Ansible Collection - NFTables

AnsibleGuy

Mar 18, 2024

USAGE

Tip: Check out the repository on GitHub

Tip: Check out the repository on GitHub

CHAPTER

ONE

1 - INSTALLATION

1.1 Ansible

See the documentation on how to install Ansible.

1.2 Dependencies

1.2.1 Using Shell

First - install nftables!

For the python library to work the installed NFTables version needs to be >= 0.9.3

```
sudo apt install nftables

# check the installed version
sudo apt policy nftables
```

The ansible-modules of this collection use the python3-nftables module to interact with nftables.

You can either install it using your package manager (*apt in the example*) or using pip (*unofficial version provided by AnsibleGuy *) on the target system.

```
# package manager
sudo apt install python3-nftables

# pip => make sure it is installed for the root user or use a virtualenv
sudo pip install ansibleguy-nftables
```

1.2.2 Using Ansible

```
- name: Installing NFTables
  ansible.builtin.package:
    name: ['nftables']  # or ['nftables', 'python3-nftables]

- name: Installing NFTables python-module
  ansible.builtin.pip:
    name: 'ansibleguy-nftables'
```

(continues on next page)

(continued from previous page)

```
- name: Enabling and starting NFTables
  ansible.builtin.service:
    name: 'nftables.service'
    state: started
    enabled: true
```

1.3 Collection

```
# unstable/latest version:
ansible-galaxy collection install git+https://github.com/ansibleguy/collection_nftables.
↪git

# install to specific director for easier development
cd $PLAYBOOK_DIR
ansible-galaxy collection install git+https://github.com/ansibleguy/collection_nftables.
↪git -p ./collections
```

Tip: Check out the repository on GitHub

CHAPTER

TWO

2 - BASIC

2.1 Documentation

- Overview
- Man Page
- Ruleset Element definition
- Statement definition

2.2 Basics

2.2.1 Running

These modules support check-mode and can show you the difference between existing and configured items:

```
# show differences
ansible-playbook nftables.yml -D

# run in check-mode (no changes are made)
ansible-playbook nftables.yml --check
```

Tip: Check out the repository on GitHub

CHAPTER

THREE

1 - BASIC MODULE ARGUMENTS

3.1 All modules

Table 1: Definition

Parameter	Type	Required	Default	Comment
debug	boolean	false	false	Used to en-/disable the debug mode
state	string	false	present	One of ‘present’, ‘absent’. Add or remove the entry

Tip: Check out the repository on GitHub

CHAPTER

FOUR

CHAINS

Warning: This module is still in development!

STATE: testing

TESTS: ansibleguy.nftables.chain

NFTables Docs:

- Documentation on chains

4.1 Definition

For basic parameters see: *Basic*

4.1.1 ansibleguy.nftables.chain

Table 1: Definition

Parameter	Type	Required	Default	Aliases	Comment
table	string	true	-	t	The name of the table
table_family	string	true	-	table_type, tt, table_fam, tt	One of: 'inet', 'ip6', 'ip', 'arp', 'bridge', 'netdev'. Table type
name	string	true	-	n, chain	The name of the chain
hook	string	false	-	h	One of: 'ingress', 'prerouting', 'forward', 'input', 'output', 'postrouting'. Chain hook
policy	string	false	-	p, pol, implicit	One of: 'accept', 'drop'. Implicit rule policy to use
type	string	false	filter	t	One of: 'filter', 'nat', 'route'. Chain type
priority	string	false	0	p, prio	One of: -400, -300, -225, -200, -150, -100, 0, 50, 100, 225, 300. Chain priority
device	string	false	-	dev	Device to use if the chains type is 'netdev'
comment	string	false	-	c, cmt	-

4.2 Usage

Changes on existing chains must be enforced using the 'force' parameter.

Be aware: If a chain changed it needs to be removed and re-added to apply those changes! **All of its rules are dropped!**

4.3 Examples

4.3.1 ansibleguy.nftables.chain

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.chain:
        table: 'main'
        table_family: 'ip'
        name: 'example'
        # hook: ''
        # policy: ''
        # type: 'filter'
        # priority: 0
        # device: ''
        # comment: ''
        # force: false
        # state: present

    - name: Adding chain to manage forward-traffic
      ansibleguy.nftables.chain:
        table: 'main'
        table_family: 'ip'
        name: 'example'
        hook: 'forward'
        policy: 'drop'

    - name: Adding comment to chain
      ansibleguy.nftables.chain:
        table: 'main'
        table_family: 'ip'
        name: 'fwd'
        hook: 'forward'
        policy: 'drop'
        comment: 'forwarding traffic'

    - name: Pulling existing chains
```

(continues on next page)

(continued from previous page)

```
    ansibleguy.nftables.list:
      target: 'chains'
    register: chains

  - name: Showing chains
    ansible.builtin.debug:
      var: chains.data

  - name: Adding sub-chain
    ansibleguy.nftables.chain:
      table: 'main'
      table_family: 'ip'
      name: 'sub'
      comment: 'chain used for some special stuff'

  - name: Removing forwarding-chain
    ansibleguy.nftables.chain:
      table: 'main'
      table_family: 'ip'
      name: 'fwd'
      state: absent
      force: true
```

Tip: Check out the repository on GitHub

CHAPTER

FIVE

COUNTERS

Warning: This module is still in development!

STATE: development

TESTS: ansibleguy.nftables.counter

NFTables Docs:

- Documentation on counters

5.1 Definition

For basic parameters see: *Basic*

5.1.1 ansibleguy.nftables.counter

5.2 Usage

5.3 Examples

5.3.1 ansibleguy.nftables.counter

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.counter:
```

Tip: Check out the repository on GitHub

CHAPTER

SIX

LIMITS

Warning: This module is still in development!

STATE: development

TESTS: ansibleguy.nftables.limit

NFTables Docs:

- Documentation on limits

6.1 Definition

For basic parameters see: *Basic*

6.1.1 ansibleguy.nftables.limit

6.2 Usage

6.3 Examples

6.3.1 ansibleguy.nftables.limit

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.limit:
```

Tip: Check out the repository on GitHub

CHAPTER

SEVEN

LIST

STATE: testing

TESTS: ansibleguy.nftables.list

7.1 Definition

For basic parameters see: *Basic*

7.1.1 ansibleguy.nftables.list

Table 1: Definition

Parameter	Type	Required	Default	Aliases	Comment
target	string	true	-	t, tgt	One of: 'tables', 'chains', 'rules'. What you want to query
filter_tables	list	false	-	ft, tables	Add the tables you want to query to this list. The table format must be '{family} {name}' as tables can have non-unique names.
filter_chains	list	false	-	fc, chains	Add the chains you want to query to this list.

7.2 Examples

7.2.1 ansibleguy.nftables.list

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
```

(continues on next page)

(continued from previous page)

```
      ansibleguy.nftables.list:
        target: 'rules'
        # filter_tables: 'ip filter'
        # filter_chains: 'ufw-not-local'

    - name: Pulling existing tables
      ansibleguy.nftables.list:
        target: 'tables'
      register: nftables_tables

    - name: Show tables
      ansible.builtin.debug:
        var: nftables_tables.data

    # ["ip filter", "ip6 filter"]

    - name: Pulling existing chains of table 'ip filter'
      ansibleguy.nftables.list:
        target: 'chains'
        filter_tables: 'ip filter'  # 'ip' = family, 'filter' = name
      register: nftables_chains

    - name: Show chains
      ansible.builtin.debug:
        var: nftables_chains.data

    # {"ip filter": ["input", "output", "route"]}

    - name: Pulling existing rules of chain 'input' in table 'ip filter'
      ansibleguy.nftables.list:
        target: 'rules'
        filter_tables: 'ip filter'
        filter_chains: 'input'
      register: nftables_rules

    - name: Show rules
      ansible.builtin.debug:
        var: nftables_rules.data

    # {"ip filter": {
    #   "input": [
    #     {"handle": "113", "rule": "fib daddr type local counter packets 0 bytes 0␣
↪return"}
    #   ]
    # }}
```

Tip: Check out the repository on GitHub

CHAPTER

EIGHT

RULES

TESTS: ansibleguy.nftables.rule | ansibleguy.nftables.rule_raw

NFTables Docs:

- Source-nat
- Destination-nat
- Masquerading

8.1 Definition

For basic parameters see: *Basic*

Table 1: Definition

Parameter	Type	Required	Default	Aliases	Comment
id	string	true	-	uid, name, identifier	Unique identifier of the rule. Used to match the configured rules with the existing ones. This id is added at the beginning of the rule's comment field.
table	string	false	-	t, target_table	The name of the table this rule should be inserted into. If only one exists you don't need to provide its name.
table_type	string	false	'ip'	tt, target_table_	One of: 'inet', 'ip6', 'ip', 'arp', 'bridge', 'netdev'. The type of the table this rule should be inserted into.
chain	string	true	-	c, target_chain	The name of the chain this rule should be inserted into.
before	string	false	-	before_id	This rule should be placed before a specific other rule. Provide the unique identifier of the other rule!
after	string	false	-	after_id	This rule should be placed after a specific other rule. Provide the unique identifier of the other rule!

8.1.1 ansibleguy.nftables.rule_raw

STATE: testing

Table 2: Definition

Parameter	Type	Required	Default	Aliases	Comment
rule	string	false for deletion else true	-	raw, line, content	The raw rule to add to the config

8.1.2 ansibleguy.nftables.rule

STATE: development

8.2 Usage

Rules are identified/matched using an **unique ID**.

You need to provide one for every rule you manage!

That ID is added at the beginning of the rule's comment field. The ID is separated from the comment using a backslash (\) as separator. Because of this that character will be replaced by an underscore (_) if found in the comment field!

8.3 Examples

8.3.1 ansibleguy.nftables.list

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Pulling existing rules
      ansibleguy.nftables.list:
        target: 'rules'
      register: rules

    - name: Show rules
      ansible.builtin.debug:
        var: rules.data
```

8.3.2 ansibleguy.nftables.rule_raw

```yaml
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.rule_raw:
        id: 'example_id'
        chain: 'target_chain'
        # table: ''
        # table_type: ''
        # before: ''
        # after: ''
        rule: 'iifname "lo" accept comment "Allow loopback traffic"'

    - name: Adding rule
      ansibleguy.opnsense.rule_raw:
        id: '11'
        chain: 'input'
        table: 'filter'
        table_type: 'ip'
        rule: 'iifname "lo" accept comment "Allow loopback traffic"'

    - name: Moving rule before rule 14
      ansibleguy.opnsense.rule_raw:
        id: '11'
        chain: 'input'
        table: 'filter'
        table_type: 'ip'
        rule: 'iifname "eno1" accept comment "Allow some traffic"'
        before: '14'

    - name: Removing
      ansibleguy.opnsense.rule_raw:
        id: '11'
        chain: 'input'
        table: 'filter'
        table_type: 'ip'
        state: absent
```

Tip: Check out the repository on GitHub

CHAPTER

NINE

SETS

Warning: This module is still in development!

STATE: development

TESTS: ansibleguy.nftables.set

NFTables Docs:

- Documentation on sets

9.1 Definition

For basic parameters see: *Basic*

9.1.1 ansibleguy.nftables.set

9.2 Usage

9.3 Examples

9.3.1 ansibleguy.nftables.set

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.set:
```

Tip: Check out the repository on GitHub

CHAPTER

TEN

TABLES

Warning: This module is still in development!

STATE: testing

TESTS: ansibleguy.nftables.table

NFTables Docs:

- Documentation on tables

10.1 Definition

For basic parameters see: *Basic*

10.1.1 ansibleguy.nftables.table

Table 1: Definition

Parameter	Type	Required	Default	Aliases	Comment
name	string	true	-	n, table	The name of the table
family	string	true	-	f, fam, type	One of: 'inet', 'ip6', 'ip', 'arp', 'bridge', 'netdev'. Table type

10.2 Usage

Changes on existing tables must be enforced using the 'force' parameter.

Be aware: If a table changed it needs to be removed and re-added to apply those changes! **All of its chains and rules are dropped!**

10.3 Examples

10.3.1 ansibleguy.nftables.table

```yaml
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.table:
        name: 'example'
        family: 'inet'
        # force: false
        # state: present

    - name: Adding inet table 'test'
      ansibleguy.nftables.table:
        name: 'test'
        family: 'inet'

    - name: Pulling existing tables
      ansibleguy.nftables.list:
        target: 'tables'
      register: tables

    - name: Showing tables
      ansible.builtin.debug:
        var: tables.data

    - name: Removing inet table 'test'
      ansibleguy.nftables.table:
        name: 'test'
        family: 'inet'
        state: absent
        force: true
```

Tip: Check out the repository on GitHub

CHAPTER

ELEVEN

VARIABLES

Warning: This module is still in development!

STATE: development

TESTS: ansibleguy.nftables.var

NFTables Docs:

- Documentation on variables

11.1 Definition

For basic parameters see: *Basic*

11.1.1 ansibleguy.nftables.var

11.2 Usage

11.3 Examples

11.3.1 ansibleguy.nftables.var

```
- hosts: all
  gather_facts: no
  become: true
  tasks:
    - name: Example
      ansibleguy.nftables.var:
```