

How we deployed a datacenter in one click

ex-Blade Network Team: Cédric Hascoët, Jean-Christophe Legatte, Loïc Pailhas,
Sébastien Hurtel, Tchadel Icard, and Vincent Bernat

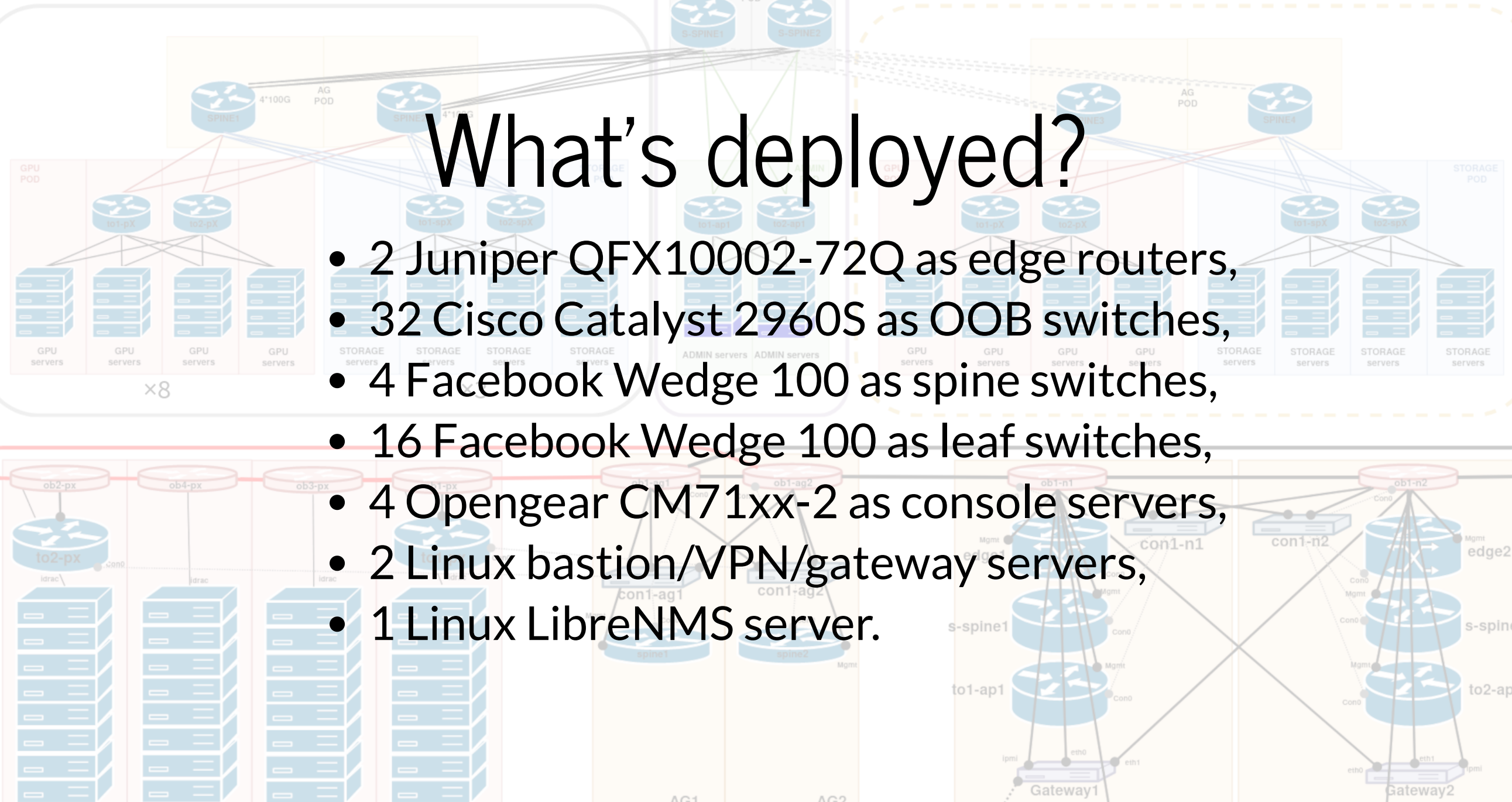
FRnOG 34 — October 1st, 2021

Production network

x5

What's deployed?

- 2 Juniper QFX10002-72Q as edge routers,
- 32 Cisco Catalyst 2960S as OOB switches,
- 4 Facebook Wedge 100 as spine switches,
- 16 Facebook Wedge 100 as leaf switches,
- 4 Opegear CM71xx-2 as console servers,
- 2 Linux bastion/VPN/gateway servers,
- 1 Linux LibreNMS server.



What's configured?

- Edge routers:
 - BGP configuration + policies
 - Routing engine protection
- BGP-based fabric (Facebook Wedge)
- Out-of-band fabric (Cisco)
- Administrative gateway (Linux)
 - ZTP
 - Firewall and NAT
 - Access to console servers
 - VPN to other sites
- External stores: DNS, IRR, RPKI, NetBox

Steps

1. Get space, power, cooling, racks, equipments, cabling done.
2. Install Debian 10 on gateway servers.
3. `./run-ansible-gitlab playbooks/site.yaml --limit=adm-gateway:\&location-ussfo03,none.`
4. Wait for all devices to autoprovision.
5. `./run-ansible-gitlab playbooks/site.yaml --limit=location-ussfo03.`

Source of truth

- No **NetBox**.
- **YAML** files versioned with **Git**.
 1. List of **devices**
 2. **Classifier**: from device name, attach properties to build a scope
 3. **Hierarchy definition** for data: given a scope, where to lookup data for a device
 4. **Data files**: flat YAML files fitted inside a hierarchy of directories

List of devices

devices:

USSF003

00B

- ob1-n1.ussfo03.blade-group.net
- ob2-n1.ussfo03.blade-group.net
- ob1-p1.ussfo03.blade-group.net
- ob2-p1.ussfo03.blade-group.net
- ob1-p2.ussfo03.blade-group.net

[...]

Classifier

matchers:

- '\.(ussfo03)\.':
 - location: '\1'
 - continent: us
- '^to([12])-[as]?p(\d+)\.':
 - member: '\1'
 - pod: '\2'
- '^to[12]-p\d+\.ussfo03\.':
 - groups:
 - tor-bgp
 - tor-bgp-compute
- '^to[12]-(p|ap|sp)\d+\.ussfo03\.':
 - os: cumulus
 - model: wedge100

Hierarchy definition

```
def searchpaths(scope):  
    paths = [  
        f"host/{scope[location]}/{scope[shorthost]]",  
        f"location/{scope[location]]",  
        f"os/{scope[os]}-{scope[model]]",  
        f"os/{scope[os]]",  
        'common'  
    ]  
    return paths
```


Data files

- Don't repeat yourself
- Data model should fit your needs

```
peer:  
  ix-sfmix:  
    rs-sfmix:  
      monitored: true  
      asn: 63055  
      remote:  
        - 206.197.187.253  
        - 2001:504:30::ba06:3055:1  
  blizzard:  
    asn: 57976  
    remote:  
      - 206.197.187.42  
      - 2001:504:30::ba05:7976:1  
    irr: AS-BLIZZARD
```

Commit by Loïc

```
commit 5c8d9169e5d6afa21b40bacbcd4bdec93d48a5b8
Author: loic pailhas <loic.pailhas@blade-group.com>
Date: Fri Sep 4 10:40:13 2020 +0200

[data] USSF003

classifier.yaml | 41 ++++++
data/groups/adm-gateway-ussfo03/bgp.yaml | 0
data/groups/adm-gateway-ussfo03/topology.yaml | 15 +++
data/groups/edge-ussfo03/bgp.yaml | 8 ++
data/groups/edge-ussfo03/system.yaml | 2 +
data/groups/spine-ussfo03/topology.yaml | 23 ++++
data/groups/sspine-ussfo03/topology.yaml | 9 ++
data/groups/tor-bgp-admin-ussfo03/topology.yaml | 3 +
data/groups/tor-bgp-compute-ussfo03/topology.yaml | 3 +
data/groups/tor-bgp-storage-ussfo03/topology.yaml | 3 +
data/groups/ussfo03/system.yaml | 3 +
data/groups/ussfo03/topology.yaml | 50 ++++++++
data/host/ussfo03/con1-ag1/topology.yaml | 16 +++
data/host/ussfo03/con1-ag2/topology.yaml | 15 +++
data/host/ussfo03/con1-n1/topology.yaml | 10 ++
data/host/ussfo03/con1-n2/topology.yaml | 10 ++
data/host/ussfo03/edge1/bgp.yaml | 7 ++
data/host/ussfo03/edge1/system.yaml | 2 +
data/host/ussfo03/edge1/topology.yaml | 126 ++++++
data/host/ussfo03/edge2/bgp.yaml | 46 ++++++
data/host/ussfo03/edge2/system.yaml | 2 +
data/host/ussfo03/edge2/topology.yaml | 123 ++++++
data/host/ussfo03/gateway1/bgp.yaml | 10 ++
data/host/ussfo03/gateway1/topology.yaml | 4 +
data/host/ussfo03/gateway2/bgp.yaml | 10 ++
data/host/ussfo03/gateway2/topology.yaml | 4 +
data/host/ussfo03/librenms1/apps.yaml | 2 +
data/host/ussfo03/librenms1/topology.yaml | 4 +
data/host/ussfo03/ob1-ag1/topology.yaml | 6 ++
data/host/ussfo03/ob1-ag2/topology.yaml | 5 +
data/host/ussfo03/ob1-n1/system.yaml | 2 +
data/host/ussfo03/ob1-n1/topology.yaml | 5 +
data/host/ussfo03/ob1-n2/system.yaml | 2 +
data/host/ussfo03/ob1-n2/topology.yaml | 6 ++
data/host/ussfo03/ob1-p1/topology.yaml | 3 +
data/host/ussfo03/ob1-p2/topology.yaml | 3 +
data/host/ussfo03/ob1-p3/topology.yaml | 3 +
data/host/ussfo03/ob1-p5/topology.yaml | 3 +
data/host/ussfo03/ob1-p8/topology.yaml | 3 +
data/host/ussfo03/ob1-sp3/topology.yaml | 3 +
data/host/ussfo03/ob2-p1/topology.yaml | 3 +
data/host/ussfo03/ob2-p2/topology.yaml | 3 +
data/host/ussfo03/ob2-p3/topology.yaml | 3 +
data/host/ussfo03/ob2-p5/topology.yaml | 3 +
data/host/ussfo03/ob2-p8/topology.yaml | 3 +
data/host/ussfo03/ob2-sp2/topology.yaml | 3 +
data/host/ussfo03/ob2-sp3/topology.yaml | 3 +
data/host/ussfo03/ob3-p1/topology.yaml | 3 +
data/host/ussfo03/ob3-p2/topology.yaml | 3 +
data/host/ussfo03/ob3-p3/topology.yaml | 3 +
data/host/ussfo03/ob3-p5/topology.yaml | 3 +
data/host/ussfo03/ob3-p8/topology.yaml | 3 +
data/host/ussfo03/ob3-sp2/topology.yaml | 3 +
data/host/ussfo03/ob3-sp3/topology.yaml | 3 +
data/host/ussfo03/ob4-p1/topology.yaml | 2 +
data/host/ussfo03/ob4-p2/topology.yaml | 3 +
data/host/ussfo03/ob4-p3/topology.yaml | 3 +
data/host/ussfo03/ob4-p5/topology.yaml | 3 +
data/host/ussfo03/ob4-p8/topology.yaml | 3 +
data/host/ussfo03/ob4-sp2/topology.yaml | 3 +
data/host/ussfo03/ob4-sp3/topology.yaml | 3 +
data/host/ussfo03/s-spine1/topology.yaml | 5 +
data/host/ussfo03/s-spine2/topology.yaml | 5 +
data/host/ussfo03/spine1/topology.yaml | 5 +
data/host/ussfo03/spine2/topology.yaml | 5 +
data/host/ussfo03/to1-ap1/topology.yaml | 5 +
data/host/ussfo03/to1-p1/topology.yaml | 5 +
data/host/ussfo03/to1-p2/topology.yaml | 5 +
data/host/ussfo03/to1-p3/topology.yaml | 5 +
data/host/ussfo03/to1-p5/topology.yaml | 5 +
data/host/ussfo03/to1-p8/topology.yaml | 5 +
data/host/ussfo03/to1-sp2/topology.yaml | 5 +
data/host/ussfo03/to1-sp3/topology.yaml | 5 +
data/host/ussfo03/to2-ap1/topology.yaml | 5 +
data/host/ussfo03/to2-p1/topology.yaml | 5 +
data/host/ussfo03/to2-p2/topology.yaml | 5 +
data/host/ussfo03/to2-p3/topology.yaml | 5 +
data/host/ussfo03/to2-p5/topology.yaml | 5 +
data/host/ussfo03/to2-p8/topology.yaml | 5 +
data/host/ussfo03/to2-sp2/topology.yaml | 5 +
data/host/ussfo03/to2-sp3/topology.yaml | 5 +
devices.yaml | 67 ++++++
jerikan/bgpptth.py | 1 +
84 files changed, 823 insertions(+), 5 deletions(-)
```

Jerikan

- Compile **configuration files** from **source of truth** and **templates**
- Faster than Ansible
- Easier to debug than Ansible
- Optionally checks generated configuration

Templates

- Using Jinja2
- Same as Ansible

```
system {
  ntp {
    {% for ntp in lookup("system", "ntp") %}
      server {{ ntp }};
    {% endfor %}
  }
  name-server {
    {% for dns in lookup("system", "dns") %}
      {{ dns }};
    {% endfor %}
  }
}
```

Error handling

```
templates/opengear/config.j2:15: in top-level template code
  config.interfaces.{{ interface }}.netmask {{ infos.address | ipaddr("netmask") }}
    continent = 'us'
    device    = 'con1-ag2.ussfo03.blade-group.net'
    environment = 'prod'
    host      = 'con1-ag2.ussfo03'
    infos    = {'address': '172.30.24.19/21'}
    interface = 'wan'
    location = 'ussfo03'
    loop     = <LoopContext 1/2>
    member   = '2'
    model    = 'cm7132-2-dac'
    os       = 'opengear'
    shorthost = 'con1-ag2'

-----
value = JerkianUndefined, query = 'netmask', version = False, alias = 'ipaddr'

[...]
    # Check if value is a list and parse each element
    if isinstance(value, (list, tuple, types.GeneratorType)):
        _ret = [ipaddr(element, str(query), version) for element in value]
        return [item for item in _ret if item]

> elif not value or value is True:
E   jinja2.exceptions.UndefinedError: 'dict object' has no attribute 'address'
```

Integration into GitLab

- Use merge request workflow
- Review changes to data files and templates
- Build generated configuration files
- Produce a diff

Integration into GitLab

```
Files changed (3) hide
edge2.ussfo03.blade-group.net/config-set.txt +7 -1
none/dns.yaml +12 -0
none/netbox.yaml +6 -0

edge2.ussfo03.blade-group.net/config-set.txt CHANGED
@@ -337,7 +337,10 @@
337 337 set interfaces et-0/0/11 disable
338 338 set interfaces et-0/0/13 disable
339 339 set interfaces et-0/0/17 disable
340 - set interfaces et-0/0/19 disable
+ set interfaces et-0/0/19 apply-groups firewall-ingress-protect
341 + set interfaces et-0/0/19 description "Transit: Telia [100G-LR4] (IC-99999)"
342 + set interfaces et-0/0/19 unit 0 family inet address 192.0.2.115/29
343 + set interfaces et-0/0/19 unit 0 family inet6 address 2001:db8:2:115::2/126
341 344 set interfaces et-0/0/23 disable
342 345 set interfaces et-0/0/25 description "Core: s-spine2 [100G-SR4]"
343 346 set interfaces et-0/0/25 hold-time up 3000 down 30
@@ -689,6 +692,7 @@
689 692 set policy-options route-filter-list T00-SPECIFIC-V6 ::/0 prefix-length-range /49-/128
690 693 set protocols lldp interface ae0
691 694 set protocols lldp interface et-0/0/1
695 + set protocols lldp interface et-0/0/19
692 696 set protocols lldp interface et-0/0/25
693 697 set protocols lldp interface et-0/0/29
694 698 set protocols lldp port-description-type interface-alias
@@ -699,8 +703,10 @@
699 703 set routing-instances internet instance-type virtual-router
700 704 set routing-instances internet instance-type virtual-router
701 705 set routing-instances internet instance-type virtual-router
706 + set routing-instances internet instance-type virtual-router
702 707 set routing-instances internet interface ae0.100
703 708 set routing-instances internet interface et-0/0/1.0
709 + set routing-instances internet interface et-0/0/19.0
704 710 set routing-instances internet interface et-0/0/25.100
705 711 set routing-instances internet interface et-0/0/29.100
706 712 set routing-instances internet interface lo0.666

none/dns.yaml CHANGED
@@ -97325,6 +97325,10 @@
...325 ...325 - name: 1.0.0.0.9.1.9.6.9.3.a.b.0.0.0.0.0.0.0.0.0.0.0.3.0.0.4.0.5.0.1.0.0.2.ip6.arpa.
...326 ...326 type: PTR
...327 ...327 value: xe-0-0-3-1-0.edge2.ussfo03.shadow.guru.
...328 + - name: et-0-0-19-0.edge2.ussfo03.shadow.guru.
...329 + type: A
...330 + value: 192.0.2.115
...331 + - name: 115.2.0.192.in-addr.arpa.
...332 + type: PTR
...333 + value: et-0-0-19-0.edge2.ussfo03.shadow.guru.
...334 + - name: et-0-0-19-0.edge2.ussfo03.shadow.guru.
...335 + type: AAAA
...336 + value: 2001:db8:2:115::2
...337 + - name: 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.1.1.0.2.0.0.8.b.d.0.1.0.0.2.ip6.arpa.
...338 + type: PTR
...339 + value: et-0-0-19-0.edge2.ussfo03.shadow.guru.
...328 ...340 - name: ae0-100.edge2.ussfo03.shadow.guru.
...329 ...341 type: A
...330 ...342 value: 69.58.92.9
```

Ansible

- Inventory generated by **Jerikan**
- Single playbook
- Idempotency is important
- `--diff` `--check` should work as expected
- `deploy` complete configuration

Further reading

- [Blog post about Jerikan+Ansible](#) (w/ demo)
- [GitHub repository](#) (free bundle: Jerikan, Ansible playbooks, data, templates and generated configuration for two datacenters)

