File Integrity Monitoring for VMware Tanzu v2.0

File Integrity Monitoring for VMware Tanzu 2.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Pivotal File Integrity Monitoring

Warning: Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

Note: Pivotal has renamed File Integrity Monitoring Add-on for PCF. The new name is Pivotal File Integrity Monitoring.

Note: Pivotal has renamed *Pivotal Cloud Foundry* to *Pivotal Platform*.

This documentation describes setting up and using Pivotal File Integrity Monitoring (FIM).

Overview

Pivotal File Integrity Monitoring provides logs of file and directory modifications in monitored paths. Operators and auditors use these logs to satisfy security requirements for file integrity monitoring within the Pivotal Platform environment.

You can use FIM to help achieve compliance standards such as the Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA).

Key Features

File Integrity Monitoring enables you to:

- Monitor Pivotal Platform VMs and containers
- Specify path patterns to exclude
- Group path patterns under low severity
- Format log output
- Provide digest calculations of files

Product Snapshot

The following table provides version and version-support information about FIM.

Warning: FIM Add-on on Windows is in beta.

Element	Details
Version	2.0.0
Release date	January 7, 2019
Compatible Pivotal Operations Manager versions	2.5, 2.6, 2.7 and 2.8
Compatible versions	2.5, 2.6, 2.7 and 2.8
Compatible Pivotal Application Service for Windows (PASW) versions	2.5, 2.6, 2.7 and 2.8
Compatible BOSH stemcells	Ubuntu Xenial and Windows 2016, 1803, 2019
IaaS support	vSphere, GCP, AWS, Azure, and OpenStack

Limitations

File Integrity Monitoring has the following limitations:

- Windows support is in beta
- If you are upgrading from FIM v1.4, you must manually uninstall the runtime configs. For more information, see Upgrading File Integrity Monitoring.

Create a pull request or raise an issue on the source for this page in GitHub

Release Notes

> **Warning:** Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

> **Note:** Pivotal has renamed File Integrity Monitoring Add-on for PCF. The new name is Pivotal File Integrity Monitoring.

> **Note:** Pivotal has renamed *Pivotal Cloud Foundry* to *Pivotal Platform*.

This topic contains release notes for Pivotal File Integrity Monitoring (FIM).

For product versions and upgrade paths, see Upgrade Planner.

v2.0.0

Release Date: January 7, 2019

Features

New features and changes in this release:

- FIM is now a tile. For information about upgrading from FIM v1.x, see Upgrading File Integrity Monitoring.
- FIM for Windows can monitor Garden containers on Windows Diego Cells. For more information, see Monitor Windows Garden Containers.

> **Warning:** FIM for Windows is currently in beta.

View Release Notes for Another Version

To view the release notes for another product version, select the version from dropdown at the top of this page.

Create a pull request or raise an issue on the source for this page in GitHub

Installing and Configuring File Integrity Monitoring

Warning: Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes how to install Pivotal File Integrity Monitoring (FIM).

Note: When you install the FIM tile using Ops Manager, FIM does not monitor the files on your BOSH Director. To apply FIM to the BOSH Director VM, see Installing File Integrity Monitoring on BOSH Director.

Prerequisites

- You must be a Pivotal Platform operator with admin rights. See Operators in the Pivotal Platform documentation.
- **Pivotal Operations Manager (Ops Manager)**. For compatible versions, see the Product Snapshot.

Install FIM

To install the FIM file on the Ops Manager Installation Dashboard:

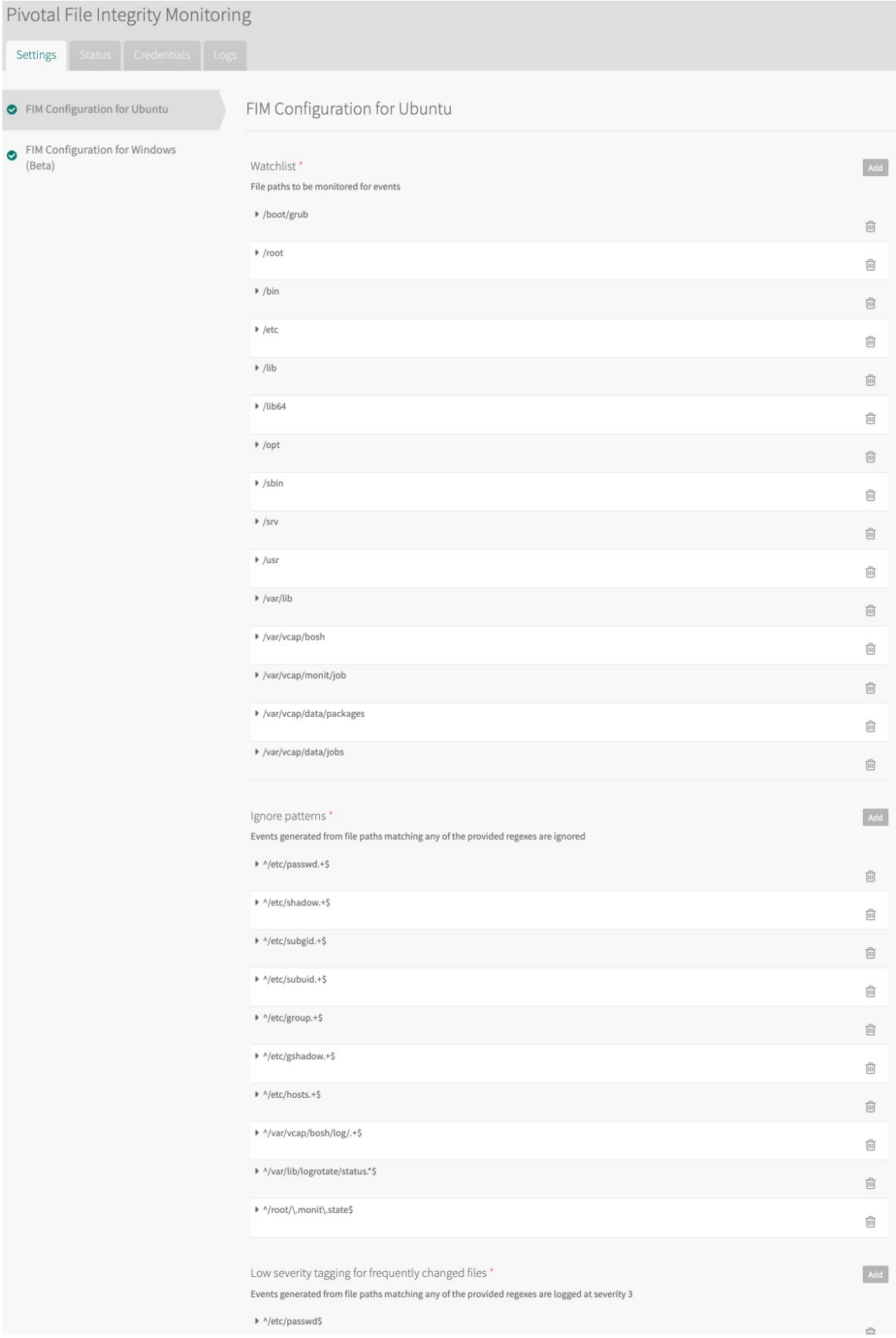
Note: If you are upgrading from v1.4 or earlier, you must follow the instructions in Upgrading FIM.

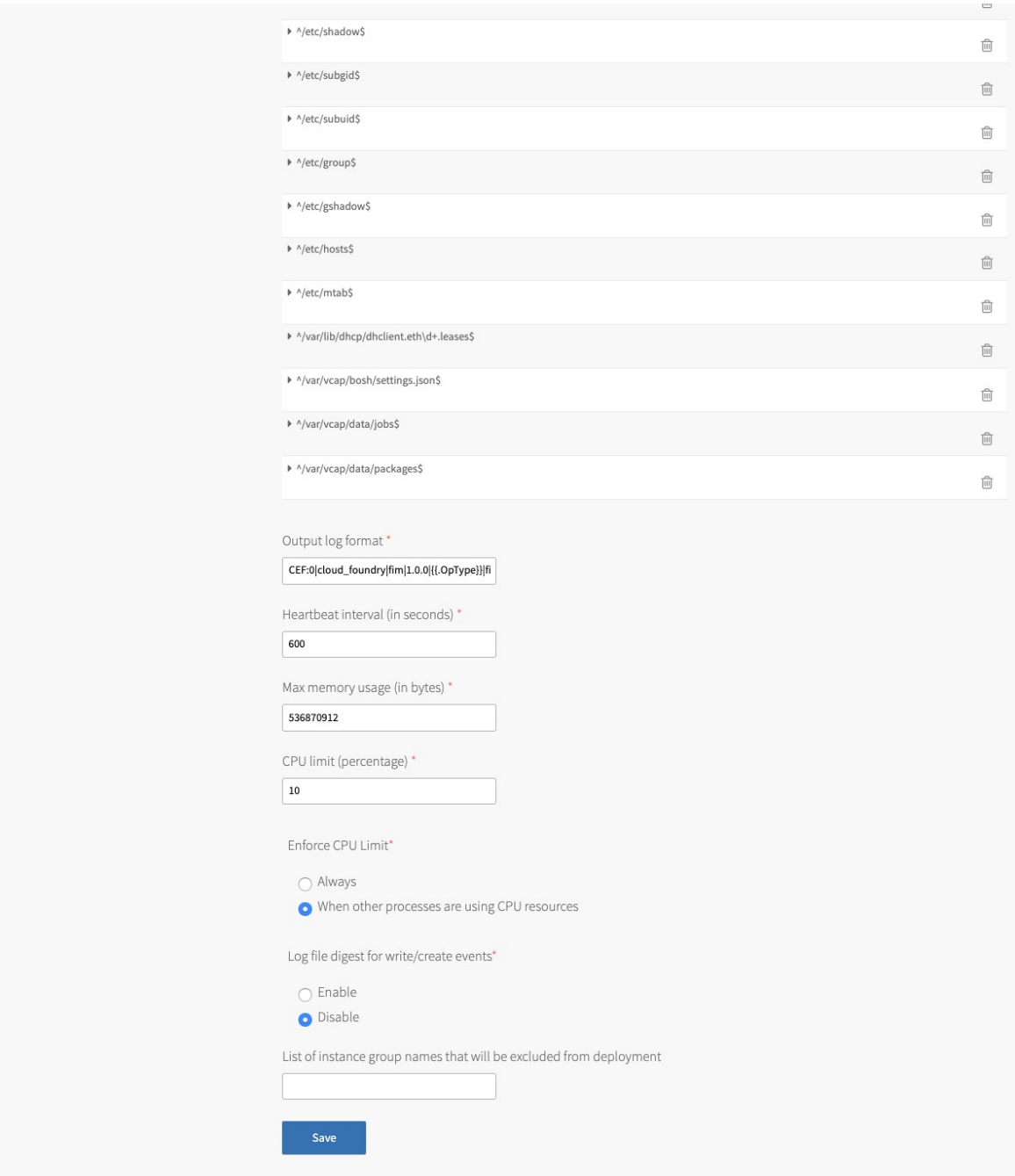
1. Download the product file from Pivotal Network.
2. Navigate to the Ops Manager Installation Dashboard and click **Import a Product** to upload the product file.
3. Under **Import a Product**, click **+** next to the version number of FIM. This adds the tile to your staging area.
4. Click the newly added **FIM** tile.

Configure FIM for Linux

To configure FIM for Linux VMs:

1. Select **FIM Configuration for Ubuntu**.





Click here to view a larger version of this image.

2. Configure the following fields:

Field	Description
Watchlist	Create a list of file paths to monitor for file system events. Click **Add** to add file paths to the list, and click the trash can icon to remove file paths from the list. For more information, see Watchlist below. **Note:** This field corresponds to `fim.dirs` in FIM v1.4 and earlier.

Ignore patterns	Create a list of files that you want FIM to ignore. Events for files matching any of the provided regular expressions are not included in the logs. Click **Add** to add files to the list, and click the trash can icon to remove files from the list. The items that you add must use Go-flavored path regular expressions. To test whether a regular expression is valid, you can use Regex101. For more information, see Ignore Patterns below. **Note:** This field corresponds to `fim.ignored_patterns` in FIM v1.4 and earlier.
Low severity tagging for frequently changed files	Create a list of files to be marked as low severity. Click **Add** to add files to the list, and click the trash can icon to remove files from the list. The items that you add must use Go-flavored path regular expressions. To test whether a regular expression is valid, you can use Regex101. For more information, see Low Severity Events below. **Note:** This field corresponds to `fim.low_severity_patterns` in FIM v1.4 and earlier.
Output log format	Enter a template for log lines. This template must be compatible with the golang package `text/template`. For more information about the **Output log format** field, see Output Log Format below. **Note:** This field corresponds to `fim.format` in FIM v1.4 and earlier.
Heartbeat interval (in seconds)	Set the heartbeat interval as follows: • To enable the heartbeat interval, set the value to an integer greater than `0` . If you set a negative value, an error occurs. • To disable the heartbeat interval, set the value to `0`. The default value is `600`. **Note:** This field corresponds to `fim.heartbeat_interval` in FIM v1.4 and earlier.
Max memory usage (in bytes)	Set a limit in bytes for the maximum amount of memory, including file cache, that FIM can use per VM. The default value is `536870912` (512 MB). **Note**: This field corresponds to `fim.memory_limit` in FIM v1.4 and earlier.

CPU limit (percentage)	Set the percentage of CPU that the FIM process can use. Integers from `1` to `100` are valid. The limit is set per core. Setting this field to `100` permits the use of one full core. The default value is `10`. **Note**: This field corresponds to `fim.cpu_limit` in FIM v1.4 and earlier.
Enforce CPU limit	Select the enforcement policy for the **CPU limit (percentage)**: - **Always**: Ensures the **CPU limit (percentage)** is always enforced - **When other processes are using CPU resources**: Permits the CPU usage to exceed the limit set by **CPU limit (percentage)** if idle CPU cycles are available The default setting is **When other processes are using CPU resources**. **Warning:** If **Enforce CPU limit** is set **Always**, verify that the **CPU limit (percentage)** is set high enough for FIM to execute correctly. If the limit is too strict, FIM fails to start. **Note**: This field corresponds to `fim.enforce_cpu_limit` in FIM v1.4 and earlier. - **Always** is equivalent to `fim.enforce_cpu_limit == true` - **When other processes are using CPU resources** is equivalent to `fim.enforce_cpu_limit == false`
Log file digest for write/create events	Choose whether to enable computing digests for write/create events using the **Enable** or **Disable** radio buttons. If you enable digests, a field for **A threshold of file size beyond which digests are not calculated (in bytes)** appears after you select the option. For more information, see File Digests below. **Note**: This field corresponds to `fim.digests` in FIM v1.4 and earlier. Setting **Log file digest for write/create events** to **Enable** is equivalent to `fim.digests == [sha256]`.
A threshold of file size beyond which digests are not calculated (in bytes)	Enter a positive value for the threshold for the maximum size of files for FIM to hash. This field only appears if you have selected **Enable** for **Log file digest for write/create events**. The default value is `10000000`. **Note**: This field corresponds to `fim.digest_threshold` in FIM v1.4 and earlier.
List of instance group names that will be excluded from deployment	Enter a comma-separated list of instance groups that you do not want FIM deployed on.

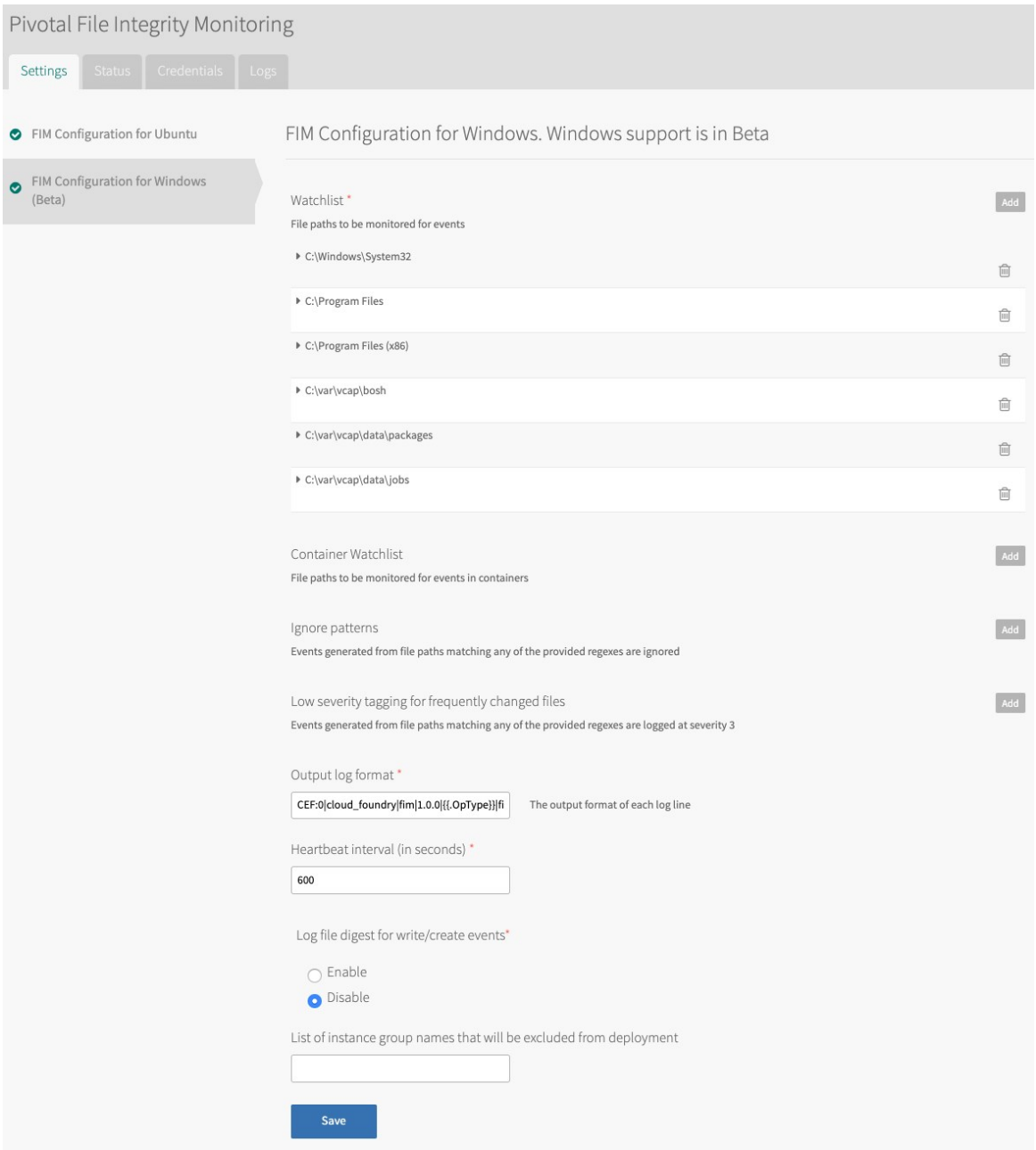
3. Click **Save**.

Configure FIM for Windows (Beta)

> **Warning:** FIM for Windows is currently in beta. To disable installing FIM on Windows VMs, follow the steps in Disable Windows below.

To configure FIM for Windows VMs:

1. Select **FIM Configuration for Windows (Beta)**.



Click here to view a larger version of this image.

2. Configure the following fields:

Field	Description

Watchlist	Create a list of file paths to monitor for file system events. Click **Add** to add file paths to the list, and click the trash can icon to remove file paths from the list. For more information, see Watchlist below. **Note:** This field corresponds to `fim.dirs` in FIM v1.4 and earlier.
Container Watchlist	Create a list of file paths to monitor for file system events per container on the Windows Diego Cell. Click **Add** to add file paths to the list, and click the trash can icon to remove file paths from the list. For example, to monitor file system events for app files, enter `C:\Users\vcap\app`. If you do not enter a file path, FIM does not monitor any file system events for containers. **Note:** The file path for generated logs from container events is relative to the file system for the Diego Cell, rather than the container. For example, a container event for the container file path `C:\Users\vcap\app\test.html` appears as a file system event in `C:\proc\PID\root\Users\vcap\app\test.html`, where PID is the process ID of the container.
Ignore patterns	Create a list of files that you want FIM to ignore. Click **Add** to add files to the list, and click the trash can icon to remove files from the list. The items that you add must use Go-flavored path regular expressions. When defining **Ignore patterns** for Windows, you must replace all single back slashes with double back slashes. To test whether a regular expression is valid, you can use Regex101. Events for files matching any of the provided regular expressions are not included in the logs. For more information, see Ignore Patterns below. **Note:** To ignore events for files in containers, you must enter regular expressions that are relative to the file system for the Diego Cell, rather than the container. To do this, enter regular expressions that start with `^C:\\proc\\[^\\]+\\root`. For example, to ignore all files in containers in the directory `C:\Users\vcap\app`, enter `^C:\\proc\\[^\\]+\\root\\Users\\vcap\\app\\.*$`. **Note:** This field corresponds to `fim.ignored_patterns` in FIM v1.4 and earlier.

Low severity tagging for frequently changed files	Create a list of files to be marked as low severity. Click **Add** to add files to the list, and click the trash can icon to remove files from the list. The items that you add must use Go-flavored path regular expressions. When defining **Low severity tagging for frequently changed files** for Windows, you must replace all single back slashes with double back slashes. To test whether a regular expression is valid, you can use Regex101. For more information, see Low Severity Events below. **Note**: This field corresponds to `fim.low_severity_patterns` in FIM v1.4 and earlier.
Output log format	Enter a template for log lines. This template must be compatible with the golang package `text/template`. For more information, see Output Log Format below. **Note**: This field corresponds to `fim.format` in FIM v1.4 and earlier.
Heartbeat interval (in seconds)	Set the heartbeat interval as follows: - To enable the heartbeat interval, set the value to an integer greater than `0` . If you set a negative value, an error occurs. - To disable the heartbeat interval, set the value to `0`. The default value is `600`. **Note**: This field corresponds to `fim.heartbeat_interval` in FIM v1.4 and earlier.
Log file digest for write/create events	Choose whether to enable computing digests for write/create events using the **Enable** or **Disable** radio buttons. If you enable digests, a field for **A threshold of file size beyond which digests are not calculated (in bytes)** appears after you select the option. For more information, see File Digests below. **Note**: This field corresponds to `fim.digests` in FIM v1.4 and earlier. Setting **Log file digest for write/create events** to **Enable** is equivalent to `fim.digests == [sha256]`.
A threshold of file size beyond which digests are not calculated (in bytes)	Enter a positive value for the threshold for the maximum size of files for FIM to hash. This field only appears if you have selected **Enable** for **Log file digest for write/create events**. The default value is `10000000`. **Note**: This field corresponds to `fim.digest_threshold` in FIM v1.4 and earlier.

List of instance group names that will be excluded from deployment	Enter a comma-separated list of instance groups that you do not want FIM deployed on.

3. Click **Save**.

Disable Windows

To disable installing FIM on Windows VMs:

1. In the FIM tile, select **FIM Configuration for Windows (Beta)**.
2. Add the instance group **windows_diego_cell** to the field **List of instance group names that will be excluded from deployment**.
3. Click **Save**.

Monitor Containers with FIM

You can use FIM to monitor:

- Garden containers on the Diego Cell VMs in
- Containers on the Diego Windows Cell VMs in Pivotal Application Service for Windows (PASW)
- Containers on the Kubernetes worker node VMs in Enterprise Pivotal Container Service (PKS)

For an example log message, see Examples of Log Messages from Containers.

Monitor Garden Containers

To configure FIM to monitor Garden containers:

1. In the FIM tile, select **FIM Configuration for Ubuntu**.
2. Add the Garden container directories to the **Watchlist** section:
   - `/var/vcap/data/grootfs/store/unprivileged/volumes/`
   - `/var/vcap/data/grootfs/store/privileged/volumes/`

   For more information about GrootFS volumes, see Volumes.
3. Add the following pattern to the **Ignore patterns** section:
   - `^/var/vcap/data/grootfs/store/(un)?privileged/volumes/[\w-]+/rootfs/.*$`

   > **Note:** When files in the Garden containers are modified, changes are made to both the `diff` and `rootfs` directories. Adding this ignore pattern means that FIM ignores files and directories in the `/var/vcap/data/grootfs/store/unprivileged/volumes/UUID/diff` directory, where `UUID` is the ID of the container.

4. Click **Save**.

Monitor Windows Garden Containers

To configure FIM to monitor Windows Garden containers:

1. In the FIM tile, select **FIM Configuration for Windows (Beta)**.
2. Add at least one directory to the **Container Watchlist** section. Pivotal recommends that you add `C:\Users\vcap\app`, which is the directory for app files.
3. Click **Save**.

Monitor Containers in PKS

To configure FIM to monitor containers on the Kubernetes worker node VMs in PKS:

1. In the FIM tile, select **FIM Configuration for Ubuntu**.
2. Add the container directory `/var/vcap/store/docker/docker/` to the **Watchlist** section.

   > **Note:** FIM writes log messages when files and directories in the `/var/vcap/store/docker/docker/overlay2/UUID/diff` directory are created, removed, or modified. `UUID` is the ID of the container.

3. Click **Save**.

Configure Forwarding for FIM Alerts

FIM writes all alerts to the BOSH logs for the VMs in your deployment.

- In Linux, these logs are located in `/var/vcap/sys/log/fim/fim.stdout.log`.
- In Windows, these logs are located in `C:\var\vcap\sys\log\fim-windows\filesnitch\job-service-wrapper.out.log`.

You can use syslog forwarding to forward the alerts to a syslog aggregator.

- **If you are using the PAS tile**: The syslog aggregator that you specify receives all alerts generated on PAS, including the FIM alerts. To configure system logging, follow the procedure in Configuring Logging in PAS.
- **If you are using the syslog BOSH release**: You can use the syslog BOSH release to forward system logs. For more information, see syslog-release in GitHub.

> **Note:** When you configure syslog forwarding, ensure there is enough disk space for the logs, and that they rotate frequently. If you are not sure how often to rotate the logs, configure the rotation to occur either hourly, or when they reach a certain configured size. VMware recommends forwarding logs to a remote syslog aggregation system.

Apply Changes from Your Configuration

Your installation is not complete until you apply your configuration changes:

1. Navigate to the **Installation Dashboard** in Ops Manager.
2. Click **Review Pending Changes**.
3. Click **Apply Changes** to complete the FIM installation.

Verify the Installation

To verify the installation for Linux:

1. `bosh ssh` into the VMs in your deployment. For more information, see BOSH SSH.
2. Enter this command:

```
touch /bin/hackertool
```

3. Enter this command:

```
grep hackertool /var/vcap/sys/log/fim/fim.stdout.log
```

4. Verify in the logs that a new file has been created. For example:

```
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5| fname="/bin/
hackertool" hostname="fim_1/3ad6ff1f-37e0-4b8a-80bd-d16b7f79c149" opname="CREAT
E" optype=1 ts=1574098829 severity=5
```

To verify the installation for Windows:

1. `bosh ssh` into the VMs in your deployment. For more information, see BOSH SSH.
2. Enter this command:

```
powershell New-Item -type File /var/vcap/data/jobs/sample_file
```

3. Enter this command:

```
powershell "Get-Content C:\var\vcap\sys\log\fim-windows\filesnitch\job-service-
wrapper.out.log | Select-String sample_file"
```

4. Verify in the logs that a new file has been created. For example:

```
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5| fname="C:\va
r\vcap\data\jobs\sample_file" hostname="no-job_1/ebee34c1-3300-4f5d-9557-bbef84
5d608c" opname="CREATE" optype=1 ts=1569953512 severity=5
```

Concepts Related to Configuring FIM

Reference the following sections when configuring FIM.

Watchlist

FIM monitors a set of critical system directories. You can configure the directories that FIM monitors by adding and removing items in the **Watchlist** section.

Watchlist for Linux

Below is the default list of file paths in **Watchlist** section of **FIM Configuration for Ubuntu**.

Component	File Paths

System binaries and configuration	`/boot/grub`
	`/root`
	`/bin`
	`/etc`
	`/lib`
	`/lib64`
	`/opt`
	`/sbin`
	`/srv`
	`/usr`
	`/var/lib`

BOSH agent	`/var/vcap/bosh` `/var/vcap/monit/job`
BOSH releases	`/var/vcap/data/packages` `/var/vcap/data/jobs`

Watchlist for Windows

Below is the default list of file paths in **Watchlist** section of **FIM Configuration for Windows**.

- `C:\Windows\System32`
- `C:\Program Files`
- `C:\Program Files (x86)`
- `C:\var\vcap\bosh`
- `C:\var\vcap\data\packages`
- `C:\var\vcap\data\jobs`

Ignore Patterns

Some monitored directories might contain files that you do not want FIM to monitor, such as files that change frequently. You can configure FIM to ignore these events by adding and removing items in the **Ignore patterns** section. Use path regular expressions.

Ignore Patterns for Linux

Below is the default list in **Ignore Patterns** section of **FIM Configuration for Ubuntu**.

Scenario	List

Temporary files created when an operator or errand runs `bosh ssh`	`^/etc/passwd.+$`
	`^/etc/shadow.+$`
	`^/etc/subgid.+$`
	`^/etc/subuid.+$`
	`^/etc/group.+$`
	`^/etc/gshadow.+$`

Temporary files created when hosts are updated	`^/etc/hosts.+$`
BOSH agent logs	`^/var/vcap/bosh/log/.+$`
Log rotation	`^/var/lib/logrotate/status.*$`
Monit state	`^/root/\.monit\.state$`

Ignore Patterns for Windows

Note: There is currently no default value for **Ignored patterns** for Windows.

When defining **Ignore patterns** for Windows, you must replace all single back slashes with double back slashes. For example, to ignore all files in the directory `C:\var\vcap\bosh\ignore_me\`, use:

```
^C:\\var\\vcap\\bosh\\ignore_me\\.*$
```

Low Severity Events

Some monitored directories might contain files that only change occasionally or files that update frequently but are low impact. You can configure FIM to log events at a lower severity by adding and removing items in the **Low severity tagging for frequently changed files** section. Use path regular expressions.

Severity can be one of the following severity levels:

- `0`: Used for heartbeats.
- `3`: Used for low severity events. These events are for files that match any of the provided regular expressions. This can be useful to filter out business-as-usual events.
- `5`: Used for all other events. This is the default severity.

Low Severity Tagging for Frequently Changed Files for Linux

Below is the default list in **Low severity tagging for frequently changed files** section of **FIM Configuration for Ubuntu**.

Scenario	List

When an operator or errand runs the `bosh ssh` a new user is created	`^/etc/passwd$`
	`^/etc/shadow$`
	`^/etc/subgid$`
	`^/etc/subuid$`
	`^/etc/group$`
	`^/etc/gshadow$`

BOSH-DNS sync and new VM creation update hosts	`^/etc/hosts$`
Attached devices and cgroups	`^/etc/mtab$`
DHCP leases	`^/var/lib/dhcp/dhclient.eth\d+.leases$`
BOSH agent configuration changes when VM created/modified	`^/var/vcap/bosh/settings.json$`
BOSH agent CHMODs jobs and packages as part of `bosh deployment`	`^/var/vcap/data/jobs$` `^/var/vcap/data/packages$`

Low Severity Tagging for Frequently Changed Files for Windows

> **Note:** There is currently no default value for **Low severity tagging for frequently changed files** for Windows.

When defining **Low severity tagging for frequently changed files** for Windows, you must replace all single back slashes with double back slashes. For example, to mark all files in the directory `C:\var\vcap\bosh\ignore_me\` as low severity, use:

```
^C:\\var\\vcap\\bosh\\ignore_me\\.*$
```

Output Log Format

By default, FIM generates messages in the Common Event Format. You can configure the output format as a Go text template using the **Output log format** field. For more information and examples of FIM log messages, see Log Messages.

Default Format

The default value of **Output log format** is:

```
"CEF:0|cloud_foundry|fim|1.0.0|{{.Optype}}|file integrity monitoring event|{{.Severity
}}| {{.KeyValues}}"
```

Example output using the default **Output log format** configuration:

```
CEF:0|cloud_foundry|fim|1.0.0|0|file integrity monitoring event|0| fname="" hostname="
diego_cell/8279dfa8-9f86-4bb1-8b92-65457d2ae989" opname="FILESNITCH CHECKIN" optype=0
ts=1492715822 severity=0
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5| fname="/etc/passwd.
lock" hostname="diego_cell/8279dfa8-9f86-4bb1-8b92-65457d2ae989" opname="CREATE" optyp
e=1 ts=1492715822 severity=5
CEF:0|cloud_foundry|fim|1.0.0|4|file integrity monitoring event|5| fname="/etc/passwd.
17721" hostname="diego_cell/8279dfa8-9f86-4bb1-8b92-65457d2ae989" opname="REMOVE" opty
pe=4 ts=1492715822 severity=5
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5| fname="/etc/group.l
ock" hostname="diego_cell/8279dfa8-9f86-4bb1-8b92-65457d2ae989" opname="CREATE" optype
=1 ts=1492715822 severity=5
CEF:0|cloud_foundry|fim|1.0.0|4|file integrity monitoring event|5| fname="/etc/group.1
7721" hostname="diego_cell/8279dfa8-9f86-4bb1-8b92-65457d2ae989" opname="REMOVE" optyp
```

```
e=4 ts=1492715822 severity=5
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5| fname="/etc/gshadow
.lock" hostname="diego_cell/8279dfa8-9f86-4bb1-8b92-65457d2ae989" opname="CREATE" opty
pe=1 ts=1492715822 severity=5
```

Note: The `FILESNITCH CHECKIN` message is a logging marker that indicates `filesnitch` is operational in the absence of any file system events.

Custom Format

You can use individual fields to configure the log format. Each individual field, is a named property provided by FIM that will be replaced during the logging action.

For example:

```
"{{.Fname}} {{.Hostname}} {{.OpName}} {{.OpType}} {{.Digests}} {{.Ts}}"
```

Example output using the above configuration:

```
/bin/binary plymouth CREATE 1 sha256=da39a3ee5e6b4b0d3255bfef95601890afd80709 14751955
74
```

The table below lists the template values you can use:

Template	Description
`{{.Fname}}`	The name of the affected file.
`{{.Hostname}}`	The hostname of the VM on which the file event originated.
`{{.OpName}}`	The type of file operation in textual format. For more information about opname, see Opname and Optype below.
`{{.OpType}}`	The type of file operation in numeric format. For more information about optype, see Opname and Optype below.
`{{.Severity}}`	The level of importance attributed to the event. For the severity levels, see Low Severity Events above.
`{{.Ts}}`	The point in time at which FIM received the file event in Unix epoch format.
`{{.Digests}}`	Key-value pairs of hash algorithms and the hash of the modified file. For more information, see File Digests below.

`{{.Json}}`	This string serializes an event into a standard JSON dictionary. The string is in the following format:
	`{"fname":"ABSOLUTE-PATH","hostname":"BOSH-VM","opname":"OPERATION-NAME","optype":OPERATION-TYPE,"ts":TIMESTAMP}`
	For example:
	`{"fname":"/bin/binary","hostname":"plymouth","opname":"CREATE","optype":1,"ts":1475195084}`

`{{.KeyValues}}`	This string serializes an event into a series of key-value pairs. The string is in the following format:
	
	`fname="ABSOLUTE-PATH" hostname="BOSH-VM" opname="OPERATION-NAME" optype=OPERATION-TYPE ts=TIMESTAMP`
	
	For example:
	
	`fname="/bin/binary" hostname="plymouth" opname="CREATE" optype=1 ts=1475195258`

Opname and Optype

Opname and optype are the type of file operation in textual and numeric format, respectively. For the possible values of the two fields see the table below:

opname	optype	Example Linux Trigger	Example Windows Trigger
`FILESNITCH CHECKIN`	0	This is a heartbeat message written to the log. This occurs during every **Heartbeat interval**. The default interval is `600` seconds. To configure this property, see Configure FIM for Linux.	This is a heartbeat message written to the log. This occurs during every **Heartbeat interval**. The default interval is `600` seconds. To configure this property, see Configure FIM for Windows (Beta).

`CREATE`	1	`touch newfile.txt`
		
		`echo 'content' > newfile2.txt`
			`Powershell New-Item -type File newfile.txt`
			
			`Powershell Add-Content -Path newfile.txt -Value 'content'`

`WRITE`	2	`echo 'hello world' >> file.txt`	`Powershell Add-Content -Path newfile.txt -Value 'content'`
`REMOVE`	4	`rm file.txt`	`Powershell rm file.txt`
`RENAME`	8	`mv file.txt file.txt.orig`	`Powershell mv file.txt file.txt.orig`
`CHMOD`	16	`chmod 0400 file.txt`	`Powershell icacls file.txt /grant administrators:F`

Note: FIM on Windows reports `WRITE` and `CHMOD` together as `WRITE|CHMOD`. The two operations are indistinguishable.

File Digests

FIM supports hashing monitored files on `WRITE` or `CREATE` events using the `sha256` algorithm. If you enable digests, FIM includes the calculated hash for the file in the logs.

If you want to show that content has changed or check which version of the file is mapped to a log entry, you can calculate the `sha256` value of a file and compare it to the value in the log.

Hashing is disabled by default.

FIM sets a threshold on the size of files, in bytes, to be hashed.

Create a pull request or raise an issue on the source for this page in GitHub

Installing File Integrity Monitoring on BOSH Director

> **Warning:** Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes how to install Pivotal File Integrity Monitoring (FIM) on BOSH Director.

When you install the FIM tile using Pivotal Operations Manager, FIM does not monitor the files on your BOSH Director. To apply FIM to the BOSH Director VM, you must do the below procedures.

Prerequisites

Before you install FIM, you must have:

- A Pivotal Platform operator user account with admin rights. See Pivotal Platform Operators.
- Pivotal Operations Manager v2.5 or later.
- A web server accessible from Ops Manager to serve the FIM binary.

Install FIM

To install FIM on your BOSH Director:

1. Download the FIM tile from Pivotal Network.
2. Unzip the FIM tile by running:

   ```
   unzip p-fim-X.X.X.pivotal -d PATH-TO-UNZIP
   ```

   For example:

   ```
   $ unzip p-fim-2.0.0.pivotal -d /tmp
   ```

3. Find and record the SHA checksum for the binary file by running:

   ```
   shasum PATH-TO-UNZIP/releases/fim-X.X.X.pivotal
   ```

   For example:

```
$ shasum /tmp/releases/fim-2.0.0.pivotal
5edf5fd2f9bf8e876b6bdc871e53b5db97593b21 fim-2.0.0.pivotal
```

4. Copy the binary file to your web server.
5. Add FIM to BOSH Director by running:

```
om  \
-t OPS-MANAGER-URL \
-u OPS-MANAGER-USERNAME \
-p OPS-MANAGER-PASSWORD \
curl -p "/api/v0/staged/director/manifest_operations/add_job_to_instance_group"
 \
-x POST \
-H "Content-Type: application/json" \
-d '{
        "add_job_to_instance_group": {
          "instance_group": "bosh",
          "job_name": "fim",
          "release_name": "fim",
          "release_url": "FIM-BINARY-URL",
          "release_sha1": "FIM-SHA1",
          "job_properties": {"fim": {}}
        }
    }'
```

Where:

- `FIM-BINARY-URL` is the URL to the binary file on your web server.
- `FIM-SHA1` is the SHA checksum for the binary file you recorded in the above step.

The output of the above command looks similar to the following:

```
Status: 201 Created
Cache-Control: no-cache, no-store
Connection: keep-alive
Content-Type: application/json; charset=utf-8
Date: Mon, 04 Nov 2019 17:09:08 GMT
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Pragma: no-cache
Referrer-Policy: strict-origin-when-cross-origin
Server: Ops Manager
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-Request-Id: 7d961c91-b7d6-428c-a68d-c36c9059f7f9
X-Runtime: 0.220906
X-Xss-Protection: 1; mode=block
{
  "add_job_to_instance_group": {
    "instance_group": "bosh",
    "job_name": "fim",
    "release_name": "fim",
    "release_url": "http://localhost:4567/fim-1.5.0.tgz",
    "release_sha1": "15c52a9e56ca8e796dd61b55a48d962e2f4e763b",
    "job_properties": {
```

```
      "fim": {}
    },
    "guid": "op-653b1111a60a",
    "product_guid": "p-bosh-eb686414b9fa37183507"
  }
}
```

6. Record the value of `guid` in the above output. If you want to delete FIM from BOSH Director, you need this value.
7. Navigate to the **Installation Dashboard** in Ops Manager.
8. Click **Review Pending Changes**.
9. Select **BOSH Director**. Do not select any other checkbox.
10. Click **Apply Changes**.

Verify FIM Installation

To verify that FIM is running on your BOSH Director:

1. SSH into the BOSH Director VM. For instructions, see SSH Into the BOSH Director VM.
2. View the status of processes running on BOSH Director by running:

   ```
   sudo monit summary
   ```

   For example:

   ```
   bosh/0:~$ sudo monit summary
   The Monit daemon 5.2.5 uptime: 4m

   Process 'system-metrics-server'     running
   Process 'nats'                      running
   Process 'postgres'                  running
   Process 'director'                  running
   Process 'worker_1'                  running
   Process 'worker_2'                  running
   Process 'worker_3'                  running
   Process 'director_scheduler'        running
   Process 'director_sync_dns'         running
   Process 'director_nginx'            running
   Process 'health_monitor'            running
   Process 'uaa'                       running
   Process 'credhub'                   running
   Process 'blobstore_nginx'           running
   Process 'fim'                       running
   System 'system_localhost'           running
   ```

3. Confirm that `fim` is present in the above output.

Uninstall FIM

To uninstall FIM from your BOSH Director:

1. Uninstall FIM by running:

```
om  \
-t OPS-MANAGER-URL \
-u OPS-MANAGER-USERNAME \
-p OPS-MANAGER-PASSWORD \
curl -p "/api/v0/staged/director/manifest_operations/add_job_to_instance_group/
FIM-GUID" \
-x DELETE \
```

Where `FIM-GUID` is the value of `guid` you recorded in Install FIM above.

Create a pull request or raise an issue on the source for this page in GitHub

Upgrading File Integrity Monitoring

> **Warning:** Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes how to upgrade Pivotal File Integrity Monitoring (FIM).

For product versions and upgrade paths, see Upgrade Planner.

Prerequisites

To ensure that you have the required component versions, see the Product Snapshot.

Replace FIM v1.x with v2.x

To uninstall FIM v1.x and install v2.x in its place:

1. SSH into the Ops Manager VM. For how to do this, see SSH into Ops Manager.
2. Delete the existing runtime configs by running:

   ```
   bosh -e BOSH-ENVIRONMENT delete-config --type=runtime --name=fim
   bosh -e BOSH-ENVIRONMENT delete-config --type=runtime --name=fim-windows
   ```

3. Install the 2.x tile. For installation instructions, see Installing File Integrity Monitoring.

Create a pull request or raise an issue on the source for this page in GitHub

Log Messages

> **Warning:** Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic provides information about log messages emitted by Pivotal File Integrity Monitoring (FIM).

You can use these samples to configure a Security Information and Event Management (SIEM) system, to verify regular activity and generate alerts for file system operations in monitored directories.

Log Output Destination

FIM produces many different logs depending on what operation is being performed.

- In Linux, these logs are located in `/var/vcap/sys/log/fim/fim.stdout.log`.
- In Windows, these logs are located in `C:\var\vcap\sys\log\fim-windows\filesnitch\job-service-wrapper.out.log`.

Log Format

FIM can emit logs in the default format or you can configure a custom format using the **Output log format** field. For information about configuring the log format, see Output Log Format.

Examples of Log Messages

This section contains sample log messages emitted by FIM. You can use these samples to configure a Security Information and Event Management (SIEM) system.

FIM Log Message Types

The list below contains an example FIM log message for each operation:

- `FILESNITCH CHECKIN`

  ```
  2019-04-05T16:00:27.353542+00:00 localhost filesnitch[6663]: CEF:0|cloud_foundry|fim|1.0.0|0|file integrity monitoring event|0|

  fname="" hostname="fim_1/f66479c7-cd37-4a99-b735-f6f41ba55f01" opname="FILESNITCH CHECKIN" optype=0 ts=1554480027 severity=0
  ```

- CREATE

```
2019-04-05T15:52:03.296265+00:00 localhost filesnitch[5990]: CEF:0|cloud_foundr
y|fim|1.0.0|1|file integrity monitoring event|5|

fname="/var/vcap/data/jobs/newfile.txt" hostname="fim_1/f66479c7-cd37-4a99-b735
-f6f41ba55f01" opname="CREATE" optype=1 ts=1554479523 severity=5
```

- WRITE

```
2019-04-05T15:52:22.230901+00:00 localhost filesnitch[5990]: CEF:0|cloud_foundr
y|fim|1.0.0|2|file integrity monitoring event|5|

fname="/var/vcap/data/jobs/file.txt" hostname="fim_1/f66479c7-cd37-4a99-b735-f6
f41ba55f01" opname="WRITE" optype=2 ts=1554479542 severity=5
```

- REMOVE

```
2019-04-05T15:52:15.636353+00:00 localhost filesnitch[5990]: CEF:0|cloud_foundr
y|fim|1.0.0|4|file integrity monitoring event|5|

fname="/var/vcap/data/jobs/file.txt" hostname="fim_1/f66479c7-cd37-4a99-b735-f6
f41ba55f01" opname="REMOVE" optype=4 ts=1554479535 severity=5
```

- RENAME

```
2019-04-05T15:52:28.707094+00:00 localhost filesnitch[5990]: CEF:0|cloud_foundr
y|fim|1.0.0|8|file integrity monitoring event|5|

fname="/var/vcap/data/jobs/file.txt" hostname="fim_1/f66479c7-cd37-4a99-b735-f6
f41ba55f01" opname="RENAME" optype=8 ts=1554479548 severity=5
```

- CHMOD

```
2019-04-05T15:52:03.297424+00:00 localhost filesnitch[5990]: CEF:0|cloud_foundr
y|fim|1.0.0|16|file integrity monitoring event|5|

fname="/var/vcap/data/jobs/newfile.txt" hostname="fim_1/f66479c7-cd37-4a99-b735
-f6f41ba55f01" opname="CHMOD" optype=16 ts=1554479523 severity=5
```

Examples of Log Messages from Containers

The list below contains examples of FIM log messages from Garden containers and Docker containers:

- For a Garden container in

```
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5|
fname="/var/vcap/data/grootfs/store/unprivileged/volumes/5c320add-ac1a-4bd7-78b
6-1129/diff/home/vcap/app/public/test.html"
```

- For a Windows Garden container in Pivotal Application Service for Windows (PASW)

```
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5|
```

```
fname="C:\proc\8174\root\Users\vcap\app\test.html"
hostname="windows_diego_cell/be1f4854-299d-47d1-98eb-60b0741a3f6b" opname="CREA
TE" optype=1 ts=1556218123 severity=5
```

- For a Docker container in Enterprise Pivotal Container Service (PKS)

```
CEF:0|cloud_foundry|fim|1.0.0|1|file integrity monitoring event|5|
fname="/var/vcap/store/docker/docker/overlay2/7e5685c735b2aa97a9680e0b81730a518
e3188afbf0f9f1529e492f98ed35f1d/diff/test.html"
hostname="worker/d1d67195-ad42-4025-83e9-0d43a193ad53" opname="CREATE" optype=1
 ts=1556217648 severity=5
```

For how to configure FIM to monitor containers, see Monitor Containers with FIM.

Create a pull request or raise an issue on the source for this page in GitHub

Troubleshooting File Integrity Monitoring

> **Warning:** Pivotal File Integrity Monitoring v2.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the Support Lifecycle Policy. To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic provides instructions to verify that Pivotal File Integrity Monitoring (FIM) works with your Pivotal Platform deployment and makes general recommendations for troubleshooting.

About Troubleshooting FIM

This topic provides help for troubleshooting the runtime behavior, to ensure that the deployment is being protected in the way you expect.

BOSH Deploy Issues

Symptom

FIM generates too much syslog activity during BOSH deploys.

Explanation

FIM monitors and reports file changes. BOSH deployments often make changes to the monitored directories and files, which generates corresponding FIM syslog activity during the deployment.

FIM watches for unexpected file changes in all the directories that you configure it to monitor. The default manifest configuration monitors files in many critical directories including `/var/vcap/data/jobs` and `/var/vcap/data/packages`. These directories are critical to the normal operation of Pivotal Platform and are monitored because they are not expected to change during operation of the platform (between BOSH deploys).

Syslog messages generated during a BOSH deploy report file changes in the `jobs` and `packages` directories in `/var/vcap/...`. BOSH deploys update the files in these directories. Thus, FIM reports file-system events that are expected. You can consider these syslog messages either as confirmation of a succeeding BOSH deployment or as false positive events.

Solution

Events occurring during a planned BOSH deployments are normal and can be safely ignored.

To avoid the additional syslog traffic during a BOSH deploy, customize the FIM release deployment

manifest to narrow the scope of FIM so that it does not include directories affected by deployments. You can do this either before you deploy BOSH (as a temporary measure) or as part of the normal FIM configuration. Consider your threat environment and risk tolerance and configure FIM accordingly.

FIM Runtime Issues

Symptom

Filesystem events are not reported. The logs are empty.

Explanation:

FIM might not be running or might be misconfigured.

Solution

- Check whether `fim` is running. `monit summary` should return the following output on success.

```
The Monit daemon 5.2.5 uptime: 1d 20h 11m

Process 'fim'                       running
```

- If the process is not running, inspect the contents of `/var/vcap/sys/log/fim/fim.std*.log` files for clues.

Symptom

Files system events are not reported from a portion of the file system.

Explanation:

FIM is configured to monitor a set of critical directories in the system. It is not configured to monitor the entire file system by default.

Solution

See Watchlist to see the default list of file paths that FIM monitors for file system events. To modify the configuration, see Configure FIM for Linux or Configure FIM for Windows depending on your installation.

Create a pull request or raise an issue on the source for this page in GitHub