Linux Forwarder Release Notes

Version 2.4.3

Downloads

Package	Kernel Version	Download URL
Rocky Linux 9	5.14.0	stairwell-2.4.3-1.el9.amd64.rpm `2557489f9aa4dbee3129c021f89e3936fa694fb6893fa216adcffb0ca1a30b42`
RHEL9	5.14.0	stairwell-2.4.3-1.el9.amd64.rpm `2557489f9aa4dbee3129c021f89e3936fa694fb6893fa216adcffb0ca1a30b42`
RHEL8	4.18.0-80	stairwell-2.4.3-1.el8.amd64.rpm `d853253a7e80cbb0dacdec846988362f4f47616b2ae4abec1c88d61170e9709d`
RHEL7	3.10.0-1160	stairwell-2.4.3-1.el7.amd64.rpm `5c2650d0fd31a8047094fe05e8880717e9646250b1cdea14ffea5f7203cd1457`
RHEL6	2.6.32	stairwell-2.4.3-1.el6.amd64.rpm `dab2fae59dd2d5abf853e4ece25a7d9a02f287a793ac6d526ad24b685f081b22`
Ubuntu 20.04	5.15	stairwell-2.4.3-1.amd64.deb `d71d180c42d7049b0755c0b5495d4b51e9135a3bbff30bb1be94ec3293e044fb`
Ubuntu 22.04	6.5	stairwell-2.4.3-1.amd64.deb `d71d180c42d7049b0755c0b5495d4b51e9135a3bbff30bb1be94ec3293e044fb`
Ubuntu 24.04	6.8	stairwell-2.4.3-1.amd64.deb `d71d180c42d7049b0755c0b5495d4b51e9135a3bbff30bb1be94ec3293e044fb`
Debian		stairwell-2.4.3-1.amd64.deb `d71d180c42d7049b0755c0b5495d4b51e9135a3bbff30bb1be94ec3293e044fb`
Checksums		checksums.txt

Changes

NEW **Recognize Windows Executable (PE) Files As Executable Files And Upload Them.**

The Stairwell Forwarder now recognizes Windows PE files similar to Linux ELF files and uploads them.

IMPROVED **Fixed A Problem On RHEL9 And Related Systems Where The Installed Audit Rules Would Generate Superfluous Events.**

Now using a canonical auditctl option to filter events based on permission.

IMPROVED **Removed Some Confusing Output Generated By The Rpm Package When Installing/Upgrading/Uninstalling The Forwarder.**

The installer rpm package now mutes the output from running the 'augenrules --load' command.

IMPROVED Optimized Auditd Rules

The audit rules for event detection have been optimized to filter out un-interesting events before they reach the forwarder. This leads to a slight increase in performance.

FIX On RHEL6 And RHEL7 Fixed An Issues Where Real-Time Events May Not Be Detected After A Reboot.

The Unix Domain socket folder location has been moved from /var/run/stairwell/ to /var/run/ to avoid effect of tmpfs filesystems being re-created after reboot.

FIX Fixed Permissions On Auditd Directories If Forwarder Is Installed Before Auditd Is Installed (Debian/Ubuntu).

The installer .deb package now sets the correct permissions (0750) on /etc/audit and /etc/audit/rules.d directories if it creates them.

FIX Fix Premature End Of Backscan If Stairwell Backend Takes Too Long To Respond.

The forwarder will now always retry sending files discovered during backscan to the Stairwell backend.

Package Installation

To install or upgrade the stairwell forwarder service, you will need to download the appropriate package and install it with your distribution's package management software.

Note: the audit service will need to be enabled for realtime events. See the section on enabling audit below.

Rocky Linux 9

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el9.amd64.rpm
sudo rpm -i stairwell-2.4.3-1.el9.amd64.rpm
```

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el9.amd64.rpm
sudo rpm -U stairwell-2.4.3-1.el9.amd64.rpm
```

RHEL9

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el9.amd64.rpm
sudo rpm -i stairwell-2.4.3-1.el9.amd64.rpm
```

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el9.amd64.rpm
sudo rpm -U stairwell-2.4.3-1.el9.amd64.rpm
```

RHEL8

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el8.amd64.rpm
sudo rpm -i stairwell-2.4.3-1.el8.amd64.rpm
```

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el8.amd64.rpm
sudo rpm -U stairwell-2.4.3-1.el8.amd64.rpm
```

RHEL7

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el7.amd64.rpm
sudo rpm -i stairwell-2.4.3-1.el7.amd64.rpm
```

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el7.amd64.rpm
sudo rpm -U stairwell-2.4.3-1.el7.amd64.rpm
```

RHEL6

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el6.amd64.rpm
sudo rpm -i stairwell-2.4.3-1.el6.amd64.rpm
```

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.el6.amd64.rpm
sudo rpm -U stairwell-2.4.3-1.el6.amd64.rpm
```

Ubuntu 20.04

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.amd64.deb
sudo apt-get install ./stairwell-2.4.3-1.amd64.deb
```

Ubuntu 22.04

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.amd64.deb
sudo apt-get install ./stairwell-2.4.3-1.amd64.deb
```

Ubuntu 24.04

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.amd64.deb
sudo apt-get install ./stairwell-2.4.3-1.amd64.deb
```

Debian

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.3/stairwell-2.4.3-1.amd64.deb
sudo apt-get install ./stairwell-2.4.3-1.amd64.deb
```

Forwarder Configuration

If this is the first time installing the forwarder on this machine, the service will need to be configured before it will activate. To configure the service, edit the configuration file in **`/etc/stairwell/config.json`** with vim or another editor of your choice, such as nano.

```
sudo vim /etc/stairwell/config.json
```

You will need your Environment ID along with your Deployment Token, which should be placed in the **`EnvId`** and **`Token`** fields, respectively

/etc/stairwell/config.json

```
{
    "logger": {
        "loglevel": "error"
    },
    "asset": {
        "idempotencyKey": "",
        "EnvId": "ABCDEF-ABCDEF-123ABC-ABCD1234",
        "Token": "ABCDEFG1234567HIJKLMNOP789012QRSTUVW345678XYZABCD901"
    },
    "interpreters": [
        "sh",
        "bash",
        "python",
        "python3",
        "go",
        "ruby",
        "perl",
        "lua",
        "Rscript"
    ],
    "ostype": "server",
    "proxyURL": "http://your.proxy.host",
    "enableEvents": true
}
```

Using a Proxy

If your environment requires a proxy, you may also set the **`proxyURL`** value to the appropriate URL:

/etc/stairwell/config.json

```
    "ostype": "server",
    "proxyURL": "http://your.proxy.host",
    "enableEvents": true
}
```

Enabling Audit

For realtime event support, the auditd service needs be enabled so that the stairwell forwarder can set rules and read events via domain socket or kernel multicast. Most distributions will have this enabled by default and will require no other special configuration, but if it is disabled on your system for some reason, you will need to enable it.

The commands to do this will differ depending on your distribution, so follow the instructions listed in the correct section below to check if auditd is enabled, and re-enable if necessary.

Enabling Audit on systemd-managed distributions

More recent distributions, such as RHEL7 and above, use Systemd, which manages services using the `systemctl` command.

To check if auditd is enabled, you can run the following command

```
sudo systemctl status auditd
```

If the service is running, you will see a status message containing **`Active: active`**.

```
● auditd.service - Security Auditing Service
   ...
   Active: active (running) since ...
```

If you see this, you should be good to go.

If the service is not running, it will say something like **`Active: inactive`** instead:

```
● auditd.service - Security Auditing Service
    ...
    Active: inactive (dead) since ...
```

If the service is inactive, you can enable the service and start it immediately with:

```
sudo systemctl enable --now
```

Enabling audit on sysvinit-managed distributions

Older systems may require the `service` and `chkconfig` commands to start and enable the service, respectively.

To see if auditd is running, run the following command:

```
sudo service auditd status
```

If the service is running, you will see somthing like the following:

```
auditd (pid  1009) is running...
```

Otherwise you will see:

> ```
> auditd is stopped
> ```

If the service is stopped, you can start it and enable it on reboot with the following two commands:

```
sudo service auditd start # start the auditd service
sudo chkconfig auditd on  # enable auditd on reboot
```