Desktopsysteme mit Chef kochen

Tilo Werner, TraSo GmbH

24. März 2015

Agenda

- Einleitung
- Präambel
- Chef
- Fazit
- Epilog

TraSo
Travel Solutions

Agenda

TraSo Travel Solutions

Zu mir und uns

- Tilo Werner, Systemadministrator
- TraSo GmbH, Sitz in Leipzig, Softwareentwicklung (Produkt xRes) für Reisebranche
- 8 Entwickler, 4 Admins, 5 Supportmitarbeiter, 1 AdGF, 1GF
- 16x Linux (Ubuntu), 3x Windows (7), 1x MS TS + X
- 9x Notebooks (mit SE-HDD), 7x Workstations
- ca. 110 Nodes (Debian/Ubuntu/CentOS) im RZ hauptsächlich virtualisiert (KVM)
- hohe Eigenständigkeit/-verantwortung

TraSo
Travel Solutions

Motivation

- vor 4 Jahren MacOS als Desktop für Admins und Entwickler, Windows im Support
- später Desktops von MacOS auf Linux migriert; neue HW mit Linux aufgesetzt
- unterschiedliche Softwareversionen
- unterschiedliche Konfigurationen
- Chef seit ca. 2 Jahren im RZ
- Chef seit ca. 1,5 Jahren auf den Desktops

TraSo Travel Solutions

Warum Chef und was ist das?

- automatisierte Konfiguration mit dem Ziel **Vereinheitlichung**
- in Ruby und Erlang (Server) geschrieben
- steht unter der Apache Lizenz
- unterstützt AIX, FreeBSD, Linux und Windows auf Clientseite
- wird von der Firma Chef (ehem. Opscode) entwickelt
- ähnliche Produkte: puppet, ansible, cfengine

TraSo Travel Solutions

Agenda

TraSo Travel Solutions

Welche Werkzeuge braucht man?

1. DNS
2. DHCP
3. PXE (TFPD + pxelinux)
4. Nicht interaktive Installation [1]
5. Git-Repository
6. Chef-Server
7. Chef-Workstation

[1] https://en.wikipedia.org/wiki/Preseed

TraSo Travel Solutions

DNS + DHCP

- Forward und Reverse-Einträge in DNS eintragen
- MAC-Adresse in DHCP eintragen

```
...
range dynamic-bootp 192.168.16.180 192.168.16.210;
filename "pxelinux.0";
next-server 192.168.16.250;
option routers 192.168.16.254;
option domain-name-servers 192.168.16.251;
...
host cherry.gs.traso.de { hardware ethernet 52:54:00:2c:82:94;
                          fixed-address 192.168.16.30; }
...
```

/etc/dhcp/dhcpd.conf

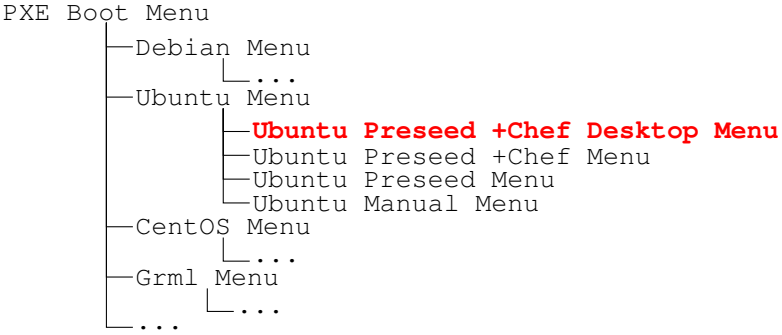
TraSo Travel Solutions

TFTP

```
1 TFTP_USERNAME="tftp"
2 TFTP_DIRECTORY="/srv/tftp"
3 TFTP_ADDRESS="0.0.0.0:69"
4 TFTP_OPTIONS="--secure"
```

/etc/default/tftpd-hpa

Menü-Struktur



Konfiguration

```
1  default bootmenu/boot-screens/vesamenu.c32
2  MENU TITLE Ubuntu Preseed +Chef Desktop Menu
3
4  LABEL ubuntu-trusty-install-64-preseed-chef-desktop
5  MENU LABEL ^1. Ubuntu 14.04 Trusty Tahr - LTS  (amd64)
6  kernel ubuntu-installer/trusty/amd64/linux
7  append vga=788 initrd=ubuntu-installer/trusty/amd64/initrd.gz auto-install/enable=true priority=critical
       preseed/url=http://pxe01.gs.traso.de/ubuntu/trusty/amd64/preseed.chef.dsk.cfg DEBCONF_DEBUG=5 -- quiet
8  LABEL EXIT
9  KERNEL pxelinux.0
```

/var/www/ubuntu/trusty/amd64/preseed.chef.desktop.menu

TraSo Travel Solutions

Allgemeine Konfiguration

```
1 ...
2 d-i mirror/http/proxy string http://aptcache.gs.traso.de:3142
3 d-i passwd/root-password-crypted password md5(geheim)
4 d-i partman-auto/method string lvm
5 d-i partman-auto-lvm/guided_size string  80%
6 ...
```

/var/www/ubuntu/trusty/amd64/preseed.chef.dsk.cfg

Partitionierung

```
1  ...
2  d-i partman-auto/expert_recipe string                                    \
3          desktop-default ::                                               \
4                  100 50 -1 ext4                                           \
5                  $defaultignore{ } $primary{ } method{ lvm }              \
6                  vg_name{ vol1 } device{/dev/sda}                         \
7                   •                                                       \
8                                                                           \
9                  20000 20000 20000 ext4                                   \
10                 $defaultignore{ } $lvmok{ } lv_name{ root } in_vg{ vol1 } \
11                 label{ root } method{ format } format{ }                 \
12                 use_filesystem{ } filesystem{ ext4 }                     \
13                 options/noatime{ noatime }                               \
14                 options/discard{ discard }                               \
15                 mountpoint{ / }                                          \
16                  •
17 ...
```

/var/www/ubuntu/trusty/amd64/preseed.chef.dsk.cfg

[1] apt-get install debian-installer; vim /usr/share/doc/debian-installer/devel/partman-auto-recipe.txt.gz

late_command

```
1 ...
2 d-i pkgsel/include string sudo openssh-server gdebi lsb-release
3 d-i preseed/late_command string in-target wget -q http://pxe01.gs.traso.de/d-i/late_command.sh -O /tmp/
      late_command.sh; \
4 in-target bash /tmp/late_command.sh
5 ...
```

/var/www/ubuntu/trusty/amd64/preseed.chef.dsk.cfg

Übergang zu Chef

```
1  #!/bin/bash
2  set -u
3  function install_ssh_keys {
4          mkdir /root/.ssh
5          wget -q http://pxe01.gs.traso.de/ssh/root_authorized_keys -O /root/.ssh/authorized_keys
6          chmod 600 /root/.ssh/authorized_keys
7          sed -i -e "s/^#*\(PasswordAuthentication\).*/\1 no/" /etc/ssh/sshd_config
8  }
9  function install_chef_client {
10         VENDOR=$(lsb_release -si | tr "[:upper:]" "[:lower:]")
11         RELEASE_NAME=$(lsb_release -sc | tr "[:upper:]" "[:lower:]")
12         ARCH=$(uname -m)
13         wget -q http://pxe01.gs.traso.de/chef-client/$VENDOR/$RELEASE_NAME/$ARCH/current.deb -O /tmp/chef-
               client.deb
14         gdebi -non-interactive -quiet /tmp/chef-client.deb
15 }
16 function main {
17         install_ssh_keys
18         install_chef_client
19 }
20 main
```

/var/www/d-i/late_command.sh

TraSo Travel Solutions

Reboot

Agenda

TraSo Travel Solutions

Environments, Roles, Cookbooks, Nodes & OHAI

- **Environment:** Netzwerksegmente, Standorte oder virtuell segmentiert [1]
- **Role:** Menge aller Kochbücher und/oder Rezepte [2]
- **Cookbook:** Menge aller Rezepte zur Umsetzung eines bestimmten Verhaltens [3]
- **Node:** Einzelner Host als Client am Chef-Server [4]
- **OHAI:** lokaler Datensammler auf Node [5]

[1] http://docs.chef.io/environments.html
[2] http://docs.chef.io/roles.html
[3] http://docs.chef.io/cookbooks.html
[4] http://docs.chef.io/nodes.html
[5] http://docs.chef.io/ohai.html

TraSo Travel Solutions

Recipes, Resources, Attributes & Templates

- **Recipe:** Beschreibt die gewünschte Konfiguration mittels pure Ruby DSL [1]
- **Resources:** DSL typische Beschreibung was getan werden soll; im Hintergrund plattformspezifisch [2]
- **Attributes:** Werden durch alle genannten gesetzt [3]
- **Templates:** Vorlagen für Dateien, embedded Ruby Syntax (Erubis) [4]

[1] http://docs.chef.io/recipes.html
[2] http://docs.chef.io/resources.html
[3] http://docs.chef.io/attributes.html
[4] http://docs.chef.io/templates.html

TraSo Travel Solutions

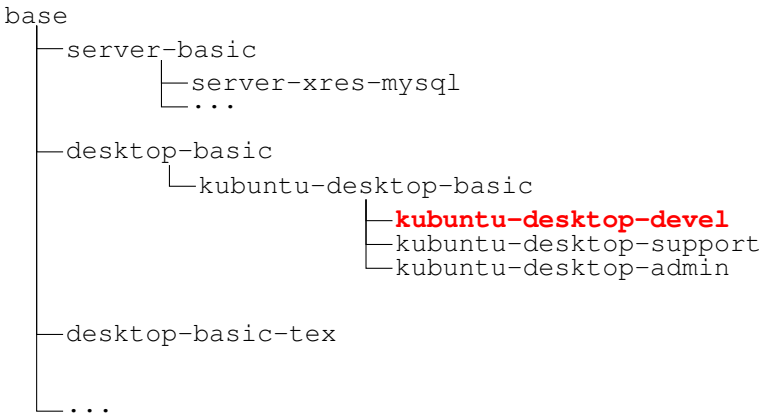
Search, Knife & Webfrontend

- **Search:** API zum Suchen [1]
  - mächtig & benutzbar in Rezepten und in Knife
- **Knife:** CLI Befehl der Chef-Workstations zur Steuerung von Server und Clients [2]
  - knife bootstrap
  - knife help
- **Webfrontend:** Funktional ein Subset des Knife Kommandos

[1] http://docs.chef.io/chef_search.html
[2] http://docs.chef.io/chef/knife.html

TraSo Travel Solutions

Unser Rollenkonzept



Environment: gs

```
{
  "name": "gs",
  "description": "Geschaeftsstelle Georg-Schumann-Strasse",
  "cookbook_versions": {
    "accounts": "= 0.9.2",
    "repos": "= 0.0.4",
    "x509": "= 1.1.0",
    "opt": "= 0.2.1"
  },
  "chef_type": "environment",
...
```

~/workspace/chef-repo % knife environment show -F json gs

Role: base

```
...
  "default_attributes": {
    "apt": {
      "packages-install": [
          "pigz",
          "vim",
          ...
      ]
    }
  },
  "chef_type": "role",
  "run_list": [
    "recipe[chef-client]",
    "recipe[hostname]",
    "recipe[backup]",
    "recipe[apt::packages]",
    "recipe[accounts]",
    ...
  ],
...
```

~/workspace/chef-repo % knife role show -F json base

TraSo Travel Solutions

Role: kubuntu-desktop-basic

```
...
  "default_attributes": {
    "apt": {
      "packages-install": [
        "kubuntu-desktop",
        "shutter",
        "simple-scan",
        "hedgewars",
        ...
      ],
      "packages-purge": [
        "flashplugin-installer"
      ]
    }
  },
  "run_list": [
    "role[desktop-basic]",
    "recipe[opt::libreoffice-stable-backports]",
    "recipe[opt::x2go-install]",
    ...
  ],
...
```

~/workspace/chef-repo % knife role show -F json kubuntu-desktop-basic

Role: kubuntu-desktop-devel

```
...
   "default_attributes": {
    "apt": {
      "packages-install": [
        "git",
        "maven",
        "terminator",
        "kcachegrind"
        ...
      ]
    }
  },
  "run_list": [
    "role[kubuntu-desktop-basic]",
    "recipe[opt::heidisql-install]",
    "recipe[opt::phpstorm-install]",
    ...
  ],
...
```

~/workspace/chef-repo % knife role show -F json kubuntu-desktop-devel

TraSo Travel Solutions

knife.rb

```
1  log_level                :info
2  log_location             STDOUT
3  node_name                'twerner'
4  client_key               '/home/twerner/workspace/chef-repo/.chef/twerner.pem'
5  validation_client_name   'chef-validator'
6  validation_key           '/home/twerner/workspace/chef-repo/.chef/chef-validator.pem'
7  chef_server_url          'https://chef.app.traso.de'
8  ssl_verify_mode          :verify_none
9  syntax_check_cache_path  '/home/twerner/workspace/chef-repo/.chef/syntax_check_cache'
10 cookbook_path           [ '/home/twerner/workspace/chef-repo/cookbooks' ]
11 cookbook_copyright       'TraSo GmbH'
12 cookbook_email           'cookbooks@traso.de'
13 cookbook_license         'apachev2'
14 knife[:editor]           = 'vim'
```

~/workspace/chef-repo/.chef/knife.rb

TraSo Travel Solutions

knife

```
1 knife bootstrap -x root cherry.gs.traso.de -N cherry.gs.traso.de -r 'role[kubuntu-desktop-devel]' -j '{"
      set_fqdn": "cherry.gs.traso.de"}' --environment gs
```

~/workspace/chef-repo %

Warten...

Einfache Paketinstallation

```
1  # Cookbook Name: apt
2  # Recipe: package
3  if not node['apt']['packages-install'].empty?
4      node['apt']['packages-install'].each do |value|
5          package value do
6              action :install
7          end
8      end
9  end
10 if not node['apt']['packages-purge'].empty?
11     node['apt']['packages-purge'].each do |value|
12         package value do
13             options "--auto-remove"
14             action :purge
15         end
16     end
17 end
18 ...
```

~/workspace/chef-repo/cookbooks/apt/recipes/packages

TraSo Travel Solutions

Paketinstallation aus Fremdquellen

```
1  case node['platform']
2      when "ubuntu"
3          apt_repository "libreoffice-stable-backports" do
4              uri "http://ppa.launchpad.net/libreoffice/libreoffice-4-4/ubuntu"
5              distribution node['lsb']['codename']
6              components ["main"]
7              keyserver "keyserver.ubuntu.com"
8              key "1378B444"
9              deb_src false
10         end
11     end
12 ...
```

~/workspace/chef-repo/cookbooks/repos/recipes/libreoffice-stable-backports.rb

```
1  deb     http://ppa.launchpad.net/libreoffice/libreoffice-4-4/ubuntu trusty main
```

/etc/apt/sources.list.d/libreoffice-stable-backports.list

TraSo Travel Solutions

Installation nach Art des Hauses I

```
1  if platform_family?('debian')
2      target_app = "heidisql"
3      remote_url = "#{node['opt']['remote_url']}/#{target_app}"
4      install_dir  = "/opt/#{target_app}"
5
6      # downloads md5-file & checks changes
7      remote_file "#{Chef::Config[:file_cache_path]}/#{target_app}.zip.md5" do
8          source "#{remote_url}/current.zip.md5"
9          # if there are changes then notify (run) install script
10         notifies :run, "bash[install #{target_app}]", :immediately
11     end
```

~/workspace/chef-repo/cookbooks/opt/recipes/heidisql-install.rb

TraSo Travel Solutions

Installation nach Art des Hauses II

```
1  bash "install␣#{target_app}" do
2      user "root"
3      cwd Chef::Config[:file_cache_path]
4      code <<-EOH
5      mkdir -p #{install_dir}
6      mkdir #{target_app}
7      cd #{target_app}
8      wget "#{remote_url}/current.zip" -O #{target_app}.zip
9      unzip #{target_app}.zip
10     rm #{target_app}.zip
11     mv #{install_dir}/portable_settings.txt ./
12     rm -rf #{install_dir}/*
13     mv * #{install_dir}
14     chown -R root:root #{install_dir}
15     EOH
16     notifies :create, "remote_file[#{install_dir}/#{target_app}.png]", :immediately
17     notifies :install, "package[wine]", :delayed
18     action :nothing
19 end
```

~/workspace/chef-repo/cookbooks/opt/recipes/heidisql-install.rb

TraSo Travel Solutions

Installation nach Art des Hauses III

```
1     template "/usr/share/applications/#{target_app}.desktop" do
2         source "#{target_app}.erb"
3         variables(
4             :install_dir => "#{install_dir}"
5         )
6         owner "root"
7         group "root"
8         mode   0644
9         notifies :run, 'execute[xdg-desktop-menu]', :immediately
10    end
11    execute "xdg-desktop-menu" do
12        command "/usr/bin/xdg-desktop-menu␣forceupdate"
13        action :nothing
14    end
15    package "wine" do
16        action :nothing
17    end
18 end
```

~/workspace/chef-repo/cookbooks/opt/recipes/heidisql-install.rb

TraSo Travel Solutions

Installation nach Art des Hauses IV

```
1  [Desktop Entry]
2  Type=Application
3  Name=HeidiSQL
4  Exec=/usr/bin/wine <%= @install_dir %>/heidisql.exe %f
5  Icon=<%= @install_dir %>/heidisql.png
6  Comment=Heidi!
7  Categories=Development;Database
8  Terminal=false
9  StartupNotify=true
10 StartupWMClass=HeidiSQL
```

~/workspace/chef-repo/cookbooks/opt/templates/default/heidisql.erb

TraSo Travel Solutions

Agenda

TraSo Travel Solutions

Was wir bereits umgesetzt haben

- Netzwerk
  - WLAN-Zugang
  - Samba-Share (Automount)
  - aptcache (Umschaltung für Laptops)
  - OpenVPN-Zugänge
- Applikationen aus Fremdquellen
  - PHPStorm, Idea, Netbeans, MySQL-Workbench, Vagrant, Virtualbox
  - X2Go, Chrome, Crossover, Yed, robomongo
  - Java8, Dell-OpenManage, LibreOffice
- Einheitlicher Aktualisierungsprozess
- Backup & Recovery

TraSo Travel Solutions

Wie es heute abläuft

- Ausrollen eines Systems dauert ca. 2h + Aufbau des AP 2h
- Inklusive der Lektüre unseres Willkommensleitfaden ist ein z.B. Entwickler in ca. 1d voll arbeitsfähig.
- Die Nutzer haben ein Basissystem, welches mit sinnvollen Defaults auf die jeweiligen Bedürfnisse angepasst ist.
- Aktualisierungen von Software aus Fremdquellen erfolgt zentral und standardisiert
- Wiederherstellung wegen Verlust oder HW-defekt eines AP dauert ca. 4h

TraSo Travel Solutions

Vorteile

- mächtig & flexibel
- schnell & skaliert
- pure Ruby DSL
- Dokumentation

TraSo Travel Solutions

Nachteile

- Lernkurve sehr steil
- Integration in Git
- Namespaces
- Komplexe Struktur

TraSo Travel Solutions

Agenda

TraSo Travel Solutions

Chef

- Version 12 (Server & Client)
- ssl_verify_mode :peer
- Refactoring
- Okkupation von Namensräumen

TraSo Travel Solutions

Automatisierung

- Benutzerverwaltung mit LDAP
- x509-Einsatz ausbauen
- Netzwerk-Segmentierung mittels VLAN
- IPSEC-Zugänge
- Migration Desktopvirtualisierung Vagrant/Virtualbox nach Chef/KVM

TraSo Travel Solutions

Diskussion

Fragen? Anregungen?

Ende

Vielen Dank für Eure Aufmerksamkeit.