Challenges and experiences of the Samba 4.0 integration in Zentyal server

Easy IT for small business

17th of May 2013

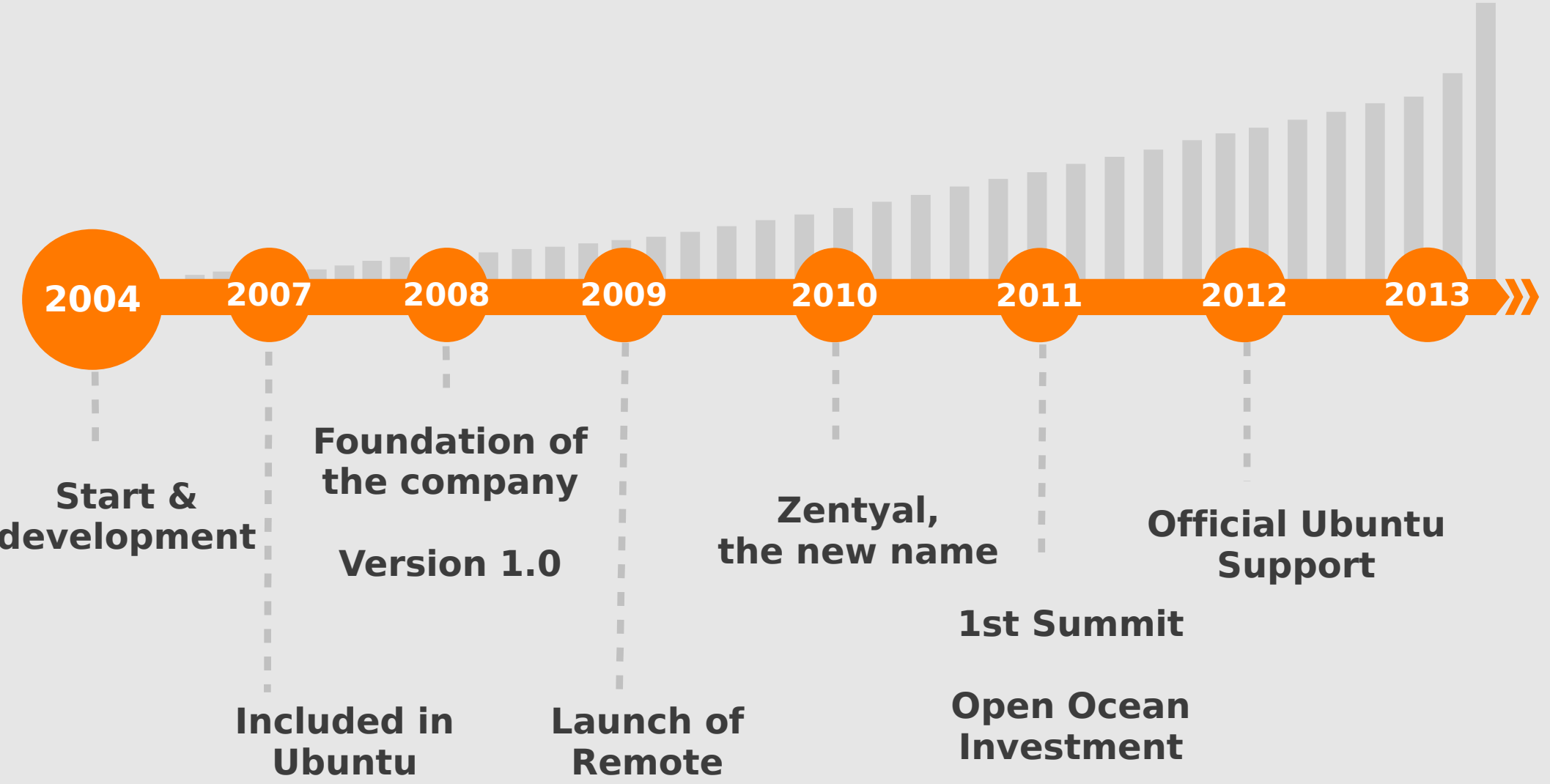
What is Zentyal?

All-in-one IT solution for SMBs, that is easy to use

Zentyal Server 3.0

- Based on Ubuntu server 12.04 LTS
- Web based interface to manage system services, written in Perl
- Modular framework
- 39 officially supported modules
  - Gateway (Firewall, proxy, traffic shapping...)
  - Infrastructure (CA, DHCP, VPN, ...)
  - Office (Antivirus, samba, ...)
  - Communications (VoIP, Zarafa, ...)

Our story


2004
2007
2008
2009
2010
2011
2012
2013
Start & development
Included in Ubuntu
Foundation of the company
Version 1.0
Launch of Remote
Zentyal, the new name
1st Summit
Open Ocean Investment
Official Ubuntu Support

Who uses Zentyal-based solutions?

Small and medium businesses

- +50.000 server installations

Large businesses and organizations

- Banks, hospitals, manufacturers, supermarket chains...

Public Administrations

- Departments of Education, Departments of Information Systems, Police and security forces

Zentyal 2.2 vs 3.0

Zentyal Server 2.2

- Samba 3 and openLDAP as backend
- ADSync to integrate in AD networks
  - Sync users through LDAP queries
  - Intercept password changes through password complexity check DLL

Zentyal Server 3.0

- Decided to integrate Samba 4.0 to provide Full AD integration
- Integration challenges:
  - Services duplication:
    - LDAP
    - Kerberos
    - DNS
  - And more we found in the way...

Challenges and solutions

LDAP synchronization

- Extend Zentyal framework with new callbacks
- Actions performed through the UI are applied to samba4 in first place, then to openLDAP
- Actions performed outside the UI, synchronized with the s4sync daemon, based in whenChanged attribute
- What we sync:
  - Users with their kerberos keys
  - Groups and user's membership
- Problems:
  - Nested groups
  - Users on different OUs

Different uid numbers

- Different UID numbers can be assigned to an user account on different servers:
  - Create user on DC A using RSAT
  - The s4sync daemon insert on openLDAP, uid number assigned
  - The user is replicated to server B
  - The s4sync daemon on server B insert it on openLDAP, different uid number can be assigned

DNS and Kerberos

- Bind as DNS server, thanks to the DLZ driver
- Heimdal daemon listening on different port
- The kerberos server to use controlled changing DNS SRV records
- Problems:
  - Synchronization issues between samba 4 database and Zentyal UI
  - Read content of DomainDnsZones and ForestDnsZones to show them in the UI

DNS dynamic updates

- DLZ only support Kerberos signed updates
- ISC DHCP server does not support them
- DLZ patched to support updates signed with TSIG keys
  - Keys loaded from file
- Bind also patched to pass the key to the DLZ driver

Migration

- Not possible yet to demote last Windows Server due to DomainDnzZones and ForestDnsZones replication issue
- An automatic script is provided:
  - Step 1. Synchronize sysvol from last DC
  - Step 2. Transfer FSMO roles to Samba
  - Step 3. Shutdown last Windows DC
- https://github.com/Zentyal/zentyal/blob/master/main/samba/src/scripts/ad-migrate

Sysvol replication

- Zentyal implement chained sysvol replication
  - Each additional DC pulls the sysvol share from its “parent”
  - GPOs must be edited in the root of the tree to avoid problems
- Transfer using “net rpc” command, which allow to replicate from Windows Servers and maintain ACLs

Antivirus

- Zentyal 2.2 used samba-vscan, now deprecated
- Zentyal 3.0 uses a daemon (zavsd) and the scannedonly VFS plugin
- scannedonly plugin patched to:
  - Avoid error deleting directory
  - Send additional information to daemon such user accessing the file and computer address
- The scannedonly module:
  - Notify zavsd daemon the files to scan
  - Including additional information such as the share, the user and computer address
- The zavsd daemon
  - Request clamd daemon to scan the files

Zentyal 3.2 roadmap

Tighter Samba 4 integration

- Support more server roles
  - Modules authenticating against external DC
  - Stand alone file server
- Multiple OU support
- Contacts and distribution lists
- Easy GPO management

Questions?

Samuel Cabrero,

Developer

scabrero@zentyal.com

www.zentyal.org