Der Vorarbeiter lässt die Puppen tanzen

Lukas Plattner

Vorstellung

Name: Lukas Plattner

Funktion: Abteilungsleiter Linux Server, Chief Information Security Officer

E-Mail: lukas.plattner@apa.at

APA-IT Informations Technologie GmbH

Die APA-Gruppe | APA – Austria Presse Agentur eG

CLEMENS PIG (VORSITZENDER DER GESCHÄFTSFÜHRUNG)
KARIN THILLER (GESCHÄFTSFÜHRERIN)

MARKETING & VERKAUF

Sales, Produktmanagement

Marketing, Kommunikation

FINANZEN & ADMINISTRATION

Rechnungswesen, Controlling, Personalmanagement

INNOVATION

APA-medialab

Business Development

NACHRICHTENAGENTUR

APA-BASISDIENST
Profitcenter

APA-MULTIMEDIA
Profitcenter

APA-FINANCE
Profitcenter

INFORMATIONSAGENTUR

APA-DEFACTO (APA-PICTUREDESK)
100%-Tochter

APA-OTS
100%-Tochter

TECHNOLOGIEAGENTUR

APA-IT (GENTICS)
100%-Tochter

BETEILIGUNGEN

KEYSTONE-SDA-ATS AG
Bern, 30%

DPA-DIGITAL SERVICES GMBH
Hamburg, 50%

DPA-AFX WIRTSCHAFTSNACHRICHTEN GMBH
Frankfurt, 24,2%

NEXT MEDIA ACCELERATOR GMBH
Hamburg, 3,2%

EPA EUROPEAN PRESSPHOTO AGENCY B.V.
Frankfurt, 6,9%

Die APA-IT in Zahlen

2
redundante Rechenzentren in Wien

2.400.000.000
PIs pro Monat

140
Mitarbeiterinnen und Mitarbeiter

30.000.000
Videos pro Monat

7.500.000
Recherchen

260.000.000
Dokumente

25.000.000 €
Jahresumsatz

Die Säulen der APA-IT

IT FÜR DIE APA-GRUPPE

DIGITAL MEDIA BASE

Vereint alle technischen Tools, die ein Medienhaus für das digitale Zeitalter benötigt.

APA-OnlineManager

Mobile Publishing Suite

APA-IT-VideoServices

APA-IT-SmartServices

GENTICS SOFTWARE

Führender österreichischer Anbieter für Enterprise Web-Content-Management und Online-Portale für die Top 500 Unternehmen sowie eGovernment-Lösungen in der DACH-Region.

Gentics CMS

Gentics Mesh

MANAGED SERVICES

Umfasst professionell betreute Server, um einwandfreien Betrieb und ständige Verfügbarkeit zu gewährleisten

Managed Server Hosting und Housing

APA-IT-Cloud

IT-Outsourcing

DRaaS / BaaS

IT-Infrastukture

CUSTOM DEVELOPMENT

Individuallösungen für Kunden, speziell für den Medienbereich.

MARS

RedSys

Loop

Archive

2

Wofür der Aufwand?

Nach ITIL

- Security Management
  - Patch Management
  - Vulnerabillity Management
- Service Delivery Management
- Change- und Releasemanagement
- Configuration Management
- Lifecyclemanagement
- …

Management View

- Zu Beginn
  - Schnelle Installation von kritischen und Sicherheitsrelevanten Patches
  - Schnelle Änderung der Passwörter für lokale User
  - Übersicht wie der Status der Konfiguration der Server ist

- Später
  - Auswertungen über die Server
  - Kennzahlen
  - ISO 27001 compliance
  - Reduktion der Stückkosten

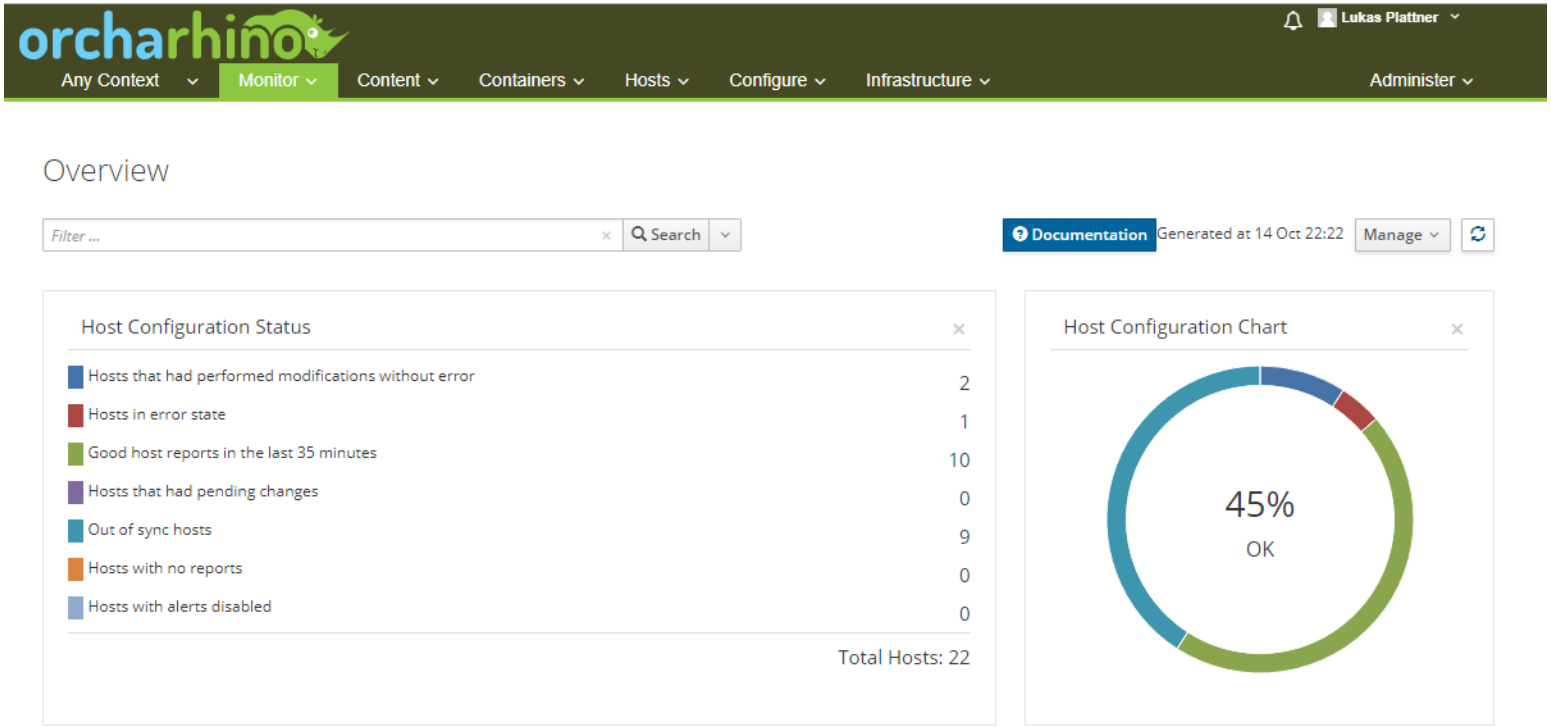
Techniker…

- Zu Beginn
  - Ausrollen einer Baseline
  - Nachvollziehbarkeit der Änderungen
  - Unterstützung diverser Derivate

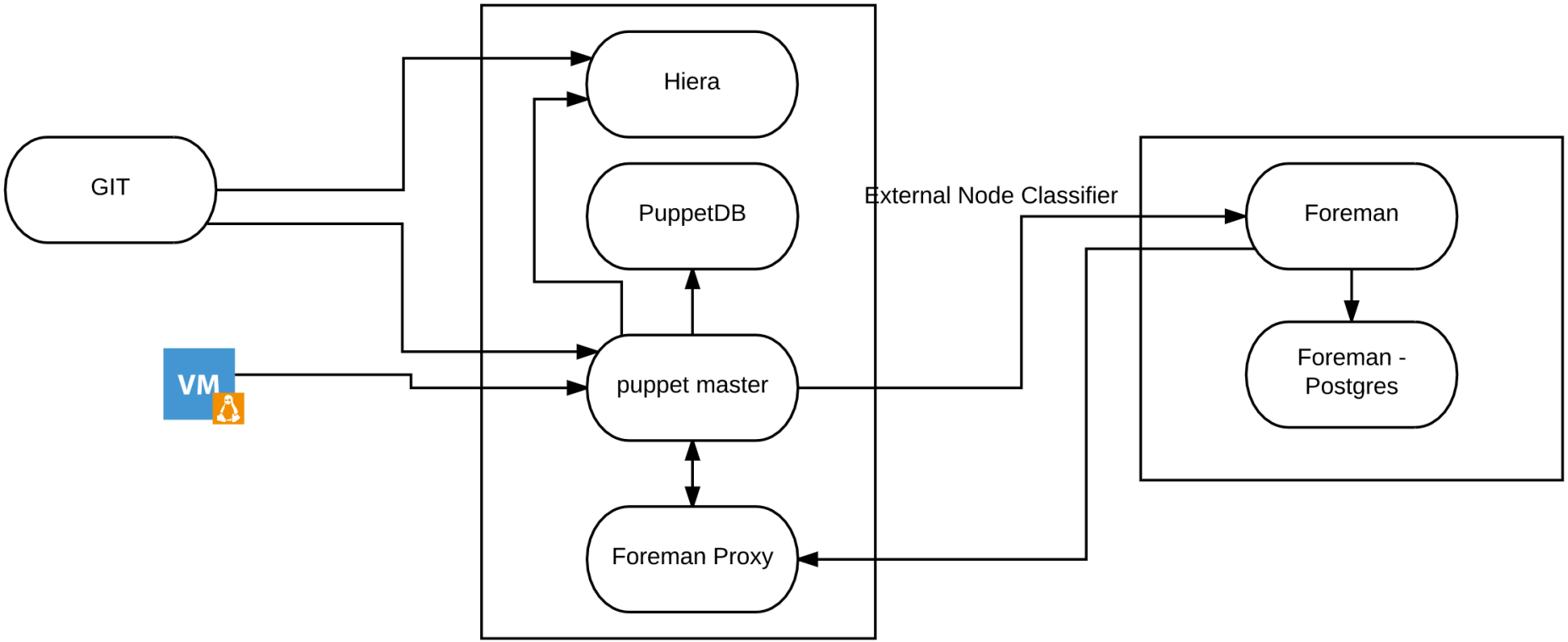
- Später
  - Usermanagement
  - Volles Management von Servern
  - Einfacheres Installieren von Modulen/Software
  - Vollautomatische Installation von (virtuellen) Servern
  - Sicherstellen das Konfiguration nicht verändert wird

3

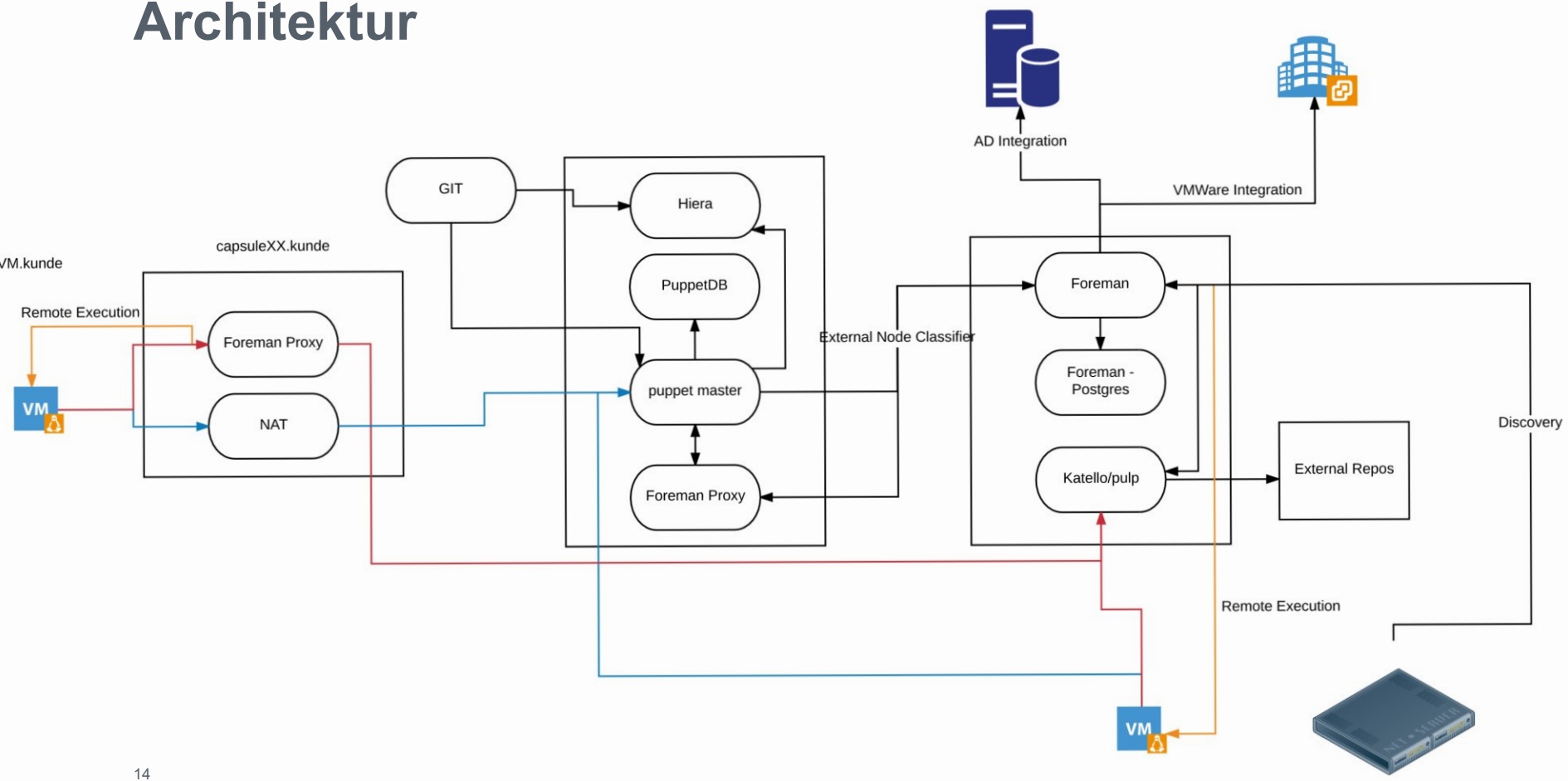
Wie sieht das denn aus?


orcharhino
Lukas Plattner
Any Context
Monitor
Content
Containers
Hosts
Configure
Infrastructure
Administer
Overview
Filter ...
Search
Documentation
Generated at 14 Oct 22:22
Manage
Host Configuration Status
Hosts that had performed modifications without error 2
Hosts in error state 1
Good host reports in the last 35 minutes 10
Hosts that had pending changes 0
Out of sync hosts 9
Hosts with no reports 0
Hosts with alerts disabled 0
Total Hosts: 22
Host Configuration Chart
45%
OK

Architektur - die Anfänge



Architektur

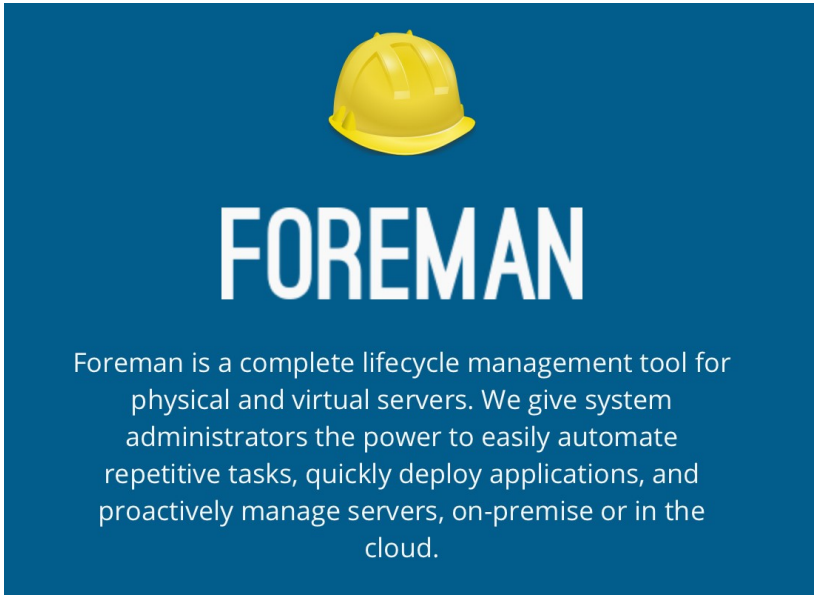


4

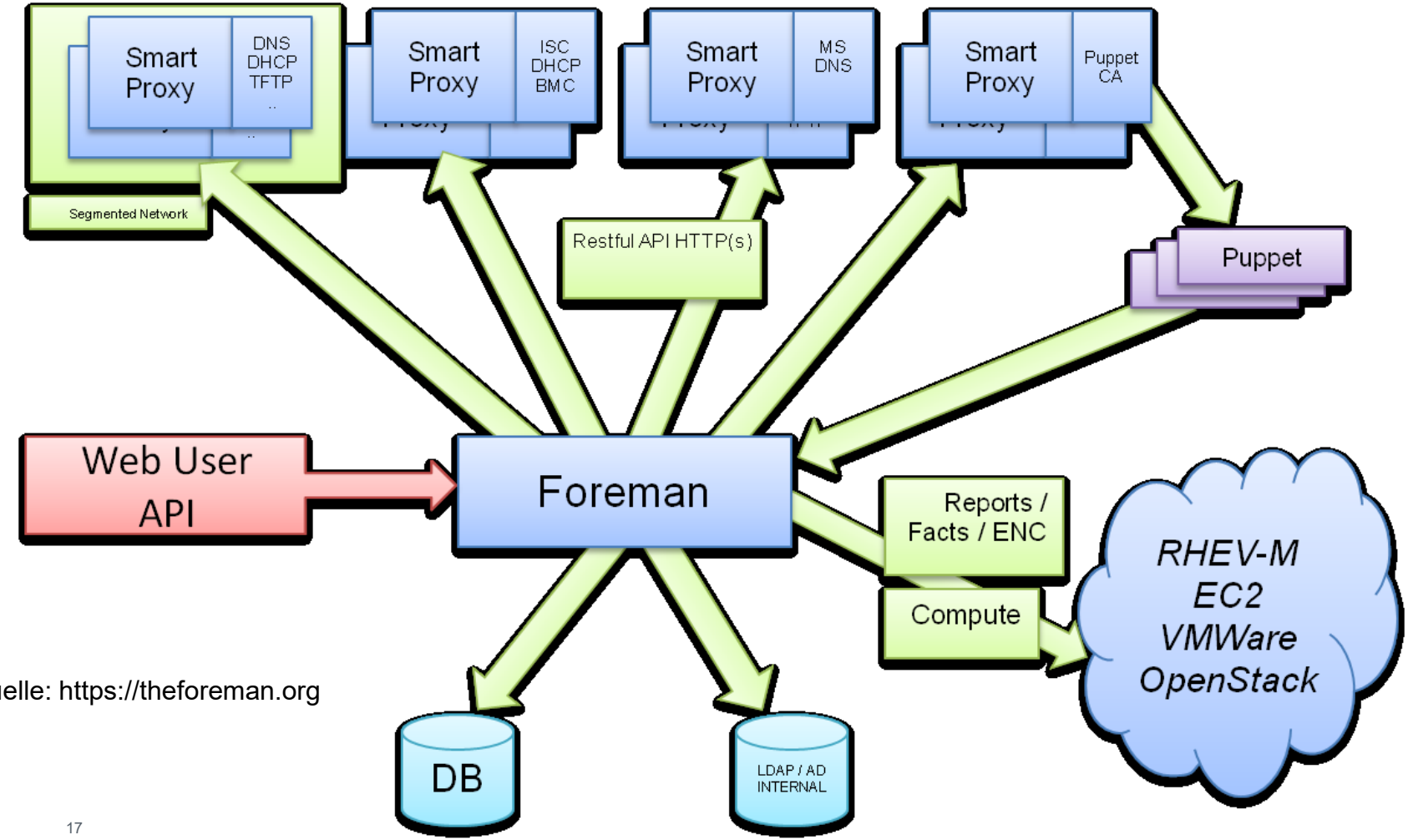
Foreman/Orcharhino

Foreman

- Modulare Managementplattform
- Interagiert via Smart Proxies und Plugins
- Integration mit LDAP/AD
- Multi Mandantenfähig
- Mächtige API
- CLI via hammer
- Aktive Community mit Unterstützung von Redhat,...



Quelle: https://theforeman.org



Quelle: https://theforeman.org

Smart Proxies

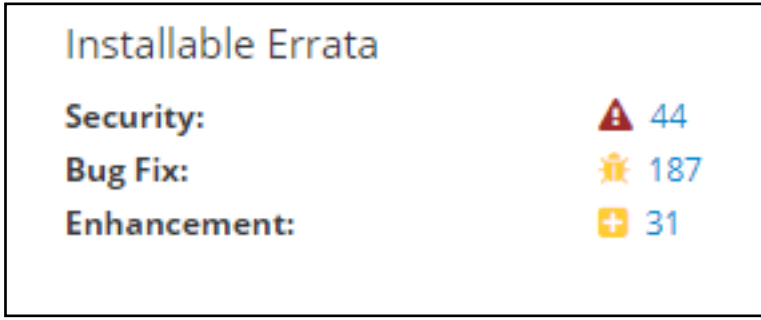
- Kommunizieren mit https/ Zertifikatsauthentifizierung
- Ebenfalls Modular
- Teilweise Endpunkte für Kommunikation mit Clients (Trennung von Netzen)

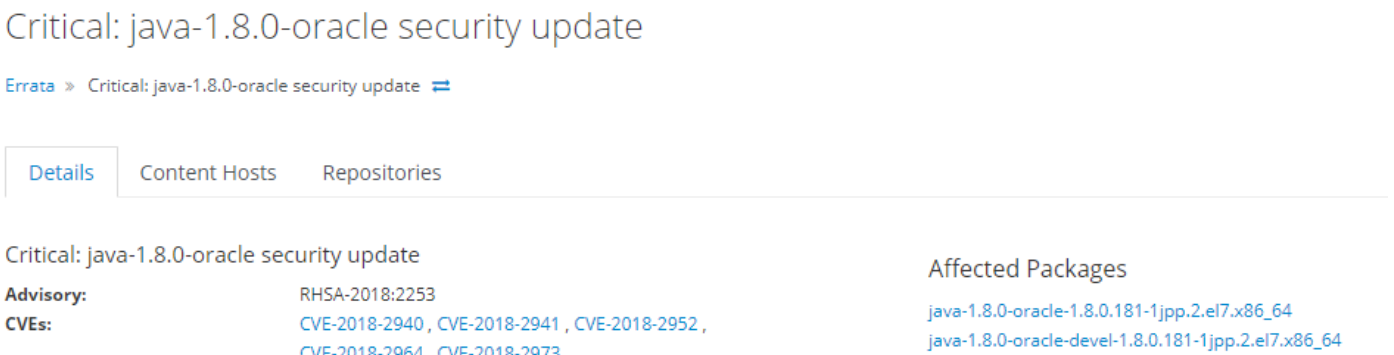
5

Katello

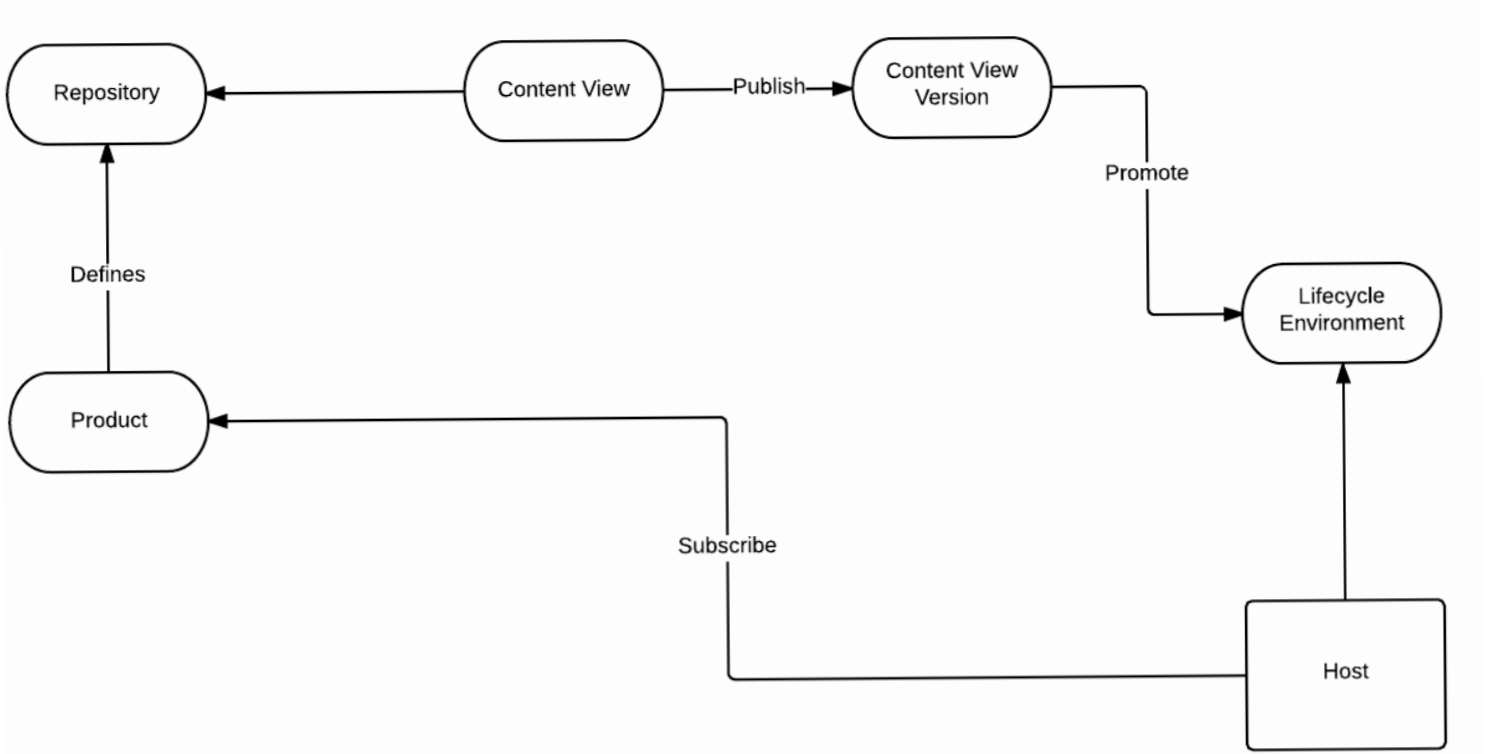
Katello

- … ein Plugin für Foreman … oder auch nicht
- Subscription und Patchmanagement
- Überblick Patchstand
- Offene Version von Redhat Satelite 6
- Repositories für RPM, docker, file, puppet und bald deb
- Life Cycle Environment – Content Views
- Errata





Subsciptions

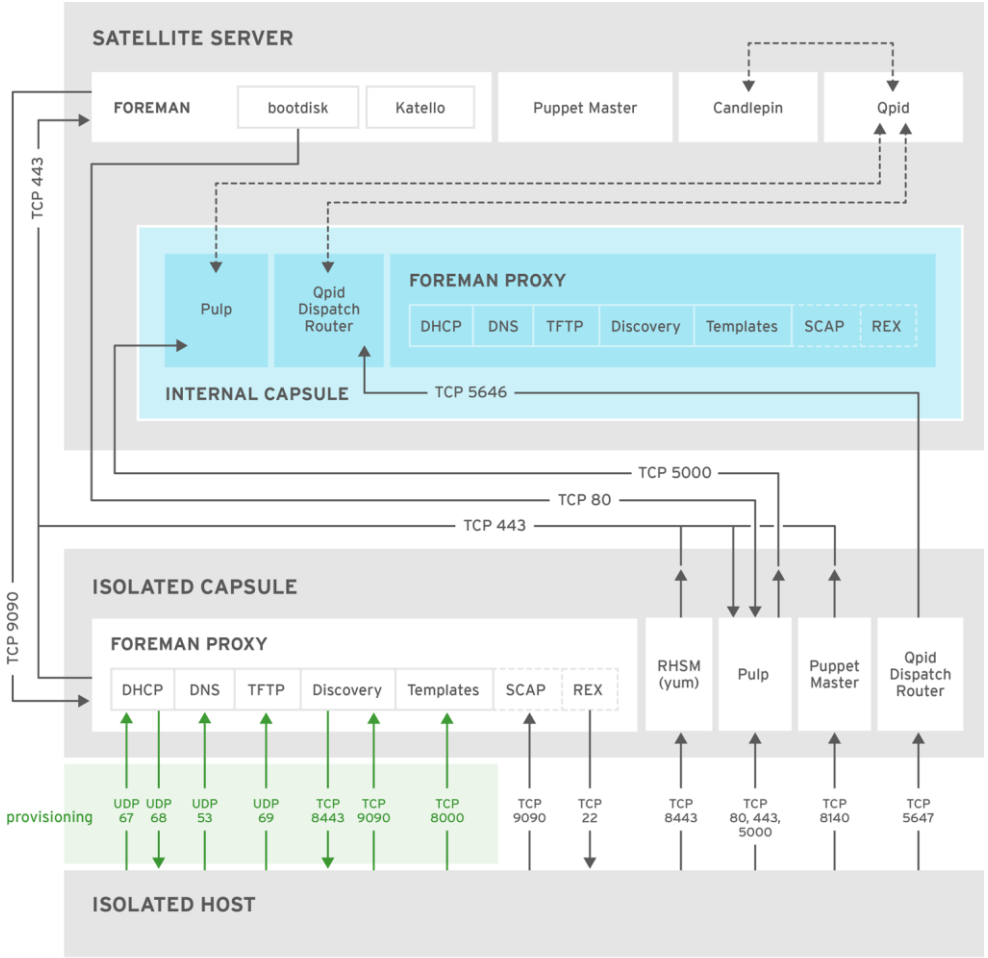


Errata

- Installation einzelner Errata auf alle Hosts die betroffen sind
- Erweitern bestehender Content Views

RHBA-2017:3203	sos bug fix update	Bug Fix Advisory - None	8 Applicable, 1 Installable	11/14/17
RHBA-2017:3201	nfs-utils bug fix update	Bug Fix Advisory - None	7 Applicable, 1 Installable	11/14/17
RHBA-2017:3197	kexec-tools bug fix update	Bug Fix Advisory - None	8 Applicable, 1 Installable	11/14/17
RHBA-2017:3205	ksh bug fix update	Bug Fix Advisory - None	1 Applicable, 1 Installable	11/14/17
RHBA-2017:3202	autofs bug fix update	Bug Fix Advisory - None	4 Applicable, 1 Installable	11/14/17
RHBA-2017:3199	device-mapper-multipath bug fix update	Bug Fix Advisory - None	8 Applicable, 1 Installable	11/14/17

Capsule



Quelle: https://access.redhat.com/documentation/en-us/red_hat_satellite/6.2/html-single/architecture_guide/index

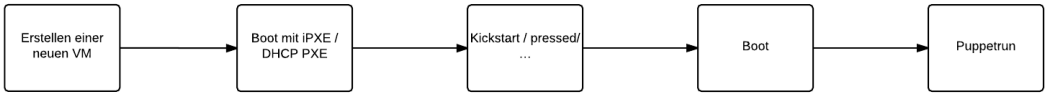
SATELLITE_439131_0317

6

Provisionierung

Compute Resources

- Große Zahl an Virtualisierungsumgebungen unterstützt
- VMware, openStack, …
- VM Verwaltung in Foreman direkt
- Consolenzugriff im Foreman (via Plugin)



Provisionierung

- Provisionierung auf Basis von Templates
- Dns, dhcp, pxe mittels Smart Proxies
- Discovery von Hardware
- Boot auch mit Bootdisk ohne DHCP möglich

```
# This template is rendered for use inside a host-specific boot disk.
#
# Copy this template to customize it, the original is read-only.

<%
interface = @host.provision_interface
bootdisk_raise(N_('Host has no provisioning interface defined')) unless interface
bootdisk_raise(N_('Host has no IP address defined')) if interface.ip.nil? || interface.ip.empty?
bootdisk_raise(N_('Host has no subnet defined')) unless interface.subnet
bootdisk_raise(N_('Host has no domain defined')) unless interface.domain
bootdisk_raise(N_('Subnet (%s) has no gateway defined'), interface.subnet) if interface.subnet.gateway.n
bootdisk_raise(N_('Subnet (%s) has no primary DNS server defined'), interface.subnet) if interface.subnet
%>

echo Foreman Bootdisk: Host image (<%= @host.name %>)

# loop over net* until the host's MAC matches
<% (0..32).each do |i| -%>
:net<%= i %>
isset ${net<%= i -%>/mac} || goto no_nic
echo net<%= i -%> is a ${net<%= i -%>/chip} with MAC ${net<%= i -%>/mac}
iseq ${net<%= i -%>/mac} <%= interface.mac -%> || goto net<%= i+1 %>
```

```
selinux --<%= @host.params['selinux-mode'] || @host.params['selinux'] || 'enforcing' %>
keyboard <%= @host.params['keyboard'] || 'us' %>
skipx

<% subnet = @host.subnet -%>
<% if subnet.respond_to?(:dhcp_boot_mode?) -%>
<% dhcp = subnet.dhcp_boot_mode? && !@static -%>
<% else -%>
<% dhcp = !@static -%>
<% end -%>
network --bootproto <%= dhcp ? 'dhcp' : "static --ip=#{@host.ip} --netmask=#{subnet.mask} --gateway=#{subnet.gateway} --nameserver=#{[subnet.dns

rootpw --iscrypted <%= root_pass %>
<% if @host.param_true?('disable-firewall') -%>
firewall --disable
<% else -%>
firewall --<%= os_major >= 6 ? 'service=' : '' %>ssh
<% end -%>
authconfig --useshadow --passalgo=<%= @host.operatingsystem.password_hash || 'sha256' %> --kickstart
timezone --utc <%= @host.params['time-zone'] || 'UTC' %>
<% if rhel_compatible -%>
services --disabled gpm,sendmail,cups,pcmcia,isdn,rawdevices,hpoj,bluetooth,openibd,avahi-daemon,avahi-dnsconfd,hidd,hplip,pcscd
```

7

Herausforderungen auf dem Weg

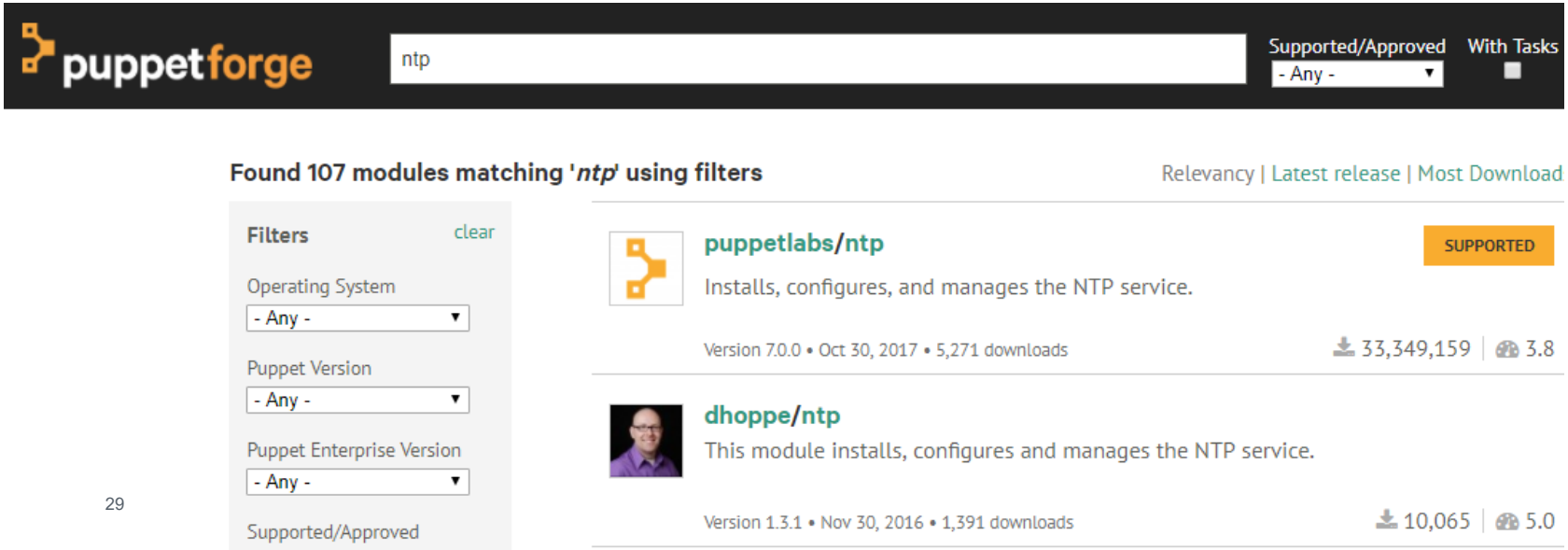
Herausforderungen

- Systemmanagement → Entwickler
- Puppet Code statt der Shell

```
case $operatingsystem {
  centos, redhat: { $service_name = 'ntpd' }
  debian, ubuntu: { $service_name = 'ntp' }
}

package { 'ntp':
  ensure => installed,
}

service { 'ntp':
  name      => $service_name,
  ensure    => running,
  enable    => true,
  subscribe => File['ntp.conf'],
}

file { 'ntp.conf':
  path    => '/etc/ntp.conf',
  ensure  => file,
  require => Package['ntp'],
  source  => "puppet:///modules/ntp/ntp.conf",
  # This source file would be located on the Puppet master at
  # /etc/puppetlabs/code/modules/ntp/files/ntp.conf
```

Herausforderungen

- Systemmanagement → Entwickler
- Puppet Code statt der Shell
- Versionsverwaltung
- Puppet-Module



Herausforderungen

- Systemmanagement → Entwickler
- Puppet Code statt der Shell
- Versionsverwaltung
- Puppet-Module
- Migration von ~600 Servern im laufenden Betrieb
- Große Anzahl an unterstützen Derivaten und Versionen
- Migration von Puppet 3 auf 4 bzw. 5

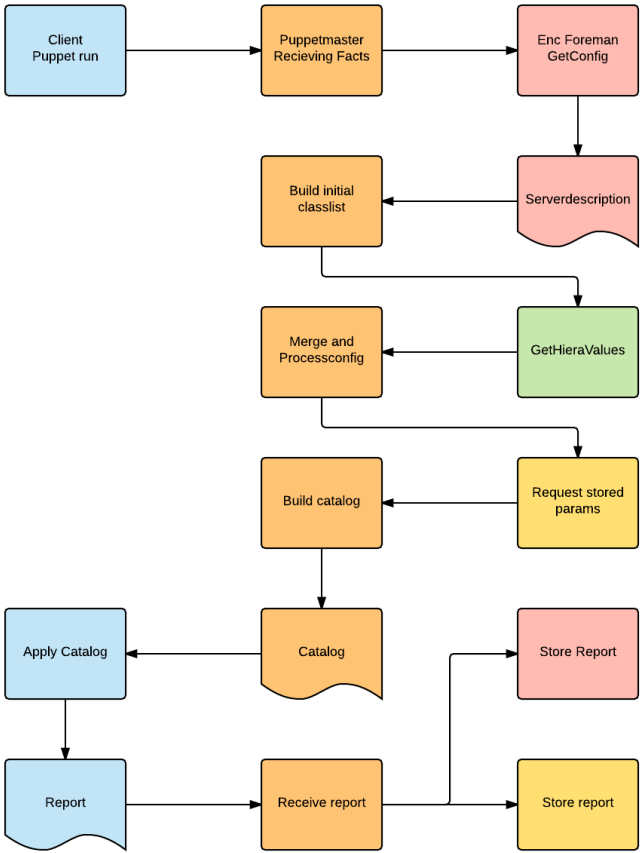
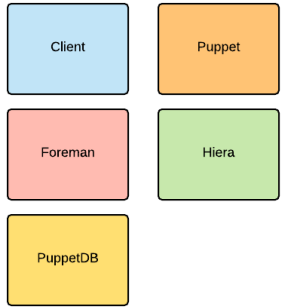
Schmerzen…

- Support „alter“ OS Versionen
- Parameter in Hiera & Klassen in Foreman
- Upgrade von Modulen bzw. Module und ihre Wartung
  - Support neuer OS Versionen
  - Abwärtskompatibilität
  - Updates
- Stressfaktor Update

Vielen Dank für Ihre Aufmerksamkeit!

+43 1 36060-6432
lukas.plattner@apa.at
www.apa-it.at

Ablauf Puppetrun



Legende