Linux Forwarder Release Notes

Version 2.2.5

Downloads

Package	Kernel Version	Download URL
RHEL8	4.18.0-80	stairwell-2.2.5-1.el8.amd64.rpm `de5155f3bfb335c75f37c0891793a1f1dda275771e9cfb2e1573b9903e9819fc`
RHEL7	3.10.0-1160	stairwell-2.2.5-1.el7.amd64.rpm `6b60df78547293d85a8bd727913d20cfcb75fc3f55a39fc88330f9bbe05fdd51`
RHEL6	2.6.32	stairwell-2.2.5-1.el6.amd64.rpm `86e559c25f8f572ca70b52a6e497c861885a195452137f203253826126b3c50a`
Checksums		checksums.txt

Changes

NEW **Remove Periodic Backscan**

Periodic backscan has been removed to bring agent parity with Windows and MacOS

IMPROVED **Improved Retry Logic**

Retry is enabled for intake and upload operations during initial backscan.

IMPROVED **Improved Cache Usage**

Deduplication for events and uploads uses less CPU and memory.

FIX **Reduce Open Filehandles**

Fixed a bug where filehandles could sometimes stay open longer than necessary.

FIX **Fix RHEL6 Service Management**

init.d script and pidfile handling have been rewritten to behave better.

Package Installation

To install or upgrade the stairwell agent 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.

RHEL8

New Installation

```
$>
curl -O https://downloads.stairwell.com/linux/2.2.5/stairwell-2.2.5-1.el8.amd64.rpm
sudo rpm -i stairwell-2.2.5-1.el8.amd64.rpm
```

Upgrade

```
$>
curl -O https://downloads.stairwell.com/linux/2.2.5/stairwell-2.2.5-1.el8.amd64.rpm
sudo rpm -U stairwell-2.2.5-1.el8.amd64.rpm
```

RHEL7

New Installation

```
$>
curl -O https://downloads.stairwell.com/linux/2.2.5/stairwell-2.2.5-1.el7.amd64.rpm
sudo rpm -i stairwell-2.2.5-1.el7.amd64.rpm
```

Upgrade

```
$>
curl -O https://downloads.stairwell.com/linux/2.2.5/stairwell-2.2.5-1.el7.amd64.rpm
sudo rpm -U stairwell-2.2.5-1.el7.amd64.rpm
```

RHEL6

New Installation

```
$>
curl -O https://downloads.stairwell.com/linux/2.2.5/stairwell-2.2.5-1.el6.amd64.rpm
sudo rpm -i stairwell-2.2.5-1.el6.amd64.rpm
```

Upgrade

```
$>
curl -O https://downloads.stairwell.com/linux/2.2.5/stairwell-2.2.5-1.el6.amd64.rpm
sudo rpm -U stairwell-2.2.5-1.el6.amd64.rpm
```

Agent 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 agent 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
```