

MAJOR WIN

Self-hosted mailbox migration with failure triage and auth hardening

Local Failures restore · backscatter cleanup · SPF / DKIM / DMARC

A specialist named **Email Migration** moved business mail onto a self-hosted stack, recovered stranded customer messages from Sync Issues / Local Failures, cleared a forged-sender backscatter flood, and finished domain authentication so the new system was usable — not merely imported.

THE PROBLEM

Cloud → self-host cutovers fail in the last mile. Local Failures folders can hold real customer mail that never reached Inbox. Spoofed envelope senders can dump thousands of bounce/NDR reports into the shared Inbox. Without SPF, DKIM, and DMARC quarantine, the domain stays easy to forge.

APPROACH

- 1 **Stand up destinations** — Create mailboxes; import history (including large PST uploads).
- 2 **Cutover plumbing** — DNS / TLS / mailbox limits.
- 3 **Local Failures triage** — Move clear customer mail to Inbox; leave ambiguous items.
- 4 **Backscatter scrub** — Clear forged-sender bounce flood; add content filters.
- 5 **Auth hardening** — Enable DKIM; verify with existing SPF + DMARC quarantine.

MEASURED OUTCOMES

Metric	Value
Main-agent JSONL lines	673
Real user messages	43

Metric	Value
Tool messages	271
Fleet rank by transcript size	#3 of 12
Local Failures scanned (combined)	643
Restored to Inbox	632
Backscatter pile before (approx)	~6,700
Inbox after cleanup (approx)	~586
Content filters added	2
Auth stack	SPF + DKIM + DMARC quarantine
Major win day (CT)	2026-09-06

WHY IT MATTERS

Migration is not done at first sync. Recovering stranded customer mail, scrubbing a spoofing-driven bounce flood, and finishing domain auth make a self-hosted cutover usable day-to-day. Tool density (271 tool msgs vs 43 user turns) is the signal.

TAKEAWAYS

- Measure mailbox agents by verified restores, inbox hygiene, and auth checks.
- Failure folders are first-class work — 632 recovered messages with receipts.
- Post-cutover hardening closes the ‘mail works and isn’t drowning’ loop.
- Never publish passwords, address lists, or raw mail bodies.

Privacy note: Patterns, aggregate counts, and auth mechanism names only. Withheld: mailbox passwords, admin credentials, server IPs, third-party addresses, message bodies, raw chats, credential files.

© 2026 SmarTekAI · <https://smartekai.net> · Patterns over voyeurism