

Mein eigener Jabber-Server mit Prosody

TÜBIX 2016, Tübingen

Robert Scheck

fedora 

Robert Scheck

Fedora Package Maintainer und Provenpackager
Fedora Ambassador und Ambassador Mentor
Paket-Maintainer von Prosody in Fedora seit 2015
Open Source Contributor und Software-Entwickler

Mail: robert@fedoraproject.org

Web: <https://fedoraproject.org/wiki/RobertScheck>



Was ist Jabber bzw. XMPP?

- ▶ Ursprünglich „Jabber“, engl. „(daher-)plappern“
- ▶ Extensible Messaging and Presence Protocol
- ▶ Unterstützte Funktionen
 - ▶ Nachrichtenübermittlung
 - ▶ Anzeigen des Online-Status
 - ▶ Konferenzen mit mehreren Benutzern
 - ▶ Dateiübertragungen
 - ▶ Peer-to-Peer-Sitzungen (via Jingle)
- ▶ XML-basiertes Protokoll



Geschichte

- ▶ Erster Jabber-Server „jabberd“ 1998 von Jeremie Miller entwickelt
- ▶ XMPP Working Group in 2002 durch die Internet Engineering Task Force
- ▶ Core-Protokolle in RFC 3920-3923 formalisiert, als offizieller Standard in 2004 verabschiedet
- ▶ XMPP Standards Foundation standardisiert auf XMPP aufbauende Protokolle (XEPs)

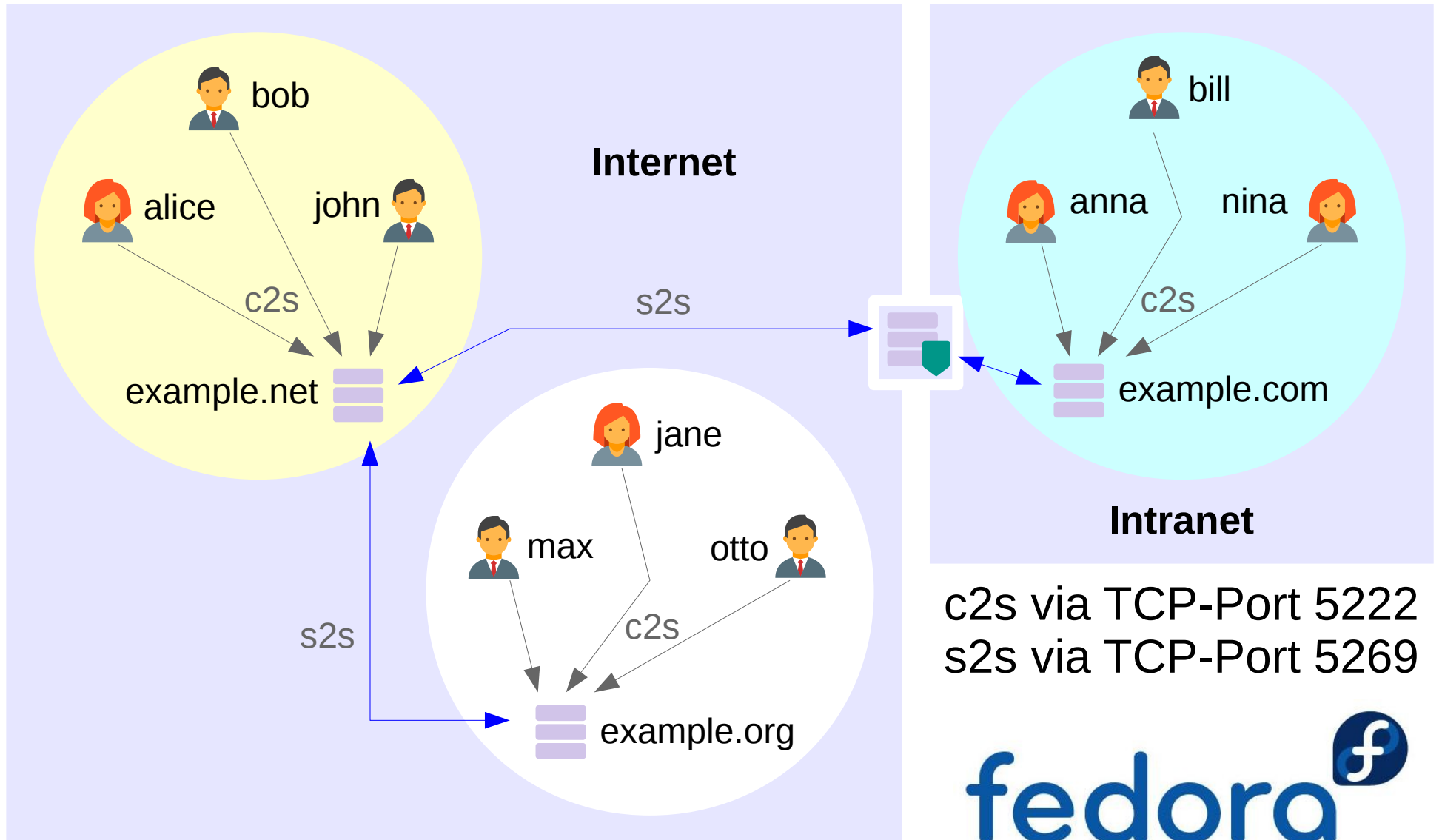


Netz-Architektur von XMPP

- ▶ Mindestens ein XMPP-Server wird benötigt
- ▶ Kommunikation zu anderen XMPP-Servern optional möglich (ähnlich wie bei SMTP)
 - ▶ XMPP Federation
- ▶ Jabber Identifier (JID) ähnelt E-Mail-Adresse
 - ▶ `alice@example.net`
- ▶ Mehrfache Anmeldung mit gleicher JID mittels Konzept der „Ressourcen“



Netz-Architektur von XMPP



Was ist Prosody?

- ▶ Lightweight XMPP-Server, früher „Ixmppd“
- ▶ Wird seit 2008 von Matthew Wild entwickelt
- ▶ Aktuelle stabile Version 0.9.10 (27.01.2016)
- ▶ Programmiert in Lua (plattformunabhängig)
- ▶ Verfügbar unter MIT-Lizenz (freie Software)
- ▶ Einfach zu installieren und konfigurieren
- ▶ Benötigt wenig Systemressourcen
- ▶ Erweiterbar über Module



Installation von Prosody

- ▶ Fedora
 - ▶ `dnf install prosody`
- ▶ Red Hat Enterprise Linux und CentOS
 - ▶ Benötigt RPM-Repository „Fedora EPEL“
 - ▶ `yum install prosody`
- ▶ Debian und Ubuntu
 - ▶ `apt-get install prosody`
- ▶ Siehe: <https://prosody.im/download>



Konfiguration von Prosody

- ▶ Datei `/etc/prosody/prosody.cfg.lua` anpassen
 - ▶ `c2s_require_encryption = true` (statt `false`)
 - ▶ `s2s_secure_auth = true` (statt `false`)
 - ▶ `authentication = "internal_hashed"` (statt `plain`)
- ▶ Selbstsigniertes SSL-Zertifikat erzeugen
 - ▶ `cd /etc/prosody/certs/`
 - ▶ `make example.net.crt`



Konfiguration von Prosody

- ▶ `/etc/prosody/conf.d/example.net.cfg.lua` als neue Datei anlegen

```
-- Section for VirtualHost example.net

VirtualHost "example.net"
  -- Assign this host a certificate for TLS, otherwise it would
  -- use the one set in the global section (if any).
  ssl = {
    key = "/etc/pki/prosody/example.net.key";
    certificate = "/etc/pki/prosody/example.net.crt";
  }

  -- Set up a SOCKS5 bytestream proxy for server-proxied file
  -- transfers:
  Component "proxy65.example.net" "example.net"
  proxy65_address = "proxy65.example.net";
  proxy65_acl = { "example.net" }
```



Konfiguration von Prosody

- ▶ Benutzer anlegen
 - ▶ `prosodyctl adduser alice@example.net`
- ▶ Dienst aktivieren und starten
 - ▶ `systemctl enable --now prosody.service`
- ▶ Firewall anpassen
 - ▶ TCP-Port 5000 (proxy65)
 - ▶ TCP-Port 5222 (c2s)
 - ▶ TCP-Port 5269 (s2s)



DNS-Anpassungen

- ▶ Wenn XMPP-Server nicht auf der Domain läuft
 - ▶ Webseite beim Provider, XMPP-Server zu Hause
- ▶ DNS-Anpassungen, z.B. beim Webhoster
 - ▶ `xmpp.example.net. IN A 192.0.2.30`
 - ▶ `_xmpp-client._tcp.example.net. ↵`
`IN SRV 10 0 5222 xmpp.example.net.`
 - ▶ `_xmpp-server._tcp.example.net. ↵`
`IN SRV 10 0 5269 xmpp.example.net.`
 - ▶ `proxy65.example.net. IN A 192.0.2.30`



Echtbetrieb-Empfehlungen

- ▶ SSL-Zertifikat einer Zertifizierungsstelle
 - ▶ Let's Encrypt (kostenlos, benötigt „certbot“)
 - ▶ StartSSL (kostenlos, Registrierung erforderlich)
 - ▶ Beliebiger CA-Reseller (ab ca. 6 EUR/Jahr)
- ▶ Eventuell DNSSEC mit DANE
- ▶ XMPP-Sicherheitstest via <https://xmpp.net>
- ▶ Regelmäßige Sicherheitsupdates des Systems



Einige XMPP-Clients

- ▶ Linux: Empathy, Gajim, Jitsi, Kopete, Pidgin
 - ▶ Textbasiert: BitlBee, Jackline, Poezio, Profanity
- ▶ OS X: Adium, Gajim, Jitsi, Monal, Pidgin
- ▶ Windows: Gajim, Jitsi, Kopete, Pidgin
- ▶ Android: ChatSecure, Conversations
- ▶ iOS: ChatSecure, Monal
- ▶ Windows Phone: Chat



Fragen?



fedora™

Vielen Dank!

