

What your infrastructure can learn from accidents

How OpenVox helps prevent incidents

17th of July 2025
OpenVox Conf
Nuremberg

Simon Hönscheid
simon@xyntion.consulting

Who am I

Simon Hönscheid

CEO and Consultant at Xyntion GmbH,
Berlin, Germany

Experience with the Puppet/OpenVox
ecosystem since 2012

IT infrastructure automation, CI/CD,
Container technologies,
cloud computing, DevOps principles, &
team building



Content

01 | IT disasters happen

02 | The 5 W questions

03 | The reality check

04 | The traceability problem

05 | Infrastructure as Code — From chaos to clarity

06 | Questions

01

IT disasters happen

»A crisis is a terrible thing to waste.«

Paul Romer, former Chief Economist of the World Bank

Incidents happen and cost millions

December 2021

- AWS US East 1
- 7 hours of downtime
- Cost: \$150 million

July 2022

- Rogers, Canada
- 15 hours – 12 million users offline
- 25 % of Canada without internet

When was your last outage?

Everything is burning Is your infrastructure currently on fire?

Friday, 4:47 p.m.:

The website is down

No one knows what was changed



* no humans or animals were harmed in the taking of this picture

Maybe this scenario sounds familiar?

02

The 5 W questions

*»These 5 questions save lives on the road.
What if we apply them to IT?«*

Key Question

The 5 W questions

From road safety to IT infrastructure

WHO was involved?

→ Git commit author, ticket assignee, reviewer

WHAT happened?

→ Config changes, code diffs, system modifications

WHEN did it occur?

→ Precise timestamps, change windows, deploy times

WHERE was the impact?

→ Affected nodes, blast radius, geographical scope

WHY did this happen?

→ Business justification, root cause, ticket reference



WHO



WHAT



WHY



WHERE



WHEN

Traditional IT vs. systematic approach

Before vs. After

- ✗ »I don't know; it wasn't me«
- ✗ »Something with the configuration«
- ✗ »It was working yesterday«
- ✗ »Is this a global issue?«
- ✗ No history of who/what/when

- ✓ Commit author identified
- ✓ Exact changes documented
- ✓ Precise timing recorded
- ✓ Impact scope defined
- ✓ Business context preserved

The Paradigm Shift

It's not about blame.
It's about understanding.

Road safety achievement:
88 % fewer deaths since 1970.

IT infrastructure:
We're still asking: »Is it working now?«

→ It's Time for systematic incident investigation!

03

The reality check

»Complex systems fail in complex ways.«

Takeaway from Richard Cook, »How Complex Systems Fail«

Incidents happen

Major IT outages 2021-2024

- Facebook: 6 hours, \$100 million loss
- AWS: 7 hours, thousands of companies offline
- GitLab: database deleted, \$10 million loss
- Rogers: 15 hours, nationwide emergency
- we haven't talked about critical infrastructure so far

04

The traceability problem

*»Without traceability, we're not doing engineering
- we're doing archaeology.«*

Michael Nygard, »Release It!«

Let's do some archaeology

A typical response?

- `ssh prod-server-17`
- `grep -ri 'error' /var/log/*`
- »Hmm, nothing...«
- [3 hours later...]
- »Oh, it was prod-server-42«



Why traceability is lacking

The perfect recipe for disaster

- ✓ Technical debt
- ✓ Heroic administrators
- ✓ Tool chaos
- ✓ Lack of processes

- ✗ »I will do it«
- ✗ ASAP culture
- ✗ Legacy everywhere
- ✗ 5 different tools
- ✗ Lack of documentation



Are you too busy to improve?



Håkan Forss @hakanforss <http://hakanforss.wordpress.com>

This illustration is inspired by and in part derived from the work by Scott Simmerman, "The Square Wheels Guy" <http://www.performancecompany.com/>

The brutal truth

»Without traceability, every incident is a crime scene where the evidence has already been destroyed.«

05

Infrastructure as Code — from chaos to clarity

» You can't debug what you can't trace.«

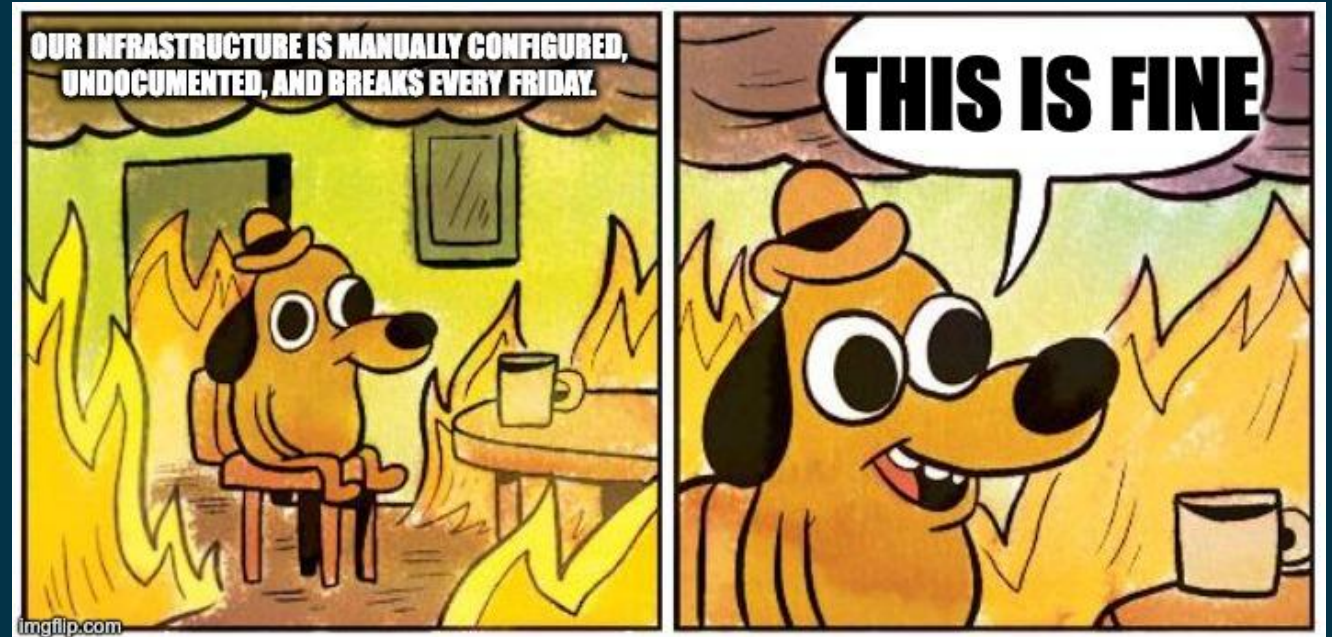
Distributed Systems Engineering Principle

Breaking the Cycle

Why traditional infrastructure management fails

- ✗ Manual changes
- ✗ Undocumented modifications
- ✗ »It worked on my machine«
- ✗ Archaeological debugging

- ✓ Every change tracked
- ✓ Full audit trail
- ✓ Instant root cause analysis

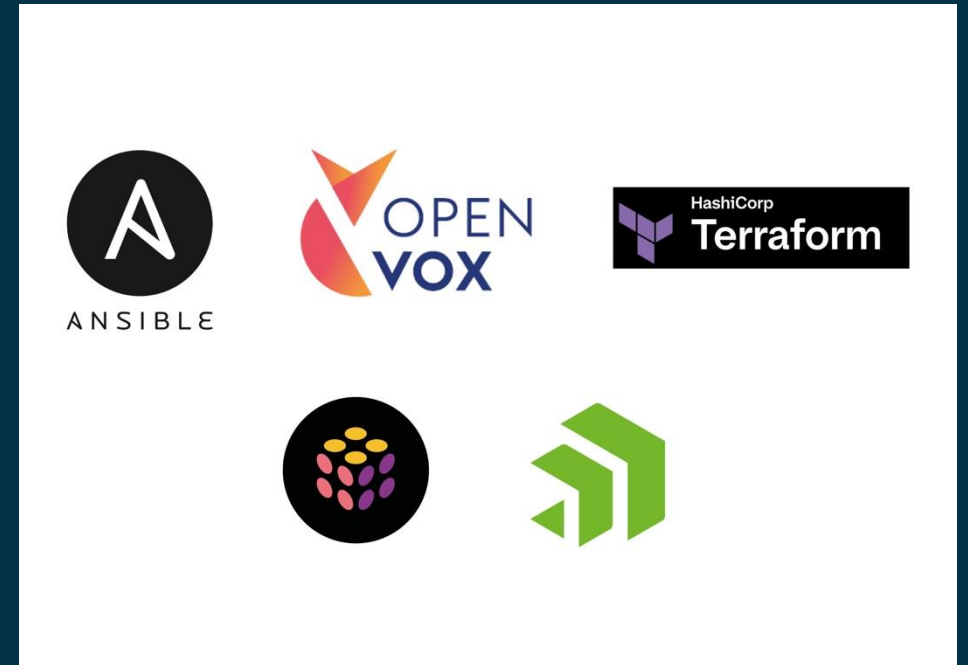


Infrastructure as Code to the rescue

- There are different tools for the same job
- Use what you and your team know best

OR

- What survived your evaluation process



OpenVox checks all the boxes

- ✓ Enterprise-ready Puppet Fork
- ✓ Git-native Workflow
- ✓ Tracability built-in
- ✓ Agent-Server model
- ✓ Agent pulls config every 30 min.
- ✓ Complete change history



Real-World Scenario

Black Friday preparation gone wrong

✓ The Ticket:

Increase worker_connections for user spike

✓ The Change:

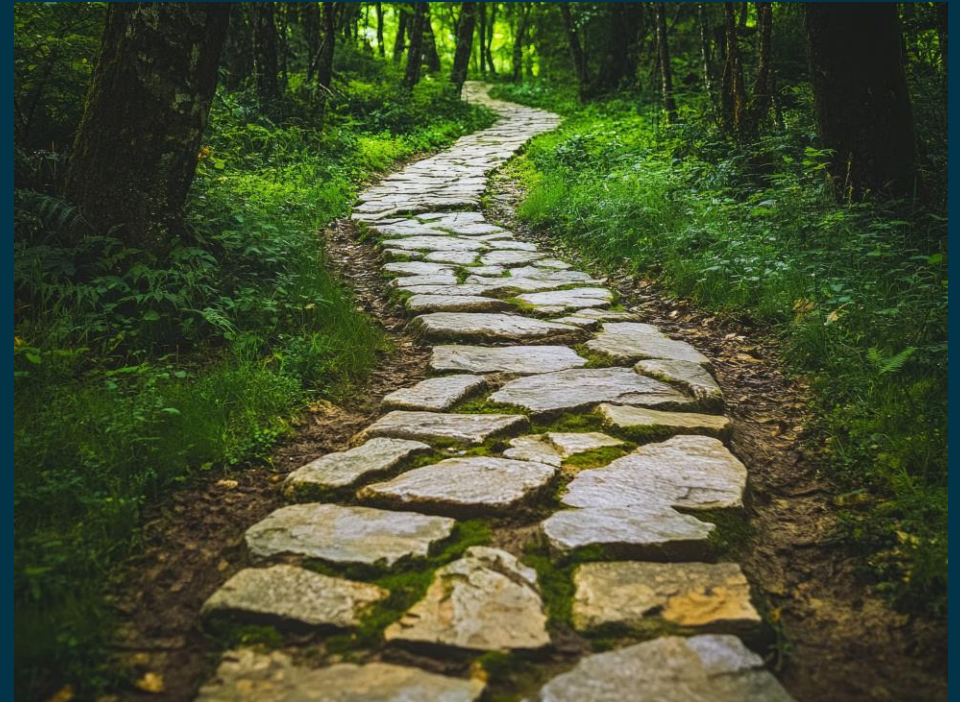
1024 to 4096 worker_connections

✓ The Problem:

Service becomes unresponsive

✓ The Question:

How do we trace this back?



Who?

Who was involved?

- ✓ A ticket for the change exists
- ✓ Personal Git identity
- ✓ Signed commits
- ✓ Review process

The image displays two overlapping screenshots from a development workflow. The top screenshot is a Jira ticket titled "We expect more traffic for Black Friday, please make sure, platform can handle the load". It includes a description about preparing for Black Friday by quadrupling worker connections, a "Tempo" section with a date range from May 01 to July 31, 2025, and a "View Report" button. The bottom screenshot is a GitHub pull request titled "feat: ECOM-1 raise nginx worker_connections to 4096 #1". It shows a commit from "SimonHoenscheid" being merged into the "production" branch. The pull request interface includes a "Conversation" tab with a comment from SimonHoenscheid linking to the Jira ticket, a "Commits" section showing the commit hash "c21635e", and a "Reviews" section where "marianhoenscheid" has approved the changes. A "Details" sidebar on the right lists assignees, reporters, and development progress.

What?

The course of the accident

✓ git show commit-id

```
commit 854099e6ba46946f92e2ddfbf88d9d6f2f8e8936
Author: Simon Hoenscheid <simon.hoenscheid@xyntion.consulting>
Date: Sat Jul 12 22:03:54 2025 +0200

    feat: ECOM-1 raise nginx worker_connections to 4096

diff --git a/data/roles/ecommerce_webserver.yaml b/data/roles/ecommerce_webserver.yaml
index 95250af..53e6f8c 100644
--- a/data/roles/ecommerce_webserver.yaml
+++ b/data/roles/ecommerce_webserver.yaml
@@ -7,4 +7,4 @@ nginx::gzip_vary: "on"
    nginx::gzip_min_length: 50
    nginx::gzip_proxied: "any"
    nginx::gzip_types: "text/plain text/css text/xml text/javascript application/x-javascript application/xml"
-nginx::worker_connections: 1024
+nginx::worker_connections: 4096
```

When?

Seconds can change everything

```
Info: Caching catalog for ecommerce-webserver-02.xyntion.consulting
Info: Applying configuration version '854099e - Simon Hoenscheid, Sat Jul 12 22:03:54 2025 +0200 : feat: ECOM-1 raise nginx worker_connections to 4096'
Notice: /Stage[main]/Nginx::Config/File[/etc/nginx/nginx.conf]/content:
--- /etc/nginx/nginx.conf      2025-07-12 20:03:07.482998226 +0000
+++ /tmp/puppet-file20250712-4818-y86nug      2025-07-12 20:04:12.510638487 +0000
@@ -10,7 +10,7 @@
events {
    accept_mutex on;
    accept_mutex_delay 500ms;
-   worker_connections 1024;
+   worker_connections 4096;
}

http {

Notice: /Stage[main]/Nginx::Config/File[/etc/nginx/nginx.conf]/content: content changed '{sha256}7f86c60ef0ed0449c80360cb5b20d37600ce4f261d226ddc603caca1cc2c
Info: Class[Nginx::Config]: Scheduling refresh of Class[Nginx::Service]
Info: Class[Nginx::Service]: Scheduling refresh of Service[Nginx]
Notice: /Stage[main]/Nginx::Service/Service[Nginx]: Triggered 'refresh' from 1 event
Notice: Applied catalog in 1.56 seconds
```

- ✓ 2:30 p.m. – Change deployed, OpenBolt Plan triggered
- ✓ 2:35 p.m. – Alarm triggered
- ✓ 2:40 p.m. – OpenVox View or Foreman show last changes
- ✓ 2:45 p.m. – Rollback and Open Bolt Plan initiated

- ✓ 2:50 p.m. – Service restored
- ✓ 2:55 p.m. – ITSM ticket created for incident
- ✓ 2:56 p.m. – Invitation to post-mortem sent

Where?

The scene of an incident

- ✓ Explicit node definitions
- ✓ Predictable blast radius
- ✓ No more surprises

```
5 class role::ecommerce_webserver () {
6     include profile::apt
7     include profile::packages
8     include profile::openssl
9     include profile::nginx_webserver
10 }
```

```
data > roles > ! ecommerce_webserver.yaml > ...
You, vor 1 Stunde | 1 author (You)
1 ---
2 nginx::ssl_protocols: "TLSv1.2 TLSv1.3"
3 nginx::ssl_ciphers: "ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-
4 nginx::ssl_ecdh_curve: "secp521r1:secp384r1:prime256v1"
5 nginx::gzip: "on"
6 nginx::gzip_vary: "on"
7 nginx::gzip_min_length: 50
8 nginx::gzip_proxied: "any"
9 nginx::gzip_types: "text/plain text/css text/xml text/javascript application/x-javascript a
10 nginx::worker_connections: 4096
```

Why?

It started with a ticket

Projects / Ecommerce / Add parent / ECOM-1

We expect more traffic for Black Friday, please make sure, platform can handle the load

Description

As Black Friday is nearing, marketing asked us to prepare the platform for the incoming extra load. As discussed in the daily this morning, please quadruple the number of worker connections. The nginx option is called `worker_connections`.

Tempo

Worklogs / PlansActivities

01 May - 31 Jul, 2025 < > View: All Data ▾

View Report

THERE ARE NO ACTIVITIES FOR YOU TO SEE WITH THE SELECTED FILTER CRITERIA.
Click below to track your time or adjust your filters.

Log TimePlan Time

Activity

Done ▾

✓ Done

⌘ Improve Task

Details ⌵

Assignee

Simon Hönscheid

Reporter

Simon Hönscheid

Create branch

Development

1 commit9 minutes ago

1 pull requestMERGED

Labels

None

Due date

Nov 27, 2025

Start date

Nov 26, 2025

Approved by

Marian Hönscheid

Requester

Alexander Pinkert

Priority

Highest

XYNTION

Why?

A Pull Request was created...

feat: ECOM-1 raise nginx worker_connections to 4096 #1

Edit< > Code

Open

SimonHoenscheid wants to merge 1 commit into `production` from `ECOM-1-we-expect-more-traffic-for-black-friday-please-make-sure-platform-can-handle-the-load`

Conversation 0

Commits 1

Checks 0

Files changed 1

+1 -1

SimonHoenscheid commented 6 minutes ago

details can be found here: <https://xyntion.atlassian.net/browse/ECOM-1>

feat: ECOM-1 raise nginx worker_connections to 4096

Verifiedc21635e

SimonHoenscheid assigned marianhoenscheid 6 minutes ago

marianhoenscheid approved these changes now

View reviewed changes

Reviewers

marianhoenscheid

Still in progress? [Convert to draft](#)

Assignees

marianhoenscheid

Labels

None yet

Projects

Why?

Check the diff

```
commit 854099e6ba46946f92e2ddfbf88d9d6f2f8e8936
Author: Simon Hoenscheid <simon.hoenscheid@xyntion.consulting>
Date: Sat Jul 12 22:03:54 2025 +0200

    feat: ECOM-1 raise nginx worker_connections to 4096

diff --git a/data/roles/ecommerce_webserver.yaml b/data/roles/ecommerce_webserver.yaml
index 95250af..53e6f8c 100644
--- a/data/roles/ecommerce_webserver.yaml
+++ b/data/roles/ecommerce_webserver.yaml
@@ -7,4 +7,4 @@ nginx::gzip_vary: "on"
  nginx::gzip_min_length: 50
  nginx::gzip_proxied: "any"
  nginx::gzip_types: "text/plain text/css text/xml text/javascript application/x-javascript application/xml"
-nginx::worker_connections: 1024
+nginx::worker_connections: 4096
```



Why?

Let's apply the change

```
Info: Caching catalog for ecommerce-webserver-02.xyntion.consulting
Info: Applying configuration version '854099e - Simon Hoenscheid, Sat Jul 12 22:03:54 2025 +0200 : feat: ECOM-1 raise nginx worker_connections to 4096'
Notice: /Stage[main]/Nginx::Config/File[/etc/nginx/nginx.conf]/content:
--- /etc/nginx/nginx.conf      2025-07-12 20:03:07.482998226 +0000
+++ /tmp/puppet-file20250712-4818-y86nug      2025-07-12 20:04:12.510638487 +0000
@@ -10,7 +10,7 @@
  events {
    accept_mutex on;
    accept_mutex_delay 500ms;
-   worker_connections 1024;
+   worker_connections 4096;
  }

  http {

Notice: /Stage[main]/Nginx::Config/File[/etc/nginx/nginx.conf]/content: content changed '{sha256}7f86c60ef0ed0449c80360cb5b20d37600ce4f261d226ddc603caca1cc2c
Info: Class[Nginx::Config]: Scheduling refresh of Class[Nginx::Service]
Info: Class[Nginx::Service]: Scheduling refresh of Service[nginx]
Notice: /Stage[main]/Nginx::Service/Service[nginx]: Triggered 'refresh' from 1 event
Notice: Applied catalog in 1.56 seconds
```


Why?

We need to revert this

```
Info: Caching catalog for ecommerce-webserver-02.xyntion.consulting
Info: Applying configuration version 'b109f06 - Simon Hoenscheid, Sat Jul 12 22:05:18 2025 +0200 : Revert "feat: ECOM-1 raise nginx worker_connections to 4096"'
Notice: /Stage[main]/Nginx::Config/File[/etc/nginx/nginx.conf]/content:
--- /etc/nginx/nginx.conf      2025-07-12 20:04:12.518638445 +0000
+++ /tmp/puppet-file20250712-6075-9er73s      2025-07-12 20:07:11.689768831 +0000
@@ -10,7 +10,7 @@
  events {
    accept_mutex on;
    accept_mutex_delay 500ms;
-   worker_connections 4096;
+   worker_connections 1024;
  }

  http {

Notice: /Stage[main]/Nginx::Config/File[/etc/nginx/nginx.conf]/content: content changed '{sha256}8f7657ebd283b5b57e57ee97476e40c0e8d1aced8db1ff35b7deefca197f259f
Info: Class[Nginx::Config]: Scheduling refresh of Class[Nginx::Service]
Info: Class[Nginx::Service]: Scheduling refresh of Service[nginx]
Notice: /Stage[main]/Nginx::Service/Service[nginx]: Triggered 'refresh' from 1 event
Notice: Applied catalog in 1.45 seconds
```

The 5 W questions in IT infrastructure

In every crisis, ask five questions

- ✓ **WHO** made the change? → Git commit author
- ✓ **WHAT** was changed? → Diff in the hiera repository
- ✓ **WHEN** did the change take place? → Update in Control Repository
- ✓ **WHERE** was the change made? → Node classification and monitoring dashboard
- ✓ **WHY** did this change happen? → Ticket in commit message

06

Questions

»The important thing is not to stop questioning.«

Albert Einstein

What your infrastructure can learn from accidents

How OpenVox helps prevent incidents

17th of July 2025
OpenVox Conf
Nuremberg

Simon Hönscheid
simon@xyntion.consulting