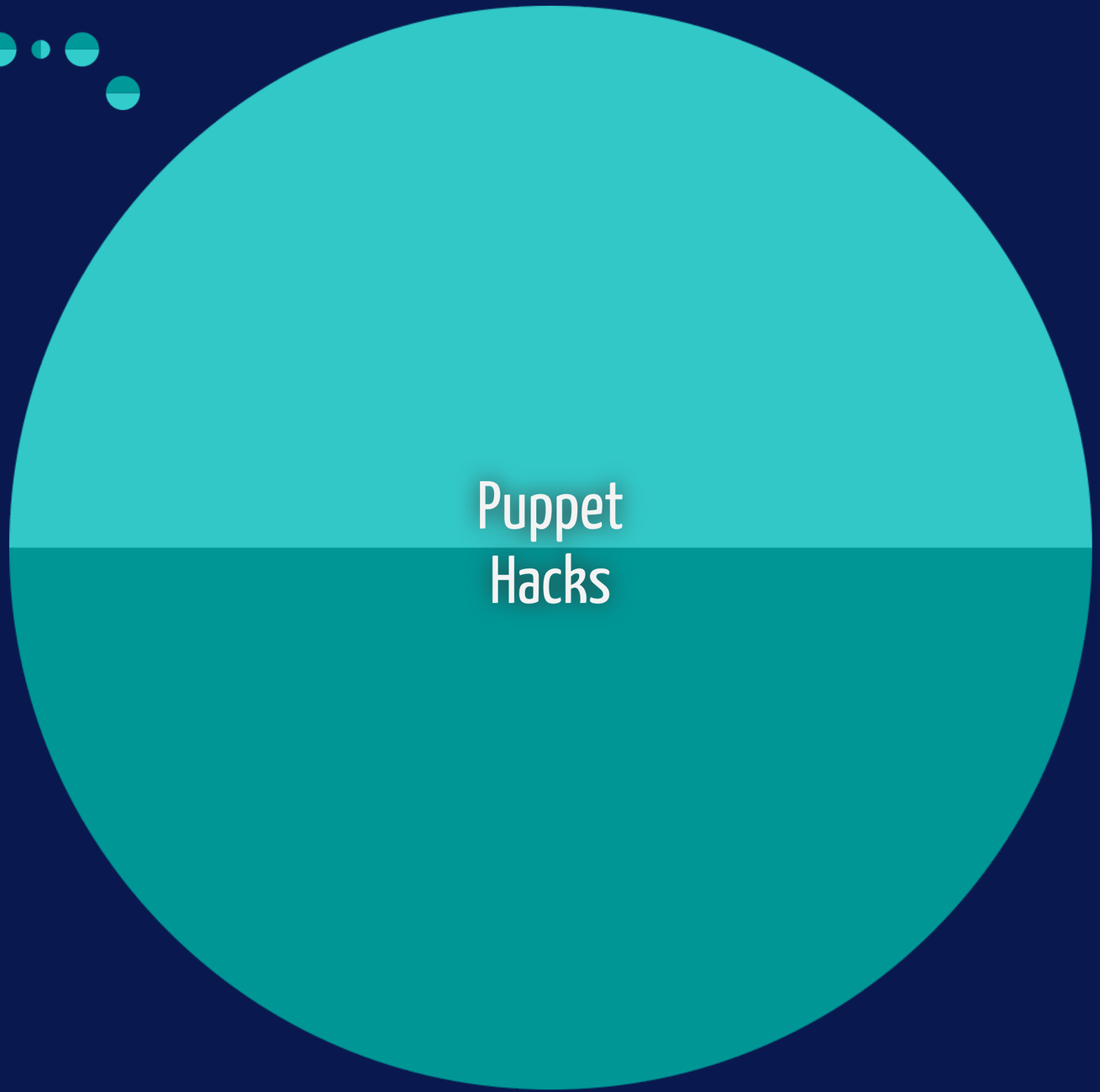
beladels



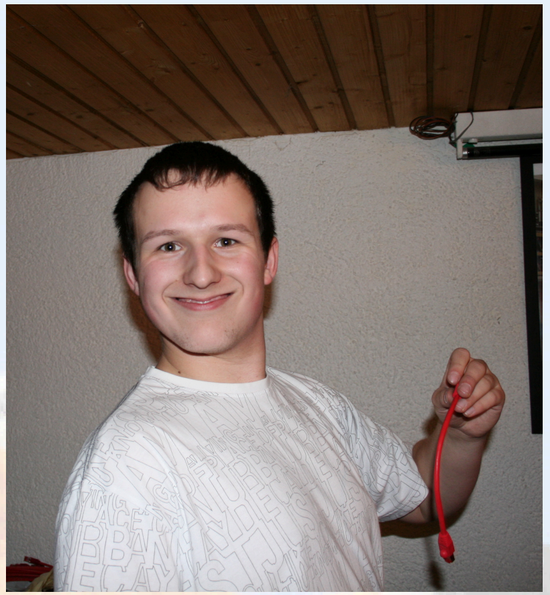
beladels

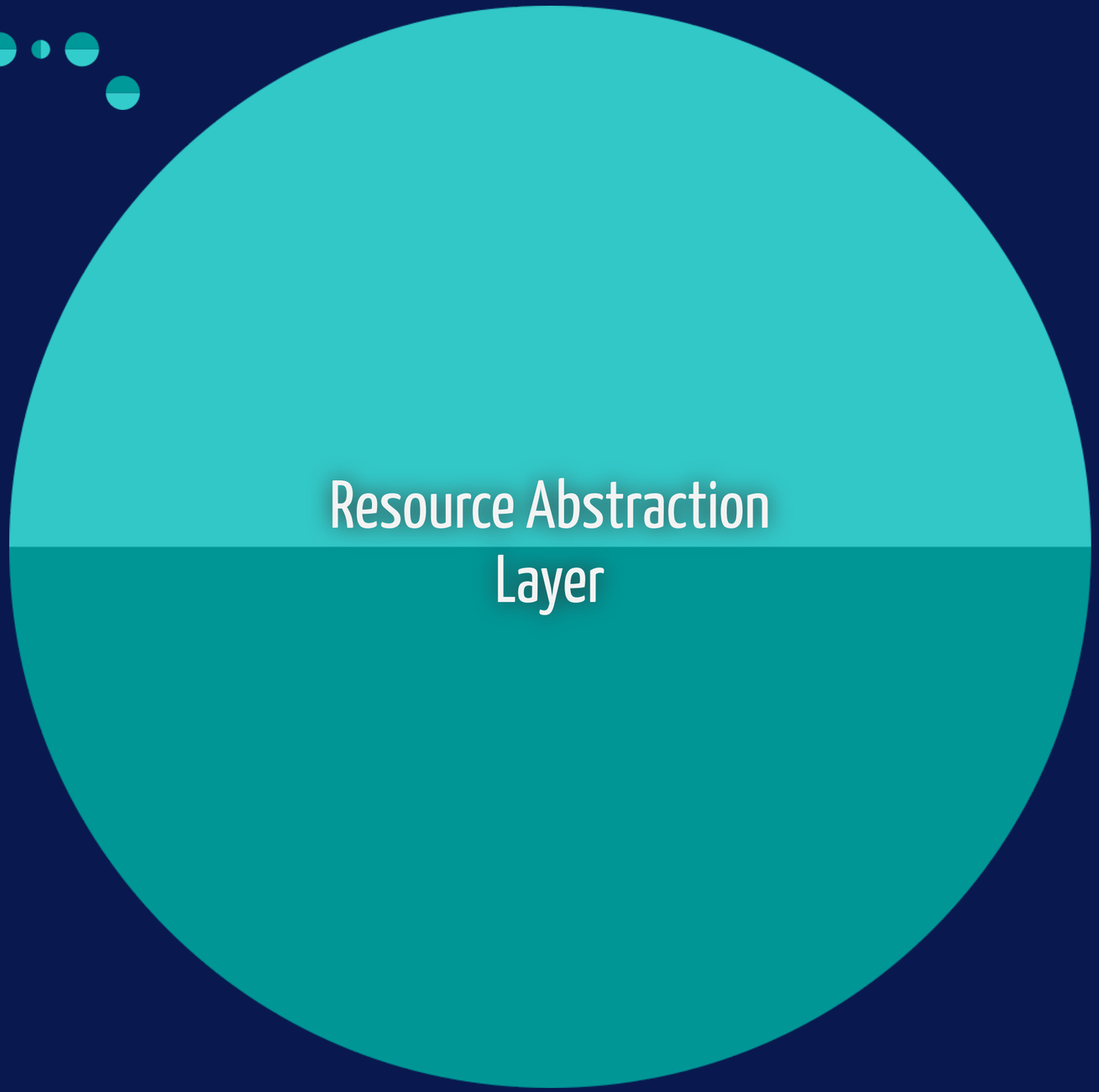
Puppet Hacks

you didn't know you were looking for

$ whoami

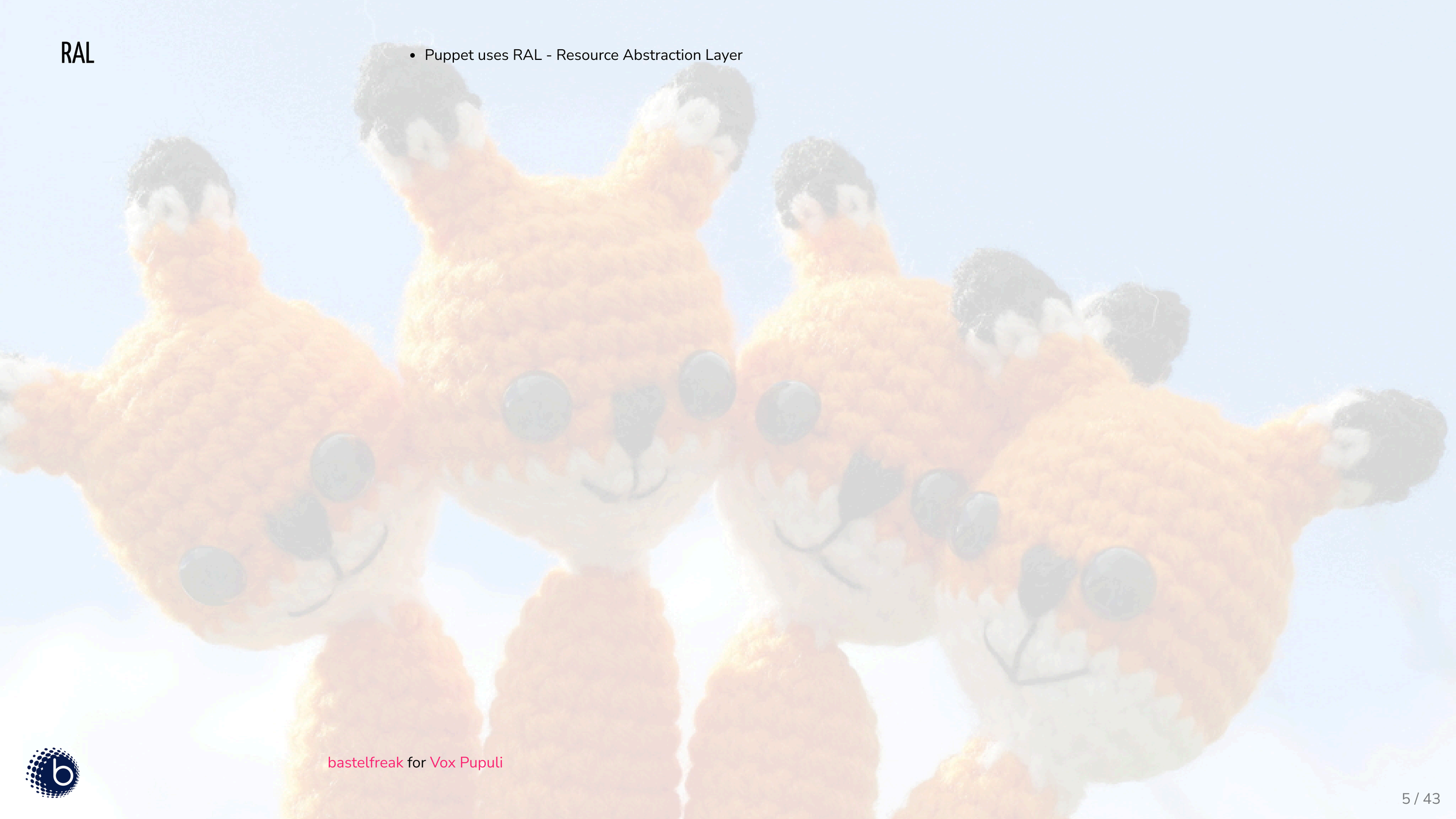
- Tim 'bastelfreak' Meusel
- Puppet Contributor since 2012
- Merging stuff on Vox Pupuli (Puppet Community) since 2015
- Vox Pupuli Project Management Committee member
- Senior IT Automation Consultant at betadots




Resource Abstraction
Layer

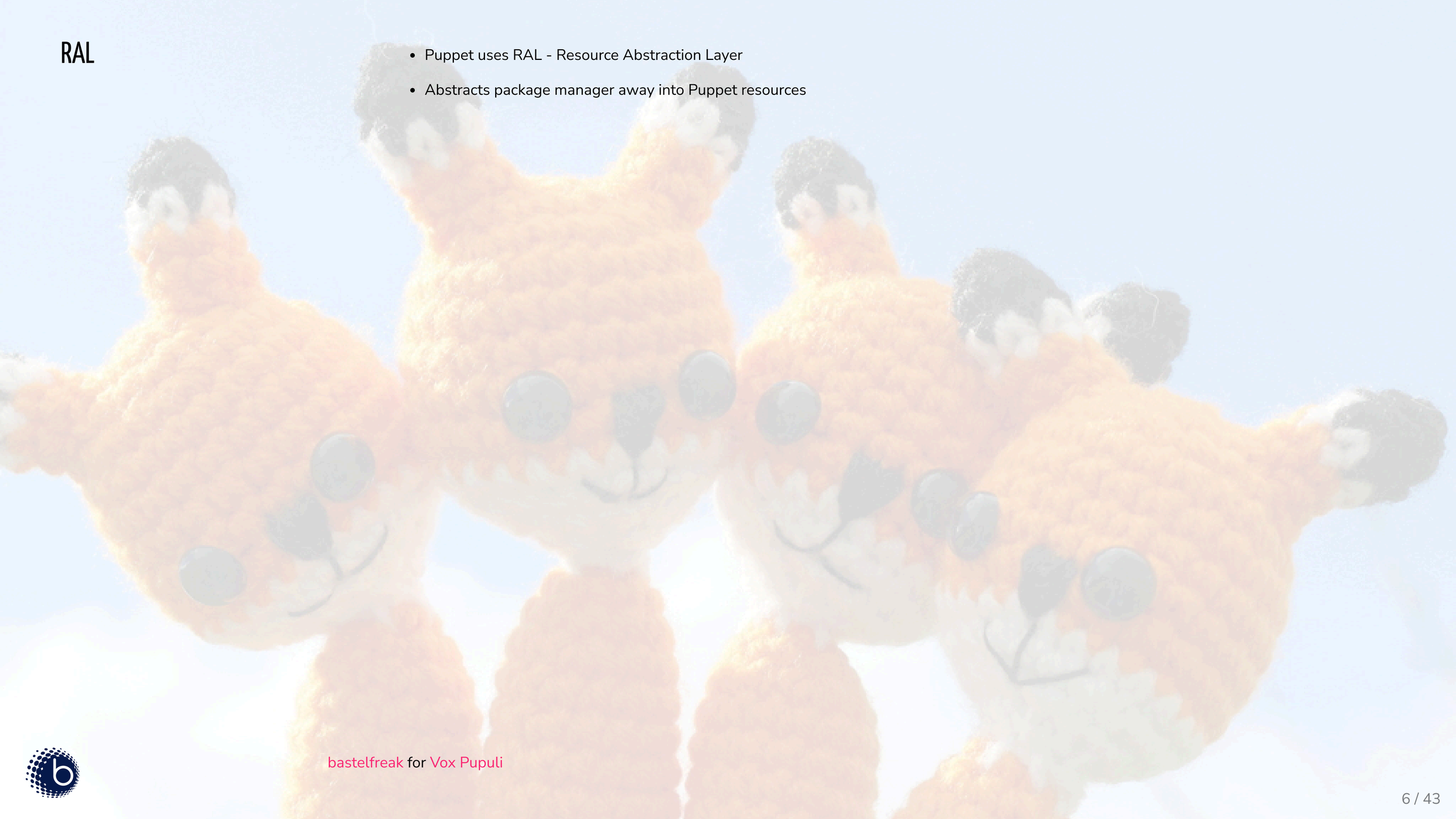
RAL

- Puppet uses RAL - Resource Abstraction Layer



RAL

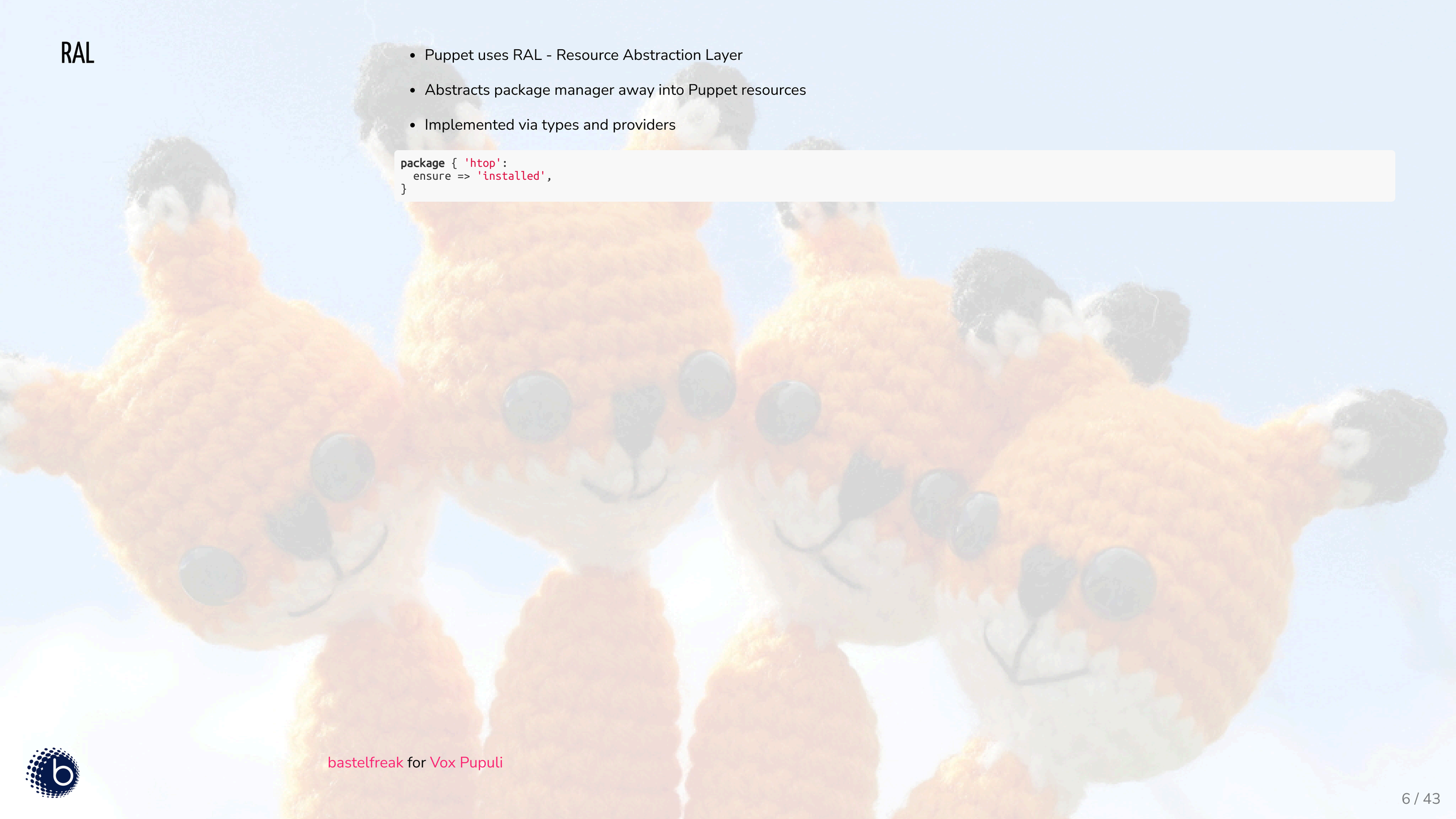
- Puppet uses RAL - Resource Abstraction Layer
- Abstracts package manager away into Puppet resources



RAL

- Puppet uses RAL - Resource Abstraction Layer
- Abstracts package manager away into Puppet resources
- Implemented via types and providers

```
package { 'htop':
  ensure => 'installed',
}
```



RAL

- Puppet uses RAL - Resource Abstraction Layer
- Abstracts package manager away into Puppet resources
- Implemented via types and providers

```
package { 'htop':
  ensure => 'installed',
}
```

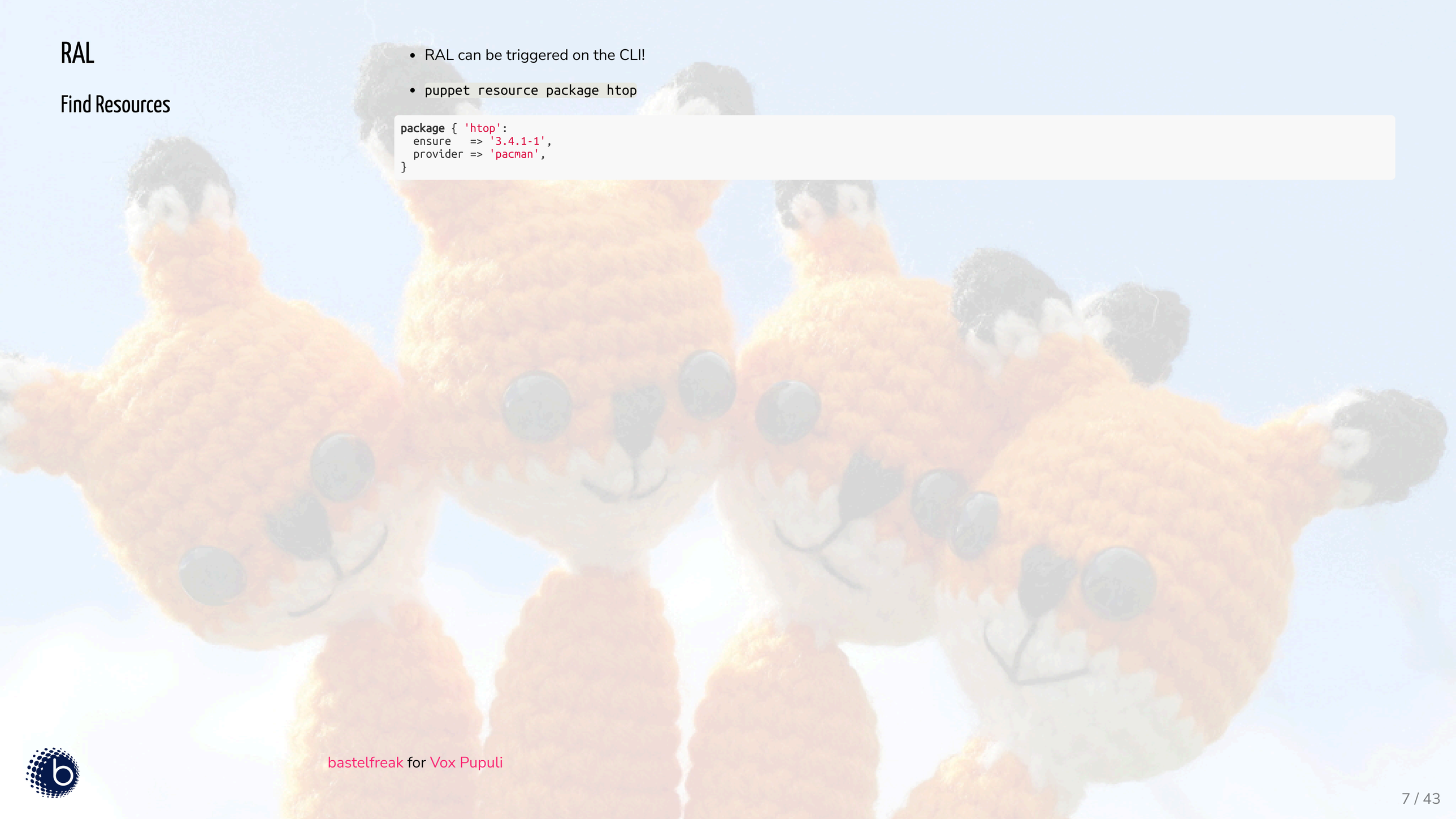
- List available types on CLI
- `puppet resource --types`

RAL

Find Resources

- RAL can be triggered on the CLI!
- `puppet resource package htop`

```
package { 'htop':
  ensure   => '3.4.1-1',
  provider => 'pacman',
}
```



RAL

Find Resources

- RAL can be triggered on the CLI!
- `puppet resource package htop`

```
package { 'htop':
  ensure   => '3.4.1-1',
  provider => 'pacman',
}
```

- Can output all instances of a resource type
- `puppet resource package`

```
package { 'yamllint':
  ensure   => '1.33.0-1',
  provider => 'pacman',
}
package { 'yard':
  ensure   => ['0.9.26'],
  provider => 'gem',
}
```

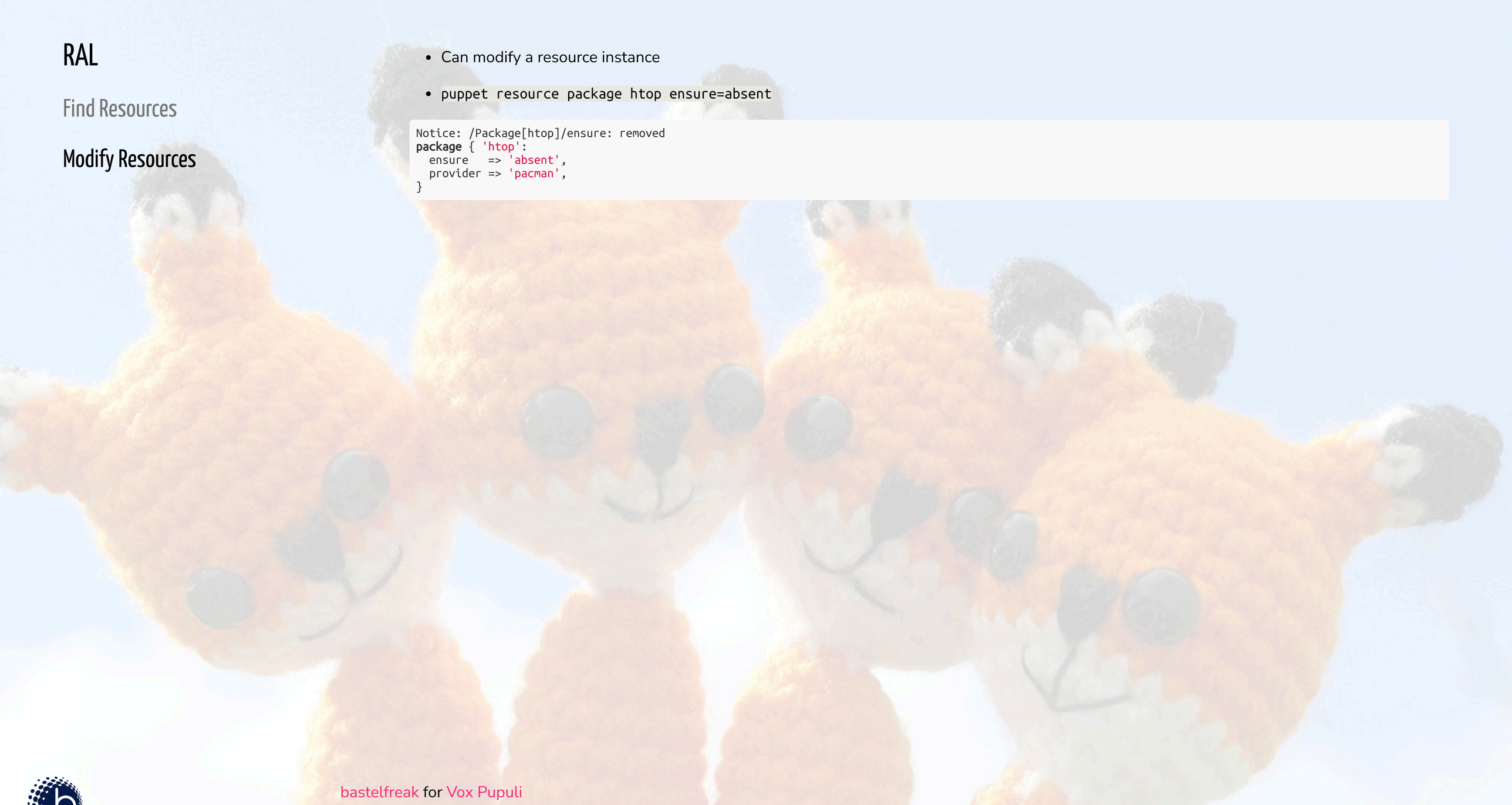
RAL

Find Resources

Modify Resources

- Can modify a resource instance
- `puppet resource package htop ensure=absent`

```
Notice: /Package[htop]/ensure: removed
package { 'htop':
  ensure   => 'absent',
  provider => 'pacman',
}
```



RAL

Find Resources

Modify Resources

- Can modify a resource instance
- `puppet resource package htop ensure=absent`

```
Notice: /Package[htop]/ensure: removed
package { 'htop':
  ensure   => 'absent',
  provider => 'pacman',
}
```

- Can modify a resource instance with debug output!
- `puppet resource package htop ensure=absent --debug`

RAL

Find Resources

Modify Resources

- Can modify a resource instance
- `puppet resource package htop ensure=absent`

```
Notice: /Package[htop]/ensure: removed
package { 'htop':
  ensure   => 'absent',
  provider => 'pacman',
}
```

- Can modify a resource instance with debug output!
- `puppet resource package htop ensure=absent --debug`
- Can simulate a change!
- `puppet resource package htop ensure=absent --debug --noop`

- puppet.com/docs/puppet/8/type#resources

resources

- Attributes

Description

This is a metatype that can manage other resource types. Any metaparams specified here will be passed on to any generated resources, so you can purge unmanaged resources but set `noop` to true so the purging is only logged and does not actually happen.

Attributes

```
resources { 'resource title':
  name               => # (namevar) The name of the type to be...
  purge              => # Whether to purge unmanaged resources.  When set...
  unless_system_user => # This keeps system users from being purged.  By...
  unless_uid         => # This keeps specific uids or ranges of uids from...
  # ...plus any applicable metaparameters.
}
```

RAL

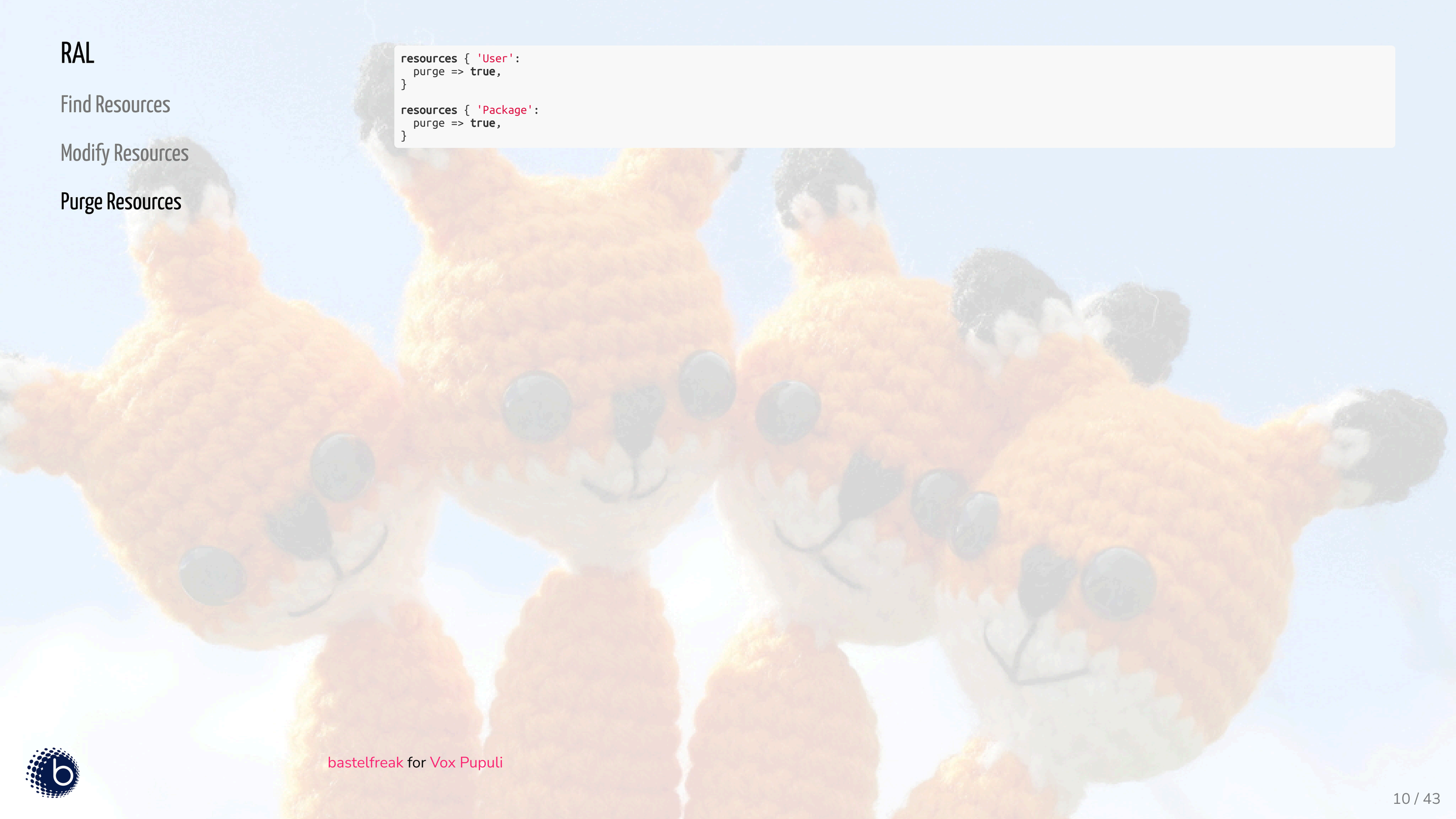
Find Resources

Modify Resources

Purge Resources

```
resources { 'User':
  purge => true,
}

resources { 'Package':
  purge => true,
}
```



RAL

Find Resources

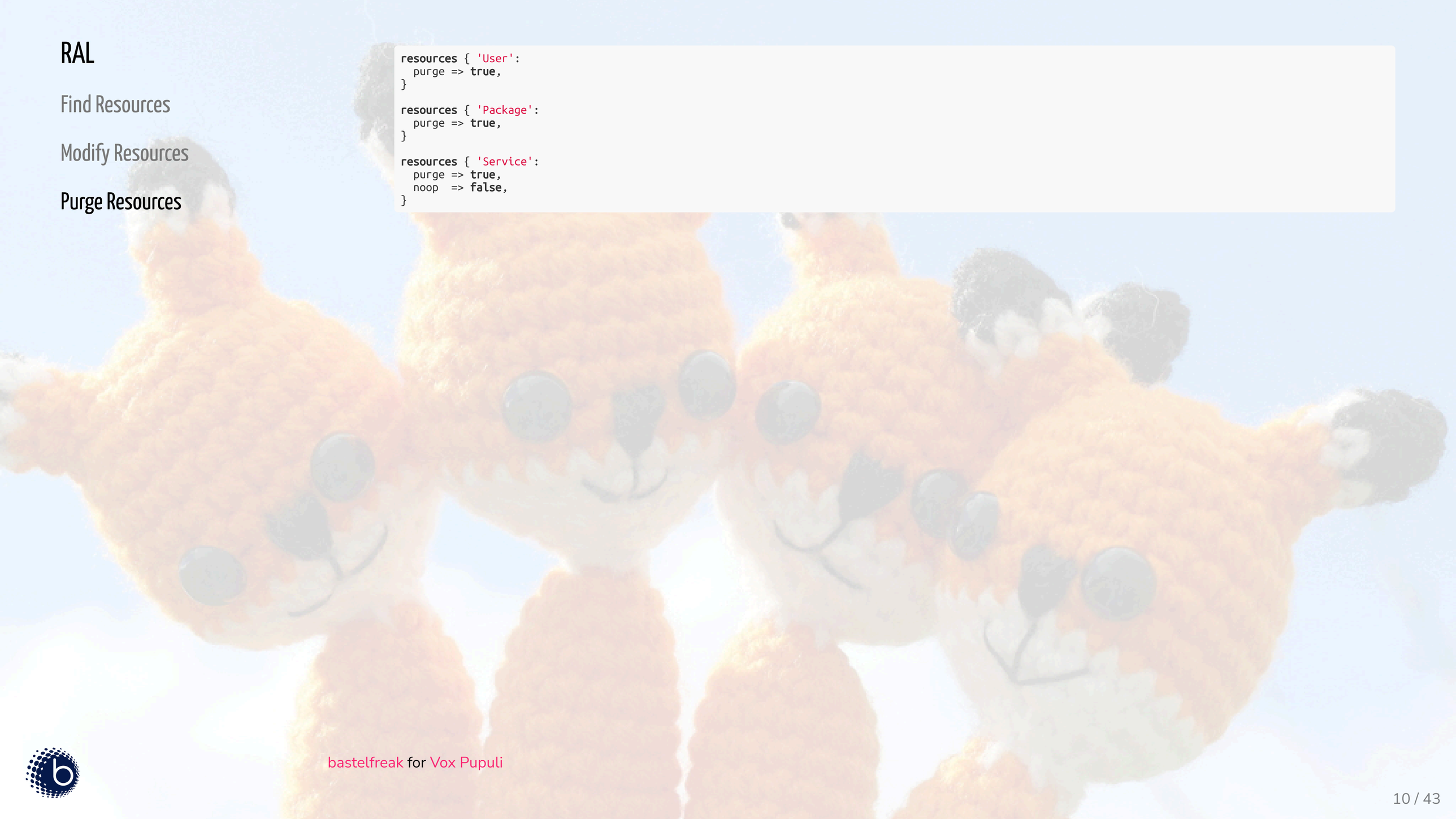
Modify Resources

Purge Resources

```
resources { 'User':
  purge => true,
}

resources { 'Package':
  purge => true,
}

resources { 'Service':
  purge => true,
  noop  => false,
}
```



- forge.puppet.com/crayfishx/purge

purge

This is a metatype to purge resources from the agent. It behaves in a similar way to the 'resources' type native in Puppet but offers more finite control over the criteria in which resources are purged.

When run without parameters the purge type takes a resource type as a title. The resource type must be one that has a provider that supports the instances method (eg: package, user, yumrepo). Any instances of the resource found on the agent that are *not* in the catalog will be purged. You can also add filter conditions to control the behaviour of purge using the if and unless parameters.

Differences to the `resources` resource

- Allows fine tuning of which resources get purged
- Not isomorphic, meaning multiple purge resource declarations can purge the same resource type
- Purging doesn't always mean destruction - you can use purge to set other attributes, not just `ensure => absent`

Examples

Eg: To remove *all* users found on the system that are not present in the catalog (caution!):

```
  purge { 'user': }
```

To remove all users found on the system but not in the catalog, unless the user has a UID below 500:

```
purge { 'user':
 unless => [ 'uid', '<=', '500' ],
}
```

You may also use regexes to filter, for example, to remove all unmanaged yumrepos unless they used for RHEL Satellite, you could do something like;

```
 purge { 'yumrepo':
   unless => [ 'baseurl', '=~', 'http://my-satellite-server.*' ],
 }
```

Theres also some other edge cases that can be solved with this pattern, when you need to make certain resources absent based on a flexible criteria (eg: you don't know the exact titles) you can't just declare them with ensure set to absent, so if you wanted to remove any package based on a pattern match of it's name you'd do

```
 purge { 'package':
   if => [ 'name', '=~', 'acme-devel-.*' ],
 }
```

Let's use `tidy`

At first glance, the `tidy` resource looks like the solution. But under the hood, `tidy` resource add's `file` resources. To the existing manifest (generate). If your manifest already contains a file => ensure, The `tidy` generator will not (it can't) create a file => absent resource to the same manifest. The annoying thing is that it doesn't tell you about it.

- Purging files and directories
- enterprisemodules.com/blog/2022/02/cleanup-temporary-files-in-puppet

The cleanup resource

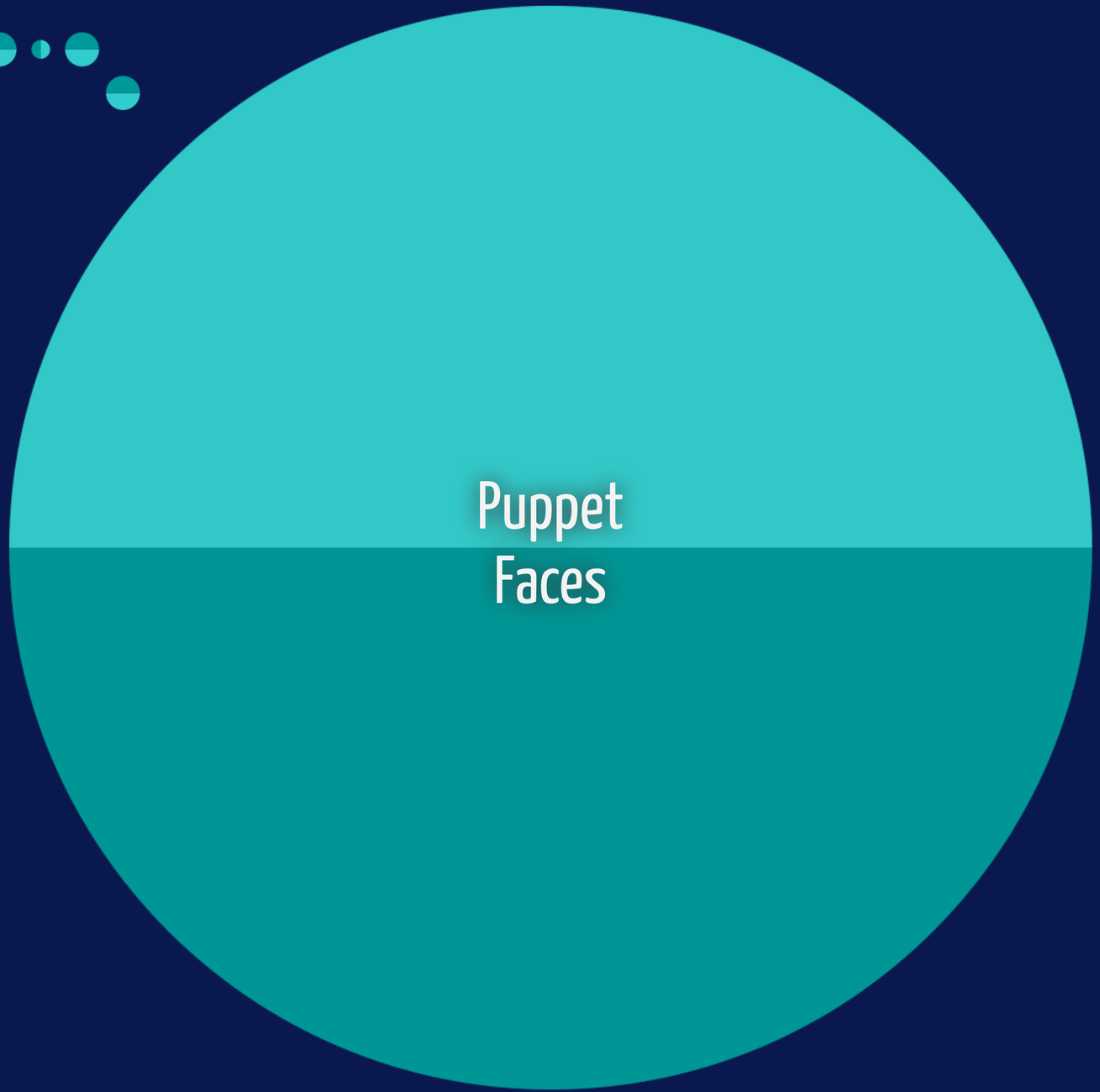
The easy_type module contains a solution for the dilemma. The cleanup resource. As the name implies, it cleans up. Let's see how we can use this.

```
file { '/data/my_temporary_file':
  ensure => 'present',
  content => 'my_data = true',
}

cleanup { '/data/my_temporary_file':}
```

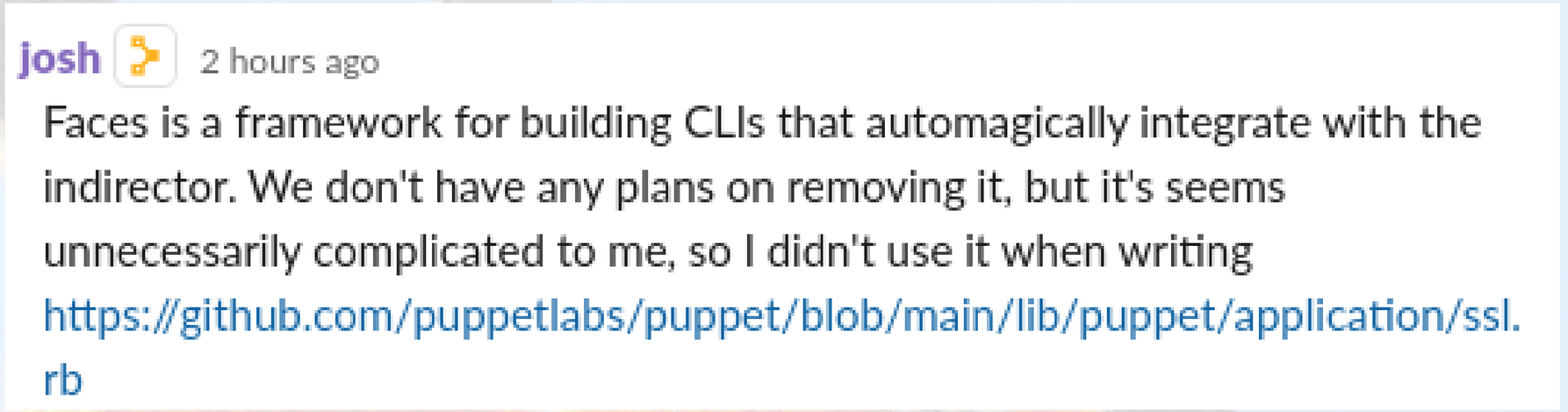
RAL

- Further documentation
- https://petersouter.xyz/the-puppet-resource-abstraction-layer-ral-explained-part-1/
- https://www.puppet.com/docs/puppet/7/man/resource


Puppet
Faces

Faces

- https://puppetcommunity.slack.com/archives/C0W1X7ZAL/p1705520404613479?thread_ts=1705511900.536469&cid=C0W1X7ZAL



Faces

- Faces were "deprecated" but won't be removed: https://www.puppet.com/docs/puppet/5.5/deprecated_api.html
- Kelsey Hightower explaining faces in 2011: https://www.youtube.com/watch?v=WUlYEJ-fpfU
- Faces are used heavily within Puppet: https://github.com/puppetlabs/puppet/tree/main/lib/puppet/face

Faces

- Faces were "deprecated" but won't be removed: https://www.puppet.com/docs/puppet/5.5/deprecated_api.html
- Kelsey Hightower explaining faces in 2011: https://www.youtube.com/watch?v=WUlYEJ-fpfU
- Faces are used heavily within Puppet: https://github.com/puppetlabs/puppet/tree/main/lib/puppet/face
- "Puppet Applications" are the successor for Faces
- github.com/puppetlabs/puppet/blob/main/lib/puppet/application.rb

Faces

config

- `puppet config print`
- `puppet config print certname`
- `puppet config print certname --section`
- `puppet config set 'option' 'value' --section 'section'`

Faces

config

catalog diff

- github.com/voxpupuli/puppet-catalog_diff
- The tool can automatically compile the catalogs for both your new and older servers/environments. It can ask the master to use PuppetDB to compile the catalog for the last known environment with the last known facts. It can then validate against PuppetDB that the node is still active. This filtered list should contain only machines that have not been decommissioned in PuppetDB (important as compiling their catalogs would also reactive them and their exports otherwise).

Faces

config

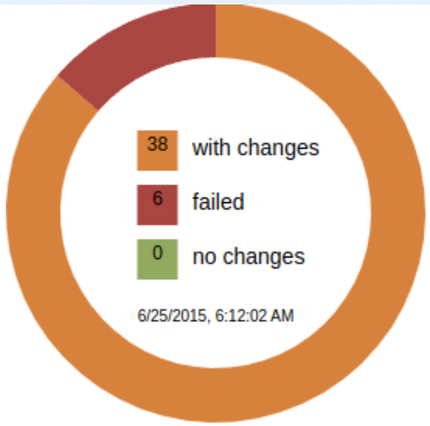
catalog diff

- `puppet catalog diff puppet.example.com/production puppet.example.com/staging --filter_old_env`
- `puppet catalog diff /foo/old/node1.example.com.json /foo/new/node1.example.com.json`
- voxpupuli.org/puppet-catalog-diff-viewer

Faces

config

catalog diff



ip-10-123-2-219.us-east-1.comput…
ip-10-123-8-184.us-east-1.compute…
ip-10-21-141-38.us-east-1.compute…
ip-10-21-200-154.us-east-1.comput…
ip-10-42-130-35.us-east-1.compute…
ip-10-9-130-88.eu-west-1.compute.i…
ip-10-127-1-3.us-east-1.compute.in…
ip-10-21-205-147.us-east-1.comput…
ip-10-246-99-87.us-east-1.compute…
ip-10-80-14-127.us-east-1.compute.i…
ip-10-106-3-228.us-east-1.compute.i…
ip-10-50-25-184.us-east-1.compute.i…
ip-10-21-188-219.us-east-1.compute.in…

ip-10-123-2-219.us-east-1.compute.internal

Diff stats

Catalog percentage added	0.15%
Catalog percentage removed	0.07%
Catalog percentage changed	0.45%
Node percentage	0.22%
Added and removed resources	+2 / -1
Node differences	9
Total resources in old	1339
Total resources in new	1340
Old catalog version	staging3/0ba7b6c
New catalog version	staging3_allnewrefs/3f1acb8

Differences 6

class[Puppet]

```
--- old
+++ new
                                          stringify_facts =>
                                        }
             agent_noop => false
+            agent_restart_command => "/usr/sbin/service puppet reload"
             agent_template => "puppet/agent/puppet.conf.erb"
             allow_any_crl_auth => false
             auth_allowed => [
```

Faces

config

catalog diff

node exports

- provide a list of exported resources in PuppetDB
- `watch 'puppet node exports'`
- forge.puppet.com/zack/exports

Faces

config

catalog diff

node exports

- provide a list of exported resources in PuppetDB
- `watch 'puppet node exports'`
- forge.puppet.com/zack/exports
- Lists all exported resources
- Can be filtered for resource types (for example File)

Faces

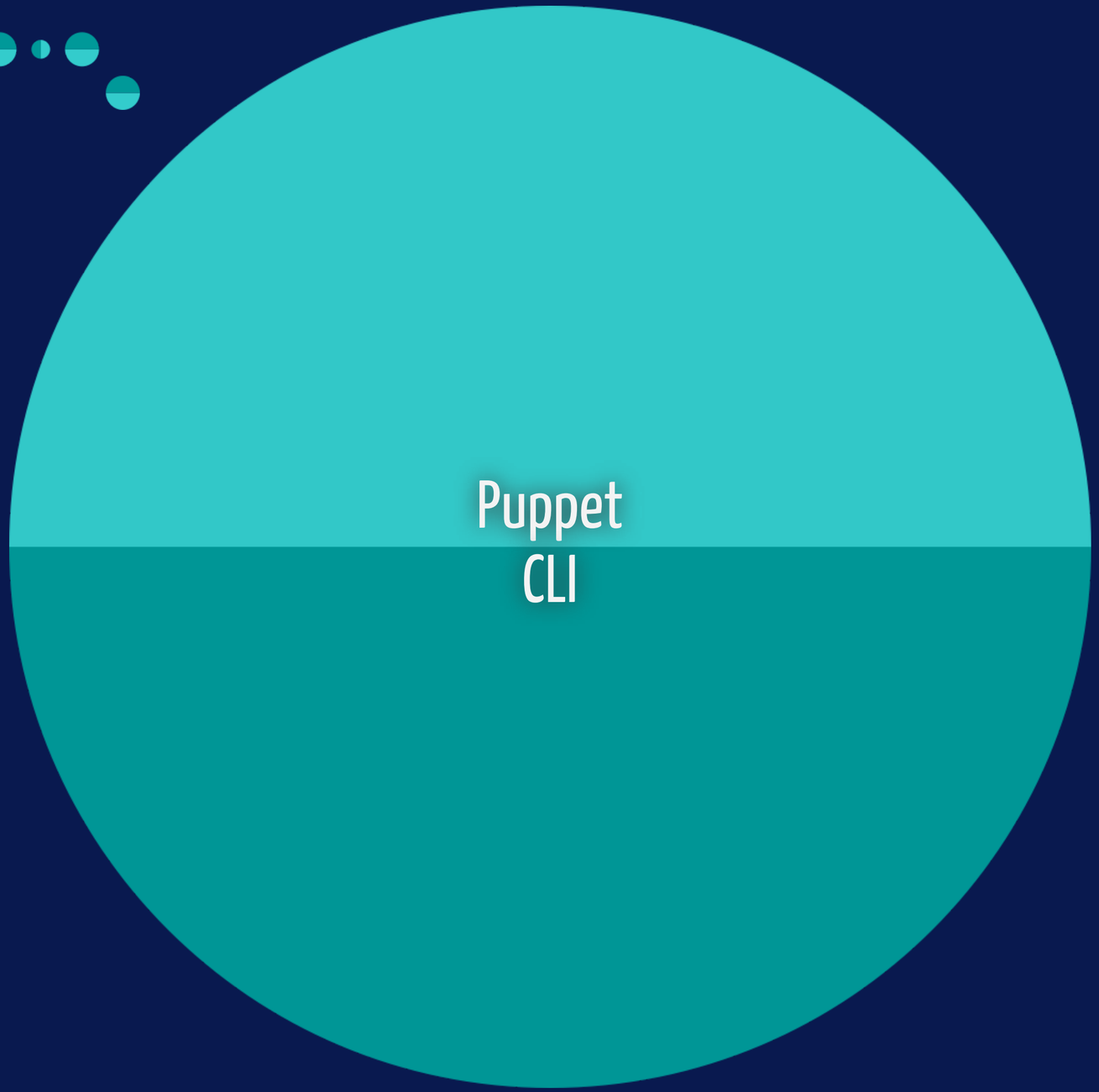
config

catalog diff

node exports

- provide a list of exported resources in PuppetDB
- `watch 'puppet node exports'`
- forge.puppet.com/zack/exports
- Lists all exported resources
- Can be filtered for resource types (for example File)
- Doesn't work properly with Puppet 8 :sadface:

```
root@puppet ~ # puppet node exports
Warning: The method 'Puppet::Network::HttpPool.http_instance'
 is deprecated. Use Puppet.runtime[:http] instead
   (file & line not available)
Error: undefined method `escape' for URI:Module
Error: Try 'puppet help node exports' for usage
root@puppet ~ #
```


Puppet
CLI

CLI

- `puppet agent -t`

CLI

- `puppet agent -t`
- `puppet agent --test`

CLI

- `puppet agent -t`
- `puppet agent --test`
- `puppet agent --verbose --no-daemonize --no-usecacheonfailure --detailed-exitcodes --no-splay --show_diff`

CLI

- `puppet agent -t`
- `puppet agent --test`
- `puppet agent --verbose --no-daemonize --no-usecacheonfailure --detailed-exitcodes --no-splay --show_diff`
- Who knows more CLI invocations?

CLI

- `puppet agent -t`
- `puppet agent --test`
- `puppet agent --verbose --no-daemonize --no-usecacheonfailure --detailed-exitcodes --no-splay --show_diff`
- Who knows more CLI invocations?
- Some Options are only available on the CLI: `puppet agent --help`
- Every config option can be set and overwritten on CLI: https://www.puppet.com/docs/puppet/8/configuration.html
- `puppet agent -t --no-noop`

CLI

trace

- `--trace` is a common option in the Ruby ecosystem
- available in puppet faces as well

```
root@puppet ~ # puppet node exports --trace
Warning: The method 'Puppet::Network::HttpPool.http_instance' is deprecated. Use Puppet.runtime[:ht
tp] instead
   (file & line not available)
Error: undefined method `escape' for URI:Module
/etc/puppetlabs/code/environments/production/modules/exports/lib/puppet/face/node/exports.rb:63:in
`block (3 levels) in <top (required)>'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/interface/action.rb+eval[wrapper]:262:in `export
s'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/application/face_base.rb:256:in `main'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/application.rb:438:in `run_command'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/application.rb:422:in `block in run'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/util.rb:700:in `exit_on_fail'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/application.rb:422:in `run'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/util/command_line.rb:144:in `run'
/opt/puppetlabs/puppet/lib/ruby/vendor_ruby/puppet/util/command_line.rb:78:in `execute'
/opt/puppetlabs/puppet/bin/puppet:6:in `<main>'
Error: Try 'puppet help node exports' for usage
root@puppet ~ #
```

CLI

trace

debug

- `puppet agent -t --debug`
- Prints all HTTP calls to puppetserver
- Lists all resources and if they are already in the desired state

CLI

trace

debug

- `puppet agent -t --debug`
- Prints all HTTP calls to puppetserver
- Lists all resources and if they are already in the desired state
- prints all debug messages
- Facter: `Facter.debug('my debug text')`
- Puppet Types/Provider: `Puppet.debug('my other debug text')`

CLI

trace

debug

http_debug

CLI

trace

debug

http_debug

- `puppet agent -t --http_debug`
- Dumps every HTTP Payload and Headers from/to Puppetserver

CLI

trace

debug

http_debug

- `puppet agent -t --http_debug`
- Dumps every HTTP Payload and Headers from/to Puppetserver
- As base64

CLI

trace

debug

http_debug

```
root@basteles-bastelknecht ~ # puppet agent -t --http_debug
Info: Using environment 'production'
opening connection to puppet.bastelfreak.org:8140...
opened
starting SSL for puppet.bastelfreak.org:8140...
SSL established, protocol: TLSv1.3, cipher: TLS_AES_128_GCM_SHA256
<- "GET /puppet/v3/file_metadatas/plugins?recurse=false&links=manage&checksum_type=sha256&source_perm
u)\r\nAccept: application/json, text/pson\r\nAccept-Encoding: gzip;q=1.0,deflate;q=0.6,identity;q=0.3
-> "HTTP/1.1 200 OK\r\n"
-> "Date: Wed, 31 Jan 2024 15:01:20 GMT\r\n"
-> "Content-Type: application/json;charset=utf-8\r\n"
-> "X-Puppet-Version: 8.3.1\r\n"
-> "Vary: Accept-Encoding, User-Agent\r\n"
-> "Content-Encoding: gzip\r\n"
-> "Transfer-Encoding: chunked\r\n"
-> "\r\n"
-> "A\r\n"
```

CLI

trace

debug

http_debug

evaltrace

- `puppet agent -t --evaltrace`
- prints all resources and their evaluation time

```
root@basteles-bastelknecht ~ # puppet agent -t --evaltrace
Info: Using environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Applying configuration version '3f53802 - Tim Meusel, Wed Jan 31 14:55:28 2024 +0100 : Add zack/exports'
Info: Stage[main]: Starting to evaluate the resource (1 of 1073)
Info: Stage[main]: Evaluated in 0.00 seconds
Info: Class[Settings]: Starting to evaluate the resource (2 of 1073)
Info: Class[Settings]: Evaluated in 0.00 seconds
Info: Class[Settings]: Starting to evaluate the resource (3 of 1073)
Info: Class[Settings]: Evaluated in 0.00 seconds
Info: Class[Main]: Starting to evaluate the resource (4 of 1073)
Info: Class[Main]: Evaluated in 0.00 seconds
Info: Class[Profiles::Base]: Starting to evaluate the resource (5 of 1073)
Info: Class[Profiles::Base]: Evaluated in 0.00 seconds
Info: Class[Profiles::Debian]: Starting to evaluate the resource (6 of 1073)
Info: Class[Profiles::Debian]: Evaluated in 0.00 seconds
Info: Class[Unattended_upgrades::Params]: Starting to evaluate the resource (7 of 1073)
```

CLI

trace

debug

http_debug

evaltrace

- `puppet agent -t --trace --evaltrace --debug --http_debug`
- All options can be combined

CLI

trace

debug

http_debug

evaltrace

- `puppet agent -t --trace --evaltrace --debug --http_debug`
- All options can be combined
- You will need a very big screen!

CLI

trace

debug

http_debug

evaltrace

timing

- `puppet facts show` # show all facts

CLI

trace

debug

http_debug

evaltrace

timing

- `puppet facts show` # show all facts
- `puppet facts show $fact` # show a single fact named fact

CLI

trace

debug

http_debug

evaltrace

timing

- `puppet facts show` # show all facts
- `puppet facts show $fact` # show a single fact named fact
- `puppet facts show --timing` # timing per fact resolution

CLI

trace

debug

http_debug

evaltrace

timing

```
root@basteles-bastelknecht ~ # puppet facts show --timing
fact 'operatingsystem', took: (0.000114) seconds
fact 'kernel', took: (0.007391) seconds
fact 'lvm_support', took: (0.000171) seconds
fact 'osfamily', took: (0.000119) seconds
fact 'aio_agent_version', took: (0.000109) seconds
fact 'os.release', took: (0.000084) seconds
fact 'operatingsystemmajrelease', took: (0.000014) seconds
fact 'operatingsystemrelease', took: (0.000015) seconds
fact 'os.architecture', took: (0.000025) seconds
fact 'architecture', took: (0.000014) seconds
fact 'os.distro.description', took: (0.000021) seconds
fact 'os.distro.release', took: (0.000038) seconds
fact 'lsbdistrelease', took: (0.000015) seconds
fact 'lsbmajdistrelease', took: (0.000024) seconds
fact 'lsbminordistrelease', took: (0.000023) seconds
fact 'os.distro.id', took: (0.000016) seconds
```

Design Pattern and Hacks

Hacks & Patterns

LLDP

- LLDP - Link Layer Distribution Protocol
- IEEE-802.1AB standard
- exchange information between direct layer 2 peers
- Common protocol for Routers, Switches *and servers*

Hacks & Patterns

LLDP

- LLDP - Link Layer Distribution Protocol
- IEEE-802.1AB standard
- exchange information between direct layer 2 peers
- Common protocol for Routers, Switches *and servers*
- Linux: github.com/lldpd/lldpd
- Puppet Module: forge.puppet.com/puppet/lldpd

LLDP

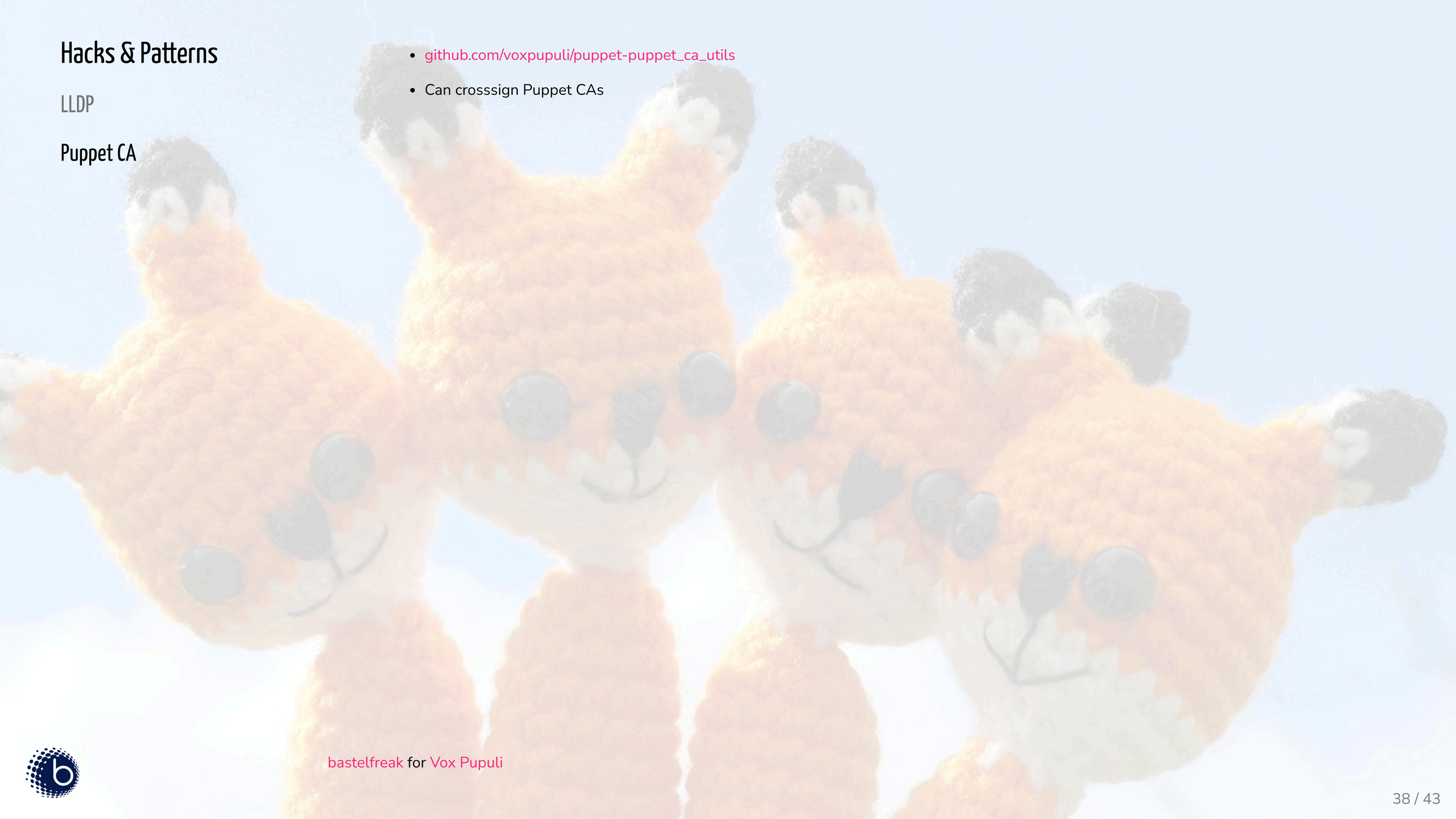
```
root@webserver01 ~ # lldpctl
-------------------------------------------------------------------------------
LLDP neighbors:
-------------------------------------------------------------------------------
Interface:    uplink, via: LLDP, RID: 1, Time: 14 days, 22:35:01
  Chassis:
    ChassisID:    mac 90:1b:0e:a4:a4:9b
    SysName:      hypervisor01.bastelfreak.org
    SysDescr:     Gentoo Linux Linux 6.1.57-gentoo-dist-hardened #1 SMP PREEMPT_DYNAMIC Mon Oct 16
    MgmtIP:       192.168.122.1
    MgmtIface:    6
    MgmtIP:       2a01:4f8:171:1152::2
    MgmtIface:    2
    Capability:   Bridge, on
    Capability:   Router, on
    Capability:   Wlan, off
    Capability:   Station, off
  Port:
    PortID:       mac fe:54:00:26:de:61
    PortDescr:    vnet4
    TTL:          120
    PMD autoneg:  supported: no, enabled: no
      MAU oper type: 10BaseTFD - UTP MAU, full duplex mode
-------------------------------------------------------------------------------
```

Hacks & Patterns

LLDP

Puppet CA

- github.com/voxpupuli/puppet-puppet_ca_utils
- Can crosssign Puppet CAs



Hacks & Patterns

LLDP

Puppet CA

- github.com/voxpupuli/puppet-puppet_ca_utils
- Can crosssign Puppet CAs
- github.com/voxpupuli/puppet-puppet_certificate
- Allow Agents to renew their own certificate
- Update CSR/SAN attributes

```
file { '/etc/puppetlabs/puppet/csr_attributes.yaml':
  ensure  => file,
  owner   => 'root',
  group   => 'root',
  mode    => '0440',
  content => epp('example/csr_attributes.yaml.epp'),
}

~> puppet_certificate { $certname:
  ensure      => present,
  waitforcert => 60,
  onrefresh   => regenerate,
}
```

Hacks & Patterns

LLDP

Puppet CA

- github.com/voxpupuli/puppet-puppet_ca_utils
- Can crosssign Puppet CAs
- github.com/voxpupuli/puppet-puppet_certificate
- Allow Agents to renew their own certificate
- Update CSR/SAN attributes

```
file { '/etc/puppetlabs/puppet/csr_attributes.yaml':
  ensure  => file,
  owner   => 'root',
  group   => 'root',
  mode    => '0440',
  content => epp('example/csr_attributes.yaml.epp'),
}

~> puppet_certificate { $certname:
  ensure      => present,
  waitforcert => 60,
  onrefresh   => regenerate,
}
```

- Puppet 8 supports auto cert renewal: puppet.com/docs/puppet/8/release_notes

Hacks & Patterns

LLDP

Puppet CA

- Use PuppetCA for personal certificates
- Use personal certificates to authenticate to local services
- `puppet ssl bootstrap --certname "$(hostname -f)-${USER}"`

```
bastelfreak@basteles-bastelknecht ~ $ puppet ssl bootstrap --certname "$(hostname -f)-${USER}"
Info: Creating a new RSA SSL key for basteles-bastelknecht.bastelfreak.org-bastelfreak
Info: csr_attributes file loading from /home/bastelfreak/.puppetlabs/etc/puppet/csr_attributes.yaml
Info: Creating a new SSL certificate request for basteles-bastelknecht.bastelfreak.org-bastelfreak
Info: Certificate Request fingerprint (SHA256): FB:46:79:F9:8D:FF:97:BB:ED:F3:7C:29:DE:D9:51:CB:06:AB:C5:31:3E:BB:1A:8F:64:FA:AA:CB:E8:17:5F:3D
Info: Certificate for basteles-bastelknecht.bastelfreak.org-bastelfreak has not been signed yet
Couldn't fetch certificate from CA server; you might still need to sign this agent's certificate (basteles-bastelknecht.bastelfreak.org-bastelfreak).
Info: Will try again in 120 seconds.
Info: csr_attributes file loading from /home/bastelfreak/.puppetlabs/etc/puppet/csr_attributes.yaml
Info: Creating a new SSL certificate request for basteles-bastelknecht.bastelfreak.org-bastelfreak
Info: Certificate Request fingerprint (SHA256): FB:46:79:F9:8D:FF:97:BB:ED:F3:7C:29:DE:D9:51:CB:06:AB:C5:31:3E:BB:1A:8F:64:FA:AA:CB:E8:17:5F:3D
Info: Downloaded certificate for basteles-bastelknecht.bastelfreak.org-bastelfreak from https://puppet:8140/puppet-ca/v1
Notice: Completed SSL initialization
bastelfreak@basteles-bastelknecht ~ $
```

Hacks & Patterns

LLDP

Puppet CA

- github.com/m0dular/ca_extend
- Extend a Open Source CA

Hacks & Patterns

LLDP

Puppet CA

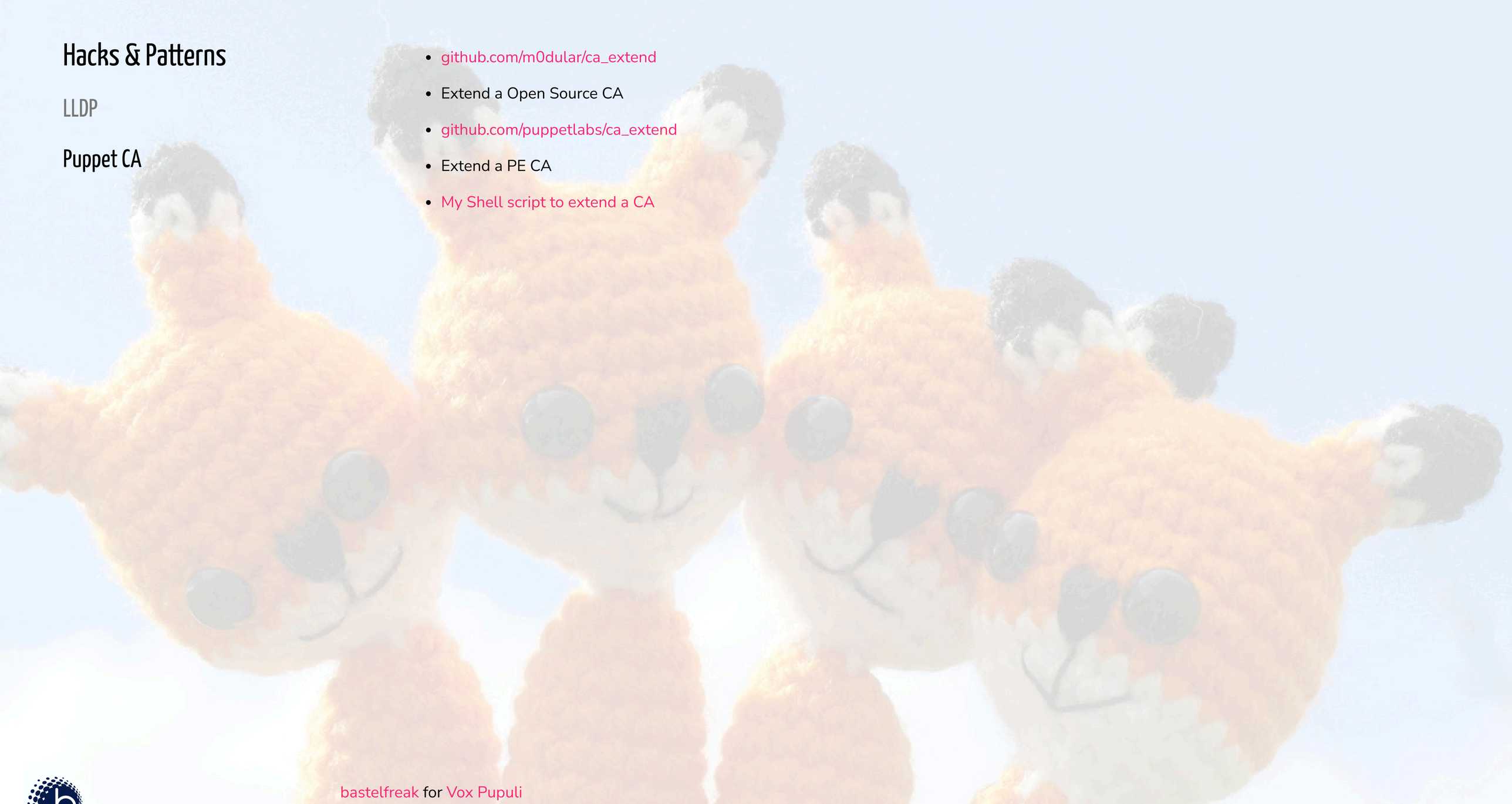
- github.com/m0dular/ca_extend
- Extend a Open Source CA
- github.com/puppetlabs/ca_extend
- Extend a PE CA

Hacks & Patterns

LLDP

Puppet CA

- github.com/m0dular/ca_extend
- Extend a Open Source CA
- github.com/puppetlabs/ca_extend
- Extend a PE CA
- My Shell script to extend a CA



Hacks & Patterns

LLDP

Puppet CA

Clusterfoo

- Use PuppetDB to dynamically build your clusters

```
# Get FQDNs for all cluster peers
$query = "inventory[certname] {
  trusted.extensions.pp_role = 'consul' and trusted.extensions.pp_region = 'eu-01'
}"
$nodes = puppetdb_query($query).map |$value| { $value["certname"] }
```

Hacks & Patterns

LLDP

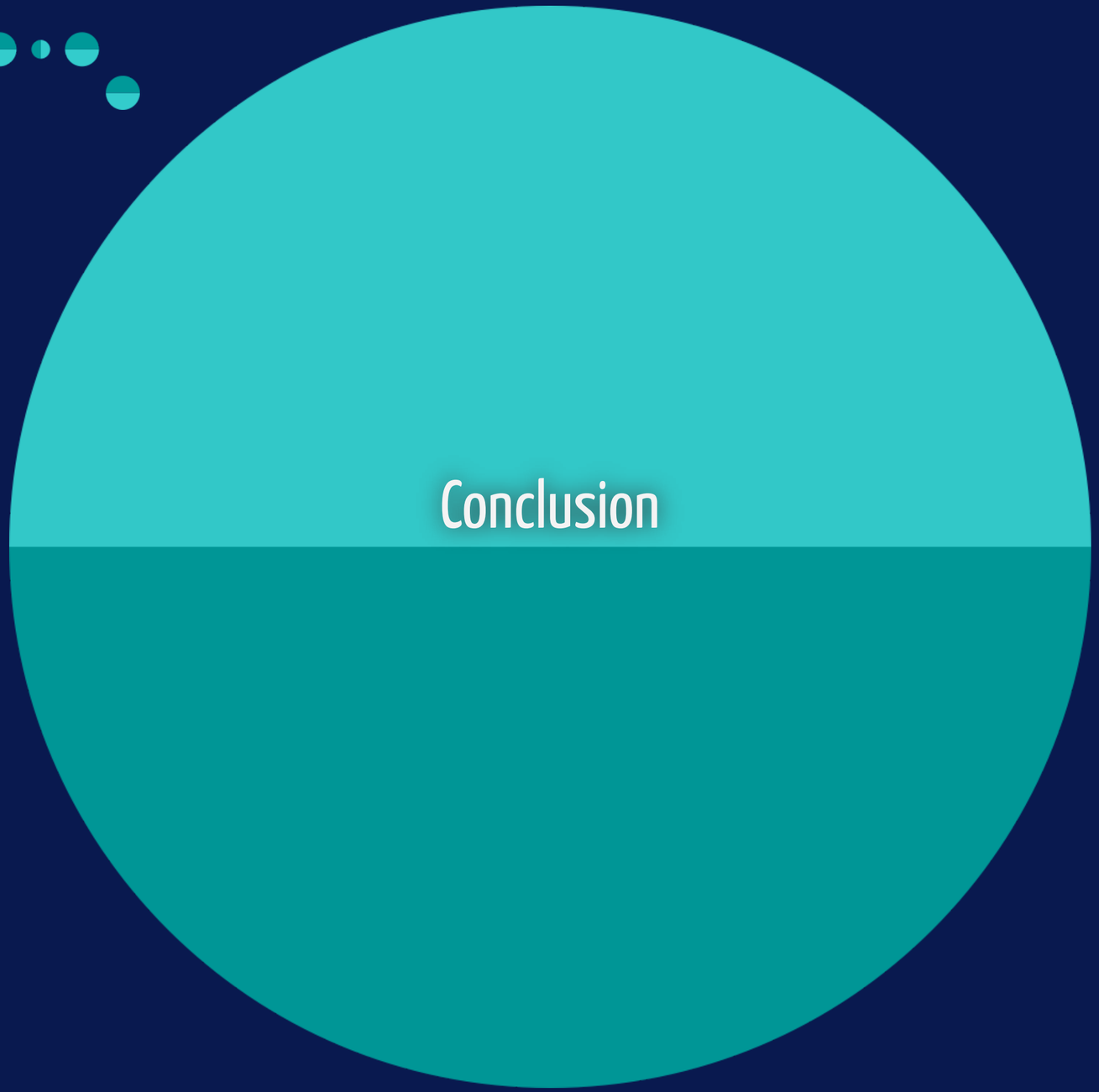
Puppet CA

Clusterfoo

- Use PuppetDB to dynamically build your clusters

```
# Get FQDNs for all cluster peers
$query = "inventory[certname] {
  trusted.extensions.pp_role = 'consul' and trusted.extensions.pp_region = 'eu-01'
}"
$nodes = puppetdb_query($query).map |$value| { $value["certname"] }
```

```
@@sshkey{$trusted['certname']:
  host_aliases => [$facts['ipaddress6'], $facts['ipaddress']],
  type         => "ssh-${type}",
  key          => $facts['ssh'][$type]['key'],
  # defaults to /etc/ssh/ so all users can use it
  #target       => '/root/.ssh/known_hosts',
  tag          => $trusted['extensions']['pp_role'],
}
## import host key
Sshkey <<| tag == $trusted['extensions']['pp_role'] and title != $trusted['certname'] |>>
```


Conclusion

Conclusion

- Puppet is very flexible and suiteable for different usecases
- There are many hidden gems and extensions available
- More docs from Puppet/Perforce for edgecases & advanced users would be awesome!

Conclusion

- Puppet is very flexible and suiteable for different usecases
- There are many hidden gems and extensions available
- More docs from Puppet/Perforce for edgecases & advanced users would be awesome!
- For feedback: `bastelfreak` on slack.puppet.com/Libera.Chat IRC or tim@bastelfreak.de
- This talk and previous ones: github.com/bastelfreak/talks

Thanks for your attention!

bastelfreak for Vox Pupuli