DSA BOF
DebConf17
Montréal, Canada
agenda

- delegation: what do we do
- membership: who are we
- looking back: what we've been up to
- moving forward: what we're planning
- IAM refresh
- cloud infrastructure
- service packaging
- contact us
delegation

• what we do:
  • maintain the Debian user database (LDAP)
  • administer Debian infrastructure in support of Debian services
  • manage some Debian services (authN, authZ, email, static websites, security mirrors, DNS, CDNs, TLAs)
  • coordinate with hosting (eg UBC) and service providers (eg Fastly)
  • work with Debian Developer colleagues in support of their services
• Aurelien Jarno (aurel32)
• Héctor Orón Martínez (zumbi)
• Julien Cristau (jcristau)
• Luca Filipozzi (lfilipoz)
• Martin Zobel-Helas (zobel)
• Paul Wise (pabs)
• Peter Palfrader (weasel)
• Stephen Gran (sgran)
• Tollef Fog Heen (tfheen)
looking back

- CDN-backed apt repositories: http://deb.debian.org ... general availability!
- experimental anycast-available apt repositories
- mergers and acquisitions
  - DebConf infrastructure ... has been very slow going
- infrastructure refresh (thank you HPE and LeaseWeb!)
  - @UBC: 4 HPE BL460c Gen9 machines, HPE BLc7000 enclosure, HPE MSA2040 SAN, 10GE switches, and FC switches for core services
  - Bytemark: HPE DL380 Gen9 machine for cdimage service
  - @Sanger: HPE DL360 Gen9 machine for snapshot service
  - @LeaseWeb: 2 HPE DL180 G6 machines for snapshot cluster
moving forward

• mergers and acquisitions
  • work with DebConf Team to decide whether to cease or complete the transition of DebConf services to DSA ... currently stalled
  • work with Alioth Team to decide how to support the transition from Alioth to «insert name of thing here when we know what it is»

• infrastructure refresh
  • bytemark refresh
  • ftp-master redux in EU and cdimage redux in NA
  • buildd/porter status: wtf sparc64, omg mips, yay arm
  • consistent out-of-band management ... because we didn't
identity & access mgmt

• Debian's IAM infrastructure is built for decentralization
  • ssh push of service-specific files generated from LDAP data
  • heavily customized schemas; crufty utilities
• started a replacement for the utilities, 'ud', but not for the schemas
• maybe we need to think about de-customizing the schemas
  • can leverage more tools
• maybe we need to think about revamping SSO (SAML, OIDC)
  • can offer authN/authZ to other services: AWS IAM, API proxies, etc.
cloud infrastructure

- DSA believes Debian infrastructure should be controlled by Debian:
  - dedicated hardware hosted in friendly data centres
  - virtual machines on hypervisors that are Debian-controlled
  - insecure hypervisors make for insecure virtual machines
- DSA still believes this but we're prepared for the conversation about leveraging offers from cloud providers (AWS, GCP, AZURE, OVH, etc.)
- we're prepared to offer SAML/OIDC services to leverage Debian credentials for cloud services
- we want to empower a Cloud Team to manage Debian LDAP group membership which translates into cloud service authorization
service packages

• whenever Debian releases our distribution, just like every other system administration team, DSA jumps through some hoops to ensure that the services we support function correctly
• typically, there are no test suites; more importantly, we don't offer our service owners a viable test environment
• we think they should use their own systems... but they don't always have access to debian.org services on which they might depend...

• what if we offered a container service?
  • service owners provide complete recipes; we build the containers
  • and we rebuild them whenever there are security updates
  • and we provide some test containers that provide mock services
requests & final thoughts

• d-i team:
  • please make deb.debian.org the default but make location-specific mirror available at priority low or medium

• apt team:
  • please work with mirror operators to implement content security policies in order to deliver hash mismatches, etc.
  • please improve apt such that it retries

• dsa team:
  • consider using CDN for security mirrors
contact us

- mailto:debian-admin@lists.debian.org
- mailto:dsa@debian.org
- irc://irc.oftc.net/debian-admin