



Dave Knight

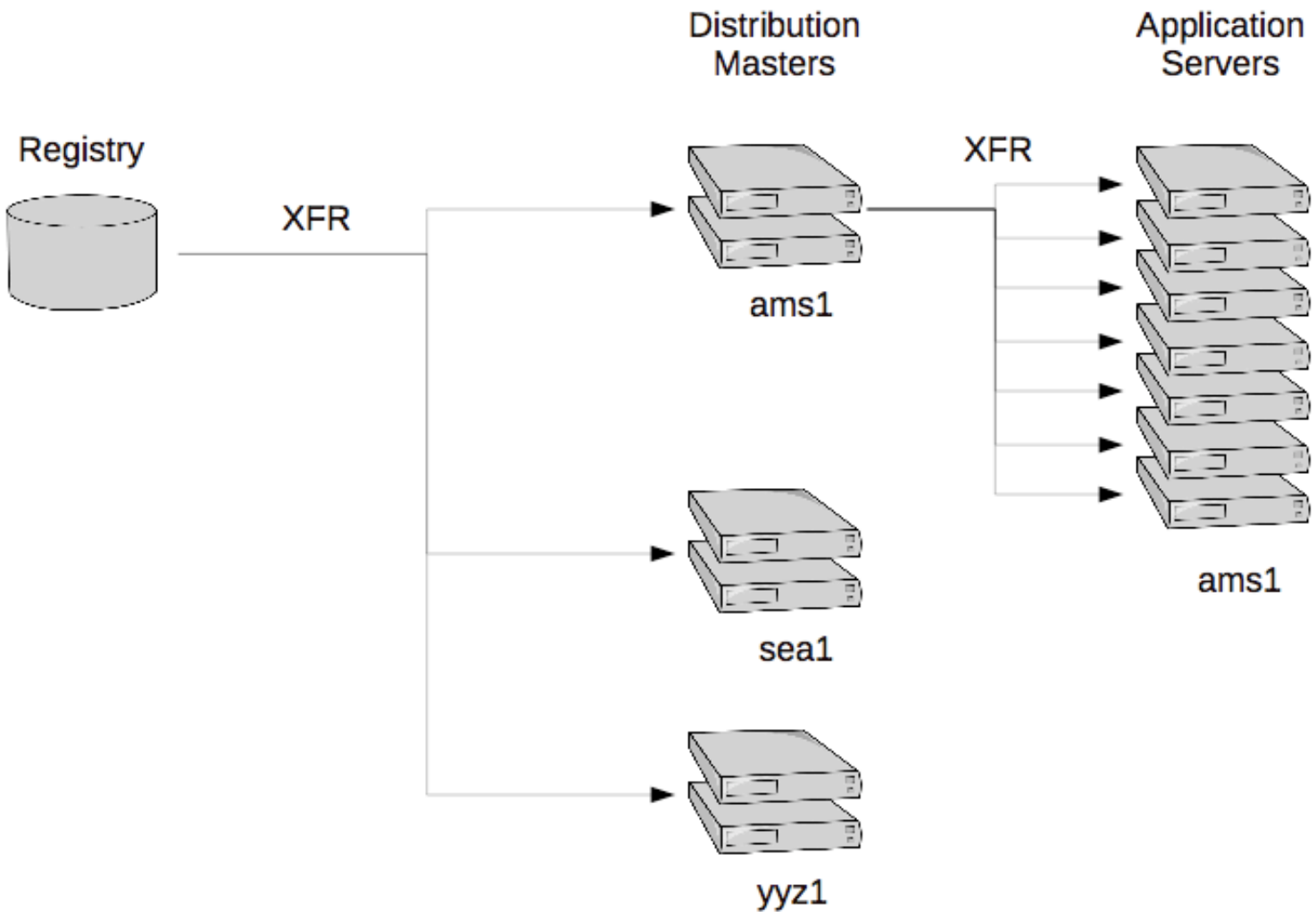
UKNOF 12, Bristol, UK



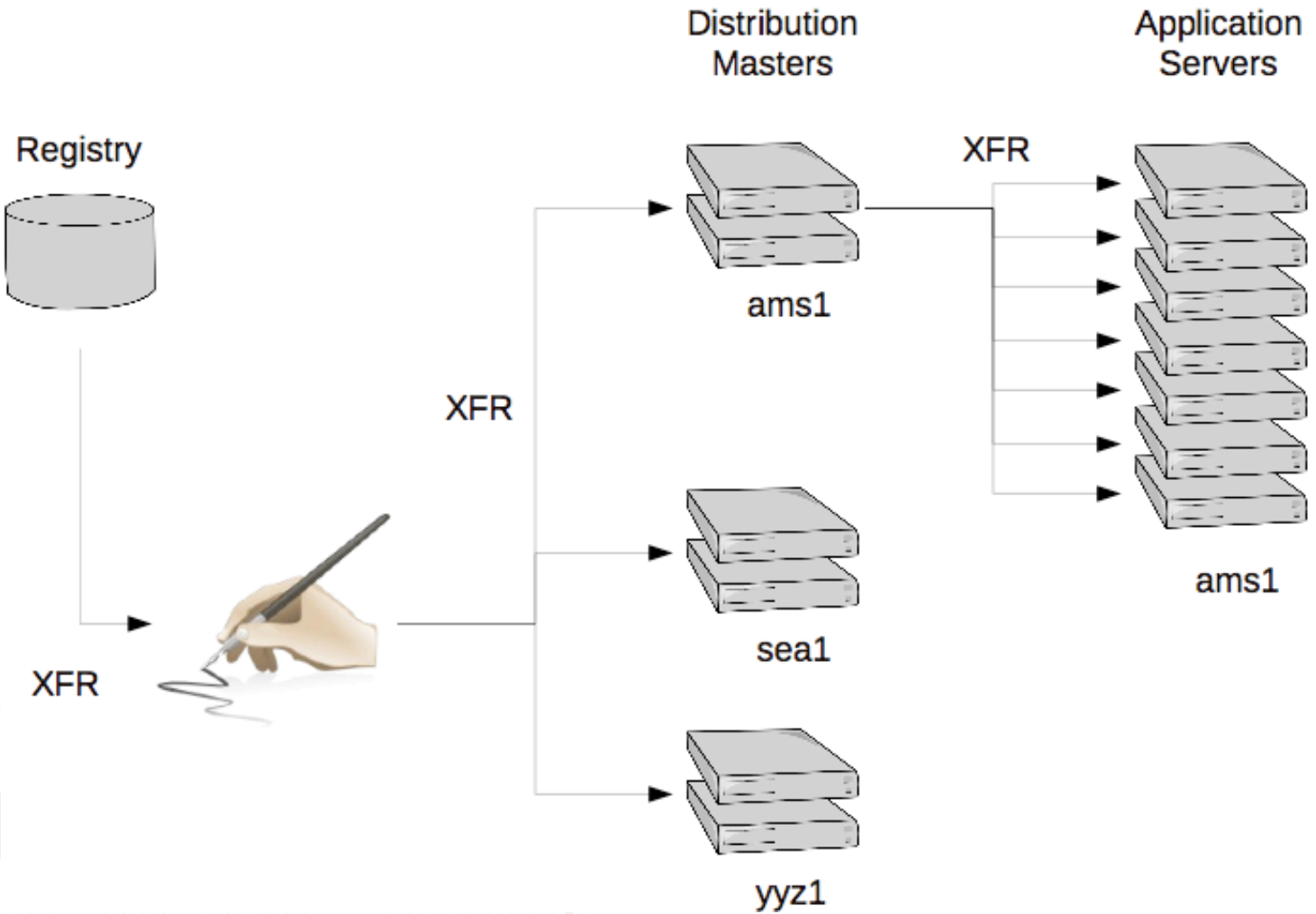
Background

- Afiliass operates the .ORG registry and DNS on behalf of PIR
- ORG has 6 servers, all of which are anycast in IPv4 and IPv6
- Nameserver nodes in North America, Europe, and Asia
- Diverse, open source platform
 - BIND9 and NSD
 - Linux and FreeBSD
 - Intel and POWER5
 - Cisco and Juniper
 - Two transit providers per node

DNS Infrastructure



DNSSEC Signer





- Decided to wait for NSEC3, RFC 5155 was published in early 2008
- Provides measures against zone enumeration
 - An NSEC record contains two canonically ordered names to show that nothing exists between them – walking the chain of NSEC records allows discovery of all names in the zone
 - An NSEC3 record contains the next hashed owner name in the hash order of the zone
- Permits gradual expansion of delegation-centric zones
 - Only secure delegations (those with a DS record) need to be signed / have an NSEC3 RR
- NSEC3 support in NSD and BIND9 by the end of 2008

Timeline

A Controlled Launch



- » June 2008
 - » RSTEP Response
- » Q4 2008 (estimated)
 - » BIND NSEC3 compatibility release
 - » HSM Integration
- » Q1 2009 (estimated)
 - » Friends & Family signed zones (pir.org, isoc.org, afilias.org, etc)
- » Q3 2009 (estimated)
 - » Expanded Friends & Family (based on results of F&F)
- » 2010 (estimated)
 - » Mainstream availability - Monitor, evaluate, then when advisable release to whole zone



Questions?

