NETCOLOGNE

WIR KÖNNEN HIER.

Heinlein Mailserverkonferenz 2011

NetCologne Communication Center

Austausch einer ISP Mail-Plattform - ohne downtime

NETCOLOGNE

WIR KÖNNEN HIER.

EHLO christian.rohmann.netcologne.de

NETCOLOGNE
WIR KÖNNEN HIER.

Christian Rohmann

- Network Engineering and Design
  - Content Delivery Platform (Internetdienste)
- Aufgaben
  - E-Mail-Plattform
  - NMS, EMS
  - Solaris
- Dipl.-Inform.(FH)

NETCOLOGNE
WIR KÖNNEN HIER.

Warum?

Was?

Wie?

Was noch?

Wieso?

NETCOLOGNE

WIR KÖNNEN HIER.

Warum?

NETCOLOGNE
WIR KÖNNEN HIER.

Ausgangsituation - Mehrere Plattformen

- netcologne.de-Postfächer
  - Beigabe zum Internetzugang
- Kundendomains
  - Paketprodukte (x Postfächer, x MB Quota)
- Weitere kleine Lösungen (Firmenübernahmen)

- Probleme
  - Hoher Pflegeaufwand
  - Keine Produktübergänge
  - Keine gemeinsame Innovation

NETCOLOGNE
WIR KÖNNEN HIER.

Ausgangssituation - netcologne.de

- 50MB Postfächer
- Nur POP3, kein IMAP
- Keine SMTP-Authentisierung (+ kein SSL)
- Webmail Horde 3 (IMP, Ingo, Turba, Kronolith)
  - Kein Onlinespeicher
  - Kein Synchronisation (Adressbuch, Kalender)
  - Keine Groupware-Funktionen

NETCOLOGNE
WIR KÖNNEN HIER.

Ausgangssituation - Mailrouting

- Keine Unterstützung für Domains
  - Einzige Domain = netcologne.de
- Adressrewriting zum Routing
  - Zustellung zum Mailstore
    crohmann@netcologne.de ->crohmann@mailstore21.netcologne.de
  - Weiterleitung per virtual alias
- Ältere Softwarekomponenten
  - Policyd v1 für z.B. Greylisting
  - Keine durchgehende IPv6 Unterstützung

NETCOLOGNE
WIR KÖNNEN HIER.

Ausgangssituation – (E-Mail-)Storage

- „Mailstore“: Sun Fire V240 / V440 Server
  - Alte Hardware + Solaris 9
  - Festplattenausbau schwierig
  - Oracle != Sun
  - ca. 40k Postfächer/Server
- Backupzeiten zu lang (RTO, RPO)

NETCOLOGNE
WIR KÖNNEN HIER.

Ausgangssituation – IMAP/POP3

- Perdition als IMAP/POP3 Proxy
  - Ermittlung des Mailstore für Postfach
  - Kein Login mittels Alias
- Cyrus POP3/IMAP
  - Indexdatenbanken
  - '.' anstatt '/' als Separator
  - NFS-Support „schwierig“

NETCOLOGNE
WIR KÖNNEN HIER.

Ziel: Gemeinsame Plattform

- Multi-Domain / Mandantenfähig
  - netcologne.de – yet another domain
- Premium-Pakete (kommerziell)
- Modernisierung sämtlicher Software
- Ablösung sämtlicher alter Hardware
  - Nicht nur Sun/Oracle-Hardware
  - Evtl. Migration auf VMware ESXi Cluster

NETCOLOGNE
WIR KÖNNEN HIER.

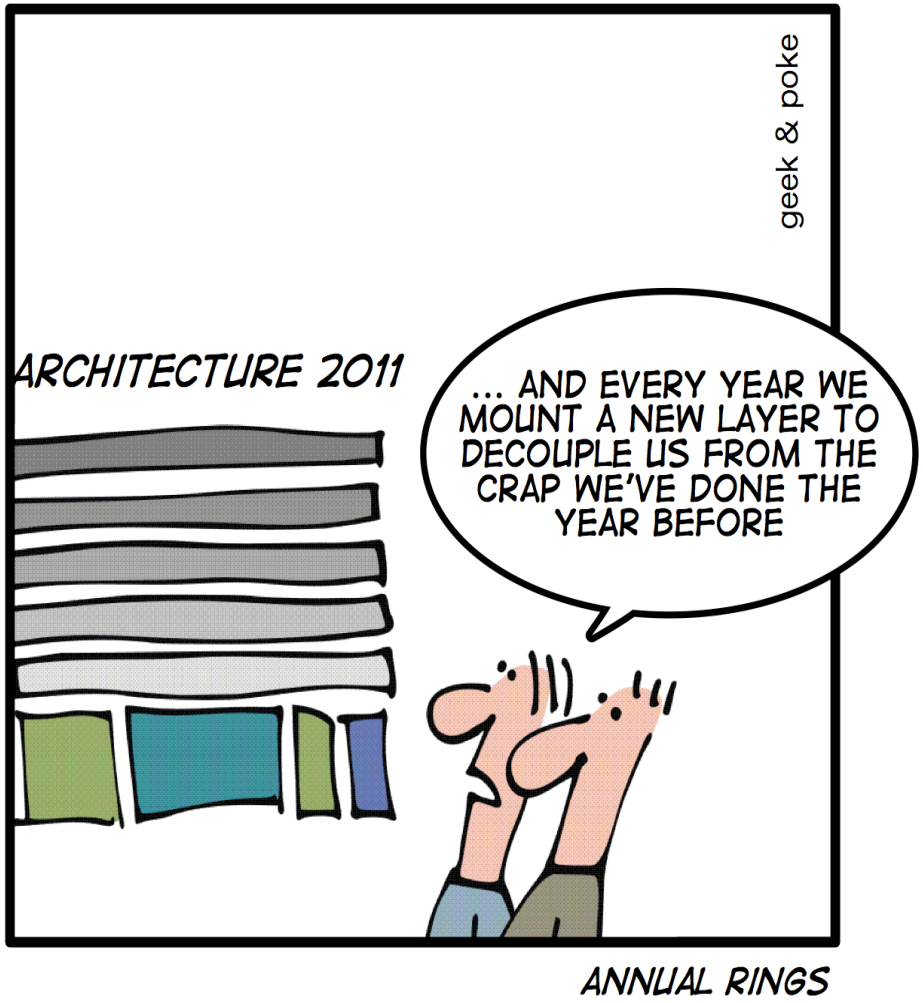
Was ?

NETCOLOGNE
WIR KÖNNEN HIER.

Layers ...

BEST PRACTICES IN APPLICATION ARCHITECTURE

TODAY: USE LAYERS TO DECOUPLE



NETCOLOGNE
WIR KÖNNEN HIER.

… Abstraktionsschichten

APPLIKATION
Webmail / PIM / Groupware / Synchronisation / ...

E-MAIL
E-Mail-Routing / - Verarbeitung / Policies / Anti-Spam / DB / ...

INFRASTUKTUR
HW / VMware / Storage (SAN, NAS) / Netze / LB / FW / ...

Operation Support System (OSS)

NETCOLOGNE
WIR KÖNNEN HIER.

Infrastruktur - Storage - Optionen

- Zwei Anwendungsfälle
  - E-Mails
  - Onlinespeicher (OX Infostore)
- Viele Möglichkeiten
  - DRBD (active/active, active/passive)
  - Cluster-FS
  - SAN
  - NAS (NFS)
  - ...

NETCOLOGNE
WIR KÖNNEN HIER.

Infrastruktur - Storage - NFS

- Entscheidung: NAS mittels NFS
  - Gleichzeitiger Zugriff (Skalierung, Redundanz)
  - Erweiterung ohne downtime
- NetApp Filer
  - Redundantes Primärsystem
  - Backup: Snapshots
  - Disaster Recovery: NearLine (SnapMirror)

NETCOLOGNE
WIR KÖNNEN HIER.

Infrastruktur - Storage - NFS-Netz

- Dedizierter Backbone für NFS Anwendungen
- Simples Design
  - 10 GigE
  - Layer 2
  - RSTP (rapid spanning-tree)
  - 802.1q (VLANs), 802.1p (Prioritäten)
  - Jumbo Frames (9k)

NETCOLOGNE
WIR KÖNNEN HIER.

Infrastruktur - Virtualisierung

- VMware ESXi 4 Cluster
  - Standortverteilt
  - Redundante Netzanbindungen
  - Speicher: NetApp Metrocluster
- Lastverteilung
  - Passende Anzahl der Gäste
  - Automatische Lastverteilung (Dynamic Resource Scheduler – DRS)

NETCOLOGNE
WIR KÖNNEN HIER.

Infrastruktur – Netz / Load balancing

- Dedizierte IP-Netze
  - Trennung Frontend / Backend
  - Einfache Regeln für Firewalls
- F5 BigIP load balancer
  - Nur „sichtbare“ Dienste (z.B. pop3.netcologne.de)
  - Vorerst kein SSL offloading
    - STARTTLS
    - bessere Logging-Qualität

NETCOLOGNE
WIR KÖNNEN HIER.

E-Mail - Mailrouting

- MTA bleibt Postfix
  - Komplett neue Konfiguration (Multidomain-Datenmodell, restrictions, RBLs, ...)
  - Kein rewriting zum Routing
  - Weiterleitungen als virtual alias (OX: sieve)
- Dovecot statt Cyrus → Dovecots Deliver als LDA
- Policyd v1 → Policyd v2 (Cluebringer)

NetCologne
Wir Können Hier.

E-Mail – POP3/IMAP Proxies

- nginx mit eigenem Auth-Modul
  - Loadbalancing über kanonischen Mailbox-Namen
  - (Zugriff mit Alias möglich)
  - Stickyness
    - Mailboxen auf NFS-Volumes (Locking, Caches)
    - Dovecot Caches / Indexe
  - Ausfallerkennung für Backends

NGINX™

NETCOLOGNE
WIR KÖNNEN HIER.

E-Mail – POP3/IMAP-Server

- Dovecot für POP3/IMAP
- Robuste Datenstruktur(en)
  - maildir++
  - Selbstheilende Indexe
- Features, Features, Features
  - Suchfunktionen (z.B. FTS)
  - sieve Module
  - ACLs
- Performance
- Sehr aktive Entwicklung, sauberer Code

DOVECOT

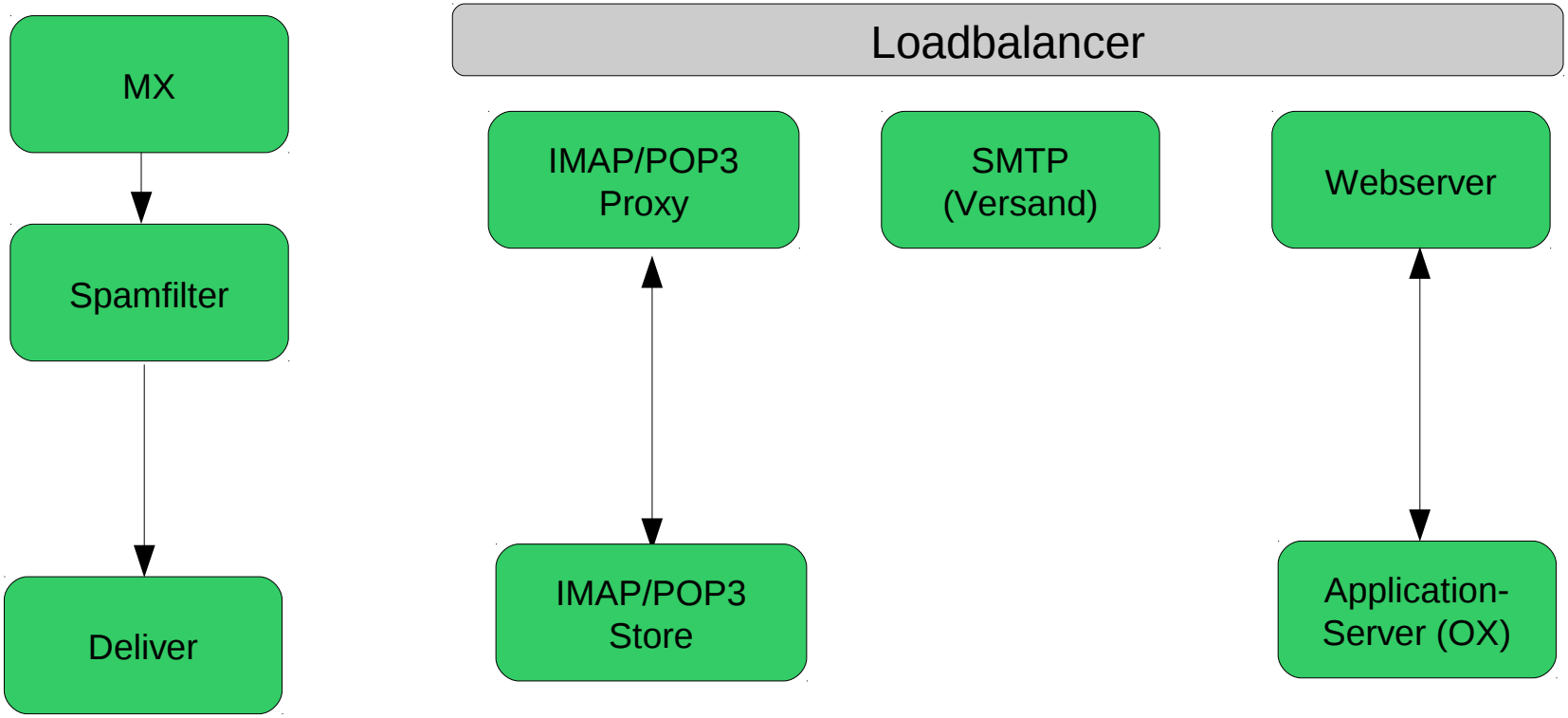
NETCOLOGNE
WIR KÖNNEN HIER.

E-Mail - Ablagestruktur Mailboxen

- (NFS-)Volume wird bestimmt (Zufall, Füllgrad, …)
- Gleichmäßige Verteilung von Mailboxen über verfügbare Volumes (Speicherplatz, IOPS)
- Verzeichnis zweistufig gehashed, „mailbox@domain„
  - Bsp.: *vol104/29/29d6/crohmann@netcologne.de*
  - 255 Verzeichnisse pro Ebene
  - Keine DB-Einträge für Verzeichnis
  - Gleichverteilung

NETCOLOGNE
WIR KÖNNEN HIER.

E-Mail / Applikation - Servergruppen



NETCOLOGNE
WIR KÖNNEN HIER.

E-Mail – Loadbalancing / HA

- Jede Server-Gruppe mittels LB/HA Mechanismen gekoppelt
  - Webserver: mod_proxy_balancer
  - POP3/IMAP: nginx mit eigenem Auth-Modul
  - Mailrouting: Postfix mit mehreren A-records
  - Sieve (nicht öffentlich): haproxy
  - MySQL
    - schreibend: master-master mit virtual IP
    - lesend: Support für mehrere DB-Server in Anwendung

NETCOLOGNE
WIR KÖNNEN HIER.

Applikation - OpenXchange

- Kein „Mailserver“
  - Anbindung an Plattform über Standardprotokolle
  - OpenXchange-GUI „nur“ HTML+JS
  - Applikations-Server in Java
- Features / Integration
  - Exchange Active Sync (EAS)
  - MAPI (MS Exchange Server in Outlook)
  - WebDAV (Infostore)
- Open Source + agile Entwicklung
- Räumliche Nähe (Olpe, Nürnberg)

NETCOLOGNE
WIR KÖNNEN HIER.

OSS – Operation Support System

- Abstraktion der Mailplattform
  - Provisioning (Aufträge durch CRM)
  - Konfiguration (E-Mail-Alias, Spamfilter, Featureset)
  - Informationsabfrage durch 1st level support tools (z.B. Quota, E-Mail-Alias, Statistiken)
- SOAP/XML

NetCologne
Wir Können Hier.

Wie?

NETCOLOGNE
WIR KÖNNEN HIER.

Migration

- Abschnitt 1 - Mailsystem (Mailrouting, Mailboxen, …)
- Abschnitt 2 - WebMail / Groupware (Horde → OX)

- Anforderungen
  - Kein Datenverlust
  - Keine downtime
  - Steuerbare Migrationsgeschwindigkeit
    - Postfachweise
    - Erkennung von Problemen
    - Support-Anfragen

NETCOLOGNE
WIR KÖNNEN HIER.

Migrationsphasen

- Phase 0 – Vorbereitung
- Phase 1 - Umstellung Mailrouting / Mailboxzugriff
- Phase 2 – Abschaltung alte MX, SMTP, POP3-proxies
- Phase 3 - Migration Postfächer Mailstore → ComCenter
- Phase 4 – Rückbau alte Mailstores

- Phase 5 – Start „comcenter.netcologne.de“
- Phase 6 - Umzug Horde → Open-Xchange
- Phase 7 – Einführung SMTP-Auth (verpflichtend)

NETCOLOGNE
WIR KÖNNEN HIER.

Phase 0 – Vorbereitung

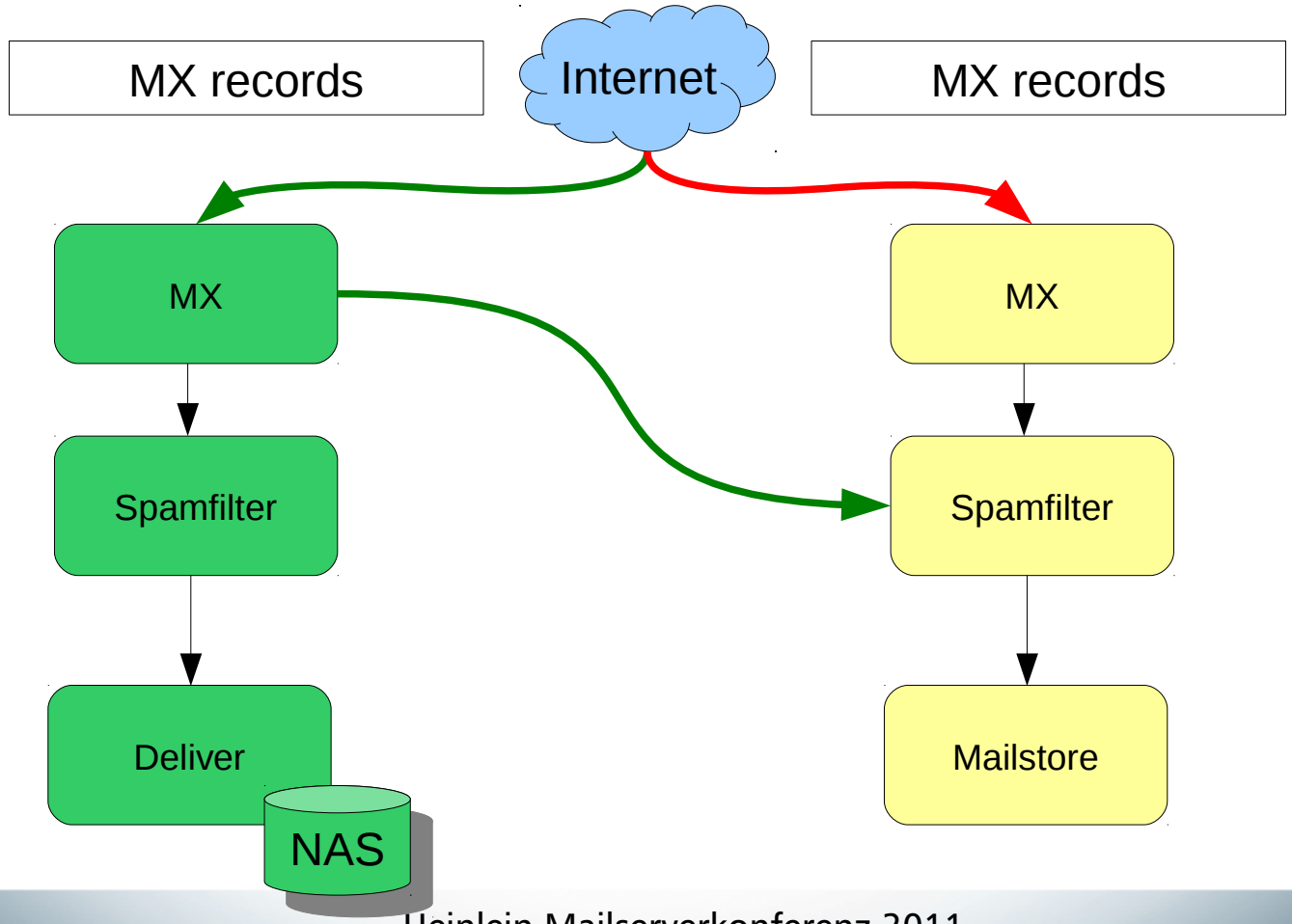
- Tests
  - Review Konfiguration
  - Tests der gesamten Funktionalitäten
  - Tests neues Provisioning
- Vorbereitungen Parallelbetrieb
  - Synchronisation neue MailDB mit Bestandsdaten
  - Ab jetzt: Parallele Datenpflege alte/neue DB
  - Migrationsstatus der Mailbox → Datenbank
- Open-Xchange Installation noch WiP

NETCOLOGNE
WIR KÖNNEN HIER.

Phase 1 – Planung Umstellung Mailrouting

NETCOLOGNE
WIR KÖNNEN HIER.

Phase 1 – Umstellung Mailrouting



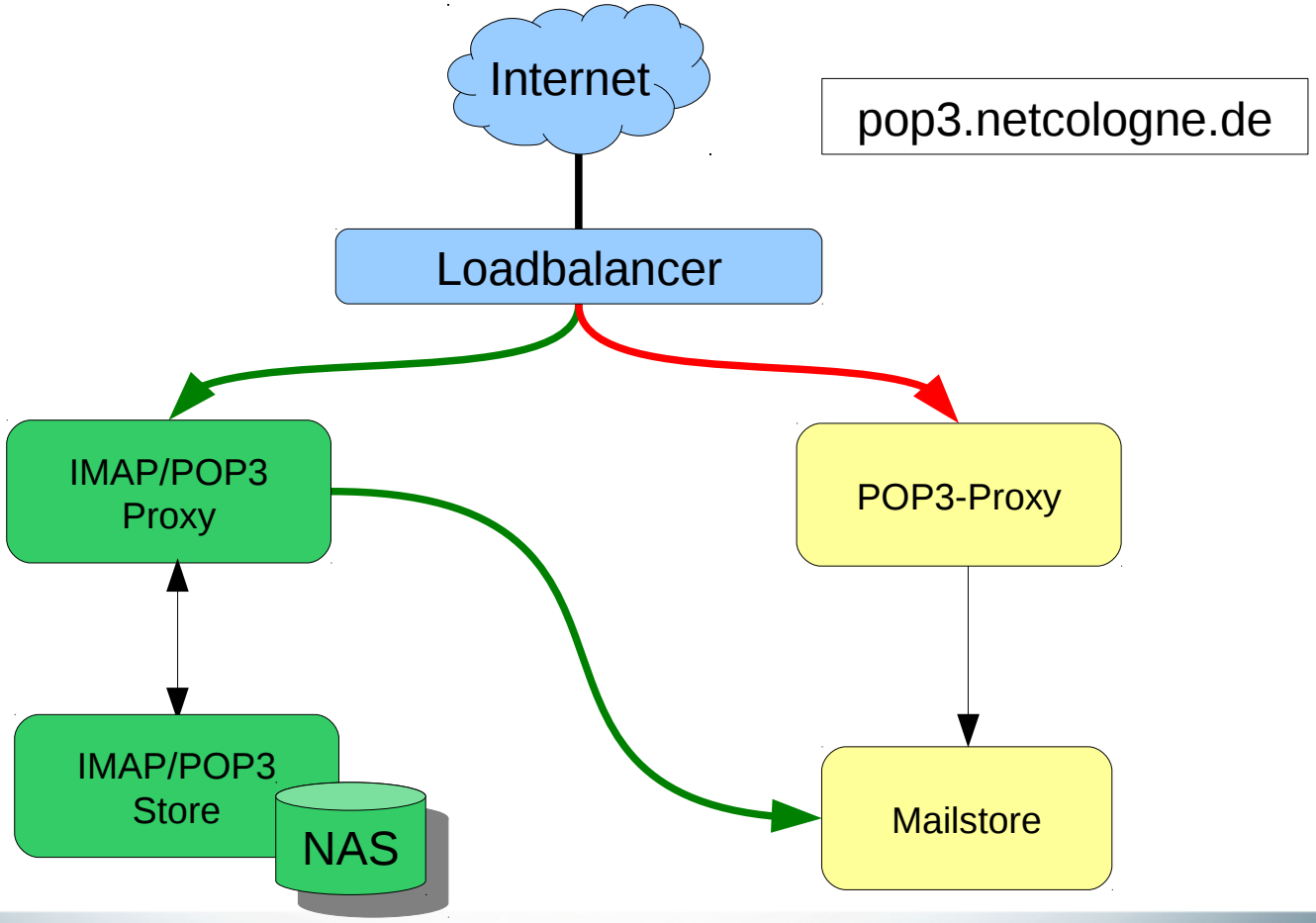
NetCologne
Wir Können Hier.

Phase 1 – Umstellung Mailrouting

- rewrite + transport-maps (mysql) für (noch) nicht migrierte Accounts → Bestandssystem
- Änderung MX records
- Kurzer Paralellbetrieb (Anti-DoS, greylisting, …)
- Umstellung Weiterleitungen
  - virtual-alias (von OX nicht unterstützt) → sieve
  - Kleinere Anpassung im NetMail

NETCOLOGNE
WIR KÖNNEN HIER.

Phase 1 – Umstellung Mailboxzugriff



NetCologne
Wir Können Hier.

Phase 1 – Umstellung Mailboxzugriff

- Nginx POP3/IMAP-proxies
  - username load balancing ins Backend
  - Per Datenbank
- Parallelbetrieb neue/alte POP3/IMAP-Proxies
  - Letzte Tests mit realen Zugriffen
  - Deaktiverung der alten Proxies im Loadbalancer
- IMAP/sieve-Zugriff für WebMail angepasst
  - Zugriff über neue IMAP-Proxies
  - IMAP separator

NETCOLOGNE
WIR KÖNNEN HIER.

Phase 2- Abschaltung alte MX

- Sämtlicher Traffic über neue Systeme
- Weichen für (noch) nicht migrierte Postfächer
  - Eingehend per rewrite + transport
  - Lesend per nginx-Modul (Zugriff auf mailstore-Server)
- Migration von Postfächern nun möglich

NetCologne
Wir Können Hier.

Phase 3 - Migration Postfächer

- Ablauf
  - Sperren des Postfachs
  - Migration direkt auf Dateisystem (cyrus2dovecot)
  - Wenn „OK“ → Änderung des Migrationsstatus
  - Freigabe des Postfachs
- Beibehaltung POP3-UIDs, IMAP-Flags, ...
- Anpassung sieve-Skript (z.B. fileinto UTF-7 → UTF-8)
- Dauer: Wenige Sekunden pro Postfach (50MB Quota)

NETCOLOGNE
WIR KÖNNEN HIER.

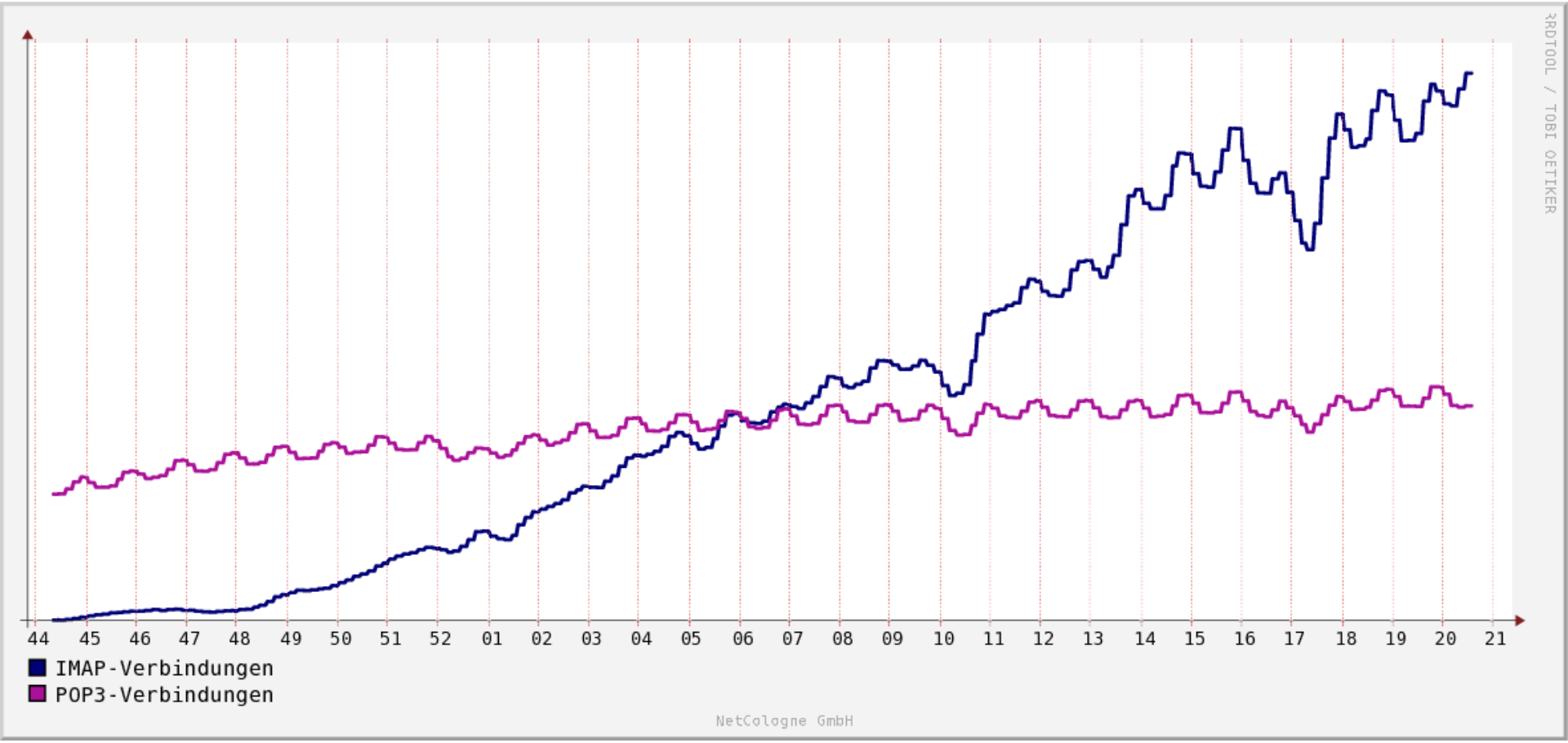
Phase 4 - Rückbau alte Mailstores

- Sämtliche Mailboxen wurden migriert
- Deaktivierung der symmetrischen Datenpflege
- Entfernen sämtlicher Weichen

- Aktivierung IMAP (imap.netcologne.de)
- Erhöhung Quota 50MB → 1GB

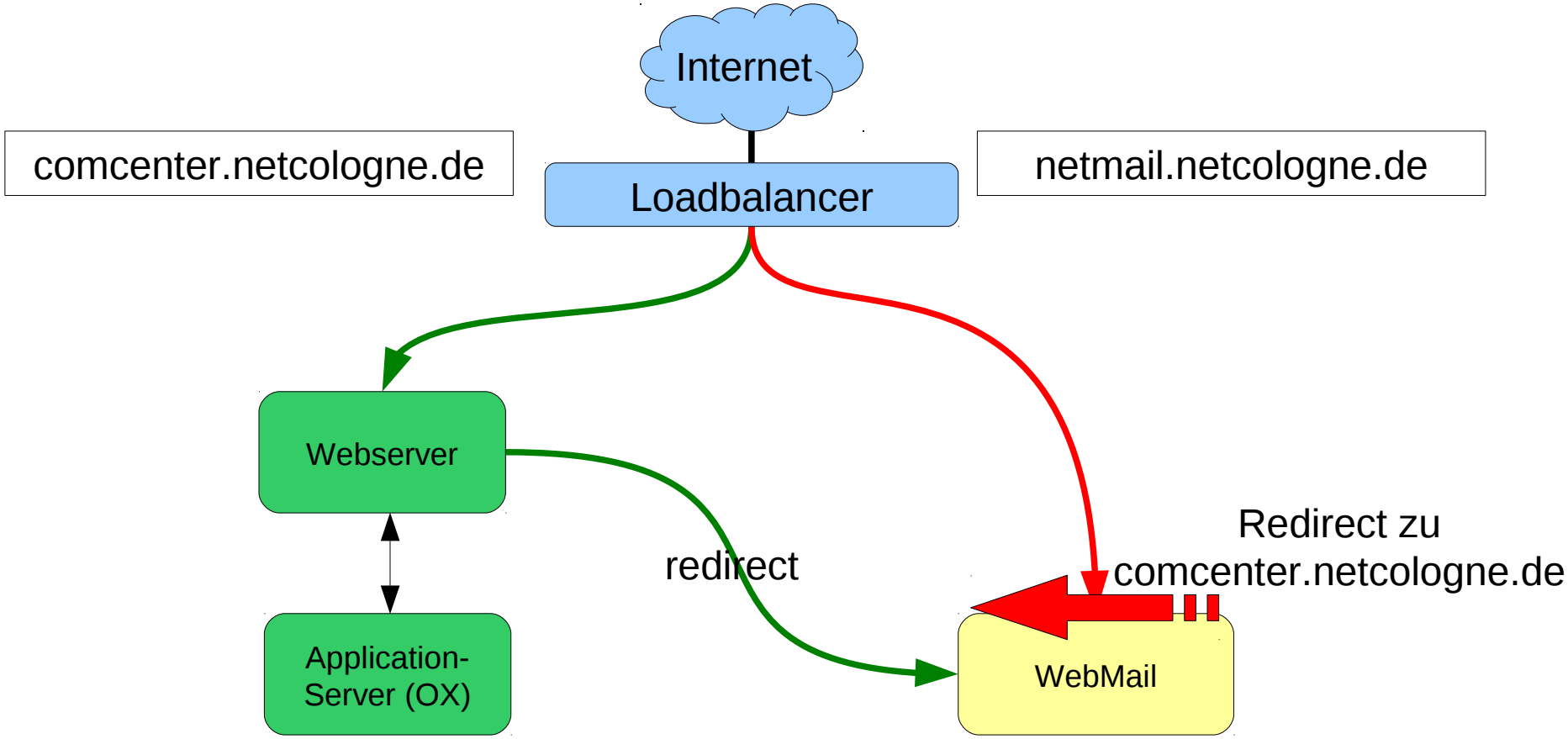
NetCologne
Wir können hier.

Verwendung von IMAP vs. POP3



NetCologne
Wir Können Hier.

Phase 5 – comcenter.netcologne.de



NETCOLOGNE
WIR KÖNNEN HIER.

Phase 5 – comcenter.netcologne.de

- Neue Portalseite
  - Redaktionelle Inhalte
- Redirect von netmail.netcologne.de
  - Login-Weiche für ComCenter(OX) vs. NetMail (Horde)
  - Zunächst 100% NetMail
- User für User Migration
  - Mitarbeiter / Tester
  - Sehr aktive User
  - Rest

NETCOLOGNE
WIR KÖNNEN HIER.

Phase 6- Horde → Open-Xchange

- Anlegen OX User
- Datenübername aus Horde
  - Mailbox bleibt unverändert (IMAP)
  - Adressbücher (vCard export → vCard import)
  - Kalender (iCal export → iCal import)
  - Konvertierung Mailfilter (sieve)
    - OX reparsed sieve-Skripte / Ingo = Schatten-DB
    - Metainfos als (sieve-)Kommentar
  - perl / php
- Nach Abschluss → Migrationsflag auf „done“

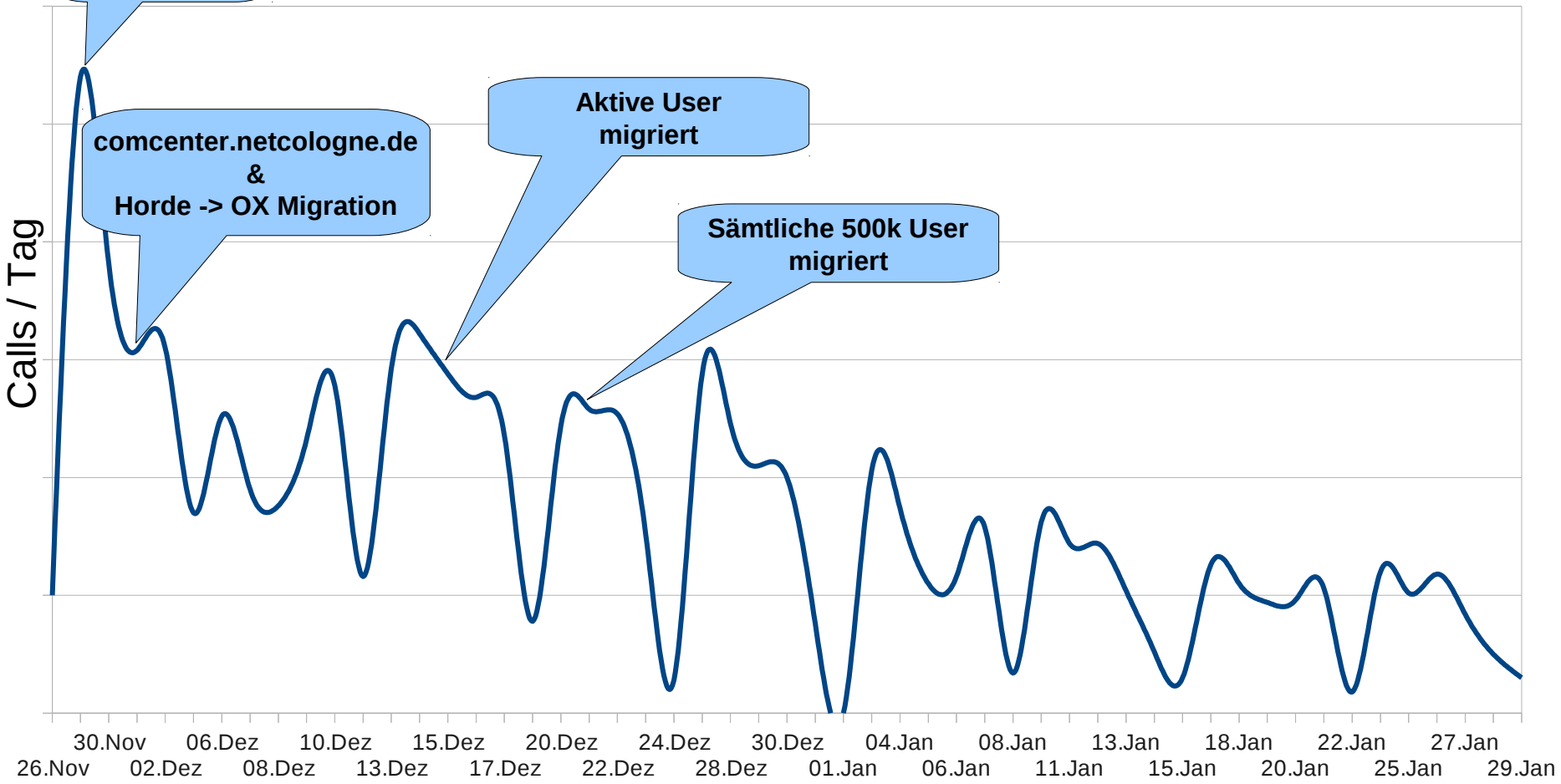
NETCOLOGNE
WIR KÖNNEN HIER.

Phase 7 - SMTP-Authentication

- Informationskampagne zur Umstellung
  - E-Mails, Anleitungen, 0800er Rufnummer
- Automatische Hinweismail: Korrelation IP → Username
- Umstellung pro Einwahlsystem (BRAS, CMTS, …)
  - Steuerung der Support-Calls
- opt. SMTP-Auth bereits vorab aktivieren

NetCologne
Wir Können Hier.

Anrufaufkommen Callcenter



NETCOLOGNE

WIR KÖNNEN HIER.

Was noch?

NETCOLOGNE
WIR KÖNNEN HIER.

Weitere Pläne

- Open-Xchange
  - Upsell (Kommerzielle Produkte)
  - Groupware
    - Ersatz für Exchange / Lotus Notes (OLOX2)
  - Synchronisation (Adressbuch, Kalender)
  - Soziale Netzwerke
  - Online-Festplatte (Infostore)
- Benuzer-individueller Spamfilter
- Antivirus

NETCOLOGNE

WIR KÖNNEN HIER.

Wieso ?

NETCOLOGNE
WIR KÖNNEN HIER.

Wieso ...

- hat NetCologne … ?
- hat NetCologne nicht … ?

NETCOLOGNE
WIR KÖNNEN HIER.

Vielen Dank

Christian Rohmann
Content Delivery Platform
Network Engineering and Design

NetCologne GmbH
Am Coloneum 9
50829 Köln

Vortag zum Download