

脆弱性対応の仕組みを Zabbix&Ansibleで作ってみた

2016/5/21

DMM.comラボ インフラ統括本部XaaS部

岩崎 惣

アジェンダ

- Zabbix & Ansibleを使ったサーバ脆弱性対応
- Ansible 2.0で実装されたNetwork module
- Network機器管理の未来を考えてみる

はじめに

近年、Heartbleedなどの危険度の高い脆弱性が話題となり関心も高くなってきました。



名前	発生日	システム	CVE
Heartbleed	2014/4/7	OpenSSL	CVE-2014-0160
CCS Injection	2014/6/5	OpenSSL	CVE-2014-0224
ShellShock	2014/9/24	Bash	CVE-2014-6271
POODLE	2014/10/14	SSLv3.0	CVE-2014-3566
Grinch	2014/12/17	Linux kernel	CVE-2014-9322
FREAK	2015/1/8	SSL/TLS	CVE-2015-0204
GHOST	2015/1/28	glibc	CVE-2015-0235
Logjam	2015/5/13	SSL/TLS	CVE-2015-1716
VENOM	2015/5/13	QEMU	CVE-2015-3456
CacheBleed	2016/3/1	SSL/TLS	CVE-2016-0702
DROWN	2016/3/1	SSL/TLS	CVE-2016-0800
ImageTragick	2016/5/3	ImageMagick	CVE-2016-3714



弊社でも仮想化やクラウド利用で大量のサーバが有り
対応にかかるコストが馬鹿にならなくなってきたので
可能な限り自動化できる仕組みを考えてみました

動画・ライブ配信



BigData基盤



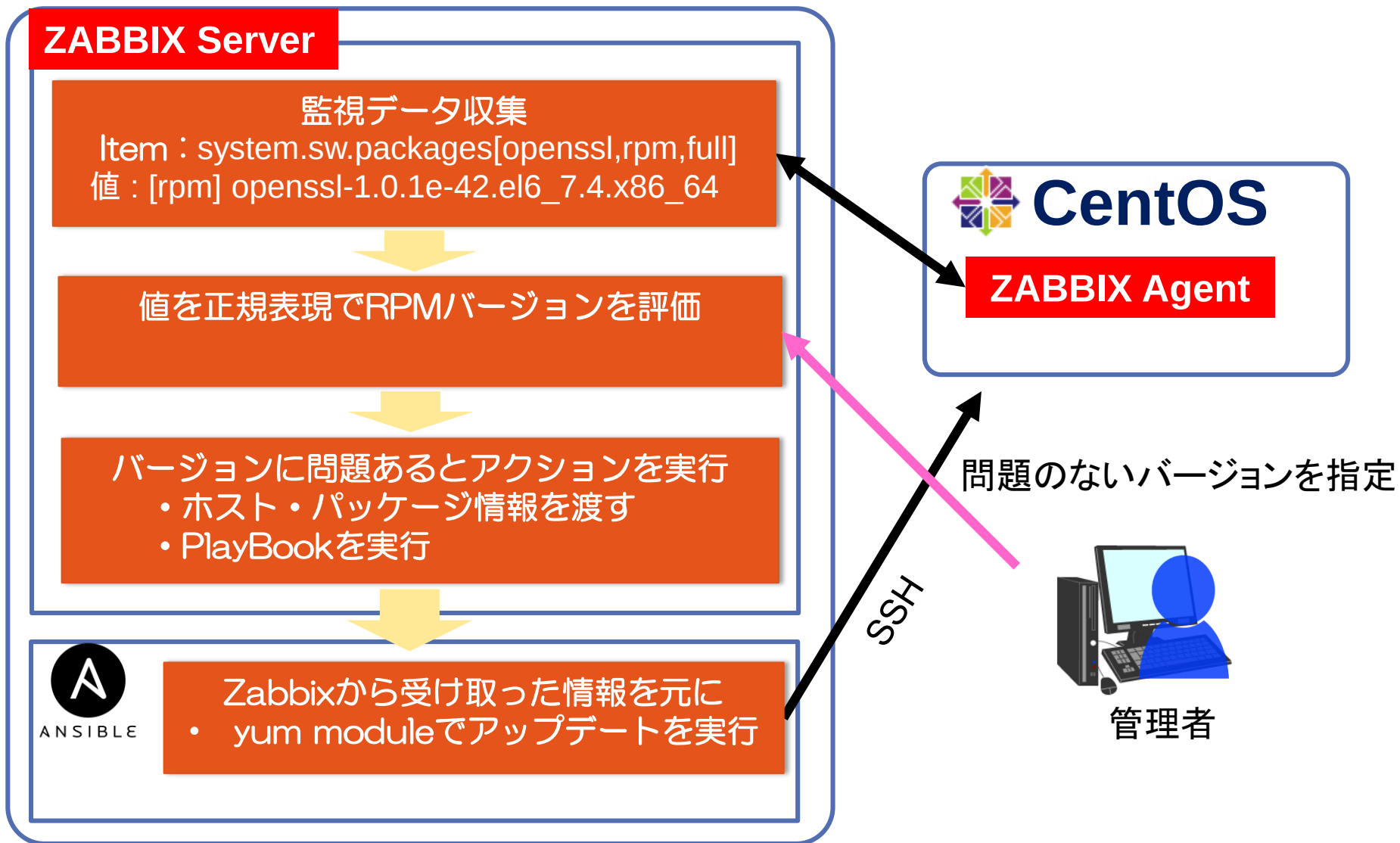
オンラインゲーム



その他サービス群



Zabbix & Ansibleで作るRPM管理の仕組み

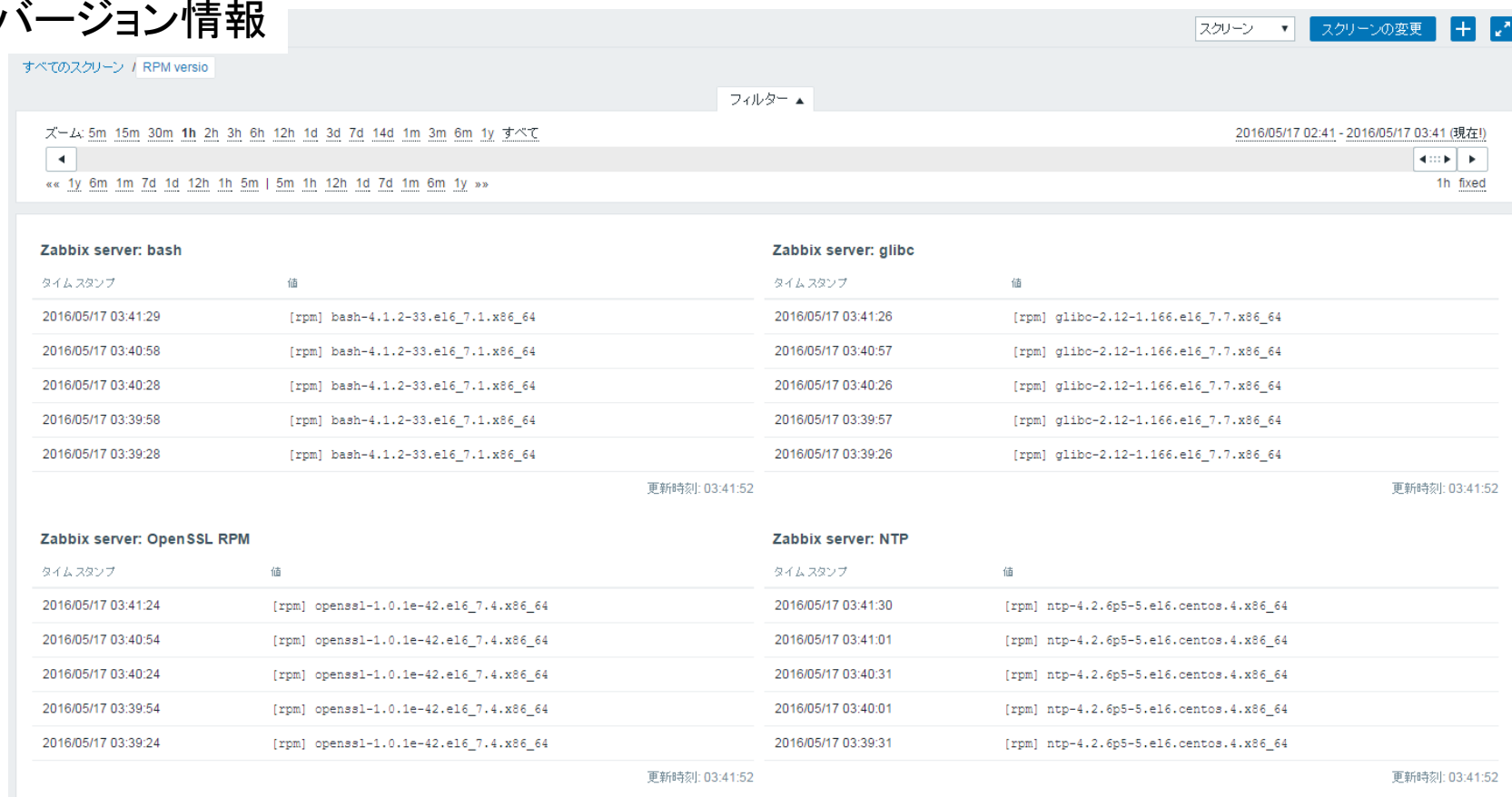


Zabbixでのバージョン情報

アイテム設定

名前 ▲	トリガー	キー	更新間隔	履歴	トレンド	タイプ	アプリケーション	ステータス
bash		system.sw.packages[bash,rpm,full]	30s	90d		Zabbixエージェント		有効
glibc		system.sw.packages["glibc-[0-9]",rpm,full]	30s	90d		Zabbixエージェント		有効
NTP		system.sw.packages["^ntp-",rpm,full]	30s	90d		Zabbixエージェント		有効
OpenSSL RPM		system.sw.packages[openssl,rpm,full]	30s	90d		Zabbixエージェント		有効

バージョン情報



JANOGということで、
ネットワーク機器でも同じようなことが
出来ないか考えてみました

Ansible

今年 1 月にAnsible 2.0がリリースされました。

RedHatから下記のようなリリース情報が出ました



The image is a screenshot of a Red Hat press release banner. The background is a dark, atmospheric photograph of a city street at night, with streetlights and a bridge visible. A large red diagonal stripe runs from the top left to the bottom right. The Red Hat logo is in the top left corner. Navigation links are at the top: 'テクノロジー' (Technology), 'サービス & サポート' (Service & Support), '世界のお客様導入事例' (World Customer Adoption Cases), and 'Red Hat について' (About Red Hat). The main headline is in large white Japanese characters. Below it is a sub-headline in smaller white Japanese characters.

redhat. テクノロジー サービス & サポート 世界のお客様導入事例 Red Hat について

プレスリリース

Red Hat、Ansibleの新機能によってネットワークでもDevOpsを実現

Ansibleのエージェントレスオートメーションフレームワークをネットワークインフラ機器に拡張、当初はArista、Cisco、Juniper等の機器をサポート

Ansible2.0で対応した機器一覧

対応機器

- A10
- Citrix
- Cumulus
- Arista EOS
- F5
- Cisco IOS, IOSXR, NXOS
- Juniper JUNOS



ARISTA



Cisco IOSのbinを変更してみる

Ansible Version: Ansible 2.0.2.0

機器 : Cisco Catalyst 2960C-12PC-L Switch



OS : IOS Version 12.2(55)EX3

```
NW015#show version
Cisco IOS Software, C2960C Software (C2960c405-UNIVERSALK9-M), Version 12.2(55)EX3, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Wed 10-Aug-11 06:40 by prod_rel_team
Image text-base: 0x00003000, data-base: 0x01A00000

ROM: Bootstrap program is C2960C boot loader
BOOTLDR: C2960C Boot Loader (C2960c405-HBOOT-M) Version 12.2(55r)EX9, RELEASE SOFTWARE (fc1)

NW015 uptime is 9 minutes
System returned to ROM by power-on
System image file is "flash:/c2960c405-universalk9-mz.122-55.EX3/c2960c405-universalk9-mz.122-55.EX3.bin"
```

Play book

```
---
- hosts: cisco
  connection: local
  gather_facts: no
  tasks:
    - name: scp file copy
      shell: sshpass -p {{ ansible_password }} scp {{ IOS_BIN_FILE }} {{ansible_user}}@{{ inventory_hostname }}:flash:c2960c405-universalk9-mz.150-2.SE2.bin

    - name: sh by cisco ios_command module
      ios_command:
        commands:
          - show boot
      << : &IOS_INFO
      host: "{{ inventory_hostname }}"
      username: "{{ ansible_user }}"
      password: "{{ ansible_password }}"
      authorize: true
      auth_pass: "{{ cisco_enable_secret }}"
      register: result

    - debug: var=result.stdout_lines

    - name: boot change
      ios_config:
        lines: ['boot system flash:c2960c405-universalk9-mz.150-2.SE2.bin']
      << : *IOS_INFO

    - name: sh by cisco ios_command module
      ios_command:
        commands:
          - show boot
      << : *IOS_INFO
      register: result

    - debug: var=result.stdout_lines
```

※ 書き方の注意として基本的にAnsibleを実行している環境で実行します

実行結果

```
[root@iwasaki playbooks]# ansible-playbook -i inventories/cisco cisco.yml
[WARNING]: log file at ansible.log is not writeable and we cannot create it, aborting

PLAY [cisco] *****

TASK [scp file copy] *****
changed: [172.17.0.100]

TASK [sh by cisco ios_command module] *****
ok: [172.17.0.100]

TASK [debug] *****
ok: [172.17.0.100] => [
  "result.stdout_lines": [
    [
      "BOOT path-list      : flash:c2960c405-universalk9-mz.122-55.EX3.bin",
      "Config file         : flash:/config.text",
      "Private Config file  : flash:/private-config.text",
      "Enable Break         : no",
      "Manual Boot          : no",
      "HELPER path-list     : ",
      "Auto upgrade         : yes",
      "Auto upgrade path    : ",
      "NVRAM/Config file",
      "  buffer size:      65536",
      "Timeout for Config",
      "  Download:         0 seconds",
      "Config Download ",
      "  via DHCP:         disabled (next boot: disabled)"
    ]
  ]
]

TASK [boot change] *****
changed: [172.17.0.100]
```

実行結果

```
TASK [sh by cisco ios_command module] *****
ok: [172.17.0.100]

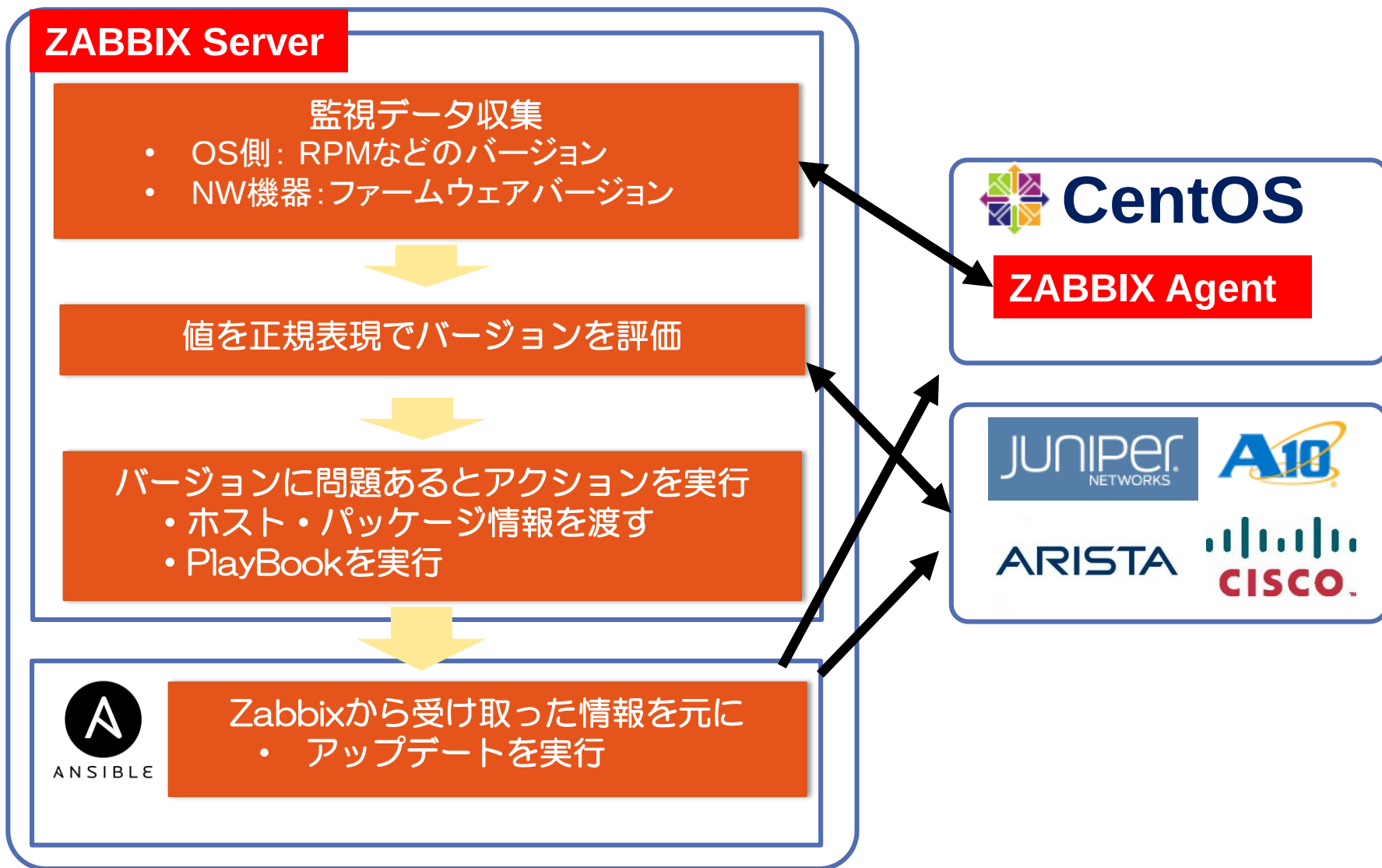
TASK [debug] *****
ok: [172.17.0.100] => {
  "result.stdout_lines": [
    [
      "BOOT path-list      : flash:c2960c405-universalk9-mz.150-2.SE2.bin",
      "Config file         : flash:/config.text",
      "Private Config file  : flash:/private-config.text",
      "Enable Break         : no",
      "Manual Boot          : no",
      "HELPER path-list     : ",
      "Auto upgrade         : yes",
      "Auto upgrade path    : ",
      "NVRAM/Config file",
      "    buffer size:     65536",
      "Timeout for Config",
      "    Download:        0 seconds",
      "Config Download ",
      "    via DHCP:         disabled (next boot: disabled)"
    ]
  ]
}

PLAY RECAP *****
172.17.0.100          : ok=5    changed=1    unreachable=0    failed=0
```

IOSをAnsibleから触ってみて

- Ansibleの仕様の的に仕方がないが初期設定では使えない
- ファームウェアアップデート可能な事はわかった
- moduleを使うととりあえずIOSのコマンド全てが利用できる
- ネットワーク機器moduleのAnsibleドキュメントは間違いが多いので自分で触ってみないとわからない部分が多い
- VLAN追加などの、設定変更での活用が望ましい

Zabbix & Ansibleで作る未来



まとめ

- 今回は、脆弱性対応のための脆弱性アップデートをクローズアップしましたが、Zabbixのアラートを基点に設定変更なども可能なのである程度自動での障害対応が可能ではないかと思います
- Ansibleは、マルチベンダーで利用している環境で力を発揮すると思いました

Thank You!!

DMM.com Labo