Linux-Netboot an der Technischen Fakultät

Sascha Krause <sk@techfak.net>
AG Rechnerbetrieb

Technische Fakultät, Universität Bielefeld

23.03.2017

Einführung

Anforderungen

Softwareverteilung

Konfiguration

Hosteigenschaften

Bootprozess

Überblick

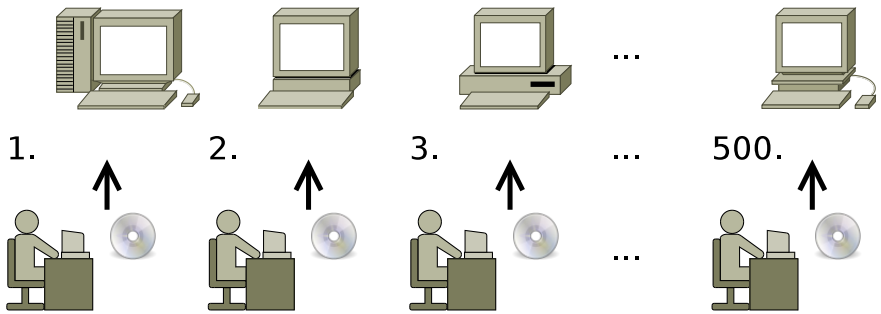
...

Einführung

Ziel

- Versorgung mehrerer hundert Arbeitsplätze mit einer zentral verwalteten GNU/Linux-Umgebung

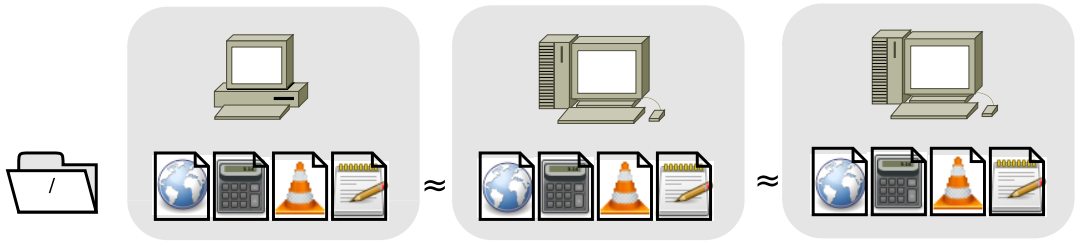
Skalierungsproblem



Manuelle Installation bei über 500 Rechnern nicht geeignet!

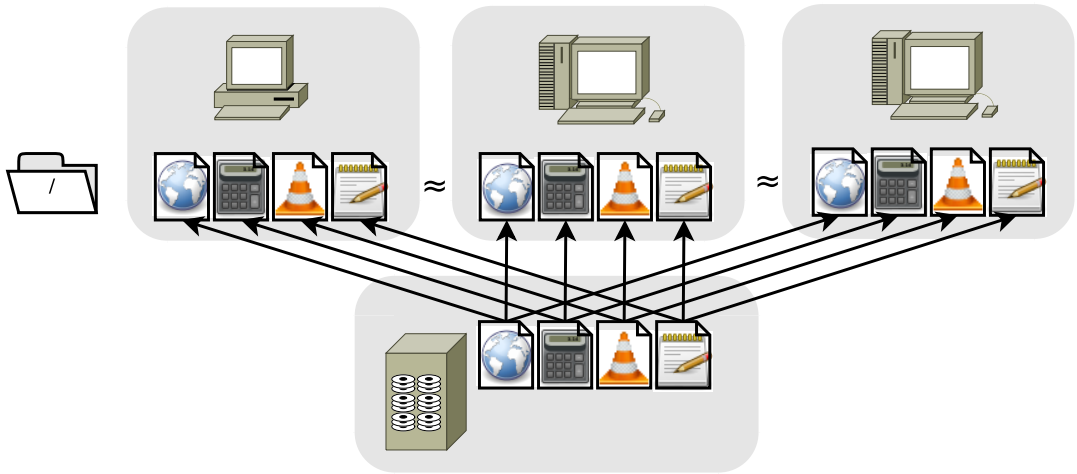
$\Rightarrow$ Anderer Ansatz notwendig!

Redundanz



Bei gleicher Installation enthalten alle Rechner *fast* gleiche Daten.

Gemeinsame Quelle

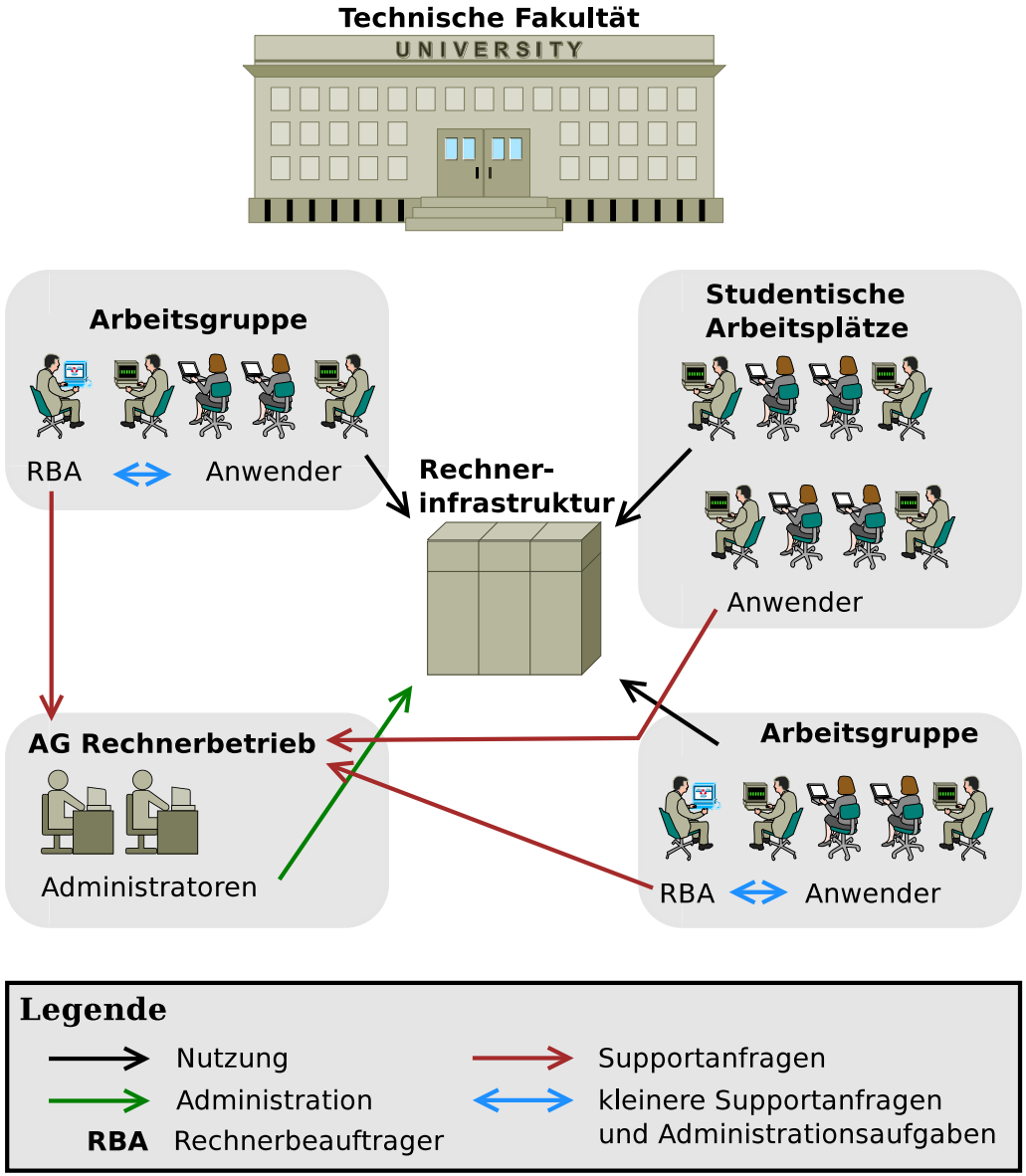


Idee: Versorgung aller Rechner aus gemeinsamer Quelle.

Anforderungen

Übersicht

Fakultät aus Sicht der Rechneradministration



Nutzer und Gruppen

- **Studierende**: Poolräume mit wechselnden Anwendern (hohe Fluktuation). Standardhardware.
- **Mitarbeiter**: Feste Arbeitsplätze für i.d.R. einen Benutzer. Maschinen laufen bei Bedarf durch. Bedarfshardware.
- **Hilfskräfte**: Poolräume mit wechselnden Anwendern (geringe Fluktuation). Hauptsächlich Standardhardware.
- **Sekretariate**: Feste Arbeitsplätze für i.d.R. einen Benutzer. Standardhardware.
- **Labore**: Dedizierte Rechner für bestimmte Projektinstallationen. Maschinen laufen bei Bedarf durch. Oft Spezialhardware.
- **Spezialfälle**: Maschinen die besonderen Anforderungen unterliegen (z.B. Projekt-Demos).

Nutzer und Gruppen

Zugehörigkeit

Nutzer gehören nicht ausschließlich nur zu einer festen Gruppe!

- **Studierende** arbeiten als **Hilfskräfte** in bei Projekten in Arbeitsgruppen (AGen) mit.
- **Mitarbeiter** sind auch als **Lehrende** im Grundstudiumszentrum Informatik (GZI) tätig.
- **Mitarbeiter** arbeiten AG-übergreifend in Projekten mit.

$\Rightarrow$ Feste Zuordnung Nutzer $\mapsto$ Rechner nicht möglich.
$\Rightarrow$ Feste Zuordnung Nutzer $\mapsto$ AG nicht mehr zeitgemäß.
$\Rightarrow$ Nutzer erwarten, dass auf allen Maschinen die gleiche Arbeitsumgebung (Programme und Einstellungen) verfügbar ist.

Software

- Distribution: jeweils aktuelles Ubuntu **GNU/Linux**
  - Standardsoftware **ohne Lizenzkosten** (Office, Browser, Multimedia, ...)
  - U.a. *XFCE* als einsteigerfreundlicher Desktop
  - Gute Kombination aus sinnvollen **Defaults** und **Konfigurierbarkeit**
  - Viele verfügbare *Pakete* speziell für Forschung und Lehre (z.B. ROS - *Robot Operating System*)
  - Hoher **Verbreitungsgrad**
- Wünschenswert: andere Distributionen für spezielle Zwecke
- 3rd-Party-Software wird per *Volume* eingebunden

Hardware

- Standardarbeitsplatz ist **x86_64**-System mit **Intel**-Grafik
- Für viele Projekte Zusatzhardware notwendig
  - spezielle **Grafikkarten**
  - spezielle **Soundkarten**
  - **Kontrollerkarten**
  - **Videoschnittkarten**
- Zukünftig **andere Architekturen** (*ARM*) denkbar

$\Rightarrow$ **Thin-Client**-Lösungen nur *sehr bedingt* geeignet

Netzwerk

- Teilnahme am Netzwerk ausschließlich per **802.1X** (Authentifizierung gegen Radiusserver und nachfolgender Zuweisung des konkreten VLANs)
- Homeverzeichnisse, Software- und Projektvolumes per **NFS**
- NFS-Zugriff nur mit **Kerberos**ticket

Administration

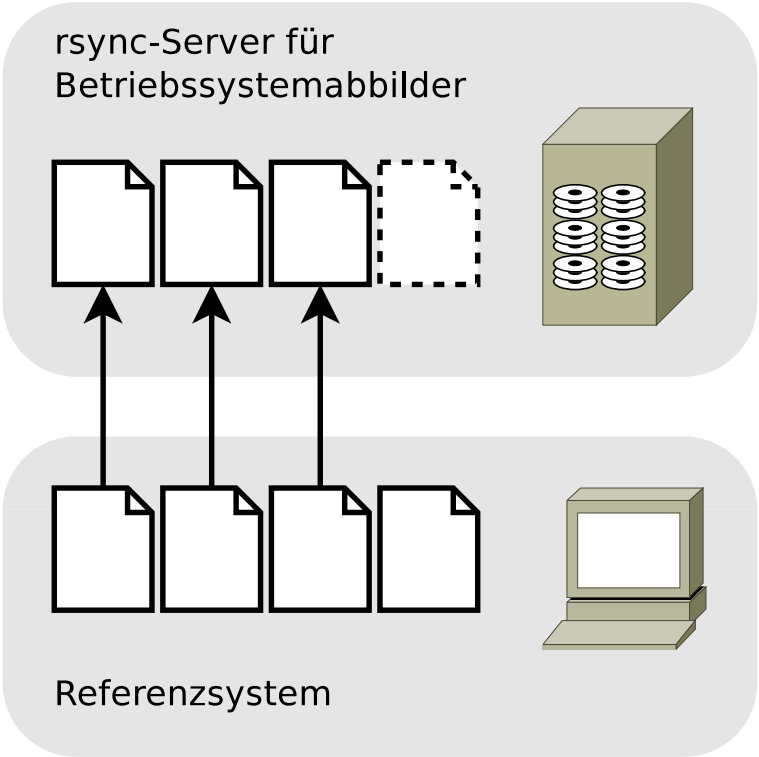
- Integration in üblichen Administrations**workflow**
- **Automatisierbarkeit** durch Scripte
- Agnostisch gegenüber Konfigurationsverwaltung
- **Simplizität**: System soll ohne viel Einarbeitungszeit auch von neuen Mitarbeitern bedient werden können
- Idealerweise **Kommandozeile** statt komplizierter Formulare
- **Robustheit**: Keine *Single-Point-of-Failures*
- **Wartbarkeit**: Bevorzugt Standard-Werkzeuge statt proprietärer Speziallösungen
- **Modularität**: Perspektivisch Auslagerung einzelner Adminstrationsaufgaben an Rechnerbeauftragte

Softwareverteilung

Überblick

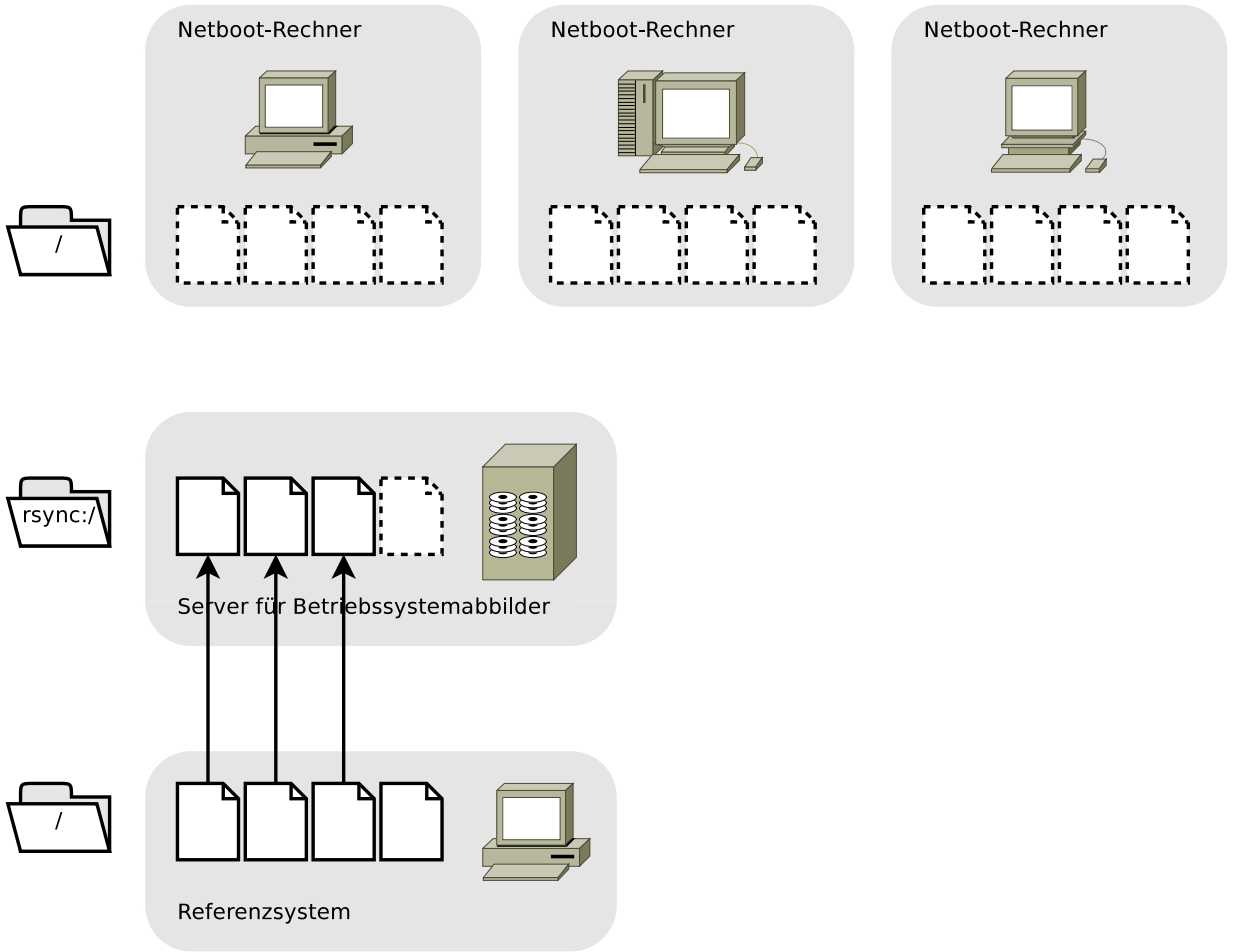
Komponenten des Netboot-Systems im Überblick

Referenzsystem



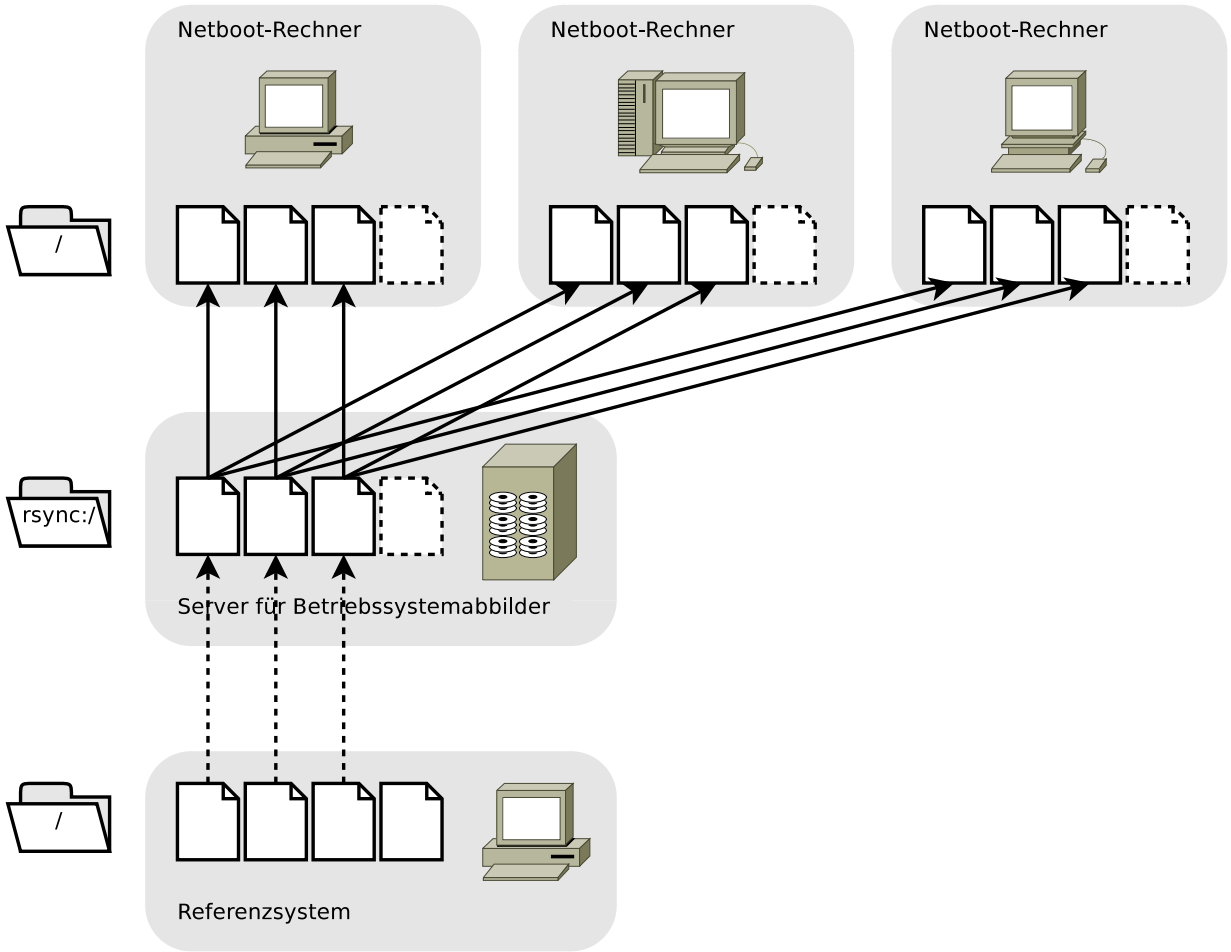
Ein Betriebssystemabbild wird erzeugt, indem die Dateien vom Referenzsystem zum Imageserver übertragen werden. Rechnerspezifische Dateien (hier die Datei rechts) werden vom Kopierprozess ausgenommen.

Paketinstallation



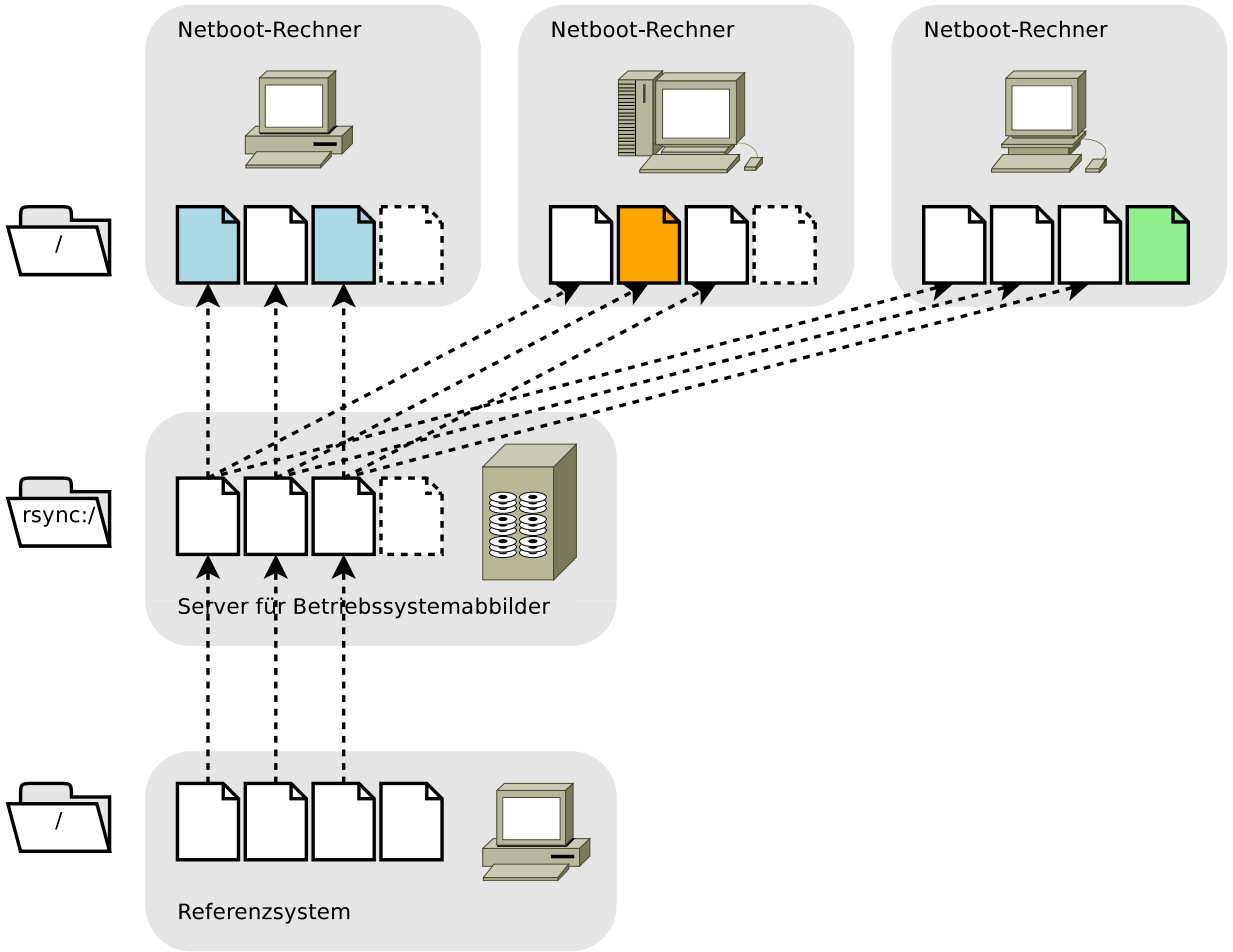
Ein neues Paket wird eingespielt.

Distribution



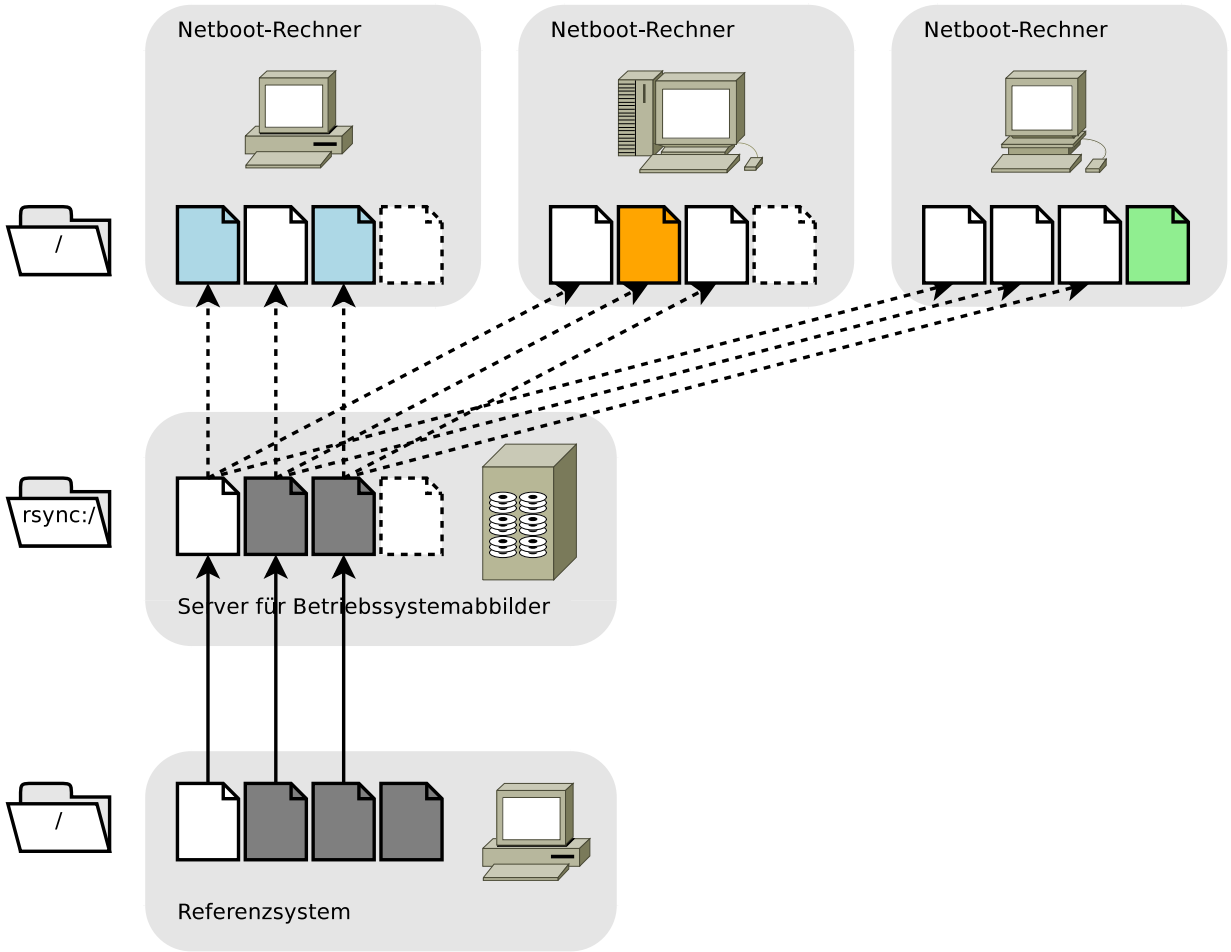
Notwendige Änderungen werden an die Clients verteilt.

Lokale Änderungen



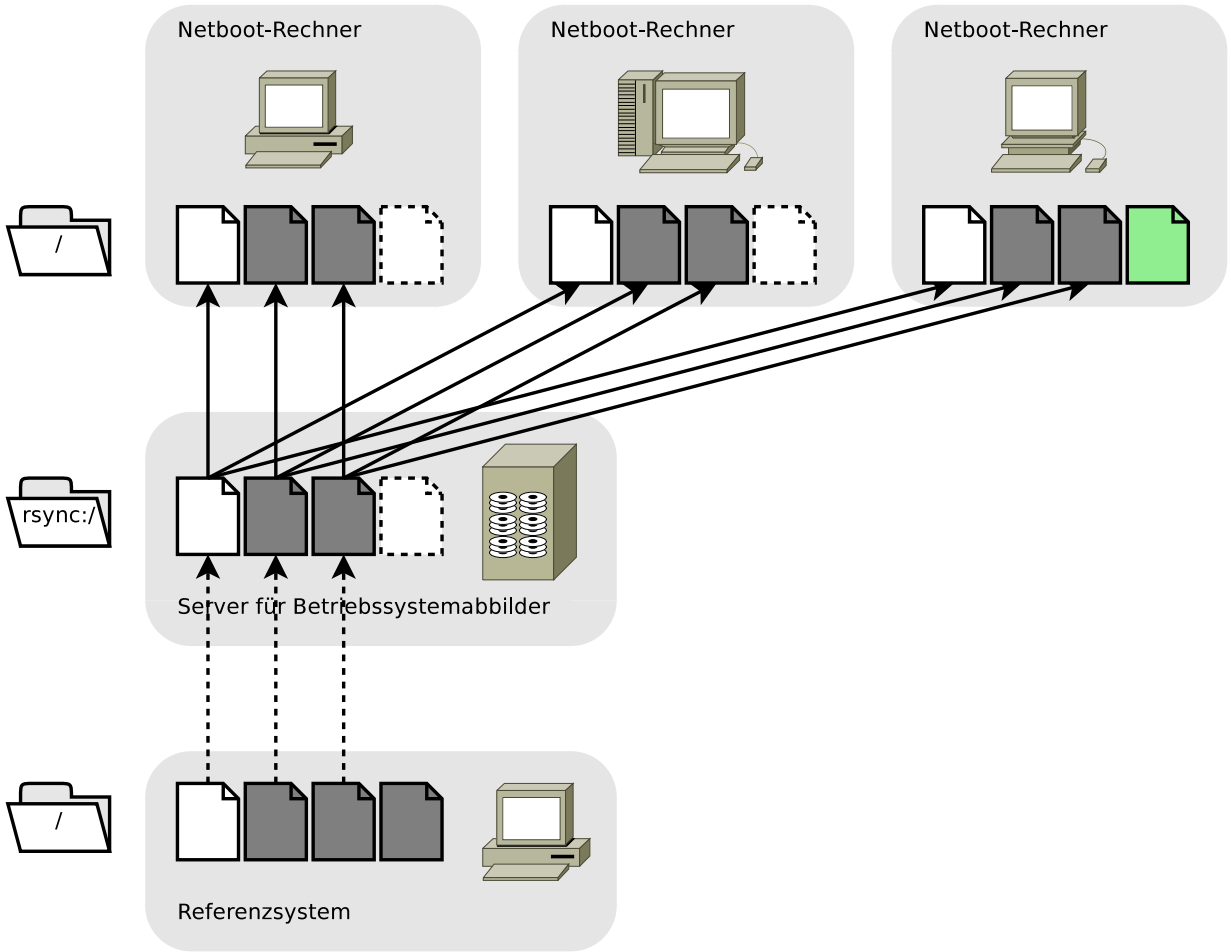
Client kann, bei Bedarf, lokale Änderungen schreiben.

Update



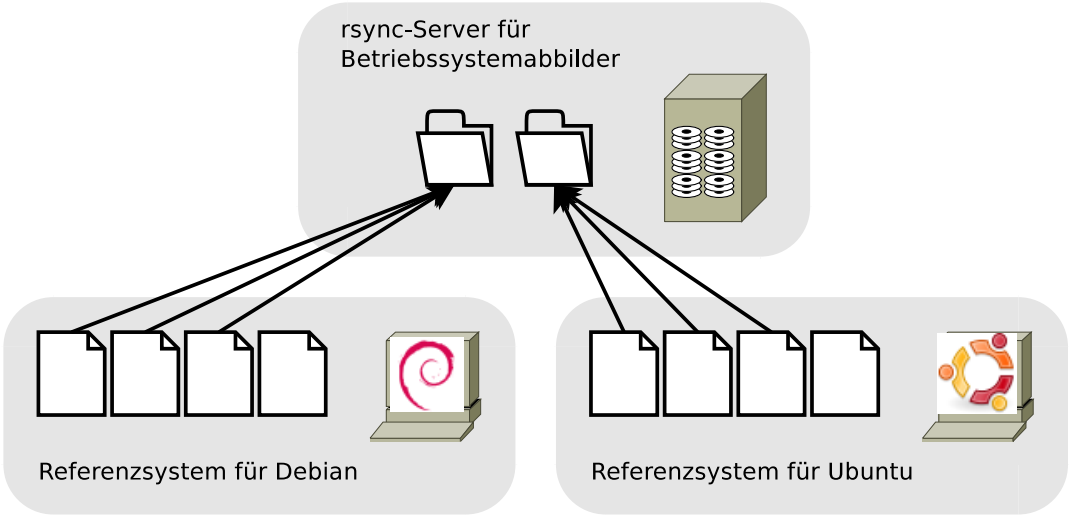
Eine Aktualisierung wird eingespielt.

Update: Client



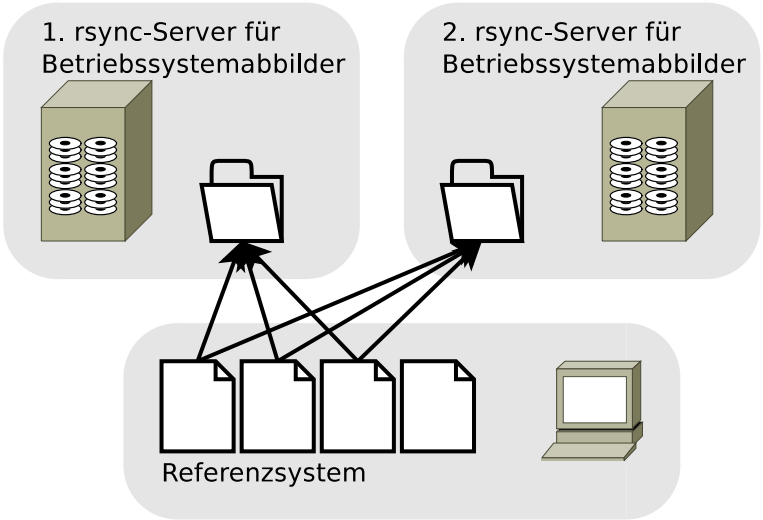
Die Aktualisierung wird an die Clients propagiert.

Releases



Auf dem Image-Server können unterschiedliche Abbilder bereitgestellt werden.

Redundanz



Mehrere Abbildserver bieten Ausfallsicherheit und bessere Lastverteilung.

Ausnahmeliste

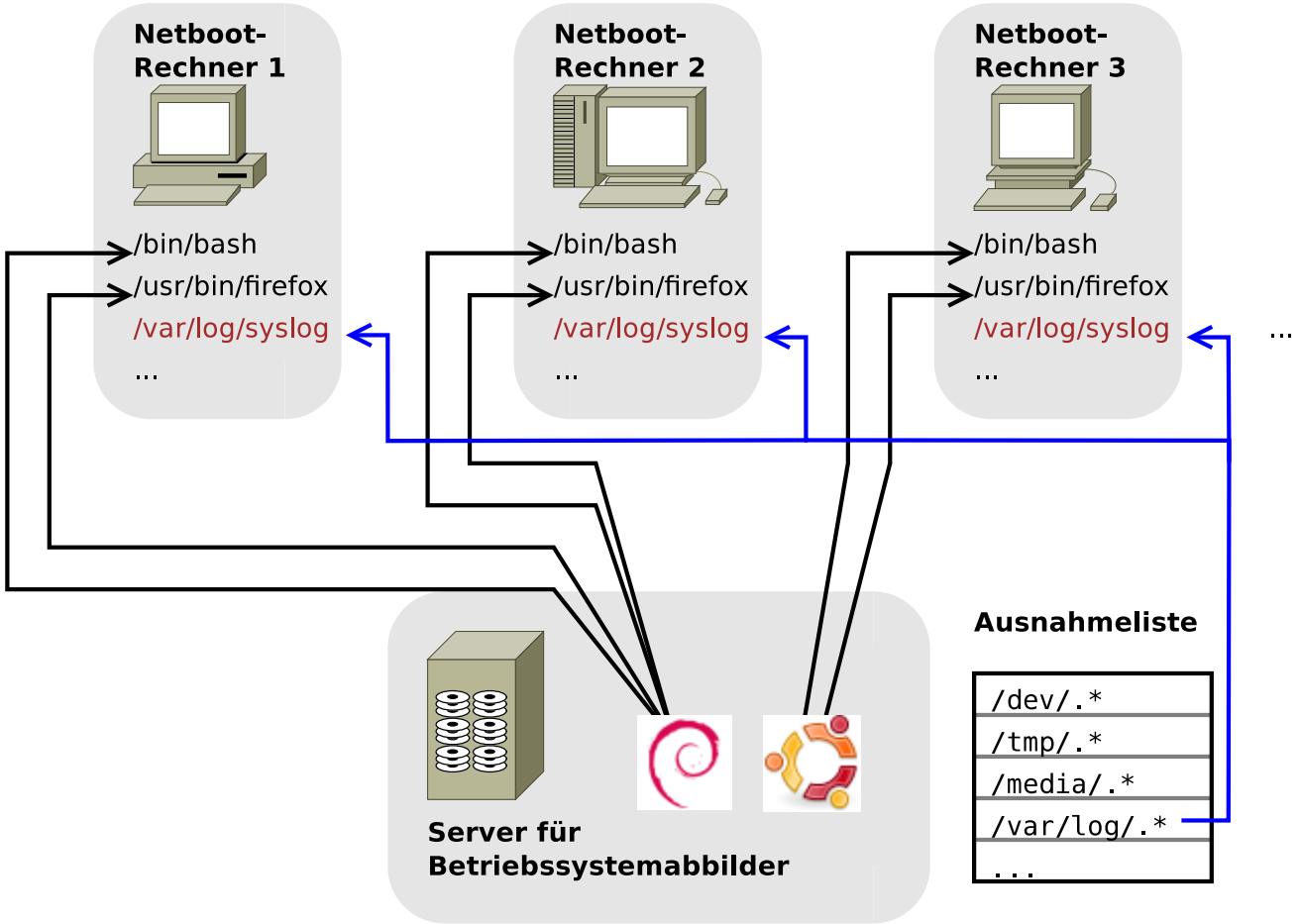
Motivation

Problem: Nicht alle Dateien dürfen von der Referenzinstallation übernommen werden (Logfiles, Cache, etc.).

Idee: Ausnahmeliste definiert, welche Dateien kopiert werden.

Ausnahmeliste

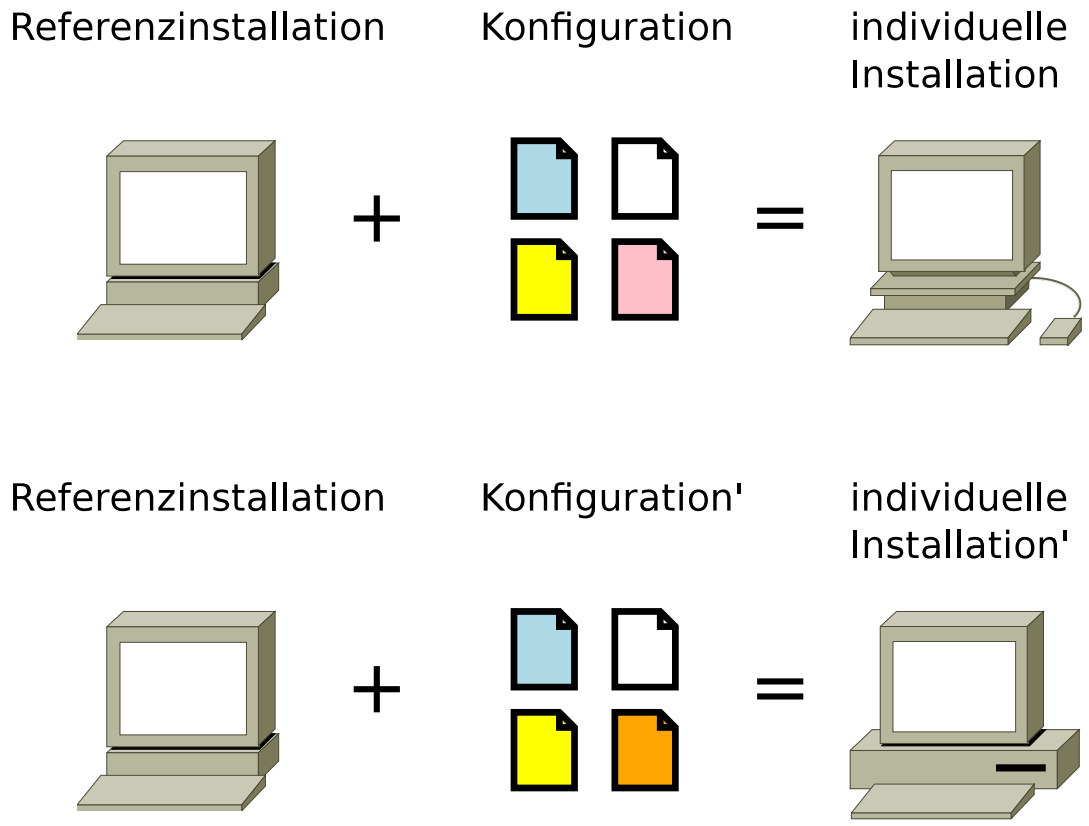
Überblick



Dank der relativ gut strukturierten Dateisystemhierarchie unter *GNU/Linux* ist eine Ausnahmeliste überschaubar.

Konfiguration

Idee



Von einer Referenzinstallation zum individuellen Netboot-Rechner.

Klassen

Motivation

Problem: Rechner braucht individuelle und AG-/Projektspezifische Konfigurationsdateien.

Idee: Konfigurationen gruppieren und Klassen bilden, welche entsprechenden Rechnern nach Bedarf zugeteilt werden.

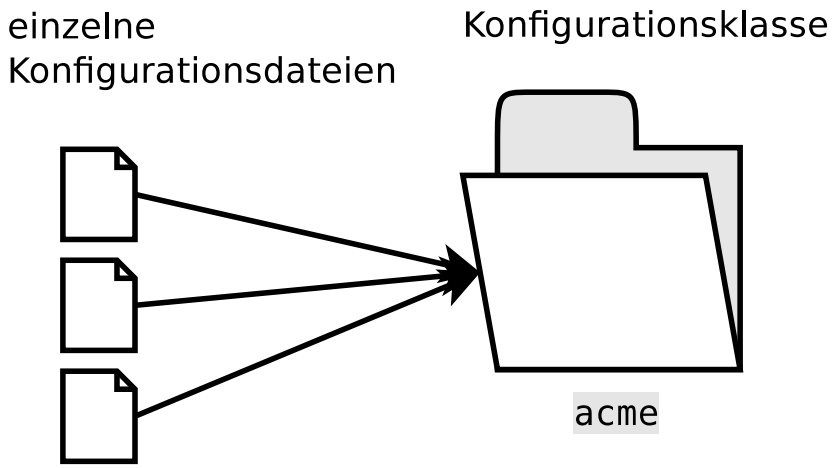
Klassen

Konzept

`lib/systemd/system/acme.service`

`etc/udev/rules.d/50-acme.rules`

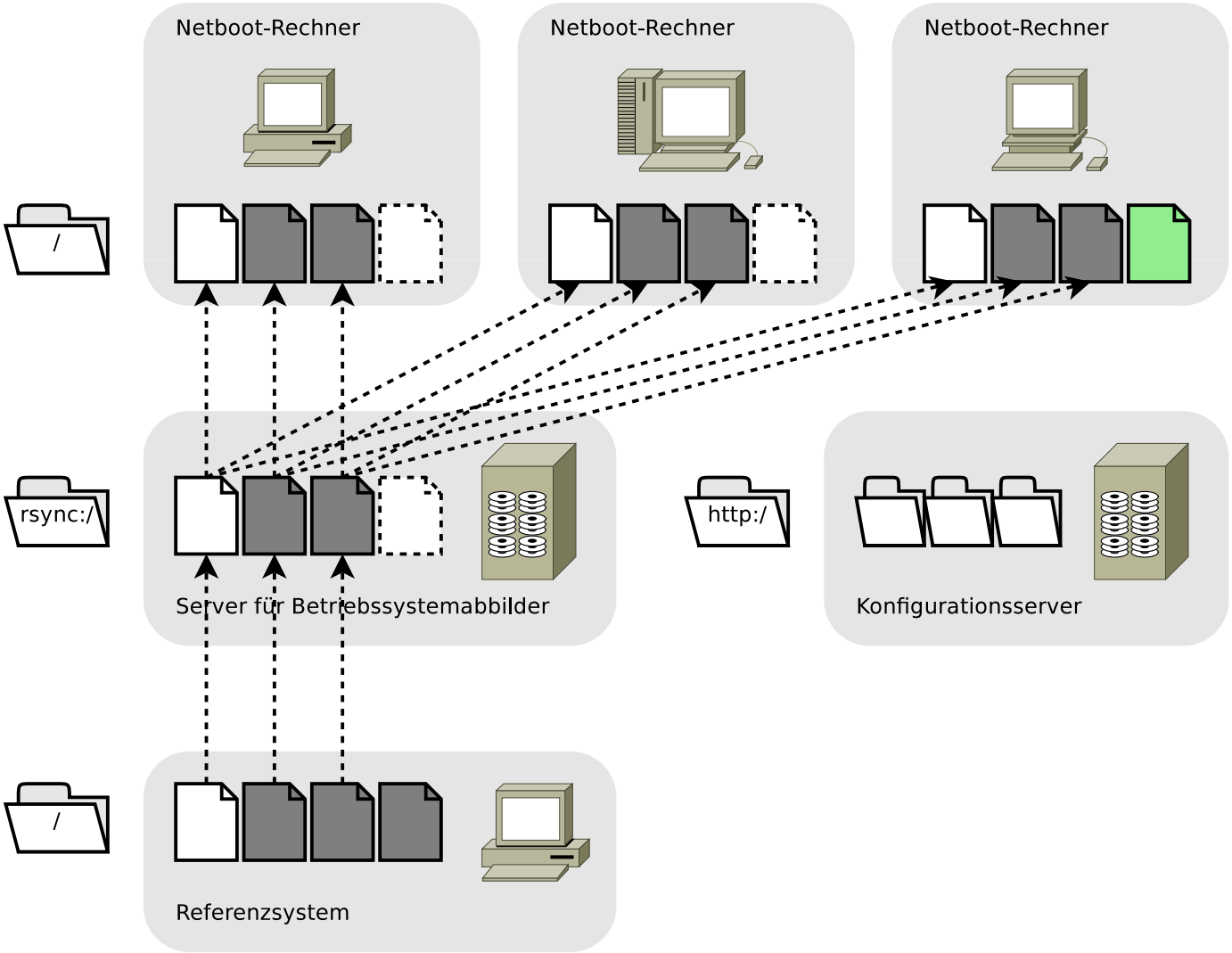
`usr/local/sbin/acme-control`



Konfigurationsdateien werden zu einer Klasse zusammengefasst.

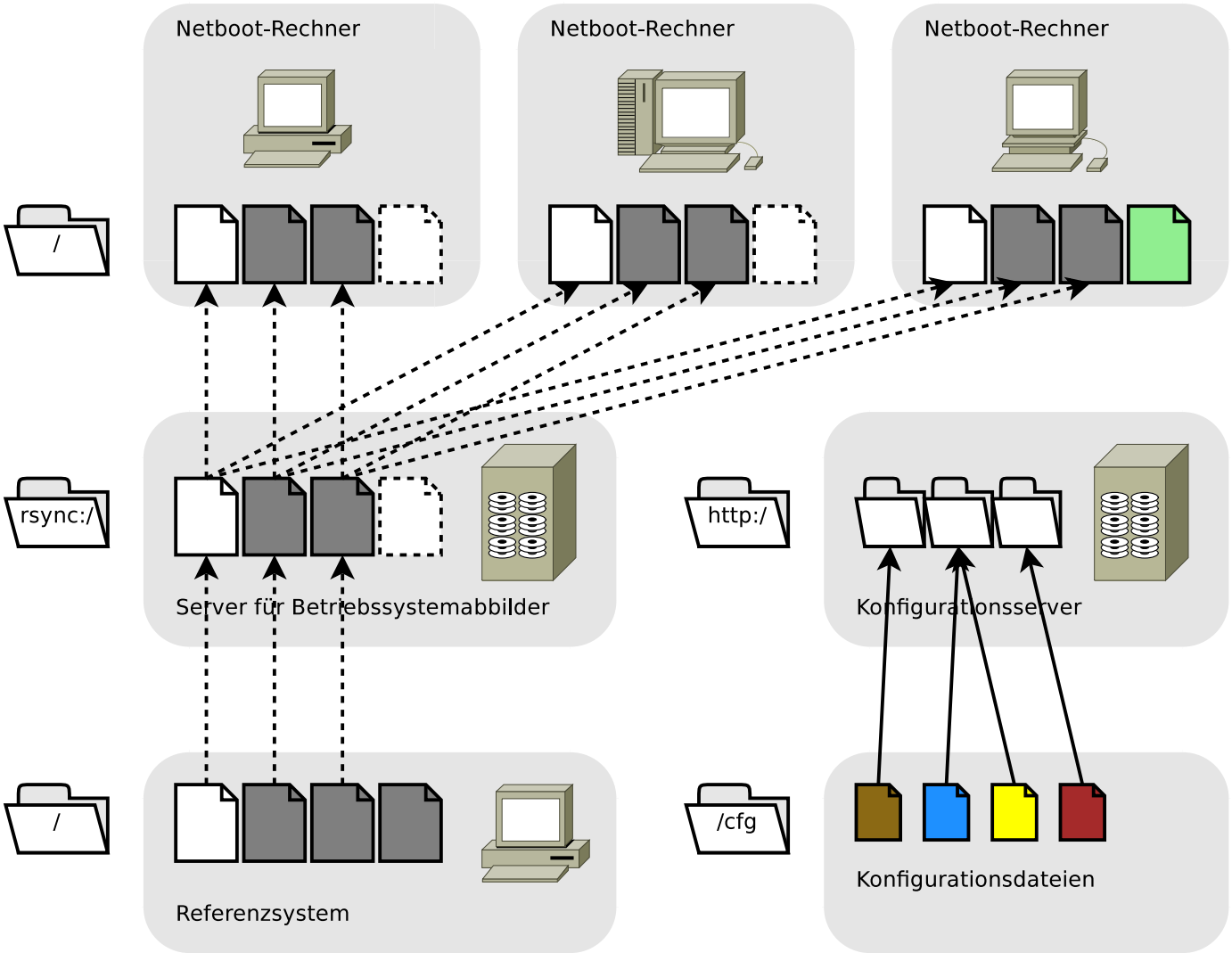
Klassen

Übersicht



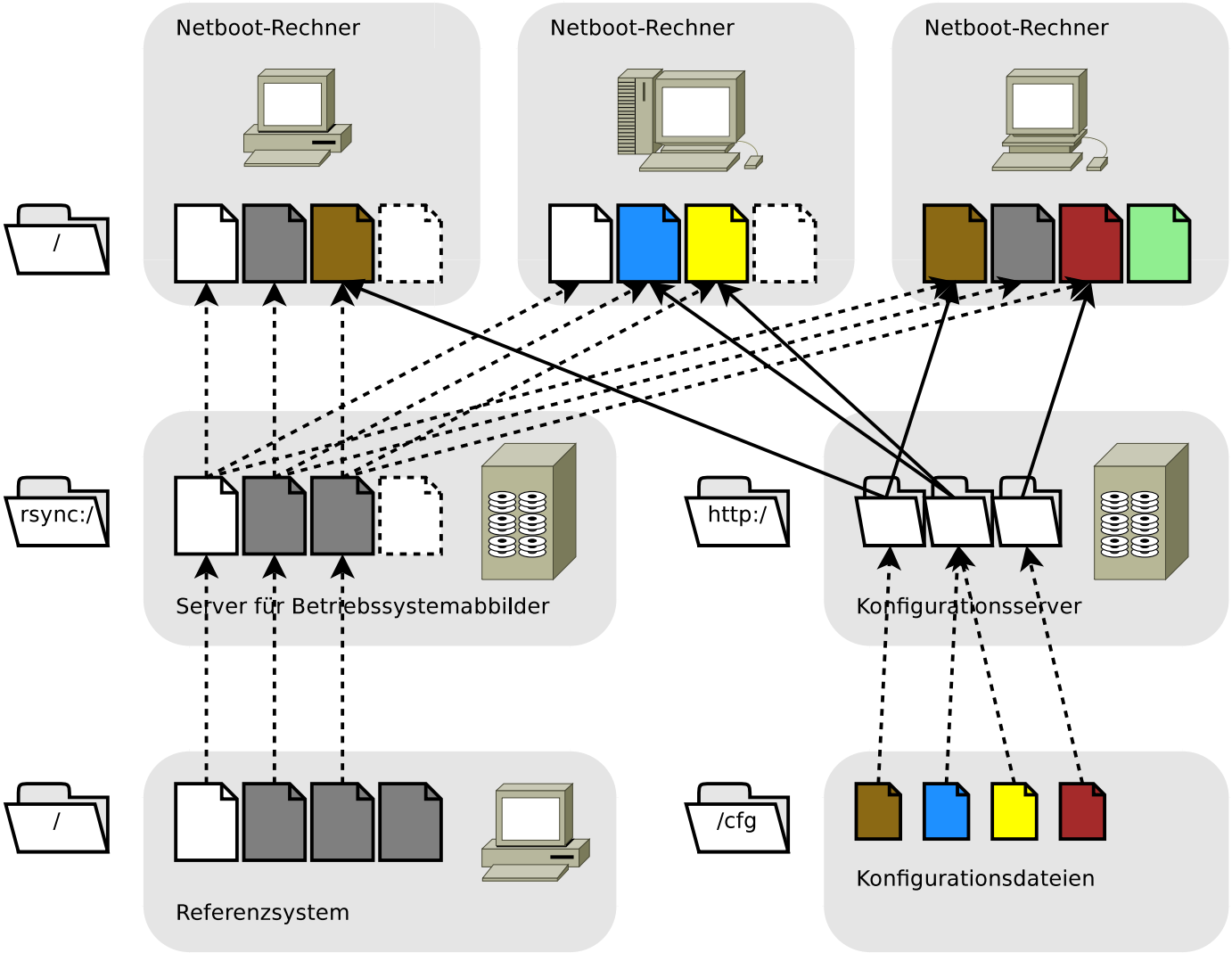
Klassen

Dateien



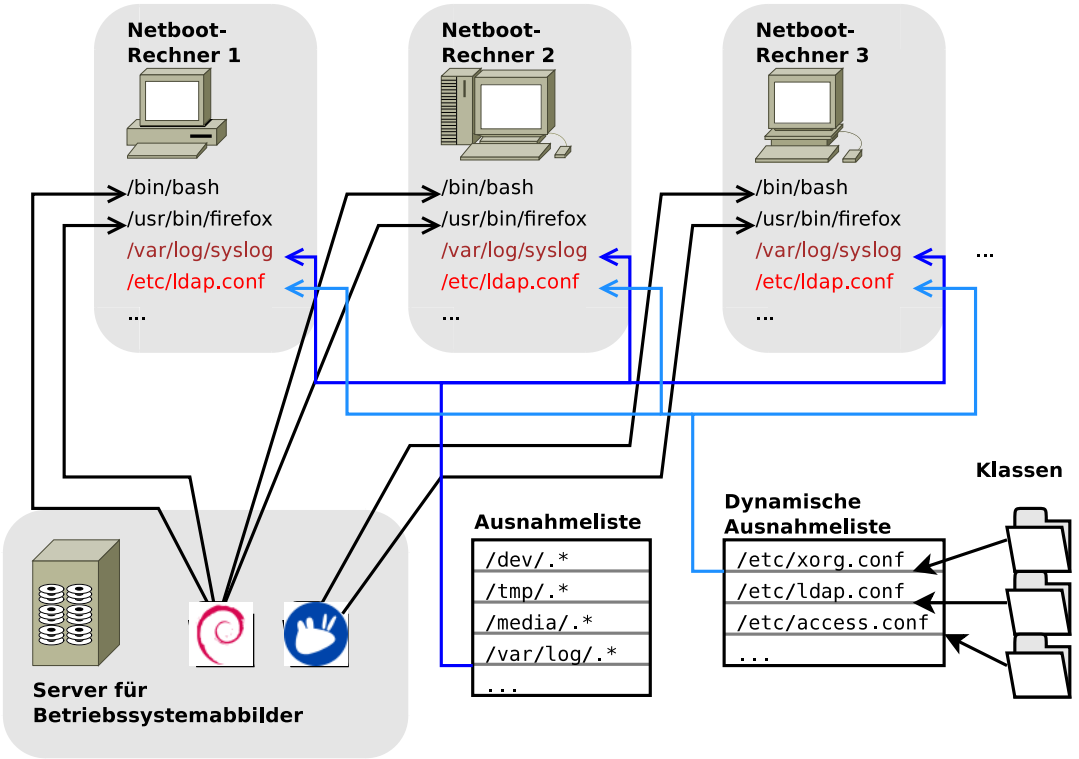
Klassen

Lokale Änderungen



Klassen

Dynamische Ausnahmeliste



Bei Aktualisierungen im Betrieb wird mit Hilfe einer dynamischen Ausnahmeliste sichergestellt, dass keine lokalen Konfigurationsdateien durch ihre Standard-Varianten aus der Referenzinstallation überschrieben werden.

Hosteigenschaften

Motivation

Problem: Eigenschaften eines Rechners müssen zugewiesen werden. Z.B. Zugehörigkeit zu Klassen, welches Betriebssystem gewünscht ist, etc.

Idee: Im **DNS**-Textrecord des Hosts hinterlegen?

***Besser*/Flexibler:** *Netenv*-Objekte per **http**.

Netenv

Übersicht

Beispiel:

host_homer:
+ag_scs
+shutdown-auto

ag_scs:
+keyboard_us
release="xenial"
architecture="amd64"

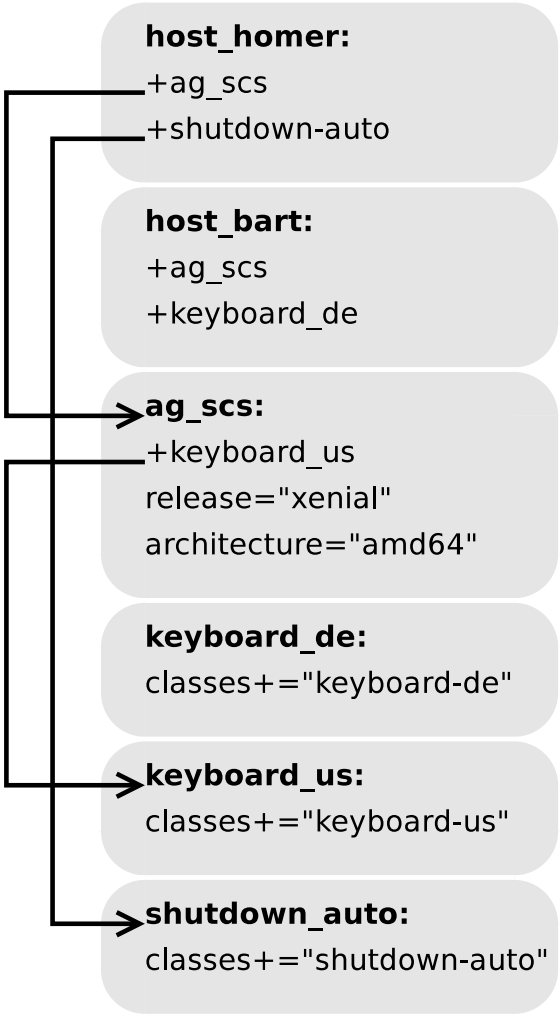
keyboard_us:
classes+="keyboard-us"

shutdown_auto:
classes+="shutdown-auto"

- Eigenschaften werden per *key=value*-Zuweisung hinterlegt (z.B. *release=xenial*)
- Objekte fassen jeweils Eigenschaften für einen bestimmten Zweck zusammen (z.B. *keyboard_us*)
- Mit Hilfe von *Includes* lassen sich Objekte modular verwenden

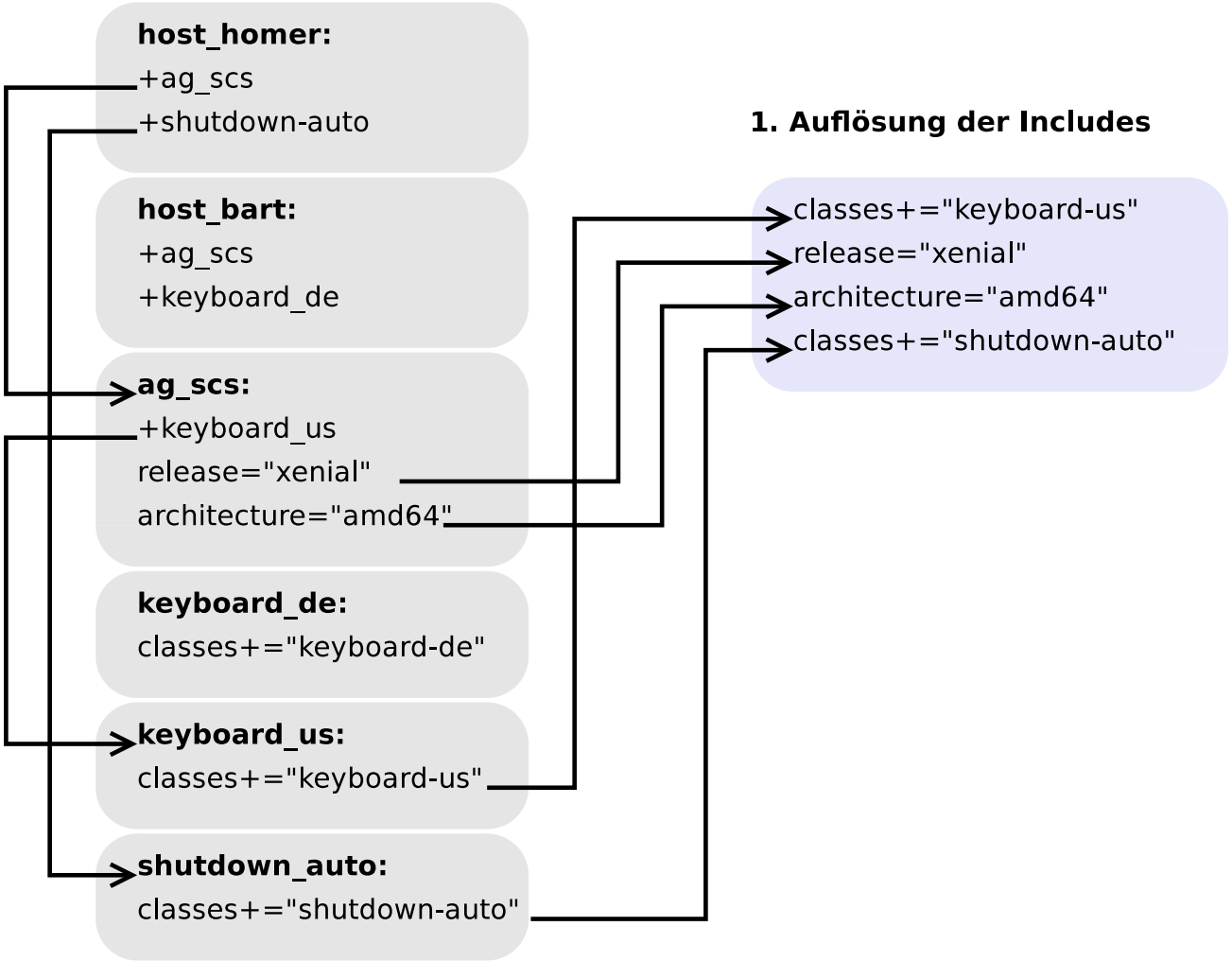
Netenv

Rekursive Auflösung des Objektes *host_homer*



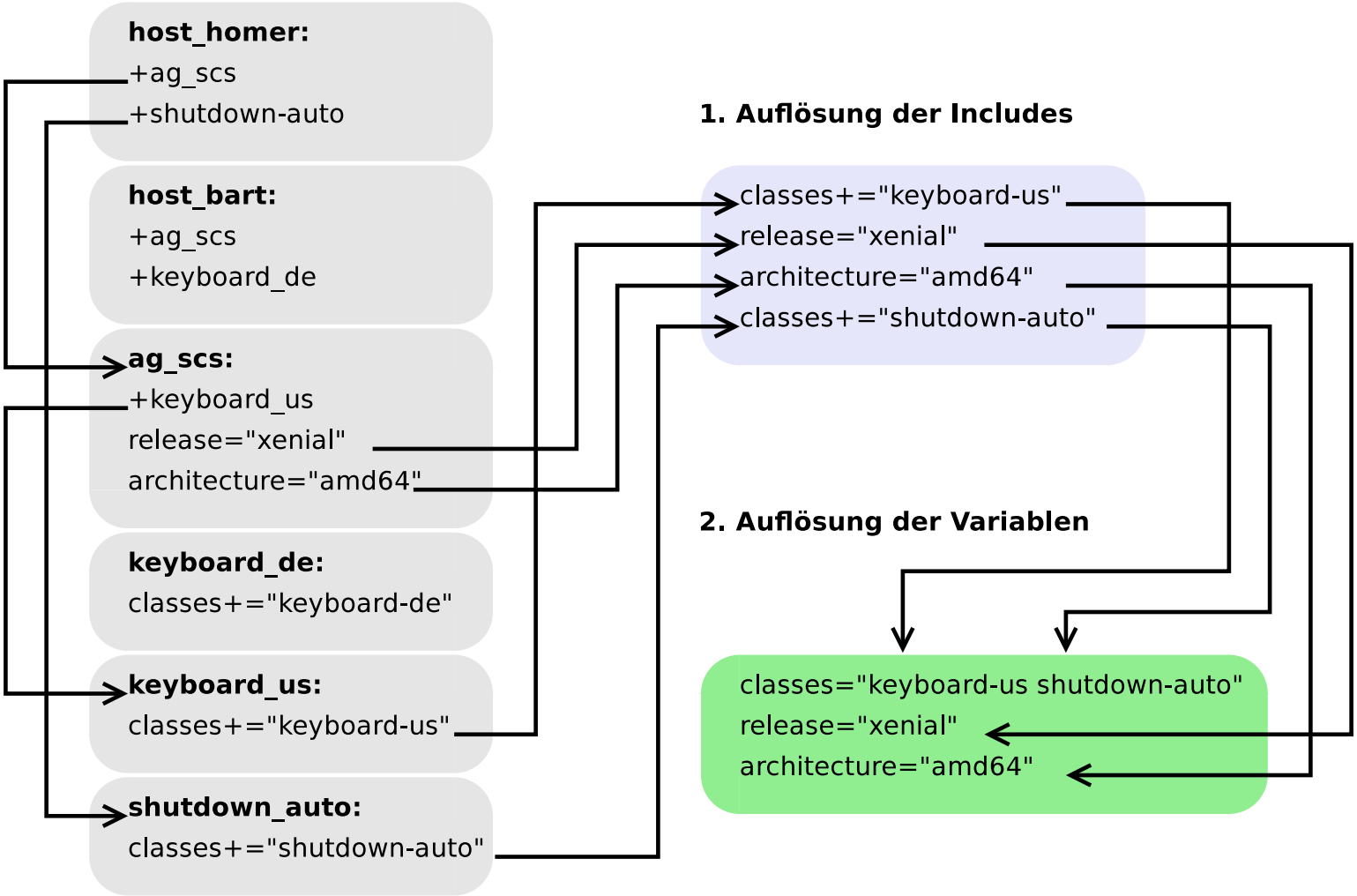
Netenv

Rekursive Auflösung des Objektes *host_homer*



Netenv

Rekursive Auflösung des Objektes *host_homer*



Netenv

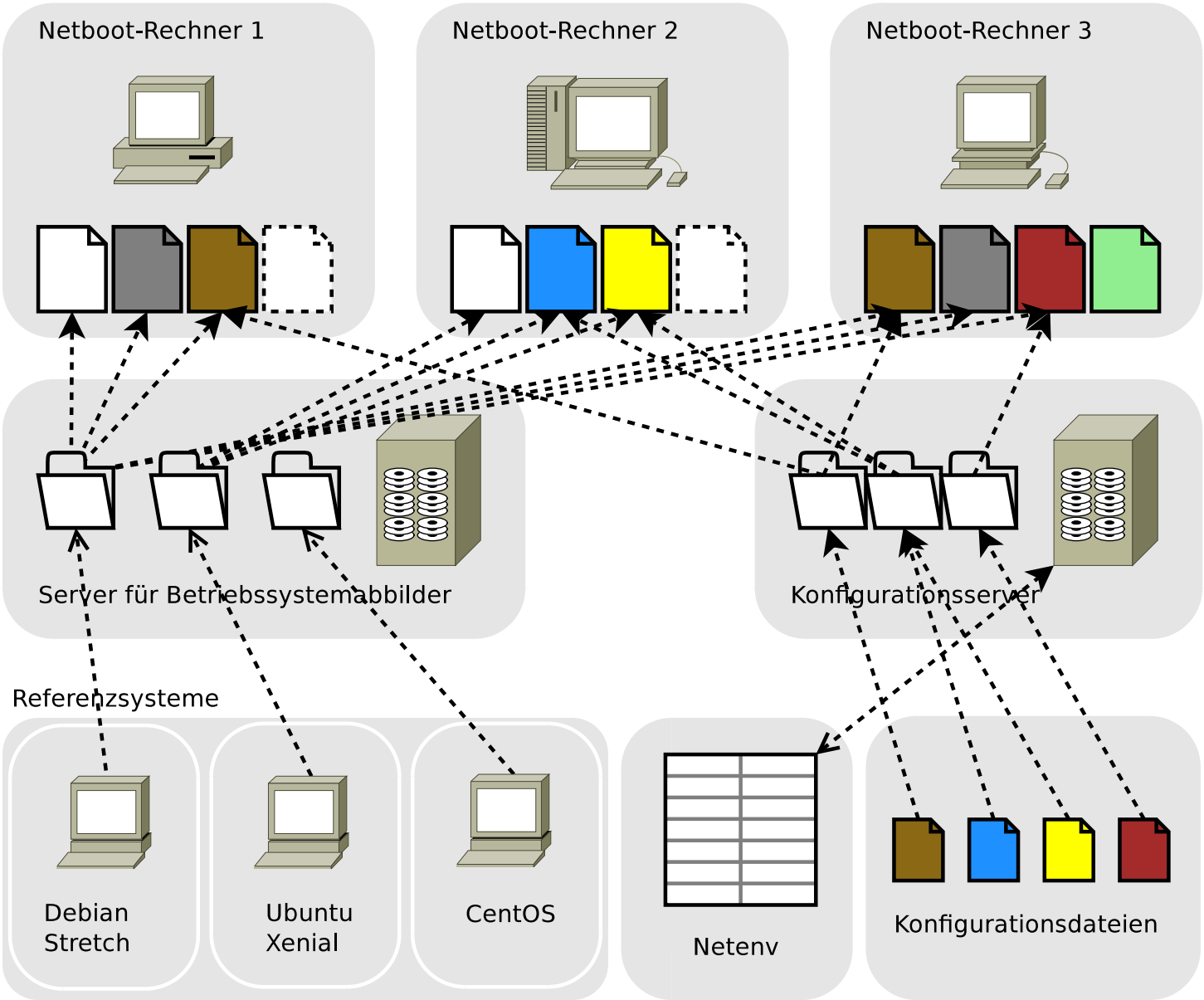
Zusammenfassung

Netenv bietet eine flexible Möglichkeit Rechner- und Gruppeneigenschaften zu organisieren:

- *key=value*-Zuweisungen
- Übersichtliche Syntax:
  Set [=], *Append* [+=] und *Include* [+]
- Modularität (durch Includes)
- Einfache Kommandozeilenwerkzeuge zur Verwaltung
- HTTP-Schnittstelle
  - Standardisiertes Sicherheitskonzept
  - Caching und Failover leicht umzusetzen
- Einfache Verarbeitung (zeilenbasiertes Format)

Netenv

Überblick



Bootprozess

kNXE

Motivation

Problem: Wie kann System vor dem Start mit all den Einstellungen auf die Platte installiert/aktualisiert werden?

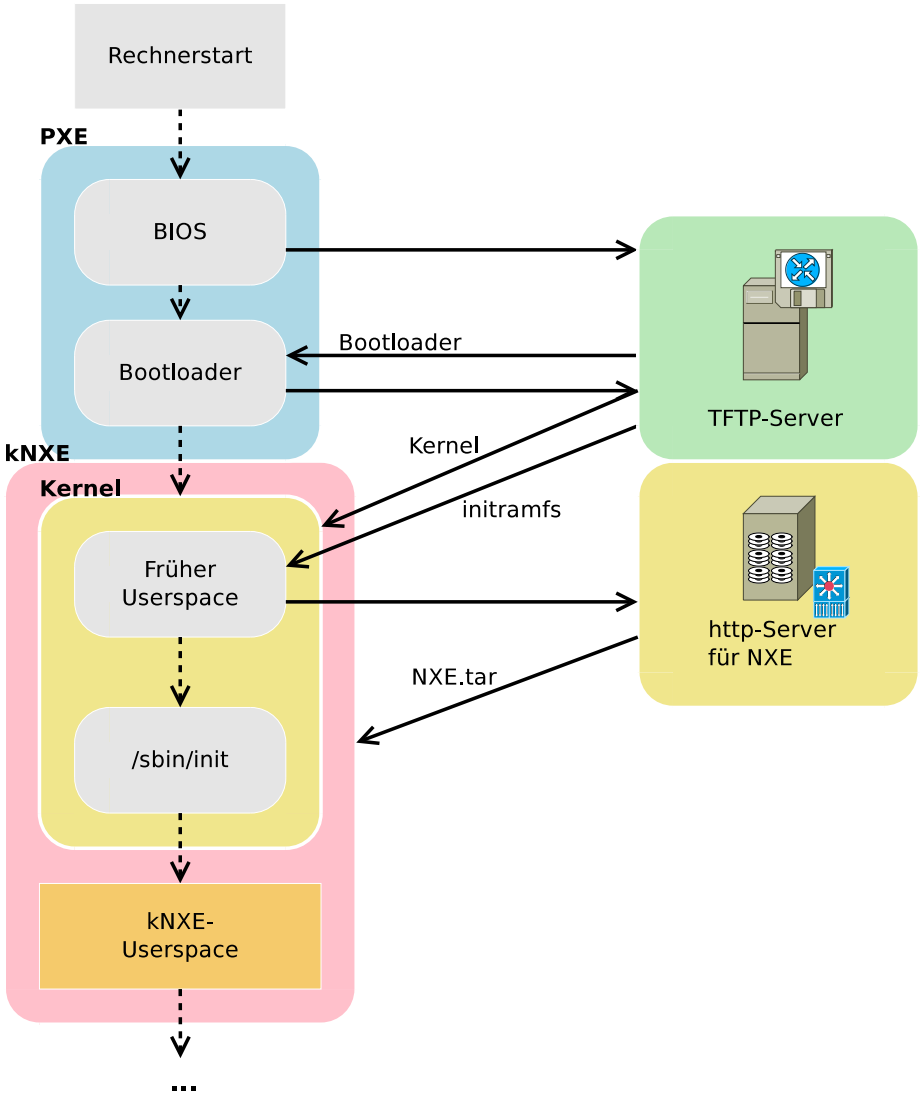
Idee: Zweistufiger Bootprozess.

- Rechner lädt zunächst per PXE das **k**exec-based **N**etboot E**x**ecution **E**nvironment (kNXE) ins RAM
- kNXE installiert/aktualisiert Betriebssystem und Konfigurationen auf die lokale Festplatte/SSD
- **kexec** lädt *Kernel* und Zielbetriebssystem ohne Rechner neuzustarten

$\Rightarrow$ Keine Änderungen am Zielbetriebssystem notwendig!
$\Rightarrow$ Per PXE-Menü ist auch Boot in lokales Windows realisierbar.

kNXE

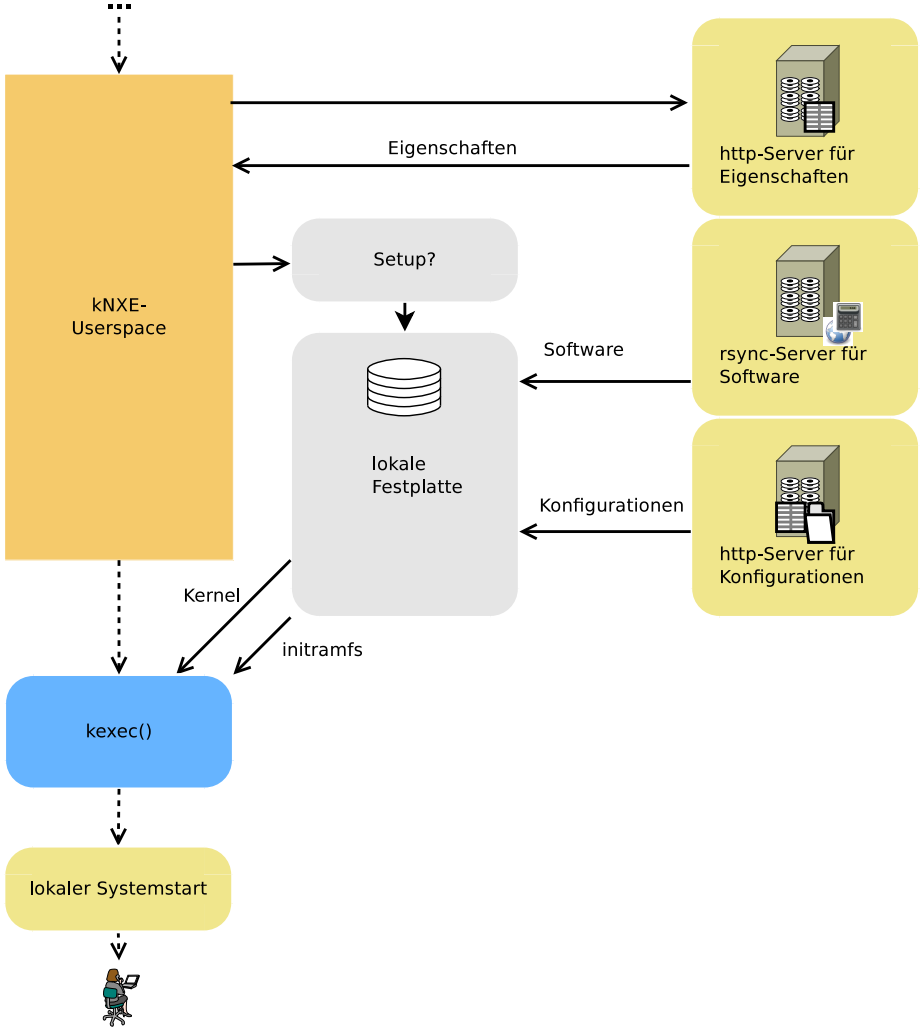
PXE



In der ersten Stufe startet der Rechner per PXE, lädt per HTTP das kNXE-System und hinterlegt es im RAM.

kNXE

Boot



kNXE überträgt das gewünschte System auf die lokale Festplatte und startet den Kernel via **kexec**.

Verschlüsselung

Motivation

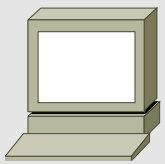
- Rechnerkonfiguration enthält sensible Daten (wie z.B. *802.1X*-Credentials, *SSH*-Keys, etc.)
- Es besteht initial keine gesicherte Verbindung zum System (DHCP, TFTP sind **nicht** sicher)
- Wie soll sich Rechner authentisieren? (*Henne-Ei-Problem*)

$\Rightarrow$ Statische Passwörter sind umständlich (RBA muss vorbeikommen zum Abholen; u.U. schwer einzugeben) und anfällig (können abgefangen oder geknackt werden).

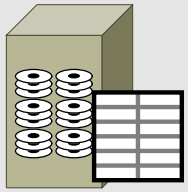
Idee: Einmalpasswort (sog. **TAN**) für den ersten Boot vergeben, mit Hilfe dessen Schlüsselaustausch innerhalb eines begrenzten Zeitfensters initialisiert werden kann.

Verschlüsselung

TAN-Verfahren



Netboot-Client



Netenv-Server

* Symmetrischer Schlüssel für Rechner 'homer' wird generiert
* Klasse 'host_homer' wird mit dem symmetrischen Schlüssel verschlüsselt

* TAN wird eingegeben
* Asymmetrisches Schlüsselpaar wird generiert
* Öffentlicher Schlüssel wird mit TAN signiert
* Signierter öffentlicher Schlüssel wird per HTTP-PUT hochgeladen

PUT /register/homer.2572cd78-2950-11e3-9180-f7d240544534

* Signatur wird geprüft
* Öffentlicher Schlüssel wird extrahiert
* Symmetrischer Schlüssel wird mit öffentlichem Schlüssel verschlüsselt
* Ergebis wird per netenv bereitgestellt

GET /host_homer

sessionkey="RiGpqCVGQm8IRm55f7br2uDKWTl5..."

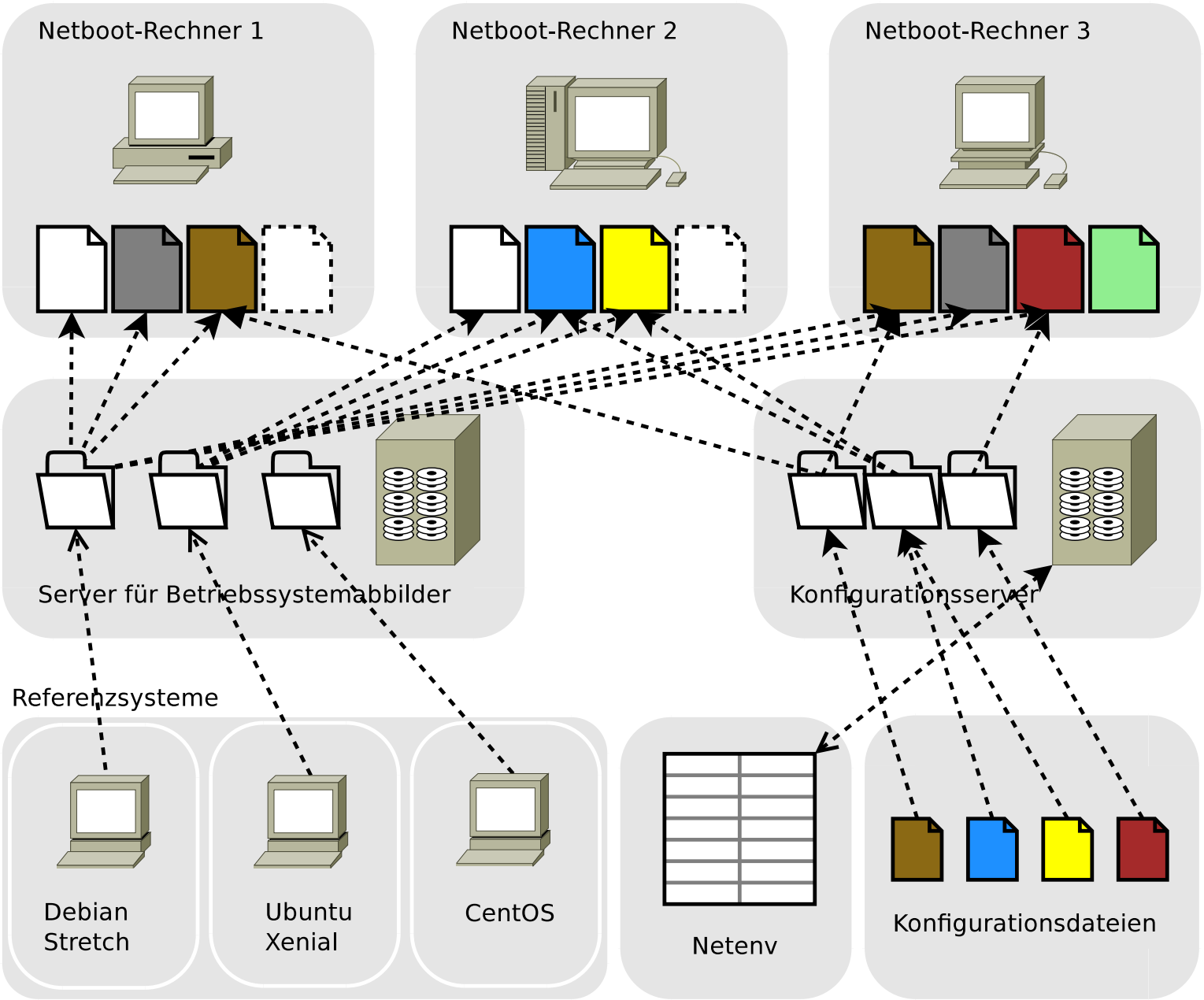
* Symmetrischer Schlüssel wird mit privatem Schlüssel entschlüsselt
* Klassen können entschlüsselt werden

Überblick

Zusammenfassung

- Einfaches **Setup** zum initialen Einrichten für Rechnerbeauftragte
- Updates von Software und Konfiguration **vor** dem Start und **regelmäßig** im laufenden Betrieb
- Distribution kann jeweils beim Boot gewählt werden
- System ist vollständig **lokal** verfügbar
- Bei Netzwerkausfall arbeitet Workstation weiter
- System ist **modular** und **erweiterbar**
- Bei Ausfall einer Komponente sind alle Anderen weiterhin verfügbar
- Adminstrationsseitig stehen einfache Werkzeuge zur Verwaltung bereit
- System mit über 500 Rechnern im Einsatz

Komponenten



Danke für die Aufmerksamkeit!

Fragen? :)

Folien unter ***https://techfak.net/~sk/netboot***