Správa Cisco prvků pomocí Ansible

Martin Bílý

bily@fit.cvut.cz
twitter: _mbily

Proč?

- Snadná úprava konfigurace většího počtu switchů
- Sjednocená konfigurace
- Šablony portů, ACL, ...
- Srozumitelnost konfigurace i pro non-cisco lidi
- Verzování git, gitlab, merge requests

Čeho můžeme dosáhnout?

Konfigurační soubor jednoho switche

```
---

ports_template: template-test

ports:
  - { port: FastEthernet0/1, mode: access, vlan: 21, description: "Franta" }
  - { port: FastEthernet0/2, mode: access, vlan: 24, description: "Karel" }
  - { port: FastEthernet0/3, mode: trunk, native: 22, allowed: 22-25, description: "Srv" }
  - { port: FastEthernet0/4, mode: shutdown }
  - { port: FastEthernet0/5, mode: shutdown }
  - { port: FastEthernet0/6, mode: access, vlan: 21, description: "Small Server"  }
# Gi0/1 uplink
```

Co budeme potřebovat?

- ansible, verze alepoň 2.1
- python 2.7
- aktivní prvky Cisco, systém IOS
- (tftp server)

Ansible, Network Modules for IOS

http://docs.ansible.com/ansible/list_of_network_modules.html

ios_command
běžné ne-konfigurační příkazy (show, copy, ...)
ios_config
konfigurační příkazy, uvedené přímo v ansible tasku
ios_template
konfigurační příkazy v podobě ansible template (Jinja .j2)
od v2.2 deprecated
ios_facts
typ, seriové číslo, verze IOS, **konfigurace**, ...
nově od v2.2

Soubory

hosts, credentials.yml, main.yml
files
group_vars all
host_vars sw-test
roles
role-name
tasks main.yml
handlers main.yml
templates tmpl.j2

main.yml

```
---

- hosts: all
  connection: local
  gather_facts: no
  any_errors_fatal: true

  roles:
  - prepare

- hosts: all
  connection: local
  gather_facts: no
  serial: 1
  roles:
  - preports

- hosts: all
  connection: local
  gather_facts: no
  roles:
  - configure
```

roles/configure/tasks/main.yml

```
- name: common config
  ios_config:
        provider: "{{ provider }}"
        config: "{{ running }}"
        lines:
        - service timestamps log datetime localtime
        - service timestamps debug datetime localtime
        - service password-encryption
        - hostname {{ inventory_hostname }}
        match: line
  notify:
        - wrmem
```

/roles/configure/handlers/main.yml

```
---

- name: wrmem
  ios_command:
        provider: "{{ provider }}"
        timeout: 120
        commands:
        - write memory
```

roles/configure/tasks/main.yml

```
- name: no spanning-tree portfast default
  ios_config:
        provider: "{{ provider }}"
        config: "{{ running }}"
        lines:
        - no spanning-tree portfast default
        match: line
  when: running.find("\nspanning-tree portfast default") != -1
  notify:
        - wrmem
```

Hierarchické skupiny (bloky)

```
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
 path tftp://1.2.3.4/periodic/$h-
 write-memory
 time-period 720
```

```
- name: archive
  ios_config:
      provider: "{{ provider }}"
      config: "{{ running }}"
      parents:
      - archive
      lines:
      - log config
      - path tftp://{{ tftp_server }}/periodic/$h-
      - write-memory
      - time-period 720
      match: line
      before:
      - no archive
# re-create sub-block config after:
      - log config
      - logging enable
      - notify syslog contenttype plaintext
      - hidekeys
      replace: block
  notify: wrmem
```

```
- name: recovery old
  ios_config:
        provider: "{{ provider }}"
        config: "{{ running }}"
        lines:
        - udld aggressive
        - errdisable recovery cause udld
        ...
        - errdisable recovery interval 180
        match: line
  when: recovery_version == "old"
  notify: wrmem
```

files/test.ports.yml

```
- name: access port
  ios_config:
        provider: "{{ provider }}"
        config: "{{ running }}"
        parents:
        - interface {{ item.port | mandatory }}
        lines:
        - description {{ item.description | mandatory }}
        - switchport access vlan {{ item.vlan |
mandatory }}
        - switchport mode access
        - switchport nonegotiate
        match: exact
         before:
        - default interface {{ item.port }}
        replace: block
        timeout: 60
    when: item.mode == "access"
    with_items: '{{ ports }}'
    notify: wrmem

-name: trunk port
  ...
-name: shutdown port
  ...
```

roles/preports/tasks/main.yml

```
---

- name: ports template
  template: src={{ ports_template }}.ports.j2 dest=files/{{ ports_template }}.ports.yml
  when: (ports_template is defined) and (ports is defined)
```

roles/preports/templates/test.ports.j2

```
---
- name: access port
{%- set port_mode='access' %}
{% include 'port_begin.j2' %}
{% raw %}
      - description {{ item.description | mandatory }}
      - switchport access vlan {{ item.vlan | mandatory }}
      - switchport mode access
      - switchport nonegotiate
{% endraw %}
{% include 'port_end.j2' %}
```

roles/preports/templates/port_begin.j2

```
{% raw %}
  ios_config:
        provider: "{{ provider }}"
        config: "{{ running }}"
        parents:
        - interface {{ item.port | mandatory }}
        lines:
{% endraw %}
```

roles/preports/templates/port_end.j2

```
{% raw %}
        match: exact
        before:
        - default interface {{ item.port }}
        replace: block
        timeout: 60
{% endraw %}
  when: item.mode == {{ "" }}{{ port_mode }}{{ "" }}
{%- raw %}
  with_items: '{{ ports }}'
  notify: wrmem
{% endraw %}
```

roles/prepare/tasks/main.yml

```
---
- name: include credentials
  include_vars: credentials.yml

- name: credentials
  set_fact:
        provider:
        username: "{{ credentials['username'] }}"
        password: "{{ credentials['password'] }}"
        host: "{{ inventory_hostname }}"
```

```
# without tftp
- name: get running-config
  ios_command:
        provider: "{{ provider }}"
        timeout: 300
        commands:
        - show running-config
  register: tmp
  until: tmp.stdout[0].find("\nend") != -1
  retries: 10
    when: use_tftp is not defined

- set_fact:
        running: "{{ tmp.stdout[0] }}"
  when: use_tftp is not defined
```

```
- set_fact:
        running: "{{ tmp.stdout[0] }}"
  when: use_tftp is not defined
```

```
# with tftp 1/3
- name: remove old config files
  file:
        state: absent
        path: /tftpboot/ansible/{{ inventory_hostname }}.cfg
  changed_when: false
- name: set prompt quiet
  ios_config:
        provider: "{{ provider }}"
        force: yes
        lines:
        - file prompt quiet
  when: use_tftp is defined
  changed_when: false
```

```
# with tftp 2/3
- name: copy running-config to tftp
  ios_command:
        provider: "{{ provider }}"
        timeout: 120
        commands:
        - copy running-config tftp://{{ tftp_server }}/ansible/{{ inventory_hostname }}.cfg
  when: use_tftp is defined
```

 # with tftp 3/3

```
- name: wait for EOF
  wait_for:
       path: /tftpboot/ansible/{{ inventory_hostname }}.cfg
       search_regex: "^end$"
  when: use_tftp is defined

- name: set_fact from tftp
  set_fact:
       running: "{{ lookup('file', '/tftpboot/ansible/{{ inventory_hostname }}.cfg') }}"
  when: use_tftp is defined
```