2
ClamAV Add-on for PCF	3
Troubleshooting ClamAV Add-on for PCF	9
Uninstalling ClamAV Add-on for PCF	11
Release Notes	12

ClamAV Add-on for PCF

Page last updated:

This topic describes how to add ClamAV to your Pivotal Cloud Foundry (PCF) deployment.

 **ClamAV Add-on for PCF v1.2 is no longer supported.** The support period for v1.2 has expired. To stay up to date with the latest software and security updates, update to more recent releases of ClamAV for PCF.

About ClamAV Add-on for PCF

This add-on may be necessary for regulatory purposes if your compliance auditor requires antivirus protection within the PCF environment. For example, auditors sometimes expect that antivirus protection be present in an environment that must comply with standards such as Payment Card Industry Data Security Standard (PCI DSS) or Health Insurance Portability and Accountability Act (HIPAA).

Prerequisites

 **Note:** ClamAV Add-on for PCF does not work on Windows.

To complete the ClamAV Add-on installation:

- You must be a PCF operator with admin rights. For more information, see [Understanding Pivotal Cloud Foundry User Types](#).
- You must have Pivotal Operations Manager (Ops Manager) v1.7 or later.
- ClamAV Add-on uses 610 MB of memory. Ensure you have at least 1 GB of memory free on each VM before deploying ClamAV Add-on.
- You must set up a local mirror to get ClamAV virus updates. For instructions on how to set up a local mirror, see [Private Local Mirrors](#) in the ClamAV documentation.

Create the ClamAV Manifest

The ClamAV manifest is a YAML file that contains runtime configuration information for ClamAV Add-on. Follow the steps below to create the ClamAV manifest for your deployment:

1. Create a file named `clamav.yml`, using the following code as a template.

```
releases:
- name: clamav
  version: 1.0.0
addons:
- name: clamav
  jobs:
  - name: clamav
    release: clamav
  properties:
    clamav:
      database_mirror: 192.0.2.1
```

2. (Required) Provide the hostname or IP address of a private ClamAV update mirror. Environments that cannot connect to the internet normally use an update mirror. If you do not specify a value, ClamAV defaults to an S3-based mirror for updates. For compliance reasons, only use the S3-based mirror in non-production environments. For how to set up a local mirror, see [Private Local Mirrors](#).
3. (Optional) If you have to use a proxy server to connect to the internet, do the following:
 - Add the `proxy_host` and `proxy_port` properties.
 - If the proxy server needs authentication, add `proxy_user` and `proxy_password` properties.

Replace the example text shown in bold:

```
releases:
- name: clamav
  version: 1.1.1
addons:
```

```
name: clamav
jobs:
  - name: clamav
    release: clamav
properties:
  clamav:
    on_access: no
    scheduled: yes
    proxy_host: proxy.localdomain
    proxy_port: 3128
    proxy_user: clamav
    proxy_password: secret
...
```

Download ClamAV Add-on

1. Download ClamAV Add-on software binary from the [Pivotal Network](#) to your local machine.
2. Copy the software binary to your Ops Manager virtual machine (VM).

```
$ scp -i PATH/TO/PRIVATE/KEY clamav-release.tar.gz ubuntu@YOUR-OPS-MANAGER-VM-IP:
```

3. Copy the ClamAV manifest, `clamav.yml` file, to your Ops Manager instance.

```
$ scp -i PATH/TO/PRIVATE/KEY clamav.yml ubuntu@YOUR-OPS-MANAGER-VM-IP:
```

4. SSH into Ops Manager.

```
$ ssh -i PATH-TO-PRIVATE-KEY ubuntu@YOUR-OPS-MANAGER-VM-IP
```

5. On the Ops Manager VM, navigate to the software binary location.

```
$ cd PATH-TO-BINARY
```

Deploy the ClamAV Add-on

Perform the following steps to deploy the ClamAV Add-on:

1. Log in to the BOSH Director.
 - For Ops Manager 1.10 or earlier:
 - i. On the Ops Manager VM, target your BOSH Director instance. For example:

```
$ bosh target YOUR-OPS-MANAGER-DIRECTOR-IP
Target set to 'Ops Manager'
Your username: director
Enter password: *****
Logged in as 'director'
```

- For Ops Manager 1.11 or later:
 - i. On the Ops Manager VM, create an alias in the BOSH CLI for your Ops Manager Director IP address. For example:

```
$ bosh2 alias-env my-env -e 10.0.0.3
```

- ii. Log in to the BOSH Director, specifying the newly created alias. For example:

```
$ bosh2 -e my-env log-in
```

2. Upload your release, specifying the path to the tarballed ClamAV binary, by running one of the following commands:
 - For Ops Manager 1.10 or earlier:

```
$ bosh upload release PATH-TO-BINARY/clamav-release.tar.gz
```

- For Ops Manager 1.11 or later:

```
$ bosh2 -e my-env upload-release PATH-TO-BINARY/clamav-release.tar.gz
```

3. List the releases by running one of the following commands, and confirm that ClamAV appears:

- For Ops Manager 1.10 or earlier:

```
$ bosh releases
```

- For Ops Manager 1.11 or later:

```
$ bosh2 -e my-env releases
```

4. Update your runtime configuration to include the ClamAV Add-on, specifying the path to the `clamav.yml` file you created above, by running one of the following commands:



Note: If you installed other BOSH add-ons, you must merge the ClamAV manifest into your existing add-on manifest. Append the contents of `clamav.yml` to your existing add-on YML file.

- For Ops Manager 1.10 or earlier:

```
$ bosh update runtime-config PATH-TO-YOUR-ADD-ON-YML.yml
```

- For Ops Manager 1.11 or later:

```
$ bosh2 -e my-env update-runtime-config --name=clamav PATH-TO-YOUR-ADD-ON-YML.yml
```

5. Verify that your runtime configuration changes match what you specified in the ClamAV manifest by running one of the following commands:

- For Ops Manager 1.10 or earlier:

```
$ bosh runtime-config
```

- For Ops Manager 1.11 or later:

```
$ bosh2 -e my-env runtime-config
```

For Example:

```
$ bosh2 -e my-env runtime-config
Acting as user 'admin' on 'micro'
releases:
- name: clamav
  version: 1.0.0

addons:
name: clamav
jobs:
- name: clamav
  release: clamav
...
```

6. Navigate to your Installation Dashboard in Ops Manager.

7. Click **Apply Changes**.

Configure Forwarding for ClamAV Alerts

The ClamAV BOSH release writes all alerts to the syslogs of the VMs in your deployment. You can use syslog forwarding to forward the alerts to a syslog aggregator.

- **Using the Pivotal Application Service (PAS) or Elastic Runtime tile:** Follow the steps to [Configure System Logging](#) in the PAS (or Elastic Runtime) tile. The syslog aggregator that you specify receives all alerts generated on PAS (or Elastic Runtime) VMs, including the ClamAV alerts.
- **Using the BOSH syslog release:** You can use the syslog BOSH release to forward system logs. For instructions, see the [syslog-release](#).

Note: When you configure syslog forwarding, ensure enough disk space for the logs. Make sure that log rotation is frequent enough. If in doubt, rotate the logs hourly or when they reach a certain size. Pivotal recommends forwarding logs to a remote syslog aggregation system.

Verify Your ClamAV Add-on Installation

1. [BOSH ssh](#) into one of the VMs in your deployment.
2. Run `monit summary`. Look for the following processes in the output:

```
The Monit daemon 5.2.4 uptime: 3d 0h 56m
Process 'clamd'           running
Process 'freshclam'      running
```

3. If `monit summary` does not list `freshclamd` and `clamd`, perform the following steps:
 - a. Try to start the ClamAV processes by running the following commands:

```
$ monit start clamd
$ monit start freshclam
```

- b. Run `monit summary` again. If you do not see the processes mentioned above, check `/var/vcap/sys/log/clamav` logs for errors.
4. If `monit summary` does list `freshclamd` and `clamd`, create a file on the VM with the following contents:

```
X5O!P%@AP[4PZX54(P^)7CC7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

This is a virus signature used to test anti-virus software.

After `clamscan` completes, a notification should appear in `/var/log/syslog`.

ClamAV Log Format

ClamAV log format is unstructured. On virus detection, the following text is sent to syslog:

```
Jul 11 17:36:35 k2lam76scmb clamd[3022]: SelfCheck: Database status OK.
Jul 11 17:42:34 k2lam76scmb clamd[3022]: /bin/infected-file: Eicar-Test-Signature FOUND
```

The logline can be generalized as follows:

```
clamd[PID]: <infected-file-path>: <virus name> FOUND
```

Enable On-Access Scan

ClamAV offers immediate file scanning upon file modification. This feature might reduce the time it takes to detect and report malware. Enable the feature through the `on_access` runtime config property, as follows.

1. In the `clamav.yml` file, add the `on_access` property under the `clamav` property, set `on_access` to `yes`:

```
releases:
- name: clamav
  version: 1.1.1

addons:
name: clamav
jobs:
- name: clamav
  release: clamav
properties:
clamav:
  on_access: yes
  scheduled: yes
```

...

2. Apply this configuration change by following the instructions from step 9, [Update your...](#), in the [Download and Deploy ClamAV Add-on](#) section above.

Disable Scheduled Scan

By default, ClamAV runs a virus scan every hour. You can disable the scan, but you cannot change the frequency.

To disable the scheduled scan, follow the steps below.

1. In the `runtime-config`, set the property `scheduled` to `no`
2. Apply the changes.

Choose the Action on Infected Files

You can configure ClamAV to take action when infected files are found. By default, a notification is sent to the syslog when an infected file is found. However, you can specify other actions, as listed in [step 2](#) below.

1. In the `clamav.yml` file, add the `action` property under the `clamav` property and, optionally, the `action_destination` property:

```
releases:
- name: clamav
  version: 1.1.7

addons:
name: clamav
jobs:
- name: clamav
  release: clamav
properties:
clamav:
  action: ACTION
  action_destination: PATH
...
```

2. Replace `ACTION` with one of the following values:
 - o `notify` — The default, only send a notification to syslog
 - o `remove` — Delete the infected file from the filesystem
 - o `move` — Move the infected file to the directory location specified by `action_destination`
 - o `copy` — Copy the infected file to the directory location specified by `action_destination`

If you don't supply an action, the function fails.

3. Replace `PATH` with the directory location where you want the infected files moved or copied to. The system does not scan the moved-to or copied-to location. If the directory path is not valid, the function fails.

Example configuration:

```
releases:
- name: clamav
  version: 1.1.7

addons:
name: clamav
jobs:
- name: clamav
  release: clamav
properties:
clamav:
  action: move
  action_destination: /var/vcap/data/clamav/found
...
```


Troubleshooting ClamAV Add-on for PCF

Page last updated:

This topic provides instructions to verify that the ClamAV-based antivirus add-on works with your Pivotal Cloud Foundry (PCF) deployment and provides general recommendations for troubleshooting and ensuring that the deployment is being protected as you expect.

ClamAV Installation Issues

Ops Manager Fails to Apply Changes

Symptom

Applying changes in Ops Manager fails. The bottom of the changelog contains an error message similar to the following:

```
...
Started updating job nats > nats/0 (12bfae02-b4af-4104-b2bd-227ff07b2d92) (canary). Done (00:02:31)
Failed updating job etcd_server > etcd_server/0 (f8e492bf-db09-4d38-8a73-5cf69d7b8a11) (canary): 'etcd_server/0 (f8e492bf-db09-4d38-8a73-5cf69d7b8a11)' is not running after update. Review logs for failed j

Error 400007: 'etcd_server/0 (f8e492bf-db09-4d38-8a73-5cf69d7b8a11)' is not running after update. Review logs for failed jobs: clamd
```

Explanation

The ClamAV mirror server was unavailable during initial deployment.

Solution

Review the manifest file, and replace the `database_mirror` key with the address of a stable mirror server. If you do not have a stable mirror server for reliable initial deployment, use the S3-based mirror: `pivotal-clamav-mirror.s3.amazonaws.com`

ClamAV Runtime Issues

ClamAV Is Not Detecting Malware

Symptom

Malware signature or sample malware is not detected, even though the ClamAV daemon is properly configured.

Explanation

Virus signatures are not up-to-date.

Solution

First, ensure that the [configuration checks](#) have been done, that the mirror server is correctly configured and is available on the network from within the PCF private subnet, and that at least one hour has elapsed. One hour is the default scan schedule interval.

If the local mirror is up-to-date and ClamAV is still failing to detect a malware sample, you might have encountered a new threat. Pivotal recommends

alerting the community via existing channels and reporting the suspicious file directly to the ClamAV team.

 **Note:** Pivotal does not provide support for ClamAV detection failures, mirror coordination, or threat tracking activity.

ClamAV Reports False Positives

Symptom

ClamAV reports a false positive result; a non-malicious file is reported to be a virus.

Explanation

ClamAV compares files to its database of known malicious patterns. ClavAV may detect a non-malicious file as a virus due to a coincidental similarity to those patterns.

Solution

Submit false positive reports to [ClamAV](#). You can also subscribe to the ClamAV email list to be kept up-to-date with ClamAV database changes.

Getting CPU Spikes While Using ClamAV

Symptom

ClamAV is taking more CPU resources than assigned in its configuration.

Explanation

ClamAV resource consumption is restricted using CGroups. ClamAV is resource-limited whenever other processes are active. However, CGroups allows ClamAV to occupy more CPU resources when all other processes are idle, because it does not impact their performance.

Solution

This is expected behavior from CGroups.

Uninstalling ClamAV Add-on for PCF

Page last updated:

This topic describes how to uninstall ClamAV from your deployment, and how to verify the uninstallation.

Uninstall ClamAV Add-on

1. Retrieve the latest runtime config by running one of the following commands:

- For Ops Manager v1.10 or earlier:

```
$ bosh runtime-config > PATH_TO_SAVE_THE_RUNTIME_CONFIG
```

- For Ops Manager v1.11 or later:

```
$ bosh2 -e my-env runtime-config > PATH_TO_SAVE_THE_RUNTIME_CONFIG
```

2. In the runtime config, remove all ClamAV properties under the `releases:` and `addons:` sections.

3. Update the runtime config.

- For Ops Manager v1.10 or earlier:

```
$ bosh update runtime-config PATH_TO_SAVE_THE_RUNTIME_CONFIG
```

- For Ops Manager v1.11 or later:

```
$ bosh2 -e my-env update-runtime-config --name=clamav PATH_TO_SAVE_THE_RUNTIME_CONFIG
```

4. Navigate to your **Installation Dashboard** in Ops Manager.

5. Click **Apply Changes**.

6. Wait for the installation to complete.

Verify the Uninstallation

1. [BOSH SSH](#) into one of the VMs in your deployment. If you are using PCF v1.11 or later, use the BOSH CLI v2. If you are using PCF v1.10 or earlier, use the BOSH CLI v1.

2. Run `monit summary`.

If ClamAV has uninstalled successfully, it should not show `clamd` or `freshclam` processes.

Release Notes

Page last updated:

This topic contains release notes for ClamAV Add-on for PCF.

v1.2.7 (GA)

Release Date: July 25, 2017

ClamAV Add-on for PCF:

- Sets ScanHTML to no if both Scheduled and On-access Scans are enabled to avoid deleted file conflicts
- This is a GA release, supported for production use

v1.2.1 (Beta)

Release Date: June 26, 2017

ClamAV Add-on for PCF:

- ClamAV works in offline environment
- Configurable whether to notify (default), isolate or delete a virus
- Note: Choose only one of the two options, Scheduled scanning (default) or On-access scanning (off by default)

v1.1.6 (Beta)


Release Date: March 30, 2017

ClamAV Add-on for PCF:

- Improved implementation of cgroups to work with diego
- Cgroup memory and cpu limits are configurable

```
properties:  
clamav.memory_limit: <Memory limit in bytes>  
clamav.cpu_limit: <CPU limit (percentage)>
```

- Allows downloading of the ClamAV database through an HTTP proxy server

-  **Note:** when upgrading from previous release, run “bosh deploy -recreate”

Known issues in this release:

- There is an intermittent issue with files being locked and not released when On-access scanning and Scheduled scanning are both enabled. To avoid this issue, only enable either On-access or Scheduled scanning, not both.

v1.0.29 (Beta)

Release Date: February 12, 2017

ClamAV Add-on for PCF:

- Bundles the clamav-0.99.2 distribution
- Restricts ClamAV resource use to 20% of CPU, 1GB of memory for stability
- Note: this release may cause a conflict with diego during startup and we recommend using 1.16 (Beta) or a more recent release

View Release Notes for Another Version

To view the release notes for another product version, select the version from the drop-down list at the top of this page.