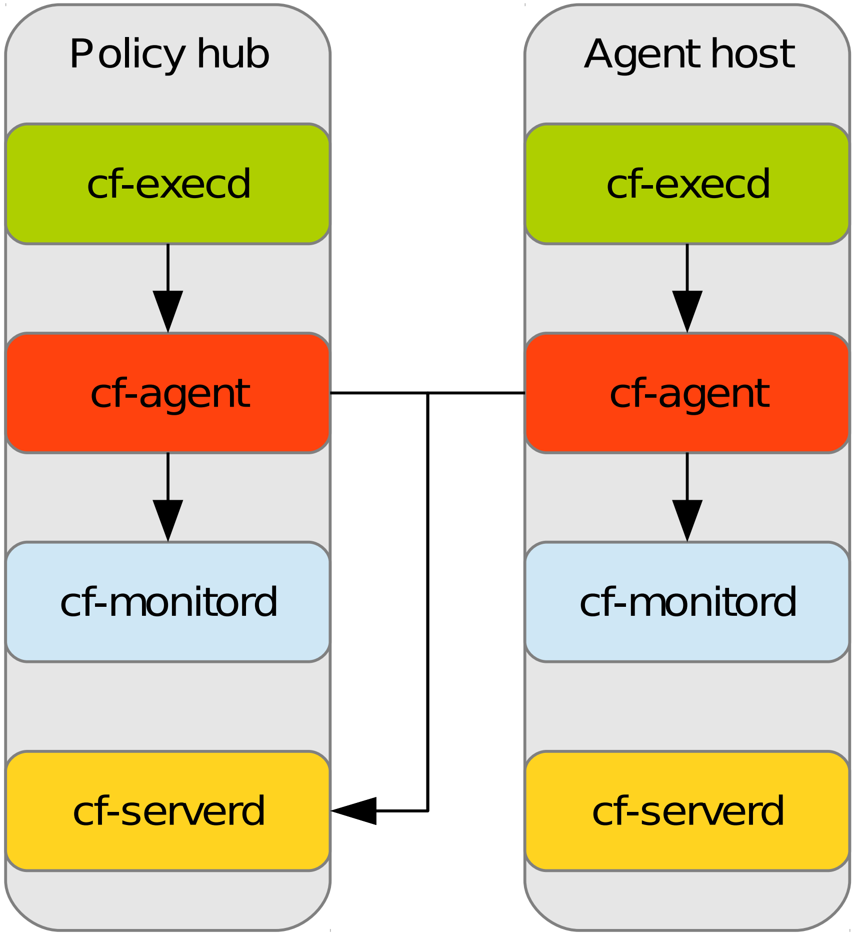
CFEngine

CFEngine

EvolveThinking

CFEngine architecture



Promise theory

- Voluntary cooperation
- Autonomous operation
- Detail reduces uncertainty

Promise theory in CFEngine

- Agents **cannot** be given external instructions or information.
- Agents **do not** rely on a central authority.
- Promises with precise declarations **have less** side affects.

What is a promise?

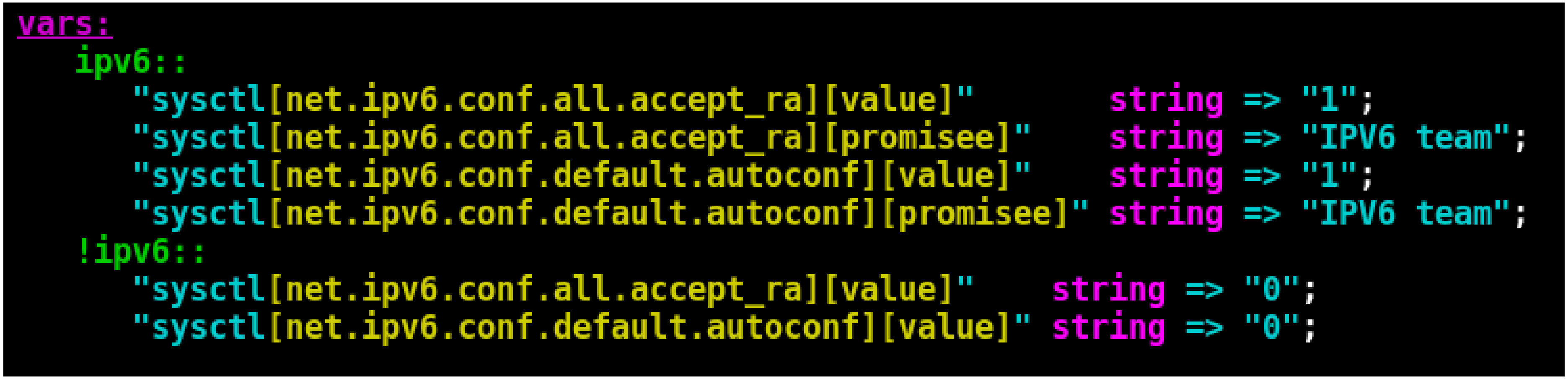
CFEngine

EvolveThinking

Promise syntax

```
“/etc/passwd” -> { “nsa_rhel5 v4.2 sec 2.2.3.1” }
   comment   => “To pass next audit”,
   Handle    => 'efl_file_perms_files',
   perms     => mog( “644”, “root”, “root” );
```

CFEngine is hard



```
vars:
   ipv6::
      "sysctl[net.ipv6.conf.all.accept_ra][value]"      string => "1";
      "sysctl[net.ipv6.conf.all.accept_ra][promisee]"   string => "IPV6 team";
      "sysctl[net.ipv6.conf.default.autoconf][value]"   string => "1";
      "sysctl[net.ipv6.conf.default.autoconf][promisee]" string => "IPV6 team";
   !ipv6::
      "sysctl[net.ipv6.conf.all.accept_ra][value]"   string => "0";
      "sysctl[net.ipv6.conf.default.autoconf][value]" string => "0";
```

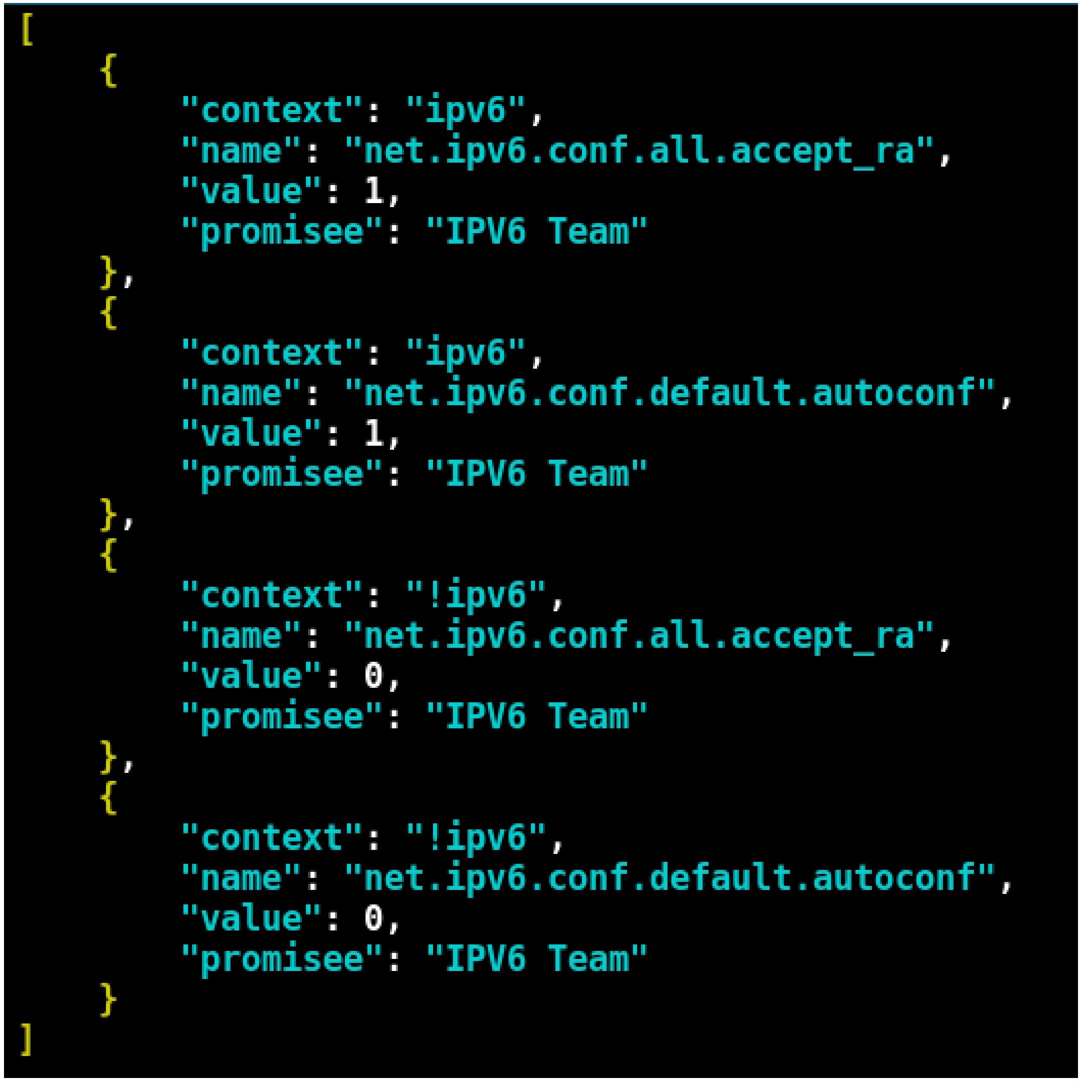
CFEngine

EvolveThinking

Evolve Free Promise library

EFL

CFEngine made easy



```
[
    {
        "context": "ipv6",
        "name": "net.ipv6.conf.all.accept_ra",
        "value": 1,
        "promisee": "IPV6 Team"
    },
    {
        "context": "ipv6",
        "name": "net.ipv6.conf.default.autoconf",
        "value": 1,
        "promisee": "IPV6 Team"
    },
    {
        "context": "!ipv6",
        "name": "net.ipv6.conf.all.accept_ra",
        "value": 0,
        "promisee": "IPV6 Team"
    },
    {
        "context": "!ipv6",
        "name": "net.ipv6.conf.default.autoconf",
        "value": 0,
        "promisee": "IPV6 Team"
    }
]
```

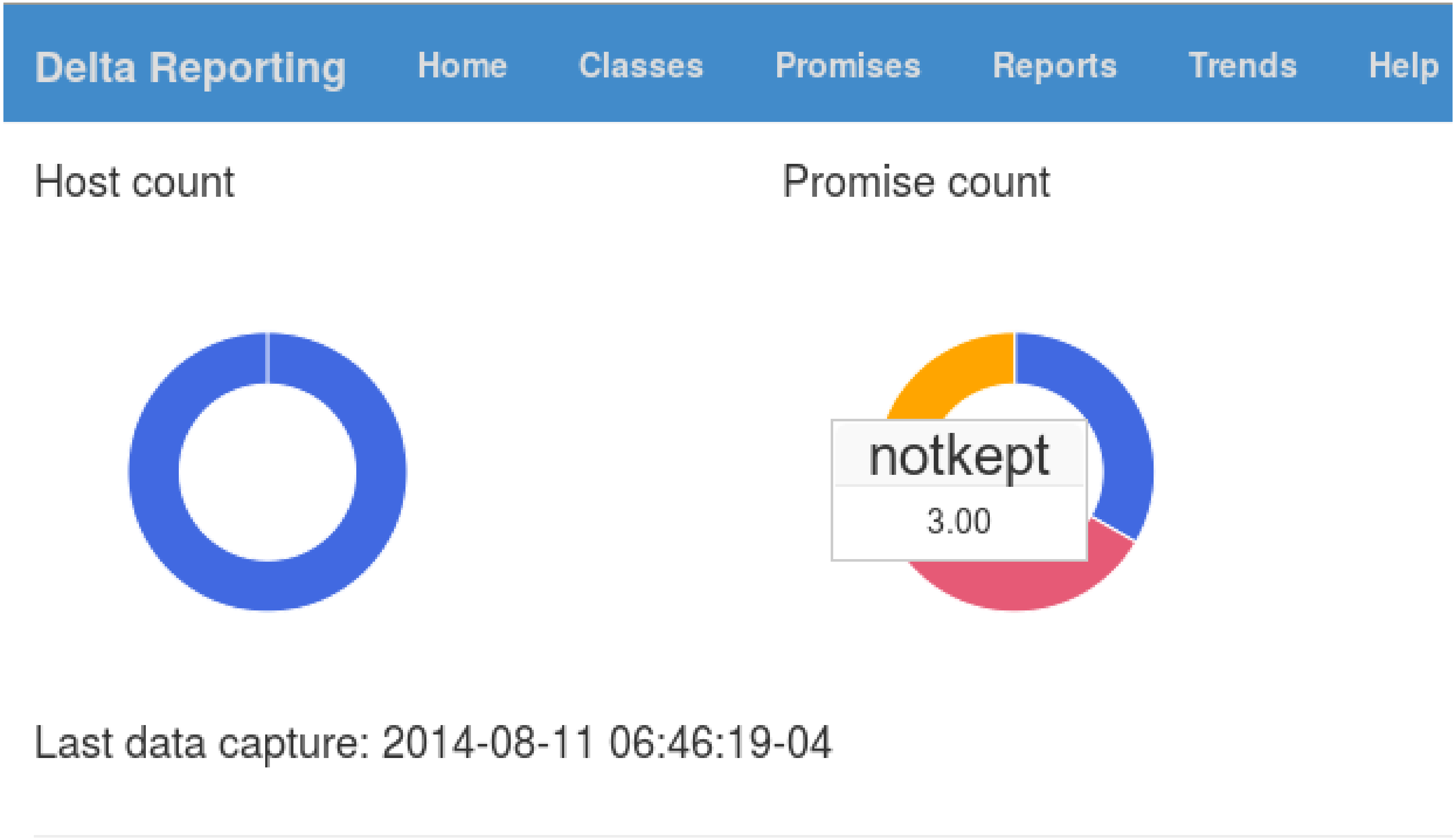
CFEngine

EvolveThinking

Simple bundles for everything

- A collection of common tunable variables.
- A template for creating your own bundles.
- A bundle for calling other bundles, in order, using methods.
- Disable a service from starting at boot.
- Enable a service to start at boot.
- Creates namespace classes by matching existing class names.
- Creates namespace classes on the output of a shell command.
- Creates namespace classes from a class expression.
- Creates namespace classs based on the hostname of the host.
- Creates namespace classes based on the IP address of the host.
- Creates namespace classes using the return status of a shell command.
- Configurable commands promises.
- Configurable file copy promises.
- Promises to delete files.
- Promise a file's contents using a template.
- Configurable file permissions promises.
- Set namespace scoped slists variables.
- Set namespace scoped strings variables.
- Report hosts seen in the last 24 hours.
- Report CFEngine internal statistics.
- Report hosts not seen in the last 24 hours.
- Promises to add, remove, or update packages.
- Promise links.
- Promises to keep a checked out copy of version control current.
- Promise CFEngine server access rules.
- Promises to configure and start a service.
- Promises to start a service that is not running.
- Promises sysctl.conf kernel settings.
- Promises live sysctl Linux kernel settings.

Delta Reporting



Host count

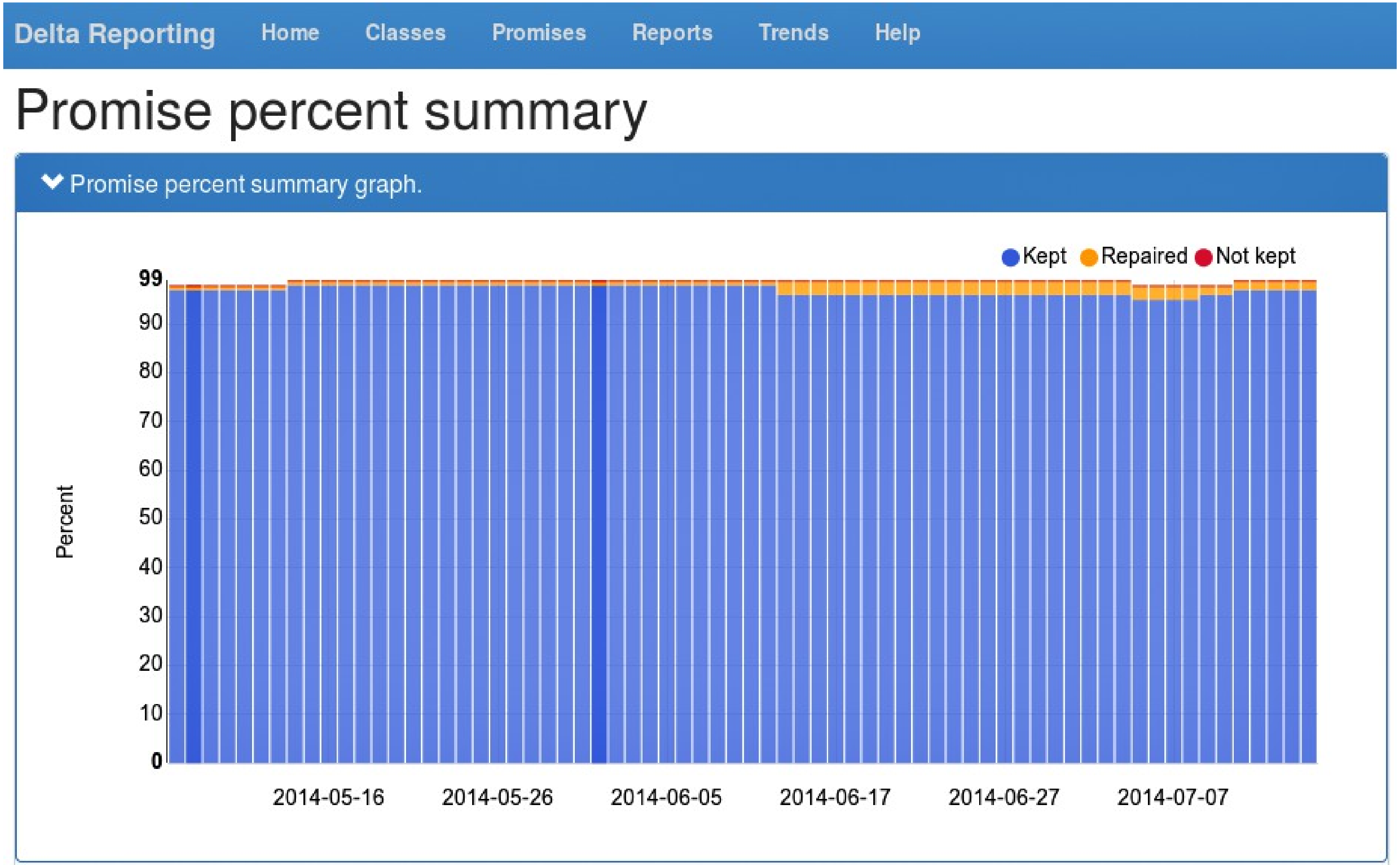
Promise count

Last data capture: 2014-08-11 06:46:19-04

CFEngine

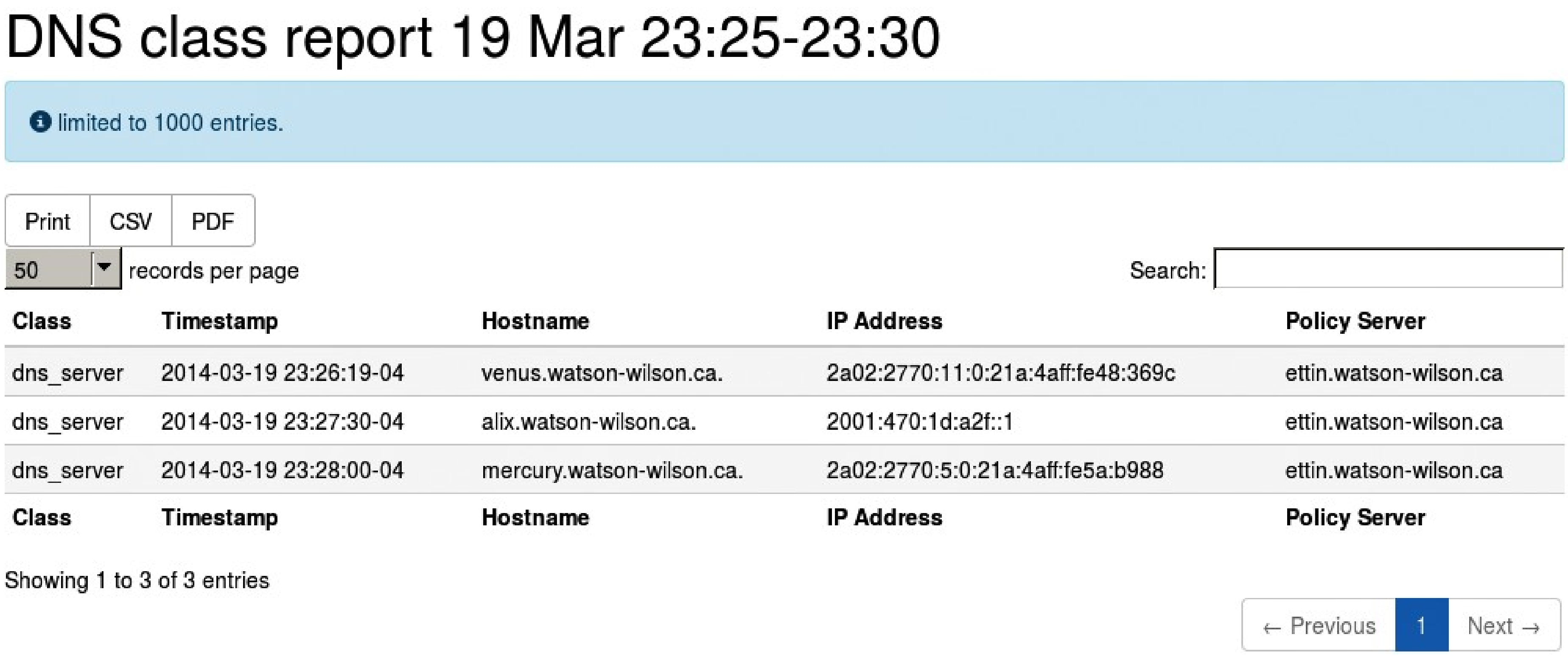
EvolveThinking

Promise compliance log



Promise percent summary

Class log



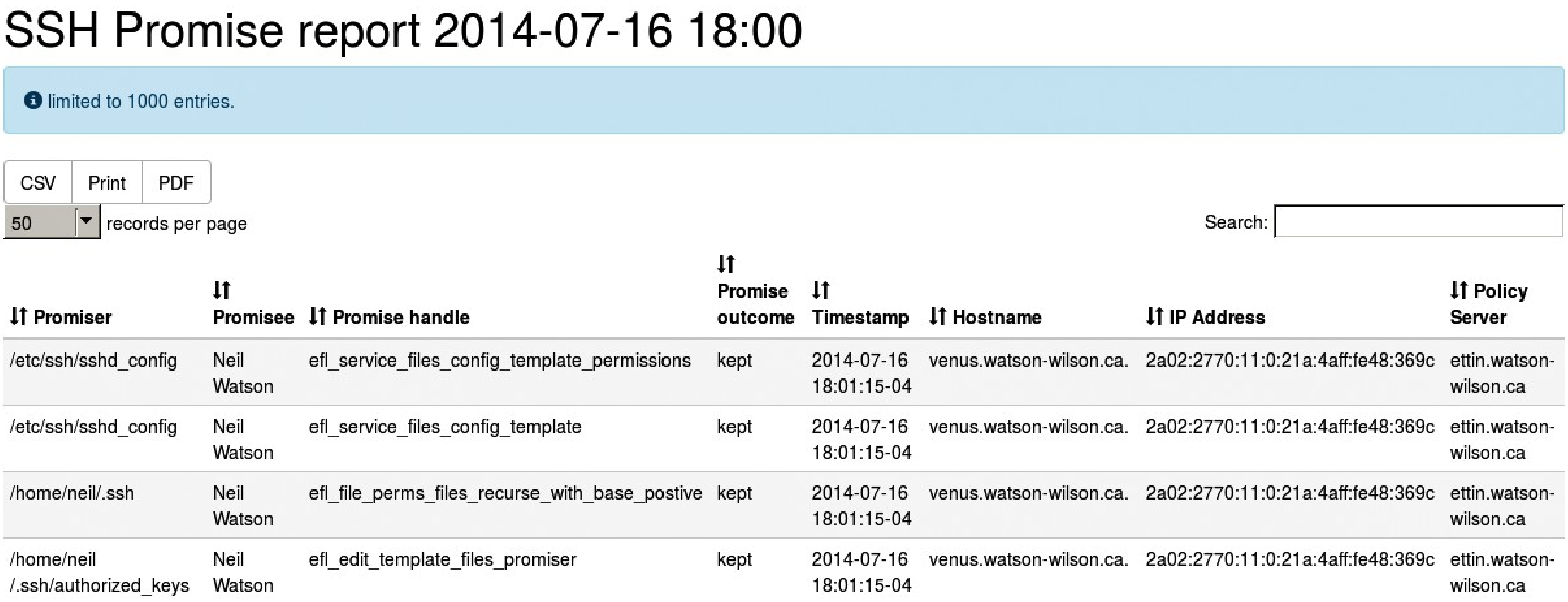
DNS class report 19 Mar 23:25-23:30

limited to 1000 entries.

Class	Timestamp	Hostname	IP Address	Policy Server
dns_server	2014-03-19 23:26:19-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca
dns_server	2014-03-19 23:27:30-04	alix.watson-wilson.ca.	2001:470:1d:a2f::1	ettin.watson-wilson.ca
dns_server	2014-03-19 23:28:00-04	mercury.watson-wilson.ca.	2a02:2770:5:0:21a:4aff:fe5a:b988	ettin.watson-wilson.ca
Class	**Timestamp**	**Hostname**	**IP Address**	**Policy Server**

Showing 1 to 3 of 3 entries

SSH configuration compliance



SSH Promise report 2014-07-16 18:00

limited to 1000 entries.

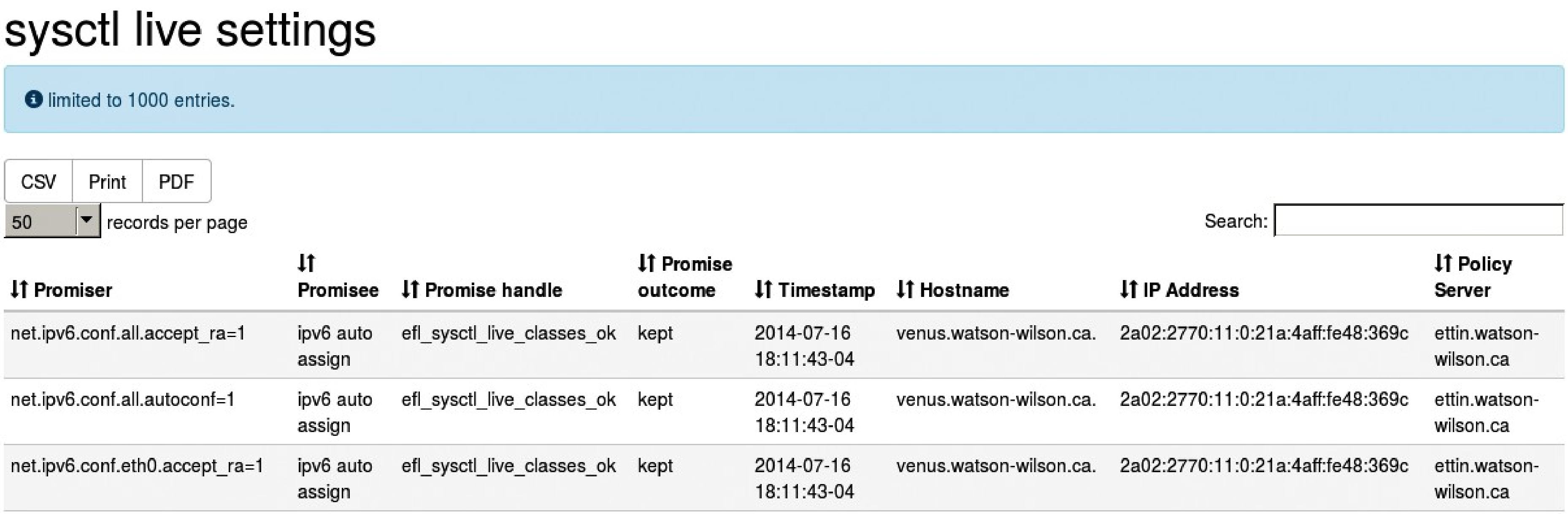
50 records per page

Promiser	Promisee	Promise handle	Promise outcome	Timestamp	Hostname	IP Address	Policy Server
/etc/ssh/sshd_config	Neil Watson	efl_service_files_config_template_permissions	kept	2014-07-16 18:01:15-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca
/etc/ssh/sshd_config	Neil Watson	efl_service_files_config_template	kept	2014-07-16 18:01:15-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca
/home/neil/.ssh	Neil Watson	efl_file_perms_files_recurse_with_base_postive	kept	2014-07-16 18:01:15-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca
/home/neil /.ssh/authorized_keys	Neil Watson	efl_edit_template_files_promiser	kept	2014-07-16 18:01:15-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca

CFEngine

EvolveThinking

Sysctl compliance



sysctl live settings

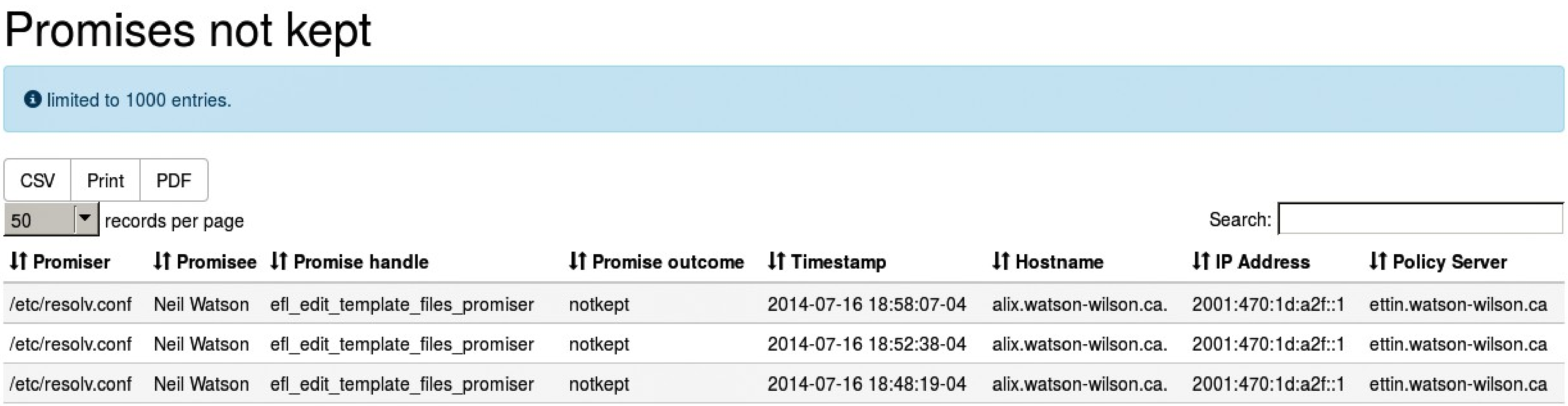
limited to 1000 entries.

50 records per page

Search:

Promiser	Promisee	Promise handle	Promise outcome	Timestamp	Hostname	IP Address	Policy Server
net.ipv6.conf.all.accept_ra=1	ipv6 auto assign	efl_sysctl_live_classes_ok	kept	2014-07-16 18:11:43-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca
net.ipv6.conf.all.autoconf=1	ipv6 auto assign	efl_sysctl_live_classes_ok	kept	2014-07-16 18:11:43-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca
net.ipv6.conf.eth0.accept_ra=1	ipv6 auto assign	efl_sysctl_live_classes_ok	kept	2014-07-16 18:11:43-04	venus.watson-wilson.ca.	2a02:2770:11:0:21a:4aff:fe48:369c	ettin.watson-wilson.ca

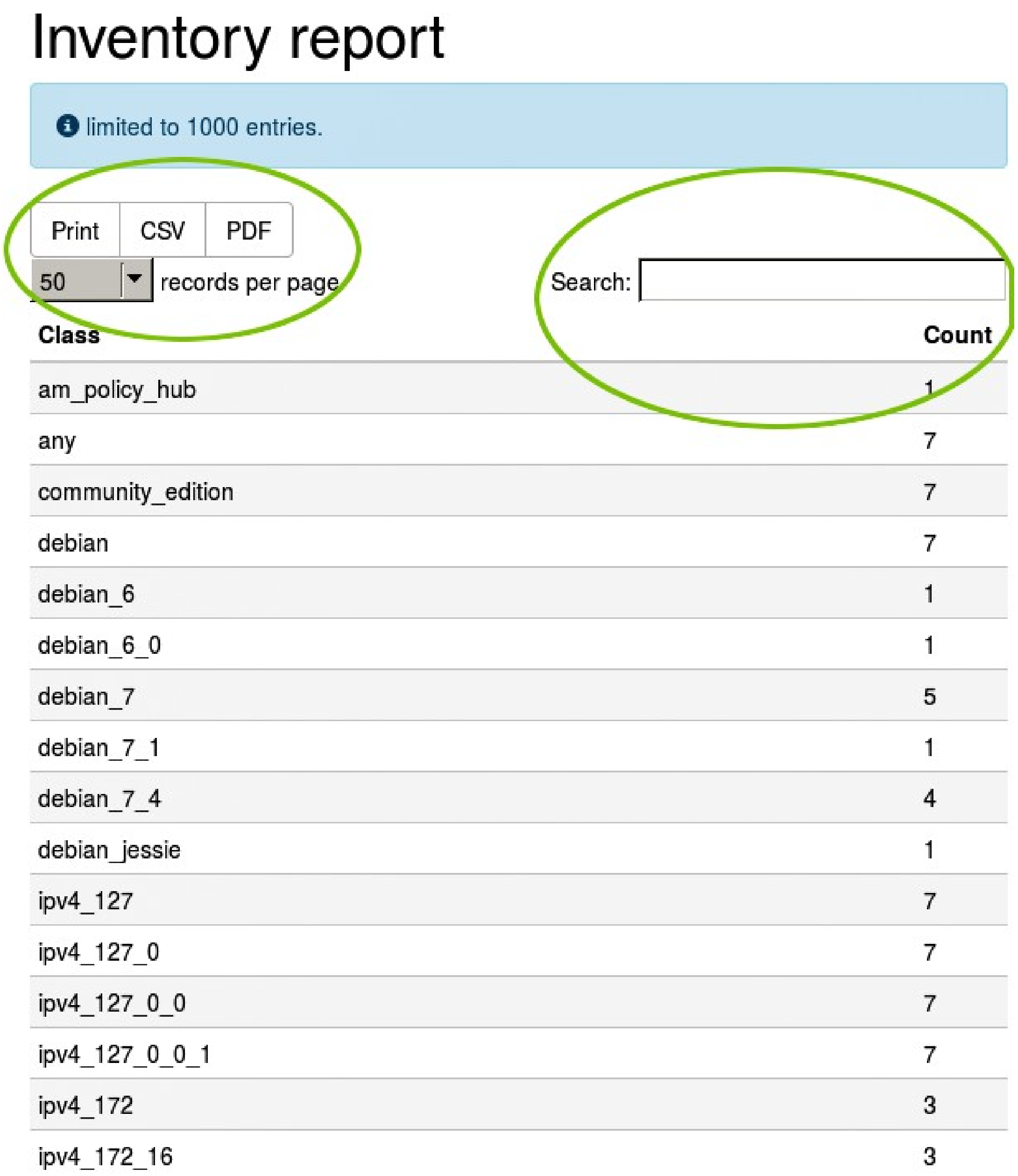
Promises kept



Promises not kept

limited to 1000 entries.

Promiser	Promisee	Promise handle	Promise outcome	Timestamp	Hostname	IP Address	Policy Server
/etc/resolv.conf	Neil Watson	efl_edit_template_files_promiser	notkept	2014-07-16 18:58:07-04	alix.watson-wilson.ca.	2001:470:1d:a2f::1	ettin.watson-wilson.ca
/etc/resolv.conf	Neil Watson	efl_edit_template_files_promiser	notkept	2014-07-16 18:52:38-04	alix.watson-wilson.ca.	2001:470:1d:a2f::1	ettin.watson-wilson.ca
/etc/resolv.conf	Neil Watson	efl_edit_template_files_promiser	notkept	2014-07-16 18:48:19-04	alix.watson-wilson.ca.	2001:470:1d:a2f::1	ettin.watson-wilson.ca



Inventory report

ℹ limited to 1000 entries.

50 records per page

Search:

Class	Count
am_policy_hub	1
any	7
community_edition	7
debian	7
debian_6	1
debian_6_0	1
debian_7	5
debian_7_1	1
debian_7_4	4
debian_jessie	1
ipv4_127	7
ipv4_127_0	7
ipv4_127_0_0	7
ipv4_127_0_0_1	7
ipv4_172	3
ipv4_172_16	3

Questions?

Contact me

- nwatson@evolvethinking.com
- Twitter neil_h_watson
- Evolvethinking.com
- http://demo.evolvethinking.com (user '**evolve**', passwd '**thinking**')