Inhaltsverzeichnis

Meta

Vox Pupuli - OpenSource Kollektiv

- Vox Pupuli
- OpenVox
- Weg vorwärts

OpenVox/Puppet - technische Grundlagen

- Zielstellung
- DSL
- Architektur

1001 Hiera: Klasse zuweisen

- meta
- site.pp
- ENC

3-Teiler

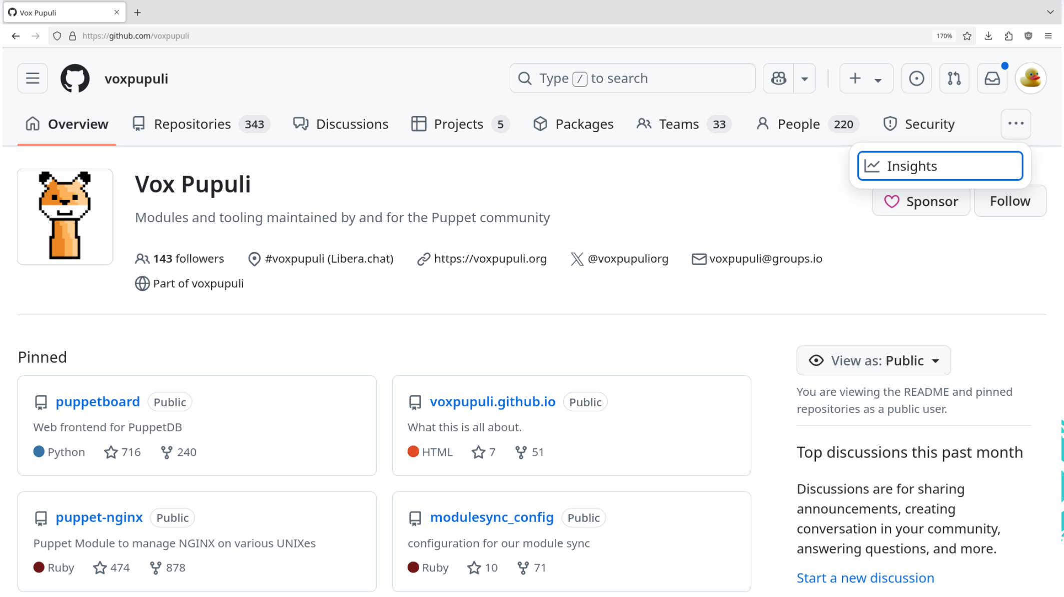
- 3 Vorträge
- Komplexität: Henne-Ei-Problem Verständnis

Interessenskonflikt

- OpenSource Kollektiv
- hauptberuflich

Gründung

- Admins + Klein-Teams
- Code-Entwicklung garantieren



Vox Pupuli

Modules and tooling maintained by and for the Puppet community

143 followers #voxpupuli (Libera.chat) https://voxpupuli.org @voxpupuliorg voxpupuli@groups.io

Part of voxpupuli

Pinned

Repository	Description	Language	Stars	Forks
puppetboard Public	Web frontend for PuppetDB	Python	716	240
voxpupuli.github.io Public	What this is all about.	HTML	7	51
puppet-nginx Public	Puppet Module to manage NGINX on various UNIXes	Ruby	474	878
modulesync_config Public	configuration for our module sync	Ruby	10	71

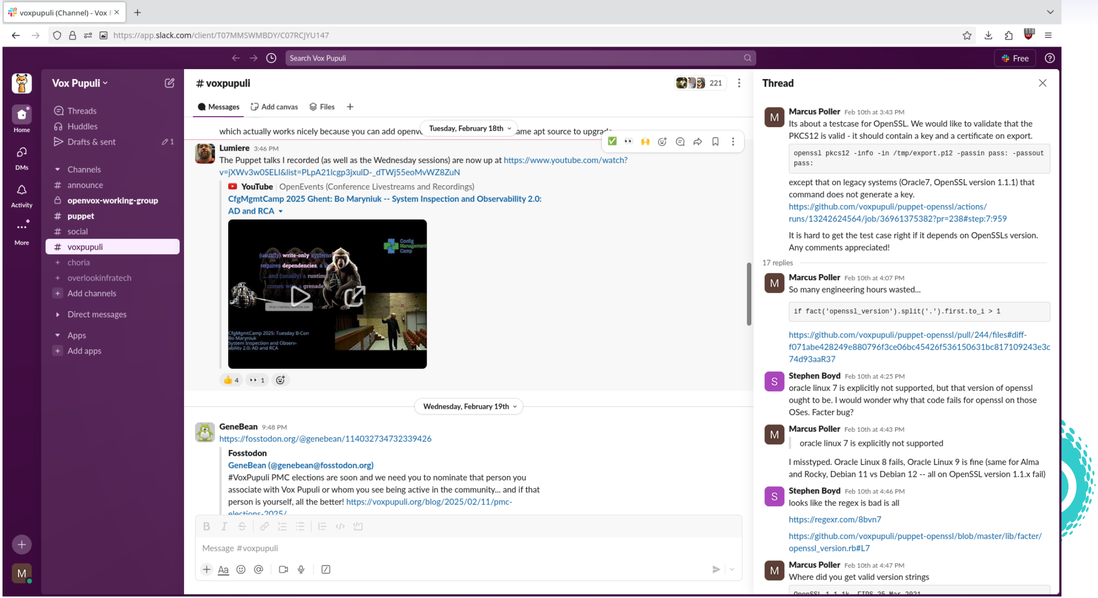
View as: Public

You are viewing the README and pinned repositories as a public user.

Top discussions this past month

Discussions are for sharing announcements, creating conversation in your community, answering questions, and more.

Start a new discussion



which actually works nicely because you can add openv… Tuesday, February 18th …ame apt source to upgrad…

Lumiere 3:46 PM
The Puppet talks I recorded (as well as the Wednesday sessions) are now up at https://www.youtube.com/watch?v=jXWv3w0SELI&list=PLpA21Icgp3jxulD-_dTWj55eoMvWZ8ZuN

YouTube | OpenEvents (Conference Livestreams and Recordings)
CfgMgmtCamp 2025 Ghent: Bo Maryniuk -- System Inspection and Observability 2.0: AD and RCA

👍 4 👀 1

Wednesday, February 19th

GeneBean 9:48 PM
https://fosstodon.org/@genebean/114032734732339426

Fosstodon
GeneBean (@genebean@fosstodon.org)
#VoxPupuli PMC elections are soon and we need you to nominate that person you associate with Vox Pupuli or whom you see being active in the community... and if that person is yourself, all the better! https://voxpupuli.org/blog/2025/02/11/pmc-elections-2025/

Thread

Marcus Poller Feb 10th at 3:43 PM
Its about a testcase for OpenSSL. We would like to validate that the PKCS12 is valid - it should contain a key and a certificate on export.

```
openssl pkcs12 -info -in /tmp/export.p12 -passin pass: -passout pass:
```

except that on legacy systems (Oracle7, OpenSSL version 1.1.1) that command does not generate a key.
https://github.com/voxpupuli/puppet-openssl/actions/runs/13242624564/job/36961375382?pr=238#step:7:959

It is hard to get the test case right if it depends on OpenSSLs version. Any comments appreciated!

17 replies

Marcus Poller Feb 10th at 4:07 PM
So many engineering hours wasted...

```
if fact('openssl_version').split('.').first.to_i > 1
```

https://github.com/voxpupuli/puppet-openssl/pull/244/files#diff-f071abe428249e880796f3ce06bc45426f536150631bc817109243e3c74d93aaR37

Stephen Boyd Feb 10th at 4:25 PM
oracle linux 7 is explicitly not supported, but that version of openssl ought to be. I would wonder why that code fails for openssl on those OSes. Facter bug?

Marcus Poller Feb 10th at 4:43 PM
> oracle linux 7 is explicitly not supported

I misstyped. Oracle Linux 8 fails, Oracle Linux 9 is fine (same for Alma and Rocky, Debian 11 vs Debian 12 -- all on OpenSSL version 1.1.x fail)

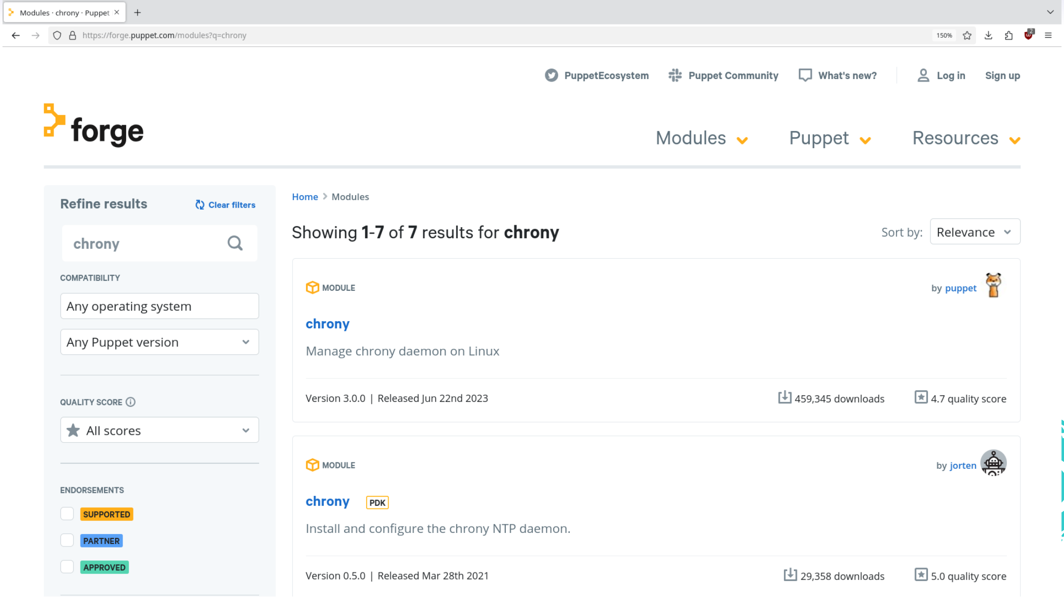
Stephen Boyd Feb 10th at 4:46 PM
looks like the regex is bad is all

https://regexr.com/8bvn7

https://github.com/voxpupuli/puppet-openssl/blob/master/lib/facter/openssl_version.rb#L7

Marcus Poller Feb 10th at 4:47 PM
Where did you get valid version strings

```
OpenSSL 1.1.1k  FIPS 25 Mar 2021
```



Refine results

Clear filters

chrony

COMPATIBILITY

Any operating system

Any Puppet version

QUALITY SCORE

All scores

ENDORSEMENTS

□ SUPPORTED

□ PARTNER

□ APPROVED

Home > Modules

Showing **1-7** of **7** results for **chrony**

Sort by: Relevance

MODULE

by puppet

chrony

Manage chrony daemon on Linux

Version 3.0.0 | Released Jun 22nd 2023

459,345 downloads

4.7 quality score

MODULE

by jorten

chrony PDK

Install and configure the chrony NTP daemon.

Version 0.5.0 | Released Mar 28th 2021

29,358 downloads

5.0 quality score

OpenVox

- Fork Puppet-Opensource

Es war einmal...

- Puppet-Conf – Entwickler treffen
- Zugriff Bugtracker
- Puppetlabs-Entwickler jeden Freitag Zeit

dann hat dreimal der CEO gewechselt und Puppetlabs wurde aufgekauft
... und ein Blogpost und ein Community-Telefonat

- keine Debian-Pakete mehr
- keine Namensrechte
- kein Puppet-Open-Source mehr
- eine EULA

Weg vorwärts

- ✓ Debianpakete `https://apt.overlookinfratech.com/`
- ✓ Container `https://github.com/OpenVoxProject/container-openvoxserver`
- □ Dokumentation → Onboarding
- □ Openvox-Conf Berlin
- □ Openvox-Conf Boston
- □ NL-Funding

Zielstellung

- Rechenzentrumsbetrieb / Hyperscaler
- Anwendungsfall 20.000 VMs - Selbstbedieninterface
- Infrastructure as Code
- Auditierfähig

Domain Specific Language

- Ressourcen (Klassen und Module)
- Ruby-Abstraktion

DSL-Einführung: Resourcen

- `puppet resource user`
- `puppet describe user`

Idempotenz

Zielzustandsbeschreibung

- `puppet apply`

vgl. RedHat Kickstart

mehr Ressourcen

- `package`
- `file` - source: fileserver, modul, dateisystem, array, refresh-events, templating Embedded Puppet Templates, Embedded Ruby Templates
- `service`

Module 1 - VoxPupuli Chrony Code

`https://github.com/voxpupuli/puppet-chrony`

Module 2 - VoxPupuli Chrony benutzen

-
  ```
  dnf erase chrony
  ```

-
  ```
  puppet module install puppetlabs-chrony
  ```

-
  ```
  puppet apply chrony.pp --show_diff
  ```

Wiederholung 1

Ressourcen

- `package`
- `file`
- `service`

werden gebündelt zu

- `class`
- Module

Es ist klar, was wir auf die SSD schreiben wollen. Jetzt fehlen noch die Daten.

Anpassungen - Daten

- `facter` / `puppet facts`
- trusted CSR-Attributes `https://www.puppet.com/docs/puppet/7/ssl_attributes_extensions#ssl_attributes_extensions`
- External Node Classifier (ENC)

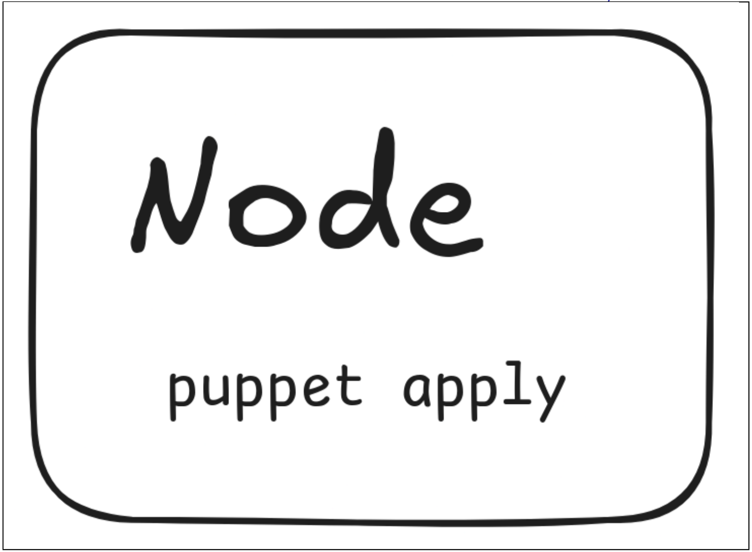
Endzustand BigCorp

- Hosts Inventardatenbank
- Inventardatenbank mit Zielzustand (ENC)
- eingebundene Module an Firmenstandards angepasst
- Bsp. Zugriffsmanagement - LDAP, oder SSH-Keyverteilung
- Bsp. Lizenzzähler - Port-Scanner Oracledatenbanken
- Bsp. ComplianceFramework - Linux Kernel IPv4 Routing
- Bsp. ComplianceFramework - /tmp hat noxec
- Bsp. DNS pro Rechenzentrum
- Bsp. NTP mit Stratum pro Rechenzentrum

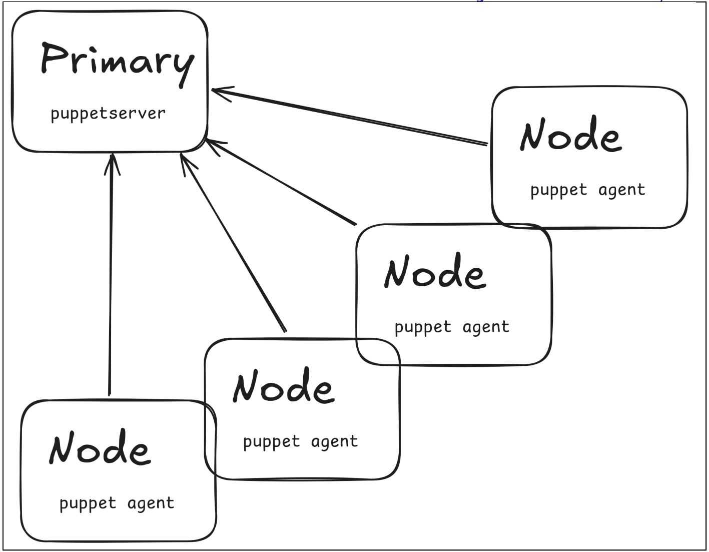
Ende des Software-Teiles

Architektur der Umgebungen

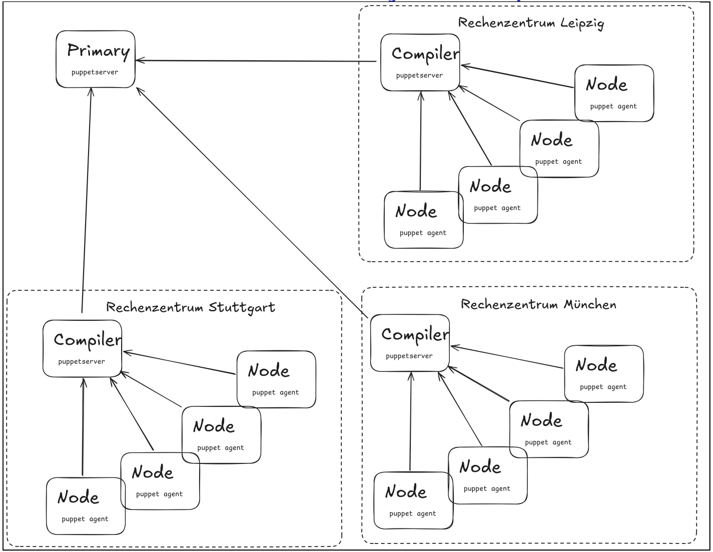
Serverless 1/3



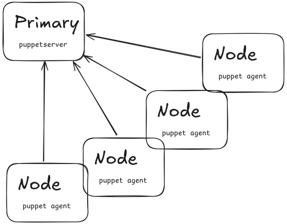
Primary - Nodes 2/3



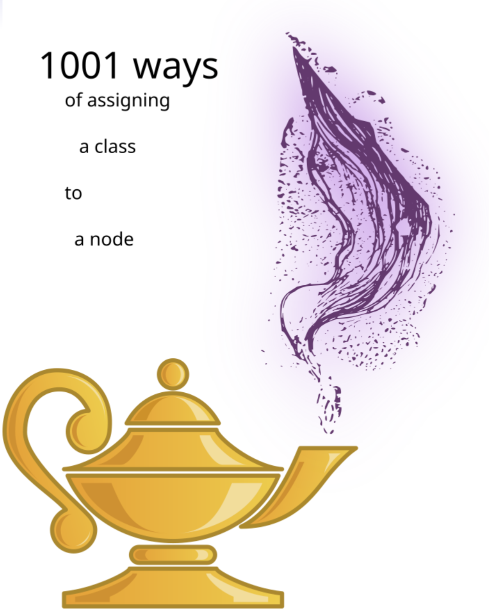
Primary - Compiler - Nodes 3/3



Vorstellung der Umgebung



- Architektur
- `puppet query` + facts
- `puppet agent --environment`



1001 ways

of assigning

a class

to

a node

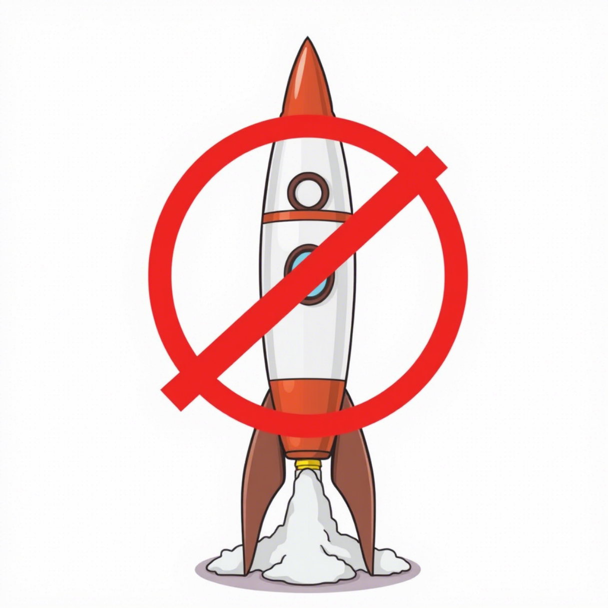
table of contents

`manifests/site.pp`

- `node{}`
- `lookup()`

External Node Classifiers

- Puppet Enterprise Web Console
- Foreman External Node Classifier



negative table of contents

- hiera intro Martin Alfke: Why does that node have that config,

  `https://dev.to/betadots/modern-puppet-node-classification-3ngk`
- puppet intro
- eyaml
- setup many teams
- setup many repositories
- setup access permissions

pattern

- present a piece of code
- articulate my experience with it

site.pp Puppet Doc style

```
node foo.bar.de {
  include bar
}
node baz.bar.de {
  include baz
}
node foo {
  inlude bar
}
node /./ {
  include companydefault
}
node /webserver/ {
  include webserer
}
```

`hiera` crash course 1/2 – automatic data binding

'hiera.yaml'

```
- name: "what's in a name?"
  paths:
    - common.yaml
```

'data/common.yaml'

```
---
profile::foo::bar: 1337
```

'modules/profile/manifests/foo.pp'

```
class profile::foo (
  $bar
){}
```

site.pp chain loading

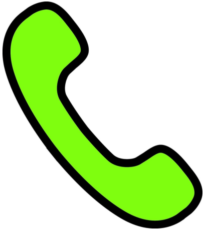
'site.pp'

```
include chainloader
```

'manifests/chainloader.pp'

```
class chainloader(
  $network_class = ’companystd::network’
){
  if $network_class && $network_class != ’disabled’ {
    include $network_class
  }
}
```

Story of Peter



`site.pp` crash course

where the magic begins

- `node` only for educational purposes
- any puppet code
- each node
- at beginning of puppet run

'/etc/puppetlabs/puppet/ssl/csr_attributes.yaml'

```
---
extension_requests:
    pp_role: webserver
```

'manifests/site.pp'

```
contain "role::${trusted.extensions.pp_role}"
```

- OID mapping `https://www.puppet.com/docs/puppet/8/config_file_csr_attributes.html`
- roles+profiles pattern

hiera crash course 2/2 – lookup()

- poors mans automatic data binding
- harder to mentally follow

'manifests/site.pp'

```
class_list=lookup('classes', Array[String], 'unique', '[]')
class_list.each |$c| {
  contain $c
}
```

`lookup()` in context – recap

```
nodes/foo.domain.yaml
  classes:
    - profile::dns
    - profile::ntp
datacenter/munich.yaml
  profile::ntp::server: ’10.0.0.1’
  classes:
    - profile::backup
common.yaml
  classes:
    - profile::companystd
```

`knockout_prefix` does not work

`site.pp` recap

- `node`
- chainloader with default classes
- chainloader by `trusted::extenions::pp_role`
- `lookup().include`

`lookup()` reloaded

- What if `classes:` was a nested data structure instead of an array?
- What if we would do class ordering?

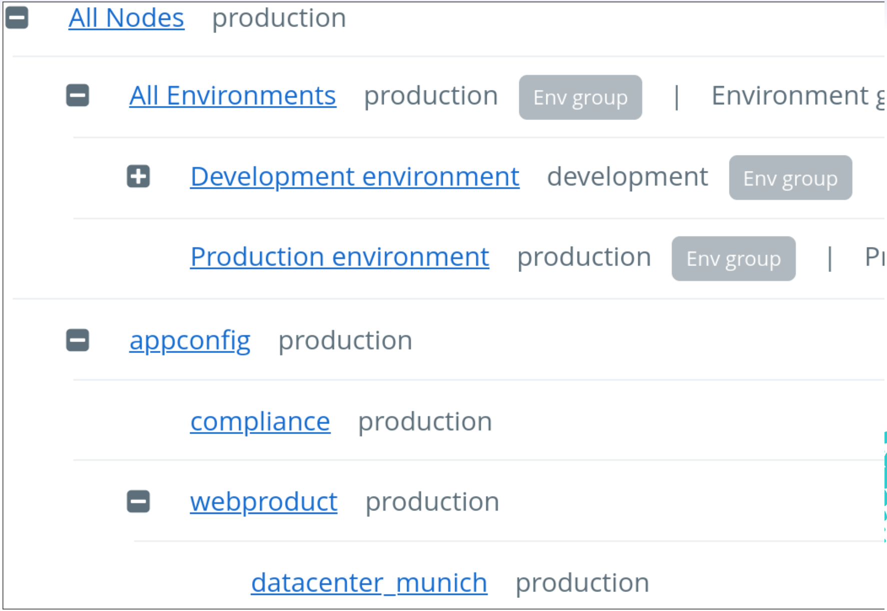
'common.yaml'

```
---
classes:
  - 10_dns
  - 10_ntp
  - 99_app
  - 50_firewall
```

External Node Classifier – ENC

scope as `site.pp`

- top scope variables
- classes
- automatic data binding
- node to environments



⊟ All Nodes production

⊟ All Environments production Env group | Environment g

⊞ Development environment development Env group

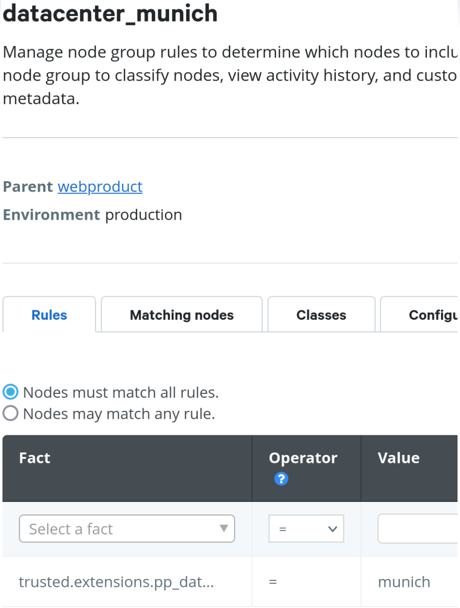
Production environment production Env group | Pr

⊟ appconfig production

compliance production

⊟ webproduct production

datacenter_munich production



datacenter_munich

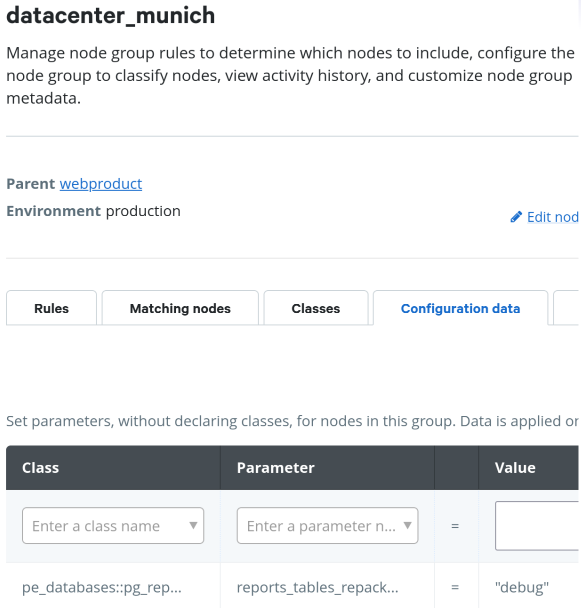
Manage node group rules to determine which nodes to inclu node group to classify nodes, view activity history, and custo metadata.

Parent webproduct

Environment production

● Nodes must match all rules.
○ Nodes may match any rule.

Fact	Operator ?	Value
Select a fact ▾	= ⌄	
trusted.extensions.pp_dat...	=	munich



datacenter_munich

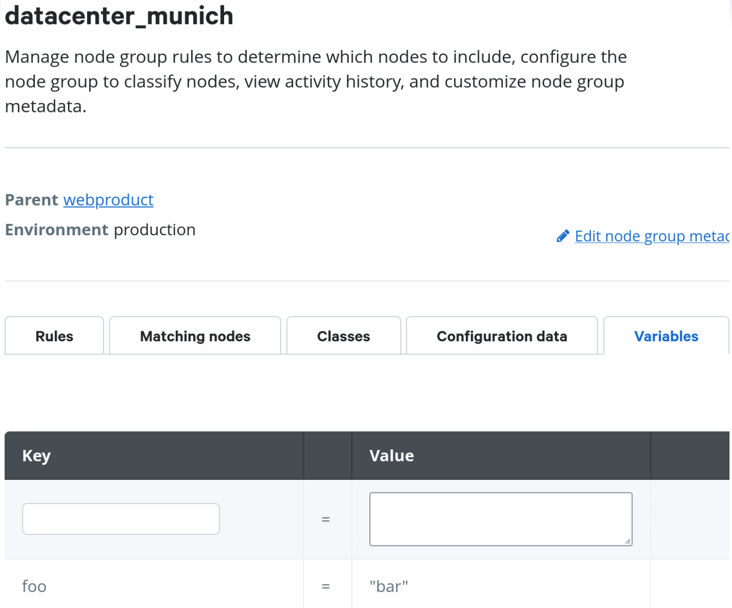
Manage node group rules to determine which nodes to include, configure the node group to classify nodes, view activity history, and customize node group metadata.

Parent webproduct

Environment production

Set parameters, without declaring classes, for nodes in this group. Data is applied or

Class	Parameter		Value
Enter a class name ▼	Enter a parameter n... ▼	=	
pe_databases::pg_rep...	reports_tables_repack...	=	"debug"



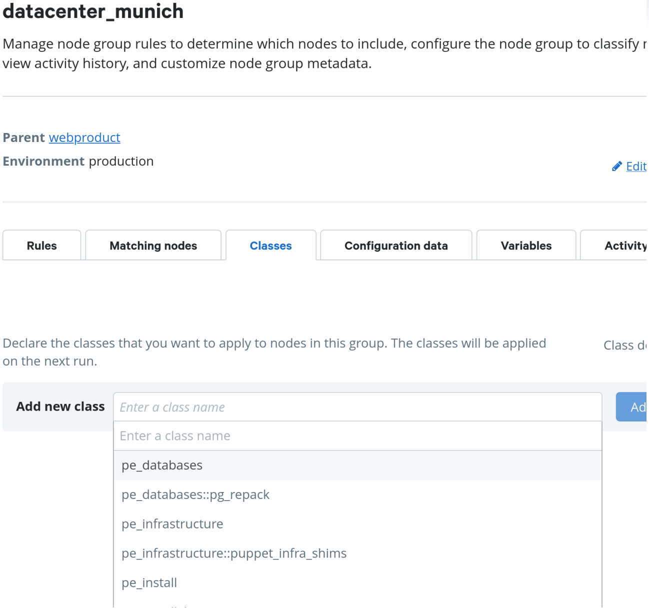
datacenter_munich

Manage node group rules to determine which nodes to include, configure the node group to classify nodes, view activity history, and customize node group metadata.

Parent webproduct

Environment production

Key		Value
	=	
foo	=	"bar"



datacenter_munich

Manage node group rules to determine which nodes to include, configure the node group to classify r
view activity history, and customize node group metadata.

Parent webproduct

Environment production

Declare the classes that you want to apply to nodes in this group. The classes will be applied on the next run.

Class d

Add new class *Enter a class name*

Enter a class name

pe_databases
pe_databases::pg_repack
pe_infrastructure
pe_infrastructure::puppet_infra_shims
pe_install

ENC story – Alex

- could you update `monitoring.conf` on my machines?
- sure. How do I find them?
- by datacenter. Munich, Berlin, Frankfurt
- there are 4.000 hosts. Are you sure?
- Noooo!
- Can you provide me a list of FQDNs?
- here you are

```
host1.example.com
host2.example.com
...
host2000.example.com
```

ENC story – Alex

```
host1.example.com
host2.example.com
...
host2000.example.com
```

- how to input?
- RegEx!

-
  ```
  (host1.example.com|host2.example.com|...|host2000.example.c
  ```
- it is called *certificate pinning*

ENC story – Alex

- problem solved!
- database down

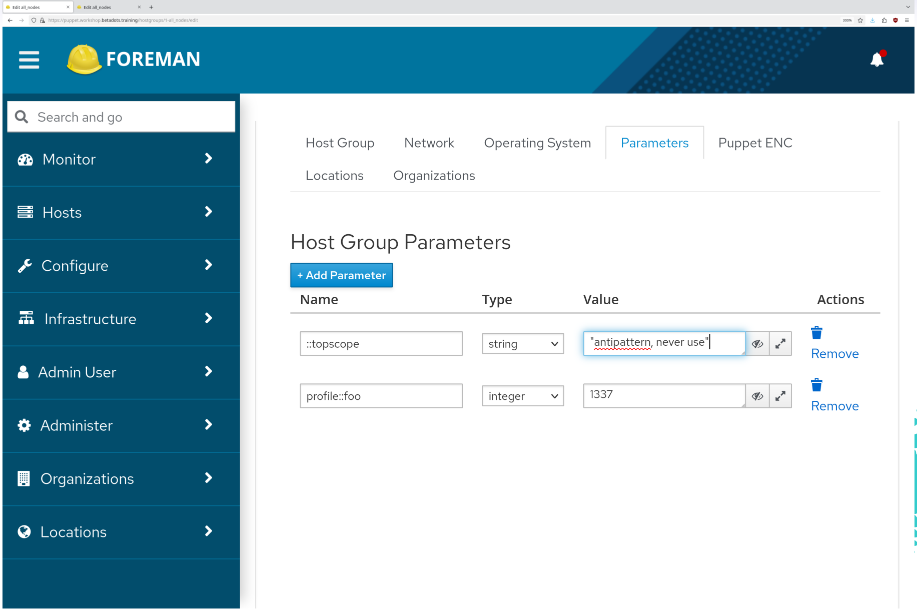
We use postgres.

We transform PQL.
We do not optimize.
Expect the spinner.

ENC RegEx story - Bernd

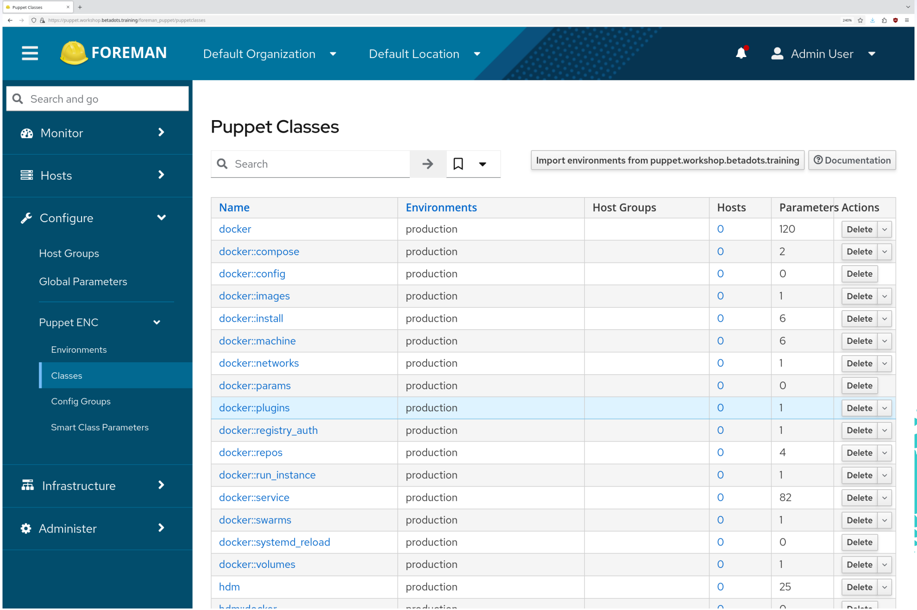
- special snowflake
- oncall 20:00
- *it is your automation system that broke our production service, all SSH-keys are gone, machine to machine communication destroyed, now you tell us why!*
- ...
- What if somebody had renamed those machines?
- Why are those called `ip` ?
-

```
for myhost in foo{00..40}; do ssh $myhost ’hostname -f ip -4 a s’; don
```



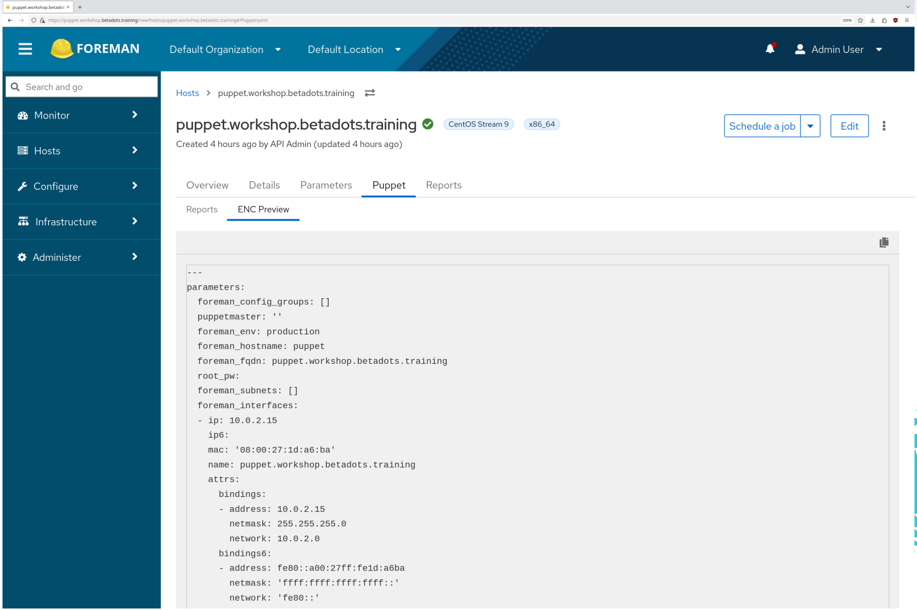
Host Group Parameters

Name	Type	Value	Actions
::topscope	string	"antipattern, never use"	Remove
profile::foo	integer	1337	Remove



Puppet Classes

Name	Environments	Host Groups	Hosts	Parameters	Actions
docker	production		0	120	Delete
docker::compose	production		0	2	Delete
docker::config	production		0	0	Delete
docker::images	production		0	1	Delete
docker::install	production		0	6	Delete
docker::machine	production		0	6	Delete
docker::networks	production		0	1	Delete
docker::params	production		0	0	Delete
docker::plugins	production		0	1	Delete
docker::registry_auth	production		0	1	Delete
docker::repos	production		0	4	Delete
docker::run_instance	production		0	1	Delete
docker::service	production		0	82	Delete
docker::swarms	production		0	1	Delete
docker::systemd_reload	production		0	0	Delete
docker::volumes	production		0	1	Delete
hdm	production		0	25	Delete
hdm::docker	production		0	0	Delete



puppet.workshop.betadots.training ✓ CentOS Stream 9 x86_64

Created 4 hours ago by API Admin (updated 4 hours ago)

```
---
parameters:
  foreman_config_groups: []
  puppetmaster: ''
  foreman_env: production
  foreman_hostname: puppet
  foreman_fqdn: puppet.workshop.betadots.training
  root_pw:
  foreman_subnets: []
  foreman_interfaces:
  - ip: 10.0.2.15
    ip6:
    mac: '08:00:27:1d:a6:ba'
    name: puppet.workshop.betadots.training
    attrs:
      bindings:
      - address: 10.0.2.15
        netmask: 255.255.255.0
        network: 10.0.2.0
      bindings6:
      - address: fe80::a00:27ff:fe1d:a6ba
        netmask: 'ffff:ffff:ffff:ffff::'
        network: 'fe80::'
```

Foreman Hostsgroups - one host, one group

https://github.com/betadots/foreman-training/tree/main/03_configmanagement#variante-2-default-host-group-plugin

Fragen