```
Started by user Aicha War
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Clone tools source codes)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ mkdir -p /Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0
[Pipeline] sh
+ git clone https://github.com/ansible/ansible.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0'...
[Pipeline] sh
+ git clone -b v2.0.0-0.1.alpha1 --depth 1
https://github.com/ansible/ansible.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.
0-0.1.alpha1'...
Note: switching to '2df6513f8d802a931e0fa88afa6dc019ba4bd6e6'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:
  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v1.0 --depth 1 https://github.com/ansible/ansible.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0'
...
Note: switching to '6a64e9f0248d402aa60faf33bc720acbcd56e50b'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0
[Pipeline] sh
+ git clone https://github.com/hashicorp/terraform.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1'.
..
[Pipeline] sh
+ git clone -b v1.0.0 --depth 1 https://github.com/hashicorp/terraform.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0
```

```
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.
0.0'...
Note: switching to 'b99f7beaad41a3290330621897e244030d020504'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v0.1.0 --depth 1 https://github.com/hashicorp/terraform.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.
1.0'...
Note: switching to 'fd889083c26a6d68fae646627323e06f5dd81730'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0
```

```
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0
[Pipeline] sh
+ git clone https://github.com/chef/chef.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2'...
Updating files:  66% (2367/3578)
Updating files:  67% (2398/3578)
Updating files:  68% (2434/3578)
Updating files:  69% (2469/3578)
Updating files:  70% (2505/3578)
Updating files:  71% (2541/3578)
Updating files:  72% (2577/3578)
Updating files:  73% (2612/3578)
Updating files:  74% (2648/3578)
Updating files:  75% (2684/3578)
Updating files:  76% (2720/3578)
Updating files:  77% (2756/3578)
Updating files:  78% (2791/3578)
Updating files:  79% (2827/3578)
Updating files:  80% (2863/3578)
Updating files:  81% (2899/3578)
Updating files:  82% (2934/3578)
Updating files:  83% (2970/3578)
Updating files:  84% (3006/3578)
Updating files:  85% (3042/3578)
Updating files:  86% (3078/3578)
Updating files:  87% (3113/3578)
Updating files:  88% (3149/3578)
Updating files:  89% (3185/3578)
Updating files:  90% (3221/3578)
Updating files:  91% (3256/3578)
Updating files:  92% (3292/3578)
Updating files:  93% (3328/3578)
Updating files:  94% (3364/3578)
Updating files:  95% (3400/3578)
Updating files:  96% (3435/3578)
Updating files:  97% (3471/3578)
Updating files:  98% (3507/3578)
Updating files:  99% (3543/3578)
Updating files: 100% (3578/3578)
Updating files: 100% (3578/3578), done.
[Pipeline] sh
+ git clone -b v18.0.0 --depth 1 https://github.com/chef/chef.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0'
...
Note: switching to '1be18b7b48e9aa2829583ca56dc4a99a07bb5ac1'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>
```

```
Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v17.0.0 --depth 1 https://github.com/chef/chef.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0'
...
Note: switching to 'a1c7f81c4956322a5095a42d8446db43d521e89a'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0
[Pipeline] sh
+ git clone https://github.com/puppetlabs/puppet.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3'...
[Pipeline] sh
+ git clone -b 8.0.0 --depth 1 https://github.com/puppetlabs/puppet.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0'
...
Note: switching to 'f431150d36545626af9ad8602cdd6a7461ca025b'.
```

```
You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b 7.0.0 --depth 1 https://github.com/puppetlabs/puppet.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0'
...
Note: switching to 'f664d6a21656f80b54b396529c84ee7e24108921'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
[Pipeline] sh
```

```
+ git clone https://github.com/hashicorp/vagrant.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4'...
[Pipeline] sh
+ git clone -b v2.0.0 --depth 1 https://github.com/hashicorp/vagrant.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.
0'...
Note: switching to 'd1cf0f77e761289f0cc0b119067ba1903a2891c9'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v1.0.0 --depth 1 https://github.com/hashicorp/vagrant.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.
0'...
Note: switching to 'aafa79fe66db687da265d790d5e67a2a7ec30d92'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Clone scripts source codes)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
```

```
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0
[Pipeline] sh
+ git clone https://github.com/geerlingguy/ansible-for-devops.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansib
le-for-devops/0'...
[Pipeline] sh
+ git clone -b 2.0 --depth 1 https://github.com/geerlingguy/ansible-for-
devops.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansib
le-for-devops/2.0'...
Note: switching to '3c069f36008699da982a96ed65c72f1de11a6e5a'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b 1.0 --depth 1 https://github.com/geerlingguy/ansible-for-
devops.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0
```

```
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansib
le-for-devops/1.0'...
Note: switching to '64198c39f6eababcabff556f3981d350c949e1ed'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4
[Pipeline] sh
+ git clone https://github.com/iwf-web/vagrant-scripts.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagra
nt-scripts/1'...
[Pipeline] sh
+ git clone -b 3.0.0 --depth 1 https://github.com/iwf-web/vagrant-
scripts.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagra
nt-scripts/3.0.0'...
Note: switching to '9158aa775ebd940aac6e84a505f34f36b341cbcd'.
```

```
You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b 2.0.4 --depth 1 https://github.com/iwf-web/vagrant-
scripts.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagra
nt-scripts/2.0.4'...
Note: switching to '0c9ae3d16127fb8b0a1a08de4aef65ddebfa89e7'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0
[Pipeline] sh
```

```
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0
[Pipeline] sh
+ git clone https://github.com/ahzhezhe/terraform-generator.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terra
form-generator/2'...
[Pipeline] sh
+ git clone -b v4.0.0 --depth 1 https://github.com/ahzhezhe/terraform-
generator.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terra
form-generator/v4.0.0'...
Note: switching to '5a3634d5f7c270d2f7ca23fcc79ec2ebdbfc7df7'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v3.0.0 --depth 1 https://github.com/ahzhezhe/terraform-
generator.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terra
form-generator/v3.0.0'...
Note: switching to '25d2b5d6600d5361d3944bb63263dba5d44b63b4'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:
  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0
[Pipeline] sh
+ git clone https://github.com/ansible-collections/community.general.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commu
nity.general/3'...
[Pipeline] sh
+ git clone -b 7.0.0 --depth 1 https://github.com/ansible-
collections/community.general.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commu
nity.general/7.0.0'...
Note: switching to 'd4aeb322bb46bcdca9de3270458c0e73cf0b7e6b'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false
```

```
[Pipeline] sh
+ git clone -b 6.0.0 --depth 1 https://github.com/ansible-
collections/community.general.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commu
nity.general/6.0.0'...
Note: switching to '42b245eabfa5774816ea962a0bd558831f101c23'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2
[Pipeline] sh
+ git clone https://github.com/tropyx/NetBeansPuppet.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBe
ansPuppet/4'...
[Pipeline] sh
+ git clone -b v2.0.0 --depth 1
https://github.com/tropyx/NetBeansPuppet.git
```

```
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBe
ansPuppet/v2.0.0'...
Note: switching to '7be05ed05e6b2d00fb10a3c5d7ac1d4f02906cf5'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v1.2 --depth 1 https://github.com/tropyx/NetBeansPuppet.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBe
ansPuppet/v1.2'...
Note: switching to 'f6d3ee05e0ad8b510b7c7bc24a45de798926f475'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Clone extra projects source codes)
[Pipeline] script
[Pipeline] {
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0
[Pipeline] sh
```

```
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1
[Pipeline] sh
+ git clone https://github.com/ricardozanini/soccer-stats.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0'...
[Pipeline] sh
+ git clone -b v0.0.2 --depth 1 https://github.com/ricardozanini/soccer-
stats.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2'...
Note: switching to '9b09b44e462f384ce91d75f8797e5a3f5bdcea43'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v0.0.1 --depth 1 https://github.com/ricardozanini/soccer-
stats.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1'...
Note: switching to 'b8ad23e3584bd1d4eb2642be3d5cb2f590cb4b3c'.
```

```
You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1
[Pipeline] sh
+ git clone https://github.com/ansible/ansible-runner.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible
-runner/1'...
[Pipeline] sh
+ git clone -b 2.0.0 --depth 1 https://github.com/ansible/ansible-
runner.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible
-runner/2.0.0'...
Note: switching to 'a869b638d6afaf99cd2a59627bbdea2ef72a3b3f'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.
```

```
If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b 1.0.1 --depth 1 https://github.com/ansible/ansible-
runner.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible
-runner/1.0.1'...
Note: switching to 'de9d2ec8c655edc14c6fc4ff01dcda8a18e8bc8f'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0
[Pipeline] sh
```

```
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0
[Pipeline] sh
+ git clone https://github.com/hashicorp/terraform-provider-azurerm.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafo
rm-provider-azurerm/2'...
Updating files:  45% (13400/29323)
Updating files:  46% (13489/29323)
Updating files:  47% (13782/29323)
Updating files:  48% (14076/29323)
Updating files:  49% (14369/29323)
Updating files:  50% (14662/29323)
Updating files:  51% (14955/29323)
Updating files:  52% (15248/29323)
Updating files:  53% (15542/29323)
Updating files:  54% (15835/29323)
Updating files:  55% (16128/29323)
Updating files:  56% (16421/29323)
Updating files:  57% (16715/29323)
Updating files:  58% (17008/29323)
Updating files:  59% (17301/29323)
Updating files:  60% (17594/29323)
Updating files:  61% (17888/29323)
Updating files:  62% (18181/29323)
Updating files:  63% (18474/29323)
Updating files:  64% (18767/29323)
Updating files:  65% (19060/29323)
Updating files:  66% (19354/29323)
Updating files:  67% (19647/29323)
Updating files:  68% (19940/29323)
Updating files:  69% (20233/29323)
Updating files:  70% (20527/29323)
Updating files:  71% (20820/29323)
Updating files:  72% (21113/29323)
Updating files:  73% (21406/29323)
Updating files:  74% (21700/29323)
Updating files:  75% (21993/29323)
Updating files:  76% (22286/29323)
Updating files:  77% (22579/29323)
Updating files:  78% (22872/29323)
Updating files:  79% (23166/29323)
Updating files:  80% (23459/29323)
Updating files:  81% (23752/29323)
Updating files:  82% (24045/29323)
Updating files:  83% (24339/29323)
Updating files:  84% (24632/29323)
Updating files:  85% (24925/29323)
Updating files:  86% (25218/29323)
Updating files:  87% (25512/29323)
Updating files:  88% (25805/29323)
Updating files:  89% (26098/29323)
Updating files:  90% (26391/29323)
Updating files:  91% (26684/29323)
Updating files:  91% (26805/29323)
Updating files:  92% (26978/29323)
Updating files:  93% (27271/29323)
Updating files:  94% (27564/29323)
Updating files:  95% (27857/29323)
Updating files:  96% (28151/29323)
Updating files:  97% (28444/29323)
Updating files:  98% (28737/29323)
Updating files:  99% (29030/29323)
Updating files: 100% (29323/29323)
Updating files: 100% (29323/29323), done.
[Pipeline] sh
+ git clone -b v3.0.0 --depth 1 https://github.com/hashicorp/terraform-
provider-azurerm.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafo
rm-provider-azurerm/v3.0.0'...
Note: switching to '8621a756ed4f3e1e14a54e99a3b24602186918df'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

Updating files:  89% (12310/13722)
Updating files:  90% (12350/13722)
Updating files:  91% (12488/13722)
Updating files:  92% (12625/13722)
Updating files:  93% (12762/13722)
Updating files:  94% (12899/13722)
Updating files:  95% (13036/13722)
Updating files:  96% (13174/13722)
Updating files:  97% (13311/13722)
Updating files:  98% (13448/13722)
Updating files:  99% (13585/13722)
Updating files: 100% (13722/13722)
Updating files: 100% (13722/13722), done.
[Pipeline] sh
+ git clone -b v2.0.0 --depth 1 https://github.com/hashicorp/terraform-
provider-azurerm.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafo
rm-provider-azurerm/v2.0.0'...
Note: switching to '2190f5565087143c6d67b05270685eda8d4f115d'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
```

```
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0
[Pipeline] sh
+ git clone https://github.com/chef/cookstyle.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cooksty
le/3'...
[Pipeline] sh
+ git clone -b v7.0.0 --depth 1 https://github.com/chef/cookstyle.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cooksty
le/v7.0.0'...
Note: switching to '6034cf7bf97ab230ff9cc29d4bec13d98177b293'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:
  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v6.0.0 --depth 1 https://github.com/chef/cookstyle.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cooksty
le/v6.0.0'...
Note: switching to '4165ded9d4a6beb525c326c6bab56eb445c5732b'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0
[Pipeline] sh
+ mkdir -p
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0
[Pipeline] sh
+ sudo -su aicha.war chmod 777
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0
[Pipeline] sh
+ git clone https://github.com/pulumi/pulumi-datadog.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4
```

```
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4'...
[Pipeline] sh
+ git clone -b v4.0.0 --depth 1 https://github.com/pulumi/pulumi-
datadog.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0'...
Note: switching to '275a9c971d4d3bf375a06cb0995489cb8ecf23ee'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] sh
+ git clone -b v3.0.0 --depth 1 https://github.com/pulumi/pulumi-
datadog.git
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0
Cloning into
'/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0'...
Note: switching to '9dd31388ddd14bb3c8da9ebc140307df63e6b675'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to
false

[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC tools  with Snyk code)
```

```
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== ansible VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0 --
detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0 ...

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/lib/ansible_test/_internal/containers.py, line 437
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in user.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/binary_modules/library/helloworld.go,
line 69
   Info: Unsanitized input from a CLI argument flows into
io.ioutil.ReadFile, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Jinja auto-escape is set to false.
   Path: test/units/plugins/filter/test_mathstuff.py, line 26
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Low] Jinja auto-escape is set to false.
   Path: test/support/network-
integration/collections/ansible_collections/ansible/netcommon/plugins/modul
e_utils/network/common/utils.py, line 639
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Low] Jinja auto-escape is set to false.
   Path: test/units/template/test_template_utilities.py, line 75
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Low] Jinja auto-escape is set to false.
   Path: test/integration/targets/var_precedence/ansible-var-precedence-
check.py, line 20
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Low] Jinja auto-escape is set to false.
   Path: test/integration/targets/var_precedence/ansible-var-precedence-
check.py, line 104
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Low] Jinja auto-escape is set to false.
```

```
   Path: test/units/template/test_template_utilities.py, line 82
   Info: jinja2.Template is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/sanity/code-smell/package-data.py, line 164
   Info: Calling extractall to extract all files from a tar file without
sanitization. This may result files outside destination directory to be
overwritten, resulting in an arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/integration/targets/ansible-galaxy-
collection/library/setup_collections.py, line 159
   Info: Calling extractall to extract all files from a tar file without
sanitization. This may result files outside destination directory to be
overwritten, resulting in an arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path:
test/lib/ansible_test/_internal/commands/sanity/validate_modules.py, line
162
   Info: Calling extractall to extract all files from a tar file without
sanitization. This may result files outside destination directory to be
overwritten, resulting in an arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/units/cli/test_galaxy.py, line 667
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/units/cli/test_galaxy.py, line 701
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/units/galaxy/test_collection.py, line 505
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/units/galaxy/test_collection.py, line 511
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/units/galaxy/test_collection.py, line 517
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
```

```
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Low] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: test/units/galaxy/test_collection.py, line 823
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/integration/targets/ansible-vault/password-script.py, line 24
   Info: Do not hardcode passwords in code. Found hardcoded password used
in PASSWORD.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/units/parsing/vault/test_vault_editor.py, line 226
   Info: Do not hardcode passwords in code. Found hardcoded password used
in new_password.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/units/parsing/vault/test_vault_editor.py, line 258
   Info: Do not hardcode passwords in code. Found hardcoded password used
in new_password.

 ✗ [Low] Deserialization of Untrusted Data
   Path:
test/lib/ansible_test/_util/controller/sanity/yamllint/yamllinter.py, line
97
   Info: Unsanitized input from a command line argument flows into
yaml.load, where it is used to deserialize an object. This may result in an
Unsafe Deserialization vulnerability.

 ✗ [Low] Deserialization of Untrusted Data
   Path:
test/lib/ansible_test/_util/controller/sanity/yamllint/yamllinter.py, line
138
   Info: Unsanitized input from a command line argument flows into
yaml.load, where it is used to deserialize an object. This may result in an
Unsafe Deserialization vulnerability.

 ✗ [Low] Insecure Xml Parser
   Path: test/lib/ansible_test/_internal/commands/coverage/xml.py, line 61
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Low] Insecure Xml Parser
   Path: test/support/integration/plugins/modules/zypper.py, line 283
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Low] Insecure Xml Parser
   Path: test/lib/ansible_test/_internal/commands/sanity/shellcheck.py,
line 89
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/copy.py, line 587
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/copy.py, line 645
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/assemble.py, line 242
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/assemble.py, line 253
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/find.py, line 496
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/find.py, line 517
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/get_url.py, line 638
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/get_url.py, line 649
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/uri.py, line 493
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/modules/uri.py, line 494
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/plugins/connection/ssh.py, line 627
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/plugins/lookup/password.py, line 271
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).
```

```
 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/module_utils/connection.py, line 63
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/vars/manager.py, line 85
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/vars/manager.py, line 128
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/plugins/inventory/__init__.py, line 316
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/plugins/inventory/__init__.py, line 320
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Insecure Temporary File
   Path: test/integration/targets/ansible-test-
sanity/ansible_collections/ns/col/tests/integration/targets/hello/files/bad
.py, line 16
   Info: Use of tempfile.mktemp is deprecated and poses a security risk

 ✗ [Low] Command Injection
   Path: test/lib/ansible_test/_util/controller/sanity/code-
smell/changelog.py, line 53
   Info: Unsanitized input from a command line argument flows into
subprocess.run, where it is used as a shell command. This may result in a
Command Injection vulnerability.

 ✗ [Low] Command Injection
   Path: test/sanity/code-smell/pymarkdown.py, line 23
   Info: Unsanitized input from a command line argument flows into
subprocess.run, where it is used as a shell command. This may result in a
Command Injection vulnerability.

 ✗ [Low] Command Injection
   Path: test/integration/targets/test_utils/scripts/timeout.py, line 13
   Info: Unsanitized input from a command line argument flows into
subprocess.run, where it is used as a shell command. This may result in a
Command Injection vulnerability.

 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/urls.py, line 875
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/urls.py, line 888
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.
```

```
 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/urls.py, line 1659
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: test/support/network-
integration/collections/ansible_collections/ansible/netcommon/plugins/modul
e_utils/network/common/config.py, line 193
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_exit_json.py, line 125
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_exit_json.py, line 127
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_exit_json.py, line 133
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_exit_json.py, line 135
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_exit_json.py, line 141
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_exit_json.py, line 143
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/executor/test_task_result.py, line 147
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: test/units/module_utils/basic/test_sanitize_keys.py, line 67
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/validate-
modules/validate_modules/main.py, line 340
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.
```

```
 ✗ [Low] Path Traversal
   Path:
test/lib/ansible_test/_util/controller/sanity/yamllint/yamllinter.py, line
93
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-
assert.py, line 13
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-dict-
iteritems.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-
smell/shebang.py, line 45
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-dict-
itervalues.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/ansible-vault/faux-editor.py, line 30
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path:
test/integration/targets/want_json_modules_posix/library/helloworld.py,
line 26
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-smart-
quotes.py, line 12
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
```

```
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/use-
compat-six.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-get-
exception.py, line 13
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/sanity/code-smell/test-constraints.py, line 19
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/target/sanity/compile/compile.py, line
15
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/target/sanity/compile/compile.py, line
20
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-
smell/metaclass-boilerplate.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-
smell/metaclass-boilerplate.py, line 25
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/sanity/code-smell/ansible-test-future-boilerplate.py, line 17
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/sanity/code-smell/ansible-test-future-boilerplate.py, line 36
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.
```

```
 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/use-
argspec-type-path.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/line-
endings.py, line 10
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/tools/collection_detail.py,
line 43
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-
unicode-literals.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/sanity/code-smell/update-bundled.py, line 71
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-
basestring.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/future-
import-boilerplate.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/future-
import-boilerplate.py, line 26
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/replace-
urlopen.py, line 11
```

```
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-dict-
iterkeys.py, line 11
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/sanity/code-smell/required-and-default-attributes.py, line 9
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/code-smell/no-main-
display.py, line 12
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/target/setup/probe_cgroups.py, line 21
   Info: Unsanitized input from a command line argument flows into
os.rmdir, where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to remove arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/ansible-galaxy-collection-
cli/files/make_collection_dir.py, line 116
   Info: Unsanitized input from a command line argument flows into path
concatenation, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to manipulate arbitrary
files.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/ansible-
runner/files/playbook_example1.py, line 24
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/ansible-
runner/files/playbook_example1.py, line 27
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/wait_for/files/write_utf16.py, line 19
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Low] Path Traversal
```

```
   Path: test/integration/targets/throttle/test_throttle.py, line 19
   Info: Unsanitized input from a command line argument flows into
os.utime, where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to manipulate arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/integration/targets/throttle/test_throttle.py, line 30
   Info: Unsanitized input from a command line argument flows into
os.unlink, where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to remove arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/sanity/code-smell/package-data.py, line 123
   Info: Unsanitized input from a command line argument flows into
shutil.copy2, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/lib/ansible_test/_util/controller/sanity/validate-
modules/validate_modules/main.py, line 2578
   Info: Unsanitized input from a command line argument flows into os.walk,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/csharp/Ansible.Become.cs, line 364
   Info: Do not hardcode credentials in code. Found username or password
credential used in a condition.

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: packaging/pep517_backend/_generate_man.py, line 280
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: packaging/release.py, line 930
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Medium] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: lib/ansible/galaxy/collection/concrete_artifact_manager.py, line
753
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Medium] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: packaging/release.py, line 778
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Medium] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: lib/ansible/galaxy/role.py, line 382
   Info: Unsanitized input from an opened tar file flows into extract,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/urls.py, line 875
   Info: Do not hardcode passwords in code. Found hardcoded password used
in a condition.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/urls.py, line 1659
   Info: Do not hardcode passwords in code. Found hardcoded password used
in a condition.

 ✗ [Medium] Server-Side Request Forgery (SSRF)
   Path: hacking/azp/download.py, line 138
   Info: Unsanitized input from a command line argument flows into
requests.get, where it is used as an URL to perform a request. This may
result in a Server Side Request Forgery vulnerability.

 ✗ [Medium] Server-Side Request Forgery (SSRF)
   Path: hacking/azp/download.py, line 152
   Info: Unsanitized input from a command line argument flows into
requests.get, where it is used as an URL to perform a request. This may
result in a Server Side Request Forgery vulnerability.

 ✗ [Medium] Server-Side Request Forgery (SSRF)
   Path: hacking/azp/download.py, line 189
   Info: Unsanitized input from a command line argument flows into
requests.get, where it is used as an URL to perform a request. This may
result in a Server Side Request Forgery vulnerability.

 ✗ [Medium] Server-Side Request Forgery (SSRF)
   Path: hacking/azp/download.py, line 197
   Info: Unsanitized input from a command line argument flows into
requests.get, where it is used as an URL to perform a request. This may
result in a Server Side Request Forgery vulnerability.

 ✗ [Medium] Server-Side Request Forgery (SSRF)
   Path: hacking/azp/download.py, line 224
   Info: Unsanitized input from a command line argument flows into
requests.get, where it is used as an URL to perform a request. This may
result in a Server Side Request Forgery vulnerability.

 ✗ [Medium] Server-Side Request Forgery (SSRF)
   Path: hacking/azp/run.py, line 87
   Info: Unsanitized input from a command line argument flows into
requests.post, where it is used as an URL to perform a request. This may
result in a Server Side Request Forgery vulnerability.

 ✗ [Medium] Path Traversal
   Path: .azure-pipelines/scripts/combine-coverage.py, line 51
   Info: Unsanitized input from a command line argument flows into
shutil.copyfile, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: lib/ansible/module_utils/basic.py, line 394
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/incidental.py, line 170
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/incidental.py, line 234
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/incidental.py, line 286
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/incidental.py, line 374
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/return_skeleton_generator.py, line 86
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: lib/ansible/modules/async_wrapper.py, line 121
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/download.py, line 149
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/incidental.py, line 238
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/incidental.py, line 432
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
```

```
   Path: lib/ansible/modules/async_wrapper.py, line 140
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: lib/ansible/modules/async_wrapper.py, line 148
   Info: Unsanitized input from a command line argument flows into
os.rename, where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to remove arbitrary files.

 ✗ [Medium] Path Traversal
   Path: lib/ansible/modules/async_wrapper.py, line 332
   Info: Unsanitized input from a command line argument flows into
shutil.rmtree, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to remove arbitrary files.

 ✗ [Medium] Path Traversal
   Path: lib/ansible/modules/async_wrapper.py, line 336
   Info: Unsanitized input from a command line argument flows into
shutil.rmtree, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to remove arbitrary files.

 ✗ [Medium] Path Traversal
   Path: hacking/azp/download.py, line 226
   Info: Unsanitized input from data from a remote resource flows into
open, where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Insecure Xml Parser
   Path: lib/ansible/plugins/shell/powershell.py, line 50
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: lib/ansible/utils/_junit_xml.py, line 278
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 215
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 219
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 224
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 228
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 232
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 320
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 339
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 347
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 350
   Info: Unsanitized input from a command line argument flows into
subprocess.check_call, where it is used as a shell command. This may result
in a Command Injection vulnerability.

 ✗ [Medium] Command Injection
   Path: hacking/azp/incidental.py, line 312
   Info: Unsanitized input from a command line argument flows into
subprocess.check_output, where it is used as a shell command. This may
result in a Command Injection vulnerability.

 ✗ [High] Regular Expression Denial of Service (ReDoS)
   Path: hacking/azp/incidental.py, line 192
   Info: Unsanitized user input from a command line argument flows into
re.search, where it is used to build a regular expression. This may result
in a Regular expression Denial of Service attack (reDOS).

 ✗ [High] Inadequate Encryption Strength
   Path: lib/ansible/module_utils/urls.py, line 573
   Info: Do not use old versions of TLS (ssl.PROTOCOL_TLSv1 used in
ssl.wrap_socket).

 ✗ [High] Inadequate Encryption Strength
   Path: lib/ansible/module_utils/urls.py, line 1217
   Info: Do not use old versions of TLS (ssl.PROTOCOL_TLSv1 used in
ssl.wrap_socket).

 ✗ [High] Inadequate Encryption Strength
   Path: lib/ansible/module_utils/urls.py, line 1228
   Info: Do not use old versions of TLS (ssl.PROTOCOL_TLSv1 used in
ssl.wrap_socket).


✔ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0

Summary:

  143 Code issues found
  4 [High]   41 [Medium]   98 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== ansible VERSION v2.0.0-0.1.alpha1 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1 ...

 ✗ [Low] Deserialization of Untrusted Data
   Path: test/integration/cleanup_ec2.py, line 140
   Info: Unsanitized input from a command line argument flows into
yaml.load, where it is used to deserialize an object. This may result in an
Unsafe Deserialization vulnerability.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/vars/__init__.py, line 56
   Info: hashlib.sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/parsing/vault/__init__.py, line 456
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Python 2 source code
   Path: test/integration/cleanup_ec2.py, line 5
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/units/executor/test_task_executor.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/integration/consul_running.py, line 1
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/integration/setup_gce.py, line 8
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/integration/cleanup_gce.py, line 5
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Path Traversal
   Path: test/integration/cleanup_ec2.py, line 58
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Path Traversal
   Path: test/integration/cleanup_ec2.py, line 140
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/rax.py, line 295
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in here.

 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/rax.py, line 295
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Use of Hardcoded Credentials
   Path: lib/ansible/module_utils/rax.py, line 307
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/fleet.py, line 5
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/vagrant.py, line 13
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/urls.py, line 84
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/linode.py, line 52
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/apache-libcloud.py, line 31
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/windows_azure.py, line 16
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/gce.py, line 30
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/nova.py, line 24
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/openshift.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/facts.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/lookup/nested.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/basic.py, line 32
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
```

```
   Path: lib/ansible/plugins/lookup/ini.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/collins.py, line 47
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/action/__init__.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/cobbler.py, line 42
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/vars/__init__.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/vmware.py, line 29
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/gce.py, line 73
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/template/__init__.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: hacking/module_formatter.py, line 21
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/lookup/consul_kv.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.
```

```
 ✗ [Low] Python 2 source code
   Path: docsite/build-site.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: examples/scripts/yaml_to_ini.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/spacewalk.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/rax.py, line 31
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/lookup/sequence.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/playbook/role/__init__.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/vbox.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/filter/core.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/consul_io.py, line 122
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/strategies/linear.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.
```

```
 ✗ [Low] Python 2 source code
   Path: lib/ansible/playbook/conditional.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/ssh_config.py, line 43
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/inventory/script.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/inventory/__init__.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/vmware.py, line 21
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: hacking/get_library.py, line 21
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/openvz.py, line 29
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: examples/scripts/uptime.py, line 5
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/rax.py, line 146
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/softlayer.py, line 13
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/cli/doc.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/freeipa.py, line 3
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/utils/module_docs.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/shell/sh.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/strategies/free.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/abiquo.py, line 25
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/strategies/__init__.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/libvirt_lxc.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/cache/jsonfile.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
```

```
   Path: samples/multi.py, line 3
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/filter/mathstuff.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/proxmox.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/ec2.py, line 29
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/cloudstack.py, line 71
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/module_utils/known_hosts.py, line 29
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/lookup/shelvefile.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/action/async.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/zabbix.py, line 31
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/zone.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.
```

```
 ✗ [Low] Python 2 source code
   Path: contrib/inventory/jail.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/executor/process/worker.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/digital_ocean.py, line 110
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/ovirt.py, line 63
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/executor/task_executor.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/cli/adhoc.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: contrib/inventory/docker.py, line 131
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/lookup/dig.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/utils/path.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/cli/pull.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.
```

```
 ✗ [Low] Python 2 source code
   Path: lib/ansible/plugins/lookup/credstash.py, line 17
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Regular Expression Denial of Service (ReDoS)
   Path: test/integration/cleanup_ec2.py, line 20
   Info: Unsanitized user input from a command line argument flows into
re.search, where it is used to build a regular expression. This may result
in a Regular expression Denial of Service attack (reDOS).

 ✗ [Low] Regular Expression Denial of Service (ReDoS)
   Path: test/integration/cleanup_ec2.py, line 28
   Info: Unsanitized user input from a command line argument flows into
re.search, where it is used to build a regular expression. This may result
in a Regular expression Denial of Service attack (reDOS).

 ✗ [Low] Regular Expression Denial of Service (ReDoS)
   Path: test/integration/cleanup_gce.py, line 30
   Info: Unsanitized user input from a command line argument flows into
re.search, where it is used to build a regular expression. This may result
in a Regular expression Denial of Service attack (reDOS).

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: lib/ansible/cli/galaxy.py, line 276
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: lib/ansible/template/__init__.py, line 81
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: hacking/module_formatter.py, line 202
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Medium] Cross-site Scripting (XSS)
   Path: docsite/_static/searchtools.js, line 463
   Info: Unsanitized input from data from a remote resource flows into
append, where it is used to dynamically construct the HTML page on client
side. This may result in a DOM Based Cross-Site Scripting attack (DOMXSS).

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 35
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 175
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 186
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 196
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: lib/ansible/galaxy/role.py, line 235
   Info: Unsanitized input from an opened tar file flows into extractfile,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Medium] Arbitrary File Write via Archive Extraction (Tar Slip)
   Path: lib/ansible/galaxy/role.py, line 273
   Info: Unsanitized input from an opened tar file flows into extract,
where it is used to extract a file from a tar archive. This may result
files outside destination directory to be overwritten, resulting in an
arbitrary file write.

 ✗ [Medium] Improper Neutralization of Directives in Statically Saved Code
   Path: lib/ansible/cli/galaxy.py, line 276
   Info: Unsanitized input from a command line argument flows into
from_string, where it is used to construct a template that gets rendered.
This may result in a Server-Side Template Injection vulnerability.

 ✗ [High] Inadequate Encryption Strength
   Path: lib/ansible/module_utils/urls.py, line 335
   Info: Do not use old versions of TLS (ssl.PROTOCOL_TLSv1 used in
ssl.wrap_socket).

 ✗ [High] Inadequate Encryption Strength
   Path: lib/ansible/module_utils/urls.py, line 545
   Info: Do not use old versions of TLS (ssl.PROTOCOL_TLSv1 used in
ssl.wrap_socket).

 ✗ [High] Inadequate Encryption Strength
   Path: lib/ansible/module_utils/urls.py, line 554
   Info: Do not use old versions of TLS (ssl.PROTOCOL_TLSv1 used in
ssl.wrap_socket).


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1
```

```
Summary:

  102 Code issues found
  3 [High]   11 [Medium]   88 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== ansible VERSION v1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0 -
-detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0
...

 ✗ [Low] Python 2 source code
   Path: test/TestPlayBook.py, line 6
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/TestRunner.py, line 6
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/inventory_api.py, line 3
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/TestConstants.py, line 3
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: test/TestInventory.py, line 1
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: docsite/build-site.py, line 19
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/runner/connection_plugins/paramiko_ssh.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: plugins/inventory/yaml.py, line 47
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/runner/__init__.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/utils/template.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: plugins/inventory/nova.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: plugins/inventory/ec2.py, line 90
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: hacking/module_formatter.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: examples/scripts/yaml_to_ini.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/inventory/__init__.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/callbacks.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
```

```
   Path: lib/ansible/utils/module_docs.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: plugins/inventory/cobbler.py, line 31
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/utils/__init__.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/runner/action_plugins/template.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: setup.py, line 3
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/runner/action_plugins/pause.py, line 18
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/ansible/inventory/script.py, line 20
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: examples/scripts/uptime.py, line 5
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/utils/__init__.py, line 302
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: lib/ansible/utils/__init__.py, line 317
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Medium] Cross-site Scripting (XSS)
   Path: docsite/_static/searchtools.js, line 463
   Info: Unsanitized input from data from a remote resource flows into
append, where it is used to dynamically construct the HTML page on client
side. This may result in a DOM Based Cross-Site Scripting attack (DOMXSS).

 ✗ [Medium] Improper Certificate Validation
   Path: lib/ansible/runner/connection_plugins/paramiko_ssh.py, line 78
   Info: The AutoAddPolicy policy used in set_missing_host_key_policy will
not reject unknown host keys. This may lead to Man-in-the-middle attacks.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 35
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 175
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 186
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/scripts/yaml_to_ini.py, line 196
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: lib/ansible/utils/template.py, line 317
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.

 ✗ [Medium] Jinja auto-escape is set to false.
   Path: hacking/module_formatter.py, line 220
   Info: jinja2.Environment is called with no autoescape argument
(autoescaping is disabled by default). This increases the risk of Cross-
Site Scripting (XSS) attacks.


✔ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0

Summary:

  34 Code issues found
  8 [Medium]   26 [Low]
```

```
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1 --
detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
...

 ✗ [Low] Hardcoded Secret
   Path: internal/communicator/ssh/communicator_test.go, line 32
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in testServerPrivateKey.

 ✗ [Low] Hardcoded Secret
   Path: internal/communicator/ssh/communicator_test.go, line 463
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in SERVER_PEM.

 ✗ [Low] Hardcoded Secret
   Path: internal/communicator/ssh/communicator_test.go, line 492
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in CLIENT_PEM.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 102
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 211
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 226
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 359
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 369
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client.go, line 139
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
```

```
   Path: internal/backend/remote-state/s3/client.go, line 189
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client.go, line 405
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote/backend_state.go, line 58
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote/backend_state.go, line 70
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote/backend_state.go, line 114
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/http/client.go, line 66
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/http/client.go, line 199
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/cloud/state.go, line 270
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/cloud/state.go, line 296
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/cloud/state.go, line 425
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/oss/client.go, line 123
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/oss/client.go, line 432
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm
```

```
 ✗ [Low] Clear Text Logging
   Path: internal/backend/remote-state/azure/helpers_test.go, line 130
   Info: Unsanitized input from sensitive credentials flows into
log.Printf, where it is logged. This may result in a clear-text logging of
sensitive information.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/oss/client_test.go, line 242
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/states/remote/remote_test.go, line 48
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/states/remote/remote_test.go, line 97
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/backend_test.go, line 258
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client_test.go, line 184
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Inadequate Encryption Strength
   Path: internal/legacy/helper/acctest/random.go, line 148
   Info: Usage of 1024 bits key in crypto.rsa.GenerateKey is considered
insecure. Use a key with at least 2048 bits.

 ✗ [Medium] Path Traversal
   Path: tools/loggraphdiff/loggraphdiff.go, line 53
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [Medium] Path Traversal
   Path: tools/loggraphdiff/loggraphdiff.go, line 57
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [Medium] Path Traversal
   Path: tools/loggraphdiff/loggraphdiff.go, line 128
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [Medium] Improper Certificate Validation
   Path: internal/backend/remote-state/http/backend.go, line 156
   Info: TrustManager might be too permissive: The client will accept any
certificate and any host name in that certificate, making it susceptible to
man-in-the-middle attacks.
```

```
 ✗ [High] Cross-site Scripting (XSS)
   Path: internal/command/testdata/login-oauth-server/oauthserver.go, line
55
   Info: Unsanitized input from an HTTP header flows into Write, where it
is used to render an HTML page returned to the user. This may result in a
Reflected Cross-Site Scripting attack (XSS).

 ✗ [High] Command Injection
   Path: tools/protobuf-compile/protobuf-compile.go, line 121
   Info: Unsanitized input from a CLI argument flows into Path in
os.exec.Cmd, where it is used as a shell command. This may result in a
Command Injection vulnerability.

 ✗ [High] Command Injection
   Path: tools/protobuf-compile/protobuf-compile.go, line 122
   Info: Unsanitized input from a CLI argument flows into Args in
os.exec.Cmd, where it is used as a shell command. This may result in a
Command Injection vulnerability.

 ✗ [High] Server-Side Request Forgery (SSRF)
   Path: internal/command/login.go, line 601
   Info: Unsanitized input from an HTTP header flows into _, where it is
used as an URL to perform a request. This may result in a Server-Side
Request Forgery vulnerability.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1

Summary:

  36 Code issues found
  4 [High]   4 [Medium]   28 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION v1.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0 ...

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/oss/client.go, line 123
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/oss/client.go, line 435
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote/backend_state.go, line 50
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote/backend_state.go, line 71
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/http/client.go, line 63
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/http/client.go, line 187
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/swift/client.go, line 266
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 99
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 203
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 218
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 351
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/client.go, line 361
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/artifactory/client.go, line 36
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm
```

```
 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client.go, line 136
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client.go, line 186
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client.go, line 402
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Inadequate Encryption Strength
   Path: internal/legacy/helper/acctest/random.go, line 145
   Info: Usage of 1024 bits key in crypto.rsa.GenerateKey is considered
insecure. Use a key with at least 2048 bits.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/s3/client_test.go, line 181
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/states/remote/remote_test.go, line 45
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/states/remote/remote_test.go, line 94
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/oss/client_test.go, line 239
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/backend/remote-state/cos/backend_test.go, line 226
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Clear Text Logging
   Path: internal/backend/remote-state/azure/helpers_test.go, line 118
   Info: Unsanitized input from sensitive credentials flows into
log.Printf, where it is logged. This may result in a clear-text logging of
sensitive information.

 ✗ [Low] Hardcoded Secret
   Path: internal/communicator/ssh/communicator_test.go, line 28
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in testServerPrivateKey.

 ✗ [Low] Hardcoded Secret
   Path: internal/communicator/ssh/communicator_test.go, line 459
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in SERVER_PEM.

 ✗ [Low] Hardcoded Secret
   Path: internal/communicator/ssh/communicator_test.go, line 488
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in CLIENT_PEM.

 ✗ [Medium] Improper Certificate Validation
   Path: internal/backend/remote-state/http/backend.go, line 155
   Info: TrustManager might be too permissive: The client will accept any
certificate and any host name in that certificate, making it susceptible to
man-in-the-middle attacks.

 ✗ [Medium] Path Traversal
   Path: tools/loggraphdiff/loggraphdiff.go, line 50
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [Medium] Path Traversal
   Path: tools/loggraphdiff/loggraphdiff.go, line 54
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [Medium] Path Traversal
   Path: tools/loggraphdiff/loggraphdiff.go, line 125
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [High] Server-Side Request Forgery (SSRF)
   Path: internal/command/login.go, line 600
   Info: Unsanitized input from an HTTP header flows into _, where it is
used as an URL to perform a request. This may result in a Server-Side
Request Forgery vulnerability.

 ✗ [High] Cross-site Scripting (XSS)
   Path: internal/command/testdata/login-oauth-server/oauthserver.go, line
55
   Info: Unsanitized input from an HTTP header flows into Write, where it
is used to render an HTML page returned to the user. This may result in a
Reflected Cross-Site Scripting attack (XSS).


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0

Summary:

  32 Code issues found
  2 [High]   4 [Medium]   26 [Low]
```

```
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION v0.1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0 ...

 ✗ [Low] Hardcoded Secret
   Path: helper/ssh/communicator_test.go, line 14
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in testServerPrivateKey.

 ✗ [Low] Command Injection
   Path: plugin/plugin_test.go, line 23
   Info: Unsanitized input from a CLI argument flows into os.exec.Command,
where it is used as a shell command. This may result in a Command Injection
vulnerability.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: terraform/terraform_test.go, line 29
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: builtin/providers/aws/resource_aws_instance.go, line 213
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Medium] Path Traversal
   Path: command/show.go, line 40
   Info: Unsanitized input from a CLI argument flows into os.Open, where it
is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0

Summary:

  5 Code issues found
  1 [Medium]   4 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2 --
detection-depth=3

Testing /Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
...

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/subversion_spec.rb, line 50
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in eq.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/subversion_spec.rb, line 226
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/mixin/shell_out_spec.rb, line 142
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/mixin/shell_out_spec.rb, line 214
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 367
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 446
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 451
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 456
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 513
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 521
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
```

```
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 844
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 870
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 926
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 991
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 1047
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 1098
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap/train_connector_spec.rb, line 101
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap/train_connector_spec.rb, line 120
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/user_create_spec.rb, line 224
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/user_create_spec.rb, line 268
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 339
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 361
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.
```

```
 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 449
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/ssh_spec.rb, line 227
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/ssh_spec.rb, line 351
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/remote_file/sftp_spec.rb, line 123
   Info: Do not hardcode passwords in code. Found hardcoded password used
in with.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 876
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 1170
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 345
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 367
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 454
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: lib/chef/provider/user/mac.rb, line 645
   Info: Do not hardcode passwords in code. Found hardcoded password used
in freeze.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2

Summary:
  32 Code issues found
  7 [Medium]   25 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION v18.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0 -
-detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0
...

 ✗ [Low] Python 2 source code
   Path: lib/chef/provider/package/yum/yum_helper.py, line 9
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/ssh_spec.rb, line 227
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/ssh_spec.rb, line 351
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 367
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 446
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 451
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 456
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 513
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.
```

```
 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 521
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/subversion_spec.rb, line 226
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/mixin/shell_out_spec.rb, line 142
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/mixin/shell_out_spec.rb, line 214
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/subversion_spec.rb, line 50
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in eq.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/user_create_spec.rb, line 203
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/user_create_spec.rb, line 242
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 339
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 361
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 449
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 844
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 870
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 926
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 991
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 1047
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 1098
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap/train_connector_spec.rb, line 101
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap/train_connector_spec.rb, line 120
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 345
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 367
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 454
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 876
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: knife/spec/unit/knife/bootstrap_spec.rb, line 1170
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.
```

```
 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/remote_file/sftp_spec.rb, line 123
   Info: Do not hardcode passwords in code. Found hardcoded password used
in with.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: lib/chef/provider/user/mac.rb, line 645
   Info: Do not hardcode passwords in code. Found hardcoded password used
in freeze.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0

Summary:

  33 Code issues found
  7 [Medium]   26 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION v17.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0 -
-detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0
...

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 367
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 446
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 451
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 456
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 513
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/git_spec.rb, line 521
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/subversion_spec.rb, line 226
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/mixin/shell_out_spec.rb, line 142
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/mixin/shell_out_spec.rb, line 214
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in with.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 337
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 359
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 447
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap/train_connector_spec.rb, line 101
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap/train_connector_spec.rb, line 120
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 844
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 870
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.
```

```
 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 926
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 991
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 1047
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 1098
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/provider/subversion_spec.rb, line 50
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in eq.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/ssh_spec.rb, line 227
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/knife/ssh_spec.rb, line 351
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Low] Python 2 source code
   Path: lib/chef/provider/package/yum/yum_helper.py, line 9
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/chef/provider/package/yum/simplejson/tool.py, line 12
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/chef/provider/package/yum/simplejson/encoder.py, line 2
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lib/chef/provider/package/yum/simplejson/decoder.py, line 2
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.
```

```
 ✗ [Medium] Path Traversal
   Path: lib/chef/provider/package/yum/simplejson/tool.py, line 25
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: lib/chef/provider/user/mac.rb, line 648
   Info: Do not hardcode passwords in code. Found hardcoded password used
in freeze.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/remote_file/sftp_spec.rb, line 123
   Info: Do not hardcode passwords in code. Found hardcoded password used
in with.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 343
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 365
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/user_v1_spec.rb, line 452
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 876
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/knife/bootstrap_spec.rb, line 1170
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0

Summary:

  35 Code issues found
  8 [Medium]   27 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3 --
detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3 ...

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/integration/util_spec.rb, line 23
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in allow.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/http/proxy_spec.rb, line 11
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in expects_proxy_connection_via.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/manager_spec.rb, line 263
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in hash_including.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/connection_spec.rb, line 42
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in Puppet.Util.Ldap.Connection.new.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 34
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 42
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 50
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 58
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/manager_spec.rb, line 277
   Info: Do not hardcode passwords in code. Found hardcoded password used
in hash_including.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/type/user_spec.rb, line 418
   Info: Do not hardcode passwords in code. Found hardcoded password used
in new.

 ✗ [Medium] Use of Hardcoded Credentials
```

```
   Path: spec/unit/provider/user/useradd_spec.rb, line 467
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/group/groupadd_spec.rb, line 210
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/user/useradd_spec.rb, line 679
   Info: Do not hardcode passwords in code. Found hardcoded password used
in each_pair.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/ssl/ssl_provider_spec.rb, line 586
   Info: Do not hardcode passwords in code. Found hardcoded password used
in load_context.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/ssl/ssl_provider_spec.rb, line 596
   Info: Do not hardcode passwords in code. Found hardcoded password used
in load_context.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/util/windows/sid_spec.rb, line 113
   Info: Do not hardcode passwords in code. Found hardcoded password used
in user.SetPassword.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/http/proxy_spec.rb, line 11
   Info: Do not hardcode passwords in code. Found hardcoded password used
in expects_proxy_connection_via.

 ✗ [High] Use of a Broken or Risky Cryptographic Algorithm
   Path: spec/unit/x509/cert_provider_spec.rb, line 288
   Info: The OpenSSL.Cipher.DES.new cipher (used in OpenSSL.Cipher.DES.new)
is insecure. Consider using AES instead.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3

Summary:

  18 Code issues found
  1 [High]   9 [Medium]   8 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION 8.0.0 ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0 -
-detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0
...

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/manager_spec.rb, line 263
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in hash_including.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 34
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 42
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 50
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 58
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/http/proxy_spec.rb, line 11
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in expects_proxy_connection_via.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/integration/util_spec.rb, line 23
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in allow.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/connection_spec.rb, line 42
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in Puppet.Util.Ldap.Connection.new.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/group/groupadd_spec.rb, line 210
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/user/useradd_spec.rb, line 467
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
```

```
   Path: spec/unit/http/proxy_spec.rb, line 11
   Info: Do not hardcode passwords in code. Found hardcoded password used
in expects_proxy_connection_via.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/type/user_spec.rb, line 418
   Info: Do not hardcode passwords in code. Found hardcoded password used
in new.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/ssl/ssl_provider_spec.rb, line 586
   Info: Do not hardcode passwords in code. Found hardcoded password used
in load_context.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/ssl/ssl_provider_spec.rb, line 596
   Info: Do not hardcode passwords in code. Found hardcoded password used
in load_context.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/user/useradd_spec.rb, line 679
   Info: Do not hardcode passwords in code. Found hardcoded password used
in each_pair.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/util/windows/sid_spec.rb, line 113
   Info: Do not hardcode passwords in code. Found hardcoded password used
in user.SetPassword.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/manager_spec.rb, line 277
   Info: Do not hardcode passwords in code. Found hardcoded password used
in hash_including.

 ✗ [High] Use of a Broken or Risky Cryptographic Algorithm
   Path: spec/unit/x509/cert_provider_spec.rb, line 288
   Info: The OpenSSL.Cipher.DES.new cipher (used in OpenSSL.Cipher.DES.new)
is insecure. Consider using AES instead.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0

Summary:

  18 Code issues found
  1 [High]   9 [Medium]   8 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION 7.0.0 ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0 -
-detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0
...

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/manager_spec.rb, line 263
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in hash_including.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/http/proxy_spec.rb, line 11
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in expects_proxy_connection_via.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/integration/util_spec.rb, line 23
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in allow.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/connection_spec.rb, line 42
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in Puppet.Util.Ldap.Connection.new.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 34
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 42
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 50
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Low] Use of Hardcoded Credentials
   Path: spec/unit/settings/file_setting_spec.rb, line 58
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in settings.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/ssl/ssl_provider_spec.rb, line 515
   Info: Do not hardcode passwords in code. Found hardcoded password used
in load_context.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/ssl/ssl_provider_spec.rb, line 525
   Info: Do not hardcode passwords in code. Found hardcoded password used
in load_context.

 ✗ [Medium] Use of Hardcoded Credentials
```

```
   Path: spec/unit/type/user_spec.rb, line 351
   Info: Do not hardcode passwords in code. Found hardcoded password used
in new.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/group/groupadd_spec.rb, line 207
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/user/useradd_spec.rb, line 358
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/provider/user/useradd_spec.rb, line 570
   Info: Do not hardcode passwords in code. Found hardcoded password used
in each_pair.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/http/proxy_spec.rb, line 11
   Info: Do not hardcode passwords in code. Found hardcoded password used
in expects_proxy_connection_via.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/util/windows/sid_spec.rb, line 113
   Info: Do not hardcode passwords in code. Found hardcoded password used
in user.SetPassword.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: spec/unit/util/ldap/manager_spec.rb, line 277
   Info: Do not hardcode passwords in code. Found hardcoded password used
in hash_including.

 ✗ [High] Use of a Broken or Risky Cryptographic Algorithm
   Path: spec/unit/x509/cert_provider_spec.rb, line 288
   Info: The OpenSSL.Cipher.DES.new cipher (used in OpenSSL.Cipher.DES.new)
is insecure. Consider using AES instead.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0

Summary:

  18 Code issues found
  1 [High]   9 [Medium]   8 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION DEFAULT ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4 --
detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4 ...

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 36
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 106
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 125
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 146
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 174
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 200
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 223
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 248
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 275
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 301
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 327
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 353
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 373
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/commands/winrm_config/command_test.rb, line 107
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/commands/ssh_config/command_test.rb, line 24
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
test/unit/plugins/guests/linux/cap/persist_mount_shared_folder_test.rb,
line 17
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/provisioners/ansible/provisioner_test.rb, line
44
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/provisioners/ansible/provisioner_test.rb, line
1183
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/providers/docker/action/login_test.rb, line 16
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in double.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/commands/winrm_config/command_test.rb, line 28
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in double.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/pushes/ftp/push_test.rb, line 13
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in double.

 ✗ [Low] Use of Hardcoded Credentials
```

```
   Path: test/unit/plugins/synced_folders/smb/synced_folder_test.rb, line
25
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in and_return.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/commands/winrm_config/command_test.rb, line 28
   Info: Do not hardcode passwords in code. Found hardcoded password used
in double.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/commands/winrm_config/command_test.rb, line 107
   Info: Do not hardcode passwords in code. Found hardcoded password used
in let.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4

Summary:

  24 Code issues found
  24 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION v2.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
--detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
...

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/provisioners/ansible/provisioner_test.rb, line
44
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/provisioners/ansible/provisioner_test.rb, line
1163
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/commands/ssh_config/command_test.rb, line 24
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
```

```
   Path: test/unit/vagrant/util/ssh_test.rb, line 35
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 77
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 96
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 114
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 133
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 151
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 169
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 187
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/vagrant/util/ssh_test.rb, line 205
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in let.

 ✗ [Low] Use of Hardcoded Credentials
   Path: test/unit/plugins/pushes/ftp/push_test.rb, line 13
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in double.

 ✗ [High] Use of a Broken or Risky Cryptographic Algorithm
   Path: lib/vagrant/util/keypair.rb, line 29
   Info: The des3 cipher (used in OpenSSL.Cipher.Cipher.new) is insecure.
Consider using AES instead.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
```

```
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0

Summary:

  14 Code issues found
  1 [High]   13 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION v1.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
--detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
...

 ✗ [Low] Python 2 source code
   Path: test/buildbot/buildbot_config/config/loader.py, line 4
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Medium] Improper Certificate Validation
   Path: lib/vagrant/downloaders/http.rb, line 25
   Info: SSL certificate verification is bypassed.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0

Summary:

  2 Code issues found
  1 [Medium]   1 [Low]


[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC scripts with Snyk code)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION DEFAULT ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION 2.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION 1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0 ...
```

```
 ✗ [Low] Python 2 source code
   Path: lamp-infrastructure/inventories/aws/ec2.py, line 95
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: lamp-infrastructure/inventories/digitalocean/digital_ocean.py,
line 104
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: dynamic-inventory/digitalocean/digital_ocean.py, line 104
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.

 ✗ [Low] Python 2 source code
   Path: dynamic-inventory/custom/inventory.py, line 5
   Info: This source file appears to be in Python 2. The Python 2
interpreter has been unsupported without security updates since January
2020. Consider porting this code to Python 3.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0

Summary:

  4 Code issues found
  4 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
```

```
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
2.0.4 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4

Summary:

✓ Awesome! No issues were found.
```

```
[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
v4.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
v3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0 --detection-depth=3
```

```
Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3 ...

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/inventory/test_stackpath_compute.py, line 92
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/inventory/test_stackpath_compute.py, line 113
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path:
tests/integration/targets/django_manage/files/base_test/simple_project/p1/p
1/settings.py, line 32
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 33
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 34
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
```

```
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 45
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 46
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 88
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 120
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 159
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 196
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 262
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 287
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 312
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 337
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 362
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 395
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.
```

```
 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/lookup/test_onepassword.py, line 53
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/lookup/test_onepassword.py, line 91
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_slack.py, line 96
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_slack.py, line 112
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/maven_artifact.py, line 620
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/ipa_user.py, line 300
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 138
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 138
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 161
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 161
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/iso_extract.py, line 185
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/iso_extract.py, line 190
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Missing protocol in ssl.wrap_socket
   Path: tests/integration/targets/java_cert/files/setupSSLServer.py, line
21
   Info: Call to deprecated method ssl.wrap_socket does not specify a
protocol, which may result in an insecure default being used

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/cobbler_sync.py, line 118
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/module_utils/opennebula.py, line 106
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/cobbler_system.py, line 240
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/rhn_channel.py, line 156
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 283
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in here.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 283
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 295
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Medium] Missing protocol in ssl.wrap_socket
   Path: plugins/modules/irc.py, line 198
   Info: Call to deprecated method ssl.wrap_socket does not specify a
protocol, which may result in an insecure default being used

 ✗ [Medium] Path Traversal
   Path: .azure-pipelines/scripts/combine-coverage.py, line 55
   Info: Unsanitized input from a command line argument flows into
shutil.copyfile, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_model_attrs.py, line 372
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.
```

```
 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/jenkins_job.py, line 350
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 215
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 265
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 298
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/zypper_repository.py, line 172
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/zypper.py, line 315
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3

Summary:

  46 Code issues found
  9 [Medium]   37 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION 7.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0 ...
```

```
 ✗ [Low] Missing protocol in ssl.wrap_socket
   Path: tests/integration/targets/java_cert/files/setupSSLServer.py, line
21
   Info: Call to deprecated method ssl.wrap_socket does not specify a
protocol, which may result in an insecure default being used

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 283
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in here.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 283
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 295
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 33
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 34
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 45
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 46
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 88
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 120
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 159
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 196
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 262
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 287
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 312
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 337
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 362
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 395
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path:
tests/integration/targets/django_manage/files/base_test/simple_project/p1/p
1/settings.py, line 32
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/lookup/test_onepassword.py, line 53
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/lookup/test_onepassword.py, line 91
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/inventory/test_stackpath_compute.py, line 92
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/inventory/test_stackpath_compute.py, line 113
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.
```

```
 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_slack.py, line 96
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_slack.py, line 112
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/cobbler_system.py, line 240
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/module_utils/opennebula.py, line 106
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/cobbler_sync.py, line 118
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/rhn_channel.py, line 156
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/ipa_user.py, line 300
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/maven_artifact.py, line 620
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 138
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 138
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 161
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 161
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/iso_extract.py, line 185
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/iso_extract.py, line 190
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/zypper_repository.py, line 173
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/zypper.py, line 315
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_model_attrs.py, line 372
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/jenkins_job.py, line 350
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 215
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 265
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 298
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Path Traversal
   Path: .azure-pipelines/scripts/combine-coverage.py, line 55
   Info: Unsanitized input from a command line argument flows into
shutil.copyfile, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Missing protocol in ssl.wrap_socket
   Path: plugins/modules/irc.py, line 198
   Info: Call to deprecated method ssl.wrap_socket does not specify a
protocol, which may result in an insecure default being used
```

```
✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0

Summary:

  46 Code issues found
  9 [Medium]   37 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION 6.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0 ...

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 283
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in here.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 283
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Use of Hardcoded Credentials
   Path: plugins/module_utils/rax.py, line 295
   Info: Do not hardcode credentials in code. Found hardcoded credential
used in a condition.

 ✗ [Low] Missing protocol in ssl.wrap_socket
   Path: tests/integration/targets/java_cert/files/setupSSLServer.py, line
21
   Info: Call to deprecated method ssl.wrap_socket does not specify a
protocol, which may result in an insecure default being used

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 131
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 131
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).
```

```
 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 154
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/jboss.py, line 154
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/iso_extract.py, line 178
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/iso_extract.py, line 183
   Info: sha1 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/maven_artifact.py, line 614
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: plugins/modules/ipa_user.py, line 294
   Info: hashlib.md5 is insecure. Consider changing it to a secure hashing
algorithm (e.g. SHA512).

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/lookup/onepassword/test_onepassword_cli_v1.py,
line 38
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_slack.py, line 96
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_slack.py, line 112
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 35
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 36
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 47
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/module_utils/cloud/test_scaleway.py, line 48
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path:
tests/integration/targets/django_manage/files/base_test/simple_project/p1/p
1/settings.py, line 32
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/lookup/onepassword/test_onepassword_cli_v2.py,
line 37
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 88
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 120
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 159
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 196
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 262
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 287
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 312
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 337
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 362
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/modules/test_java_keystore.py, line 395
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/inventory/test_stackpath_compute.py, line 92
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] Hardcoded Secret
   Path: tests/unit/plugins/inventory/test_stackpath_compute.py, line 113
   Info: Avoid hardcoding values that are meant to be secret. Found a
hardcoded string used in here.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/cobbler_sync.py, line 111
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/module_utils/opennebula.py, line 71
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/cobbler_system.py, line 233
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Low] no~hostname~verification
   Path: plugins/modules/rhn_channel.py, line 140
   Info: Using context that has been passed from
ssl._create_unverified_context will result with no hostname verification.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/jenkins_job.py, line 343
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_model_attrs.py, line 365
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 208
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.
```

```
 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 258
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/spectrum_device.py, line 291
   Info: xml.etree.ElementTree.fromstring is considered insecure. Use an
analog from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/zypper.py, line 307
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Medium] Insecure Xml Parser
   Path: plugins/modules/zypper_repository.py, line 166
   Info: xml.dom.minidom.parseString is considered insecure. Use an analog
from the defusedxml package.

 ✗ [Medium] Missing protocol in ssl.wrap_socket
   Path: plugins/modules/irc.py, line 191
   Info: Call to deprecated method ssl.wrap_socket does not specify a
protocol, which may result in an insecure default being used

 ✗ [Medium] Path Traversal
   Path: .azure-pipelines/scripts/combine-coverage.py, line 55
   Info: Unsanitized input from a command line argument flows into
shutil.copyfile, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to read arbitrary files.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0

Summary:

  46 Code issues found
  9 [Medium]   37 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4 ...
```

```
✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION v2.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION v1.2
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2
```

```
Summary:

✔ Awesome! No issues were found.


[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC extra projects with Snyk code)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0 ...


✔ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0

Summary:

✔ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
v0.0.2 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2 ...


✔ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2
```

```
Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
v0.0.1 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1 ...

 ✗ [Low] Cryptographic Issues
   Path: test/utils/common.py, line 27
   Info: Key size of 1024 bits used in key_size is considered insecure for
RSA. Use a key with at least 2048 bits.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1

Summary:
  1 Code issues found
  1 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION 2.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0 ...

 ✗ [Medium] Path Traversal
   Path: ansible_runner/__main__.py, line 767
   Info: Unsanitized input from a command line argument flows into
shutil.rmtree, where it is used as a path. This may result in a Path
Traversal vulnerability and allow an attacker to remove arbitrary files.

 ✗ [Medium] Path Traversal
   Path: ansible_runner/__main__.py, line 864
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: ansible_runner/__main__.py, line 871
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: ansible_runner/__main__.py, line 877
   Info: Unsanitized input from a command line argument flows into
os.remove, where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to remove arbitrary files.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0

Summary:

  4 Code issues found
  4 [Medium]


[Pipeline] echo
something failed
[Pipeline] echo
```

```
=============== https://github.com/ansible/ansible-runner.git VERSION 1.0.1
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1 ...

 ✗ [Medium] Path Traversal
   Path: ansible_runner/interface.py, line 163
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1

Summary:

  1 Code issues found
  1 [Medium]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2 ...

 ✗ [Low] Inadequate Encryption Strength
   Path: vendor/github.com/hashicorp/terraform-plugin-
testing/helper/acctest/random.go, line 175
   Info: Usage of 1024 bits key in crypto.rsa.GenerateKey is considered
insecure. Use a key with at least 2048 bits.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/openpgp/packet/public_key.go, line 307
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
```

```
   Path:
vendor/golang.org/x/crypto/openpgp/packet/symmetrically_encrypted.go, line
81
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path:
vendor/golang.org/x/crypto/openpgp/packet/symmetrically_encrypted.go, line
285
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/google/uuid/hash.go, line 52
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/Azure/go-autorest/autorest/adal/token.go, line
247
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/gofrs/uuid/generator.go, line 273
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/services/legacy/virtual_machine_resource.go, line 47
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/services/legacy/migration/legacy_vmss_v0_to_v1.go, line
721
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/pkcs12/pbkdf.go, line 19
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/software.sslmate.com/src/go-pkcs12/pkcs12.go, line 469
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/hashicorp/go-azure-
sdk/sdk/auth/client_credentials.go, line 210
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/services/keyvault/encrypted_value_data_source.go, line
137
```

```
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/software.sslmate.com/src/go-pkcs12/pbkdf.go, line 20
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/ssh/keys.go, line 1430
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/openpgp/packet/public_key_v3.go, line
81
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/tools/internal/pkgbits/encoder.go, line 60
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/google/uuid/hash.go, line 44
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/gofrs/uuid/generator.go, line 252
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/newrelic/new_relic_monitor_resource_test.go,
line 27
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/newrelic/new_relic_monitor_resource_test.go,
line 43
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/newrelic/new_relic_monitor_resource_test.go,
line 62
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_tag_rule_resource_test.go, line 26
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_tag_rule_resource_test.go, line 41
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_tag_rule_resource_test.go, line 59
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_tag_rule_resource_test.go, line 74
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_resource_test.go, line 28
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_resource_test.go, line 44
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_resource_test.go, line 63
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_resource_test.go, line 79
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_tag_rule_resource_test.go,
line 26
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_tag_rule_resource_test.go,
line 41
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_tag_rule_resource_test.go,
line 59
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_sub_account_tag_rule_resource_test.go,
line 74
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_monitor_resource_test.go, line 27
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_monitor_resource_test.go, line 43
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_monitor_resource_test.go, line 62
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Low] Use of Hardcoded Credentials
   Path: internal/services/logz/logz_monitor_resource_test.go, line 78
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in email.

 ✗ [Medium] Use of Hardcoded Credentials
   Path: vendor/software.sslmate.com/src/go-pkcs12/pkcs12.go, line 37
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in DefaultPassword.

 ✗ [Medium] Path Traversal
   Path: internal/tools/generator-resource-id/main.go, line 1063
   Info: Unsanitized input from a CLI argument flows into os.WriteFile,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: internal/tools/update-api-version/main.go, line 79
   Info: Unsanitized input from a CLI argument flows into os.WriteFile,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: internal/tools/update-api-version/main.go, line 105
   Info: Unsanitized input from a CLI argument flows into os.WriteFile,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [Medium] Path Traversal
   Path: internal/tools/update-api-version/main.go, line 62
   Info: Unsanitized input from a CLI argument flows into os.ReadDir, where
it is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to get a list of arbitrary files.

 ✗ [Medium] Path Traversal
   Path: internal/services/arckubernetes/testdata/install_agent.py, line
221
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.

 ✗ [Medium] Path Traversal
   Path: examples/arckubernetes/testdata/install_agent.py, line 221
   Info: Unsanitized input from a command line argument flows into open,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to read arbitrary files.
```

```
 ✗ [Medium] Clear Text Logging
   Path: vendor/golang.org/x/tools/internal/imports/imports.go, line 114
   Info: Unsanitized input from sensitive credentials flows into
log.Printf, where it is logged. This may result in a clear-text logging of
sensitive information.

 ✗ [High] Server-Side Request Forgery (SSRF)
   Path: vendor/github.com/Azure/go-autorest/autorest/azure/rp.go, line 94
   Info: Unsanitized input from an HTTP header flows into _, where it is
used as an URL to perform a request. This may result in a Server-Side
Request Forgery vulnerability.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2

Summary:

  47 Code issues found
  1 [High]   8 [Medium]   38 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION v3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0 ...

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/gofrs/uuid/generator.go, line 157
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/google/uuid/hash.go, line 44
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/openpgp/packet/public_key_v3.go, line
81
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/gofrs/uuid/generator.go, line 178
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/Azure/go-autorest/autorest/adal/token.go, line
244
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path:
vendor/golang.org/x/crypto/openpgp/packet/symmetrically_encrypted.go, line
81
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path:
vendor/golang.org/x/crypto/openpgp/packet/symmetrically_encrypted.go, line
285
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/google/uuid/hash.go, line 52
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/openpgp/packet/public_key.go, line 307
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/manicminer/hamilton/auth/clientcredentials.go,
line 197
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/pkcs12/pbkdf.go, line 19
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/services/compute/migration/legacy_vmss.go, line 718
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/services/legacy/virtual_machine_resource.go, line 45
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: internal/services/keyvault/encrypted_value_data_source.go, line
120
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm
```

```
 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/ssh/keys.go, line 1457
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Inadequate Encryption Strength
   Path: vendor/github.com/hashicorp/terraform-plugin-
sdk/v2/helper/acctest/random.go, line 142
   Info: Usage of 1024 bits key in crypto.rsa.GenerateKey is considered
insecure. Use a key with at least 2048 bits.

 ✗ [Medium] Path Traversal
   Path: internal/tools/generator-resource-id/main.go, line 1041
   Info: Unsanitized input from a CLI argument flows into os.WriteFile,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to write arbitrary files.

 ✗ [High] Server-Side Request Forgery (SSRF)
   Path: vendor/github.com/Azure/go-autorest/autorest/azure/rp.go, line 94
   Info: Unsanitized input from an HTTP header flows into _, where it is
used as an URL to perform a request. This may result in a Server-Side
Request Forgery vulnerability.


✔ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0

Summary:

  18 Code issues found
  1 [High]   1 [Medium]   16 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION v2.0.0 ==================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0 ...

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/data_source_shared_image_version_te
st.go, line 14
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.
```

```
 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line 27
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line 60
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line 93
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
132
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
169
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
202
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
235
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 21
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 66
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.
```

```
 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 102
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 142
   Info: Do not hardcode passwords in code. Found Hardcoded password saved
in password.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/pkcs12/pbkdf.go, line 19
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: azurerm/internal/services/compute/resource_arm_virtual_machine.go,
line 43
   Info: The SHA1 hash (used in crypto.sha1.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/openpgp/packet/public_key.go, line 307
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/terraform-providers/terraform-provider-
azuread/azuread/data_users.go, line 97
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/hashicorp/go-getter/checksum.go, line 147
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/satori/go.uuid/generator.go, line 162
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path:
vendor/golang.org/x/crypto/openpgp/packet/symmetrically_encrypted.go, line
81
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path:
vendor/golang.org/x/crypto/openpgp/packet/symmetrically_encrypted.go, line
285
```

```
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/terraform-providers/terraform-provider-
azuread/azuread/data_groups.go, line 97
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/satori/uuid/uuid.go, line 466
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/Azure/go-autorest/autorest/adal/token.go, line
226
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/google/uuid/hash.go, line 52
   Info: The SHA1 hash (used in crypto.sha1.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/ssh/keys.go, line 1311
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/aws/aws-sdk-go/service/s3/sse.go, line 80
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/hashicorp/go-getter/folder_storage.go, line 63
   Info: The MD5 hash (used in crypto.md5.Sum) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/aws/aws-sdk-go/service/s3/body_hash.go, line 31
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/aws/aws-sdk-go/service/s3/body_hash.go, line 72
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/aws/aws-sdk-go/service/s3/body_hash.go, line 207
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/hashicorp/go-getter/checksum.go, line 145
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm
```

```
 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/satori/go.uuid/generator.go, line 143
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/golang.org/x/crypto/openpgp/packet/public_key_v3.go, line
81
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/satori/uuid/uuid.go, line 447
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/google/uuid/hash.go, line 44
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/data_source_shared_image_version_te
st.go, line 13
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in username.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line 26
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line 59
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line 92
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
131
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
168
```

```
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
201
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_image_test.go, line
234
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 20
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 65
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 101
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Use of Hardcoded Credentials
   Path:
azurerm/internal/services/compute/tests/resource_arm_shared_image_version_t
est.go, line 141
   Info: Do not hardcode credentials in code. Found Hardcoded username
credential used in userName.

 ✗ [Low] Inadequate Encryption Strength
   Path: vendor/github.com/hashicorp/terraform-plugin-
sdk/helper/acctest/random.go, line 145
   Info: Usage of 1024 bits key in crypto.rsa.GenerateKey is considered
insecure. Use a key with at least 2048 bits.

 ✗ [Low] Use of Password Hash With Insufficient Computational Effort
   Path: vendor/github.com/hashicorp/go-getter/decompress_testing.go, line
163
   Info: The MD5 hash (used in crypto.md5.New) is insecure. Consider
changing it to a secure hash algorithm

 ✗ [High] Path Traversal
   Path: vendor/github.com/hashicorp/go-getter/get_file_unix.go, line 48
   Info: Unsanitized input from the request URL flows into os.Symlink,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to create arbitrary symlinks.

 ✗ [High] Path Traversal
   Path: vendor/github.com/hashicorp/go-getter/get_file_unix.go, line 85
   Info: Unsanitized input from the request URL flows into os.Symlink,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to create arbitrary symlinks.

 ✗ [High] Path Traversal
   Path: vendor/github.com/hashicorp/go-getter/get_file_windows.go, line 97
   Info: Unsanitized input from the request URL flows into os.Symlink,
where it is used as a path. This may result in a Path Traversal
vulnerability and allow an attacker to create arbitrary symlinks.

 ✗ [High] Path Traversal
   Path: vendor/github.com/hashicorp/go-getter/get_file_unix.go, line 89
   Info: Unsanitized input from the request URL flows into os.Open, where
it is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [High] Path Traversal
   Path: vendor/github.com/hashicorp/go-getter/get_file_windows.go, line
115
   Info: Unsanitized input from the request URL flows into os.Open, where
it is used as a path. This may result in a Path Traversal vulnerability and
allow an attacker to open arbitrary files.

 ✗ [High] Server-Side Request Forgery (SSRF)
   Path: vendor/github.com/Azure/go-autorest/autorest/azure/rp.go, line 94
   Info: Unsanitized input from an HTTP header flows into _, where it is
used as an URL to perform a request. This may result in a Server-Side
Request Forgery vulnerability.


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0

Summary:

  55 Code issues found
  6 [High]   49 [Low]


[Pipeline] echo
something failed
[Pipeline] echo
============== https://github.com/chef/cookstyle.git VERSION DEFAULT
==================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3 --detection-depth=3
```

```
Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION v7.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION v6.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0 ...


✓ Test completed

Organization:      code-mdh
```

```
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4

Summary:

✓ Awesome! No issues were found.


[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION v4.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0

Summary:

✓ Awesome! No issues were found.
```

```
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION v3.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk code test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0 --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0 ...


✓ Test completed

Organization:      code-mdh
Test type:         Static code analysis
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0

Summary:

✓ Awesome! No issues were found.


[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC tools with Snyk manifest)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== ansible VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0 --
all-projects --detection-depth=3
Failed to get dependencies for all 2 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== ansible VERSION v2.0.0-0.1.alpha1 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1 --all-projects --detection-depth=3
Could not detect supported target files in
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1.
Please see our documentation for supported languages and target files:
https://snyk.co/udVgQ and make sure you are in the right directory.
[Pipeline] echo
something failed
[Pipeline] echo
```

```
=============== ansible VERSION v1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0 -
-all-projects --detection-depth=3
Could not detect supported target files in
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0.
Please see our documentation for supported languages and target files:
https://snyk.co/udVgQ and make sure you are in the right directory.
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1 --
all-projects --detection-depth=3
✗ 1/2 potential projects failed to get dependencies.
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1/go
.mod:
  The "go" command is not available on your system. To scan your
dependencies in the CLI, you must ensure you have first installed the
relevant package manager.

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1...

Organization:      code-mdh
Package manager:   npm
Target file:       website/package-lock.json
Project name:      terraform-docs-preview
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
Licenses:          enabled

✓ Tested
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


[Pipeline] echo
=============== terraform VERSION v1.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION v0.1.0 ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0 --all-projects --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0...

Tested 51 dependencies for known issues, found 31 issues, 200 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade middleman@3.3.2 to middleman@4.4.0 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-3237242] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-3360028] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-MIDDLEMANCORE-20359] in
middleman-core@3.3.2
    introduced by middleman@3.3.2 > middleman-core@3.3.2 and 2 other
path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-20229] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-HAML-20341] in haml@4.0.5
    introduced by middleman@3.3.2 > haml@4.0.5
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-HAML-20362] in haml@4.0.5
    introduced by middleman@3.3.2 > haml@4.0.5
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20230] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ IP Spoofing [Medium Severity][https://security.snyk.io/vuln/SNYK-RUBY-
RACK-20399] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20400] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Information Exposure [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-538324] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-72567] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Arbitrary File Existence Exposure [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-SPROCKETS-20199] in
sprockets@2.12.0
    introduced by middleman@3.3.2 > middleman-sprockets@3.3.2 >
sprockets@2.12.0 and 2 other path(s)
  ✗ Improper minification of non-boolean comparisons [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-UGLIFIER-20236] in
uglifier@2.5.0
    introduced by middleman@3.3.2 > uglifier@2.5.0
  ✗ Remote Code Execution [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-KRAMDOWN-585939] in
kramdown@1.3.3
    introduced by middleman@3.3.2 > kramdown@1.3.3
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-569598] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ DLL Loading Issue [High Severity][https://security.snyk.io/vuln/SNYK-
RUBY-FFI-22037] in ffi@1.9.3
    introduced by middleman@3.3.2 > middleman-core@3.3.2 > listen@1.3.1 >
rb-inotify@0.9.3 > ffi@1.9.3 and 5 other path(s)
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-SPROCKETS-22032] in
sprockets@2.12.0
    introduced by middleman@3.3.2 > middleman-sprockets@3.3.2 >
sprockets@2.12.0 and 2 other path(s)
  ✗ Denial of Service (DoS) [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JSON-560838] in
json@1.8.1
    introduced by middleman@3.3.2 > uglifier@2.5.0 > json@1.8.1

  Upgrade middleman-minify-html@3.1.1 to middleman-minify-html@3.3.0 to fix
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-20229] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-3237242] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-3360028] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-MIDDLEMANCORE-20359] in
middleman-core@3.3.2
    introduced by middleman@3.3.2 > middleman-core@3.3.2 and 2 other
path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20230] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ IP Spoofing [Medium Severity][https://security.snyk.io/vuln/SNYK-RUBY-
RACK-20399] in rack@1.5.2
```

```
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20400] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Information Exposure [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-538324] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Request Forgery (CSRF) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-572377] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-72567] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-569598] in
activesupport@4.0.4
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 and 5 other path(s)
  ✗ DLL Loading Issue [High Severity][https://security.snyk.io/vuln/SNYK-
RUBY-FFI-22037] in ffi@1.9.3
    introduced by middleman@3.3.2 > middleman-core@3.3.2 > listen@1.3.1 >
rb-inotify@0.9.3 > ffi@1.9.3 and 5 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-I18N-72582] in i18n@0.6.9
    introduced by middleman@3.3.2 > middleman-core@3.3.2 > i18n@0.6.9 and
11 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-569066] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-TZINFO-2958048] in
tzinfo@0.3.39
    introduced by middleman@3.3.2 > middleman-core@3.3.2 >
activesupport@4.0.4 > tzinfo@0.3.39 and 5 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)

  Upgrade rack-contrib@1.1.0 to rack-contrib@1.2.0 to fix
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@1.5.2
```

```
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20230] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ IP Spoofing [Medium Severity][https://security.snyk.io/vuln/SNYK-RUBY-
RACK-20399] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20400] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Information Exposure [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-538324] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Request Forgery (CSRF) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-572377] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-72567] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Request Forgery (CSRF) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACKCONTRIB-20391] in
rack-contrib@1.1.0
    introduced by rack-contrib@1.1.0
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-569066] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)

  Upgrade redcarpet@3.0.0 to redcarpet@3.5.1 to fix
  ✗ Cross-site Scripting (XSS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-REDCARPET-1059089] in
redcarpet@3.0.0
    introduced by redcarpet@3.0.0
  ✗ Cross-site Scripting (XSS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-REDCARPET-20212] in
redcarpet@3.0.0
    introduced by redcarpet@3.0.0

  Upgrade thin@1.5.1 to thin@1.6.0 to fix
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20230] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ IP Spoofing [Medium Severity][https://security.snyk.io/vuln/SNYK-RUBY-
RACK-20399] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-20400] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Information Exposure [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-538324] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Request Forgery (CSRF) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-572377] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-72567] in rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-569066] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@1.5.2
    introduced by rack-contrib@1.1.0 > rack@1.5.2 and 10 other path(s)


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by middleman@3.3.2 > middleman-core@3.3.2 > erubis@2.7.0 and
2 other path(s)
  No upgrade or patch available



Organization:      code-mdh
Package manager:   rubygems
```

```
Target file:       website/Gemfile.lock
Project name:      v0.1.0/website
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0
Licenses:          enabled

-------------------------------------------------------

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0...

Organization:      code-mdh
Package manager:   npm
Target file:       website/source/package.json
Project name:      terraform
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0
Licenses:          enabled

✓ Tested
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0 for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


Tested 2 projects, 1 contained vulnerable paths.



[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2 --all-
projects --detection-depth=3
Are you sure this a Gemfile.lock?
If it is, please file an issue on Github:
https://github.com/treycordova/gemfile/issues.
Regardless, gemfile parsed whatever you gave it.
✗ 4/7 potential projects failed to get dependencies.
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/chef-
bin/Gemfile:
  Could not read chef-bin/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/chef-
config/Gemfile:
  Could not read chef-config/Gemfile lockfile: can't test without
dependencies.
```

```
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/chef-
utils/Gemfile:
  Could not read chef-utils/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/kitchen
-tests/Gemfile:
  Could not read kitchen-tests/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2...

Tested 153 dependencies for known issues, found 2 issues, 5 vulnerable
paths.


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by chef@18.2.44-x64-mingw-ucrt > erubis@2.7.0 and 1 other
path(s)
  No upgrade or patch available
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@2.2.6.4
    introduced by chef@18.2.44-x64-mingw-ucrt > chef-zero@15.0.11 >
rack@2.2.6.4 and 2 other path(s)
  This issue was fixed in versions: 3.0.0.beta1



Organization:      code-mdh
Package manager:   rubygems
Target file:       Gemfile.lock
Project name:      2
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
Licenses:          enabled

-------------------------------------------------------

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2...

Organization:      code-mdh
Package manager:   rubygems
Target file:       knife/Gemfile.lock
Project name:      2/knife
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
Licenses:          enabled
```

```
✓ Tested 1 dependencies for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.

-------------------------------------------------------

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2...

Tested 157 dependencies for known issues, found 2 issues, 2 vulnerable
paths.


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by berkshelf@8.0.5 > chef@18.1.29-x64-mingw-ucrt >
erubis@2.7.0
  No upgrade or patch available
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@2.2.6.4
    introduced by berkshelf@8.0.5 > chef@18.1.29-x64-mingw-ucrt > chef-
zero@15.0.11 > rack@2.2.6.4
  This issue was fixed in versions: 3.0.0.beta1



Organization:      code-mdh
Package manager:   rubygems
Target file:       omnibus/Gemfile.lock
Project name:      2/omnibus
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2
Licenses:          enabled


Tested 3 projects, 2 contained vulnerable paths.



[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION v18.0.0 ==================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0 -
-all-projects --detection-depth=3
✗ 5/7 potential projects failed to get dependencies.
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/c
hef-bin/Gemfile:
  Could not read chef-bin/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
```

```
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/c
hef-config/Gemfile:
  Could not read chef-config/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/c
hef-utils/Gemfile:
  Could not read chef-utils/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/k
itchen-tests/Gemfile:
  Could not read kitchen-tests/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/k
nife/Gemfile:
  Could not read knife/Gemfile lockfile: can't test without dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0..
.

Tested 141 dependencies for known issues, found 10 issues, 32 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade chef@18.0.0-universal-mingw32 to chef@18.0.169 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by chef@18.0.0-universal-mingw32 > aws-sdk-s3@1.111.1 > aws-
sdk-core@3.125.1 > jmespath@1.4.0 and 5 other path(s)
```

```
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)

  Upgrade chef-bin@18.0.0 to chef-bin@18.0.169 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by chef@18.0.0-universal-mingw32 > aws-sdk-s3@1.111.1 > aws-
sdk-core@3.125.1 > jmespath@1.4.0 and 5 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)

  Upgrade cheffish@17.0.0 to cheffish@17.1.5 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by chef@18.0.0-universal-mingw32 > erubis@2.7.0 and 1 other
path(s)
  No upgrade or patch available
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@2.2.3
    introduced by chef@18.0.0-universal-mingw32 > chef-zero@15.0.11 >
rack@2.2.3 and 2 other path(s)
  This issue was fixed in versions: 3.0.0.beta1



Organization:      code-mdh
Package manager:   rubygems
Target file:       Gemfile.lock
Project name:      v18.0.0
Open source:       no
```

```
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0
Licenses:          enabled

-------------------------------------------------------

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0..
.

Tested 144 dependencies for known issues, found 10 issues, 16 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade berkshelf@7.2.2 to berkshelf@8.0.0 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by omnibus@8.2.7 > aws-sdk-s3@1.111.1 > aws-sdk-core@3.125.1
> jmespath@1.4.0 and 6 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3

  Upgrade omnibus@8.2.7 to omnibus@8.3.2 to fix
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by omnibus@8.2.7 > aws-sdk-s3@1.111.1 > aws-sdk-core@3.125.1
> jmespath@1.4.0 and 6 other path(s)

  Upgrade omnibus-software@4.0.0 to omnibus-software@22.11.239 to fix
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by omnibus@8.2.7 > aws-sdk-s3@1.111.1 > aws-sdk-core@3.125.1
> jmespath@1.4.0 and 6 other path(s)


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 >
erubis@2.7.0
  No upgrade or patch available
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@2.2.3
    introduced by berkshelf@7.2.2 > chef@17.9.26-universal-mingw32 > chef-
zero@15.0.11 > rack@2.2.3
  This issue was fixed in versions: 3.0.0.beta1



Organization:      code-mdh
Package manager:   rubygems
Target file:       omnibus/Gemfile.lock
Project name:      v18.0.0/omnibus
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0
Licenses:          enabled


Tested 2 projects, 2 contained vulnerable paths.



[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION v17.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0 -
-all-projects --detection-depth=3
✗ 4/6 potential projects failed to get dependencies.
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/c
hef-bin/Gemfile:
  Could not read chef-bin/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
```

```
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/c
hef-config/Gemfile:
  Could not read chef-config/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/c
hef-utils/Gemfile:
  Could not read chef-utils/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/k
itchen-tests/Gemfile:
  Could not read kitchen-tests/Gemfile lockfile: can't test without
dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0..
.

Tested 128 dependencies for known issues, found 11 issues, 51 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade chef@17.0.0-universal-mingw32 to chef@17.0.242 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
```

```
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)

  Upgrade chef-bin@17.0.0 to chef-bin@17.0.242 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)

  Upgrade chef-config@17.0.0 to chef-config@17.0.242 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)
```

```
  Upgrade chef-telemetry@1.0.14 to chef-telemetry@1.0.29 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)

  Upgrade cheffish@16.0.12 to cheffish@16.0.26 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)

  Upgrade chefstyle@1.5.7 to chefstyle@1.5.8 to fix
  ✗ Improper Input Validation [Low
Severity][https://security.snyk.io/vuln/SNYK-RUBY-REXML-1244518] in
rexml@3.2.4
    introduced by chefstyle@1.5.7 > rubocop@1.5.2 > rexml@3.2.4

  Upgrade inspec-core-bin@4.24.8 to inspec-core-bin@4.24.26 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)

  Upgrade ohai@17.0.0 to ohai@17.0.42 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)

  Upgrade webmock@3.11.0 to webmock@3.11.1 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by chef-config@17.0.0 > addressable@2.7.0 and 23 other
path(s)


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by chef@17.0.0-universal-mingw32 > erubis@2.7.0 and 1 other
path(s)
  No upgrade or patch available
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@2.2.3
    introduced by chef@17.0.0-universal-mingw32 > chef-zero@15.0.3 >
rack@2.2.3 and 2 other path(s)
  This issue was fixed in versions: 3.0.0.beta1



Organization:      code-mdh
Package manager:   rubygems
Target file:       Gemfile.lock
Project name:      v17.0.0
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0
Licenses:          enabled

-------------------------------------------------------

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0..
.

Tested 121 dependencies for known issues, found 11 issues, 26 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade berkshelf@7.1.0 to berkshelf@7.2.0 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237233] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237237] in
rack@2.2.3
```

```
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3360233] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by ohai@16.8.1 > chef-config@16.7.61 > addressable@2.7.0 and
12 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3

  Upgrade ohai@16.8.1 to ohai@16.10.4 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by ohai@16.8.1 > chef-config@16.7.61 > addressable@2.7.0 and
12 other path(s)

  Upgrade omnibus@8.0.9 to omnibus@8.0.15 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by ohai@16.8.1 > chef-config@16.7.61 > addressable@2.7.0 and
12 other path(s)
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by omnibus@8.0.9 > aws-sdk-s3@1.86.2 > aws-sdk-core@3.110.0
> jmespath@1.4.0 and 3 other path(s)

  Upgrade omnibus-software@4.0.0 to omnibus-software@22.11.239 to fix
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ADDRESSABLE-1316242] in
addressable@2.7.0
    introduced by ohai@16.8.1 > chef-config@16.7.61 > addressable@2.7.0 and
12 other path(s)
```

```
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JMESPATH-2859799] in
jmespath@1.4.0
    introduced by omnibus@8.0.9 > aws-sdk-s3@1.86.2 > aws-sdk-core@3.110.0
> jmespath@1.4.0 and 3 other path(s)


Issues with no direct upgrade or patch:
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 >
erubis@2.7.0
  No upgrade or patch available
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@2.2.3
    introduced by berkshelf@7.1.0 > chef@16.7.61-universal-mingw32 > chef-
zero@15.0.3 > rack@2.2.3
  This issue was fixed in versions: 3.0.0.beta1



Organization:      code-mdh
Package manager:   rubygems
Target file:       omnibus/Gemfile.lock
Project name:      v17.0.0/omnibus
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0
Licenses:          enabled


Tested 2 projects, 2 contained vulnerable paths.



[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3 --
all-projects --detection-depth=3
Failed to get dependencies for all 3 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION 8.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0 -
-all-projects --detection-depth=3
Failed to get dependencies for all 3 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
```

```
something failed
[Pipeline] echo
=============== puppet VERSION 7.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0 -
-all-projects --detection-depth=3
Failed to get dependencies for all 3 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4 --
all-projects --detection-depth=3
✗ 2/3 potential projects failed to get dependencies.
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4/Gemf
ile:
  Could not read Gemfile lockfile: can't test without dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4/go.m
od:
  The "go" command is not available on your system. To scan your
dependencies in the CLI, you must ensure you have first installed the
relevant package manager.

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4...

Organization:      code-mdh
Package manager:   npm
Target file:       website/package-lock.json
Project name:      vagrant-docs
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4
Licenses:          enabled

✓ Tested
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4 for
known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


[Pipeline] echo
=============== vagrant VERSION v2.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
--all-projects --detection-depth=3
✗ 1/2 potential projects failed to get dependencies.
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
/Gemfile:
  Could not read Gemfile lockfile: can't test without dependencies.
Please run `bundle install` first or if this is a custom file name re-run
with --file=path/to/custom.gemfile.lock --package-manager=rubygems

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
...

Tested 59 dependencies for known issues, found 44 issues, 367 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade middleman-hashicorp@0.3.28 to middleman-hashicorp@0.3.29 to fix
  ✗ XML External Entity (XXE) Injection [Low
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-1055008] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-BOOTSTRAPSASS-174549] in
bootstrap-sass@3.3.7
    introduced by middleman-hashicorp@0.3.28 > bootstrap-sass@3.3.7
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-BOOTSTRAPSASS-450237] in
bootstrap-sass@3.3.7
    introduced by middleman-hashicorp@0.3.28 > bootstrap-sass@3.3.7
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-BOOTSTRAPSASS-450238] in
bootstrap-sass@3.3.7
    introduced by middleman-hashicorp@0.3.28 > bootstrap-sass@3.3.7
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-BOOTSTRAPSASS-450239] in
bootstrap-sass@3.3.7
    introduced by middleman-hashicorp@0.3.28 > bootstrap-sass@3.3.7
  ✗ Denial of Service (DoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-1583442] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Access Control Bypass [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-3357693] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Information Exposure [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-538324] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-72567] in rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  ✗ DLL Loading Issue [High Severity][https://security.snyk.io/vuln/SNYK-
RUBY-FFI-22037] in ffi@1.9.18
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 >
compass@1.0.3 > rb-inotify@0.9.10 > ffi@1.9.18 and 4 other path(s)
```

```
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-1293239] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ XML External Entity (XXE) Injection [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-1726792] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ XML External Entity (XXE) Injection [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-20299] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Use of vulnerable libxml2 [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-20432] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-22013] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-22014] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Use After Free [High Severity][https://security.snyk.io/vuln/SNYK-
RUBY-NOKOGIRI-2413994] in nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Regular Expression Denial of Service (ReDoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-2620374] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Out-of-bounds Write [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-2630623] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-2630898] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Improper Handling of Unexpected Data Type [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-2840634] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ NULL Pointer Dereference [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-3052880] in
nokogiri@1.8.0
```

```
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Command Injection [High Severity][https://security.snyk.io/vuln/SNYK-
RUBY-NOKOGIRI-459107] in nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Uncontrolled Memory Allocation [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-534637] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-552159] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-NOKOGIRI-72433] in
nokogiri@1.8.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > capybara@2.4.4 > nokogiri@1.8.0 and 7 other path(s)
  ✗ Cross-site Scripting (XSS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-REDCARPET-1059089] in
redcarpet@3.4.0
    introduced by middleman-hashicorp@0.3.28 > redcarpet@3.4.0
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-SPROCKETS-22032] in
sprockets@2.12.4
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
sprockets@3.5.0 > sprockets@2.12.4 and 2 other path(s)
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-TZINFO-2958048] in
tzinfo@1.2.3
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > activesupport@4.2.8 > tzinfo@1.2.3 and 7 other path(s)
  ✗ Denial of Service (DoS) [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-JSON-560838] in
json@2.1.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 >
uglifier@2.7.2 > json@2.1.0


Issues with no direct upgrade or patch:
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-3237242] in
activesupport@4.2.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > activesupport@4.2.8 and 7 other path(s)
  This issue was fixed in versions: 6.1.7.1, 7.0.4.1
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-3360028] in
activesupport@4.2.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > activesupport@4.2.8 and 7 other path(s)
  This issue was fixed in versions: 6.1.7.3, 7.0.4.3
  ✗ Deserialization of Untrusted Data [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ACTIVESUPPORT-569598] in
activesupport@4.2.8
```

```
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > activesupport@4.2.8 and 7 other path(s)
  This issue was fixed in versions: 5.2.4.3, 6.0.3.1
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-ERUBIS-20482] in
erubis@2.7.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > erubis@2.7.0 and 3 other path(s)
  No upgrade or patch available
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-I18N-72582] in i18n@0.7.0
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > i18n@0.7.0 and 15 other path(s)
  This issue was fixed in versions: 0.8.0
  ✗ Remote Code Execution [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-KRAMDOWN-585939] in
kramdown@1.13.2
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 >
kramdown@1.13.2
  This issue was fixed in versions: 2.3.0
  ✗ Cross-site Scripting (XSS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-MIDDLEMANCORE-20359] in
middleman-core@3.4.1
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 and 3 other path(s)
  This issue was fixed in versions: 4.1.2
  ✗ Web Cache Poisoning [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-1061917] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 3.0.0.beta1
  ✗ Arbitrary Code Injection [Critical
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848599] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 2.0.9.1, 2.1.4.1, 2.2.3.1
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-2848600] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 2.0.9.1, 2.1.4.1, 2.2.3.1
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3237240] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 2.0.9.2, 2.1.4.2, 2.2.6.2, 3.0.4.1
  ✗ Denial of Service (DoS) [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-3356639] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 2.0.9.3, 2.1.4.3, 2.2.6.3, 3.0.4.2
  ✗ Directory Traversal [High
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-569066] in
rack@1.6.8
```

```
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 2.1.3
  ✗ Cross-site Request Forgery (CSRF) [Medium
Severity][https://security.snyk.io/vuln/SNYK-RUBY-RACK-572377] in
rack@1.6.8
    introduced by middleman-hashicorp@0.3.28 > middleman@3.4.1 > middleman-
core@3.4.1 > rack@1.6.8 and 15 other path(s)
  This issue was fixed in versions: 2.1.4, 2.2.3



Organization:      code-mdh
Package manager:   rubygems
Target file:       website/Gemfile.lock
Project name:      v2.0.0/website
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
Licenses:          enabled


[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION v1.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
--all-projects --detection-depth=3
Failed to get dependencies for all 2 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC scripts with Snyk manifest)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION 2.0 ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION 1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1 --all-projects --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1...

Organization:      code-mdh
Package manager:   composer
Target file:       composer.lock
Project name:      iwf-web/vagrant-scripts
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1
Licenses:          enabled

✓ Tested
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1 for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0 --all-projects --detection-depth=3
```

```
Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0...

Organization:      code-mdh
Package manager:   composer
Target file:       composer.lock
Project name:      iwf-web/vagrant-scripts
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0
Licenses:          enabled

✓ Tested
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0 for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
2.0.4 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4 --all-projects --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4...

Organization:      code-mdh
Package manager:   composer
Target file:       composer.lock
Project name:      iwf-web/vagrant-scripts
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4
Licenses:          enabled

✓ Tested
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4 for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2 --all-projects --detection-depth=3
```

```
Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2...

Organization:      code-mdh
Package manager:   npm
Target file:       package-lock.json
Project name:      terraform-generator
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2
Licenses:          enabled

✓ Tested 29 dependencies for known issues, no vulnerable paths found.

Next steps:
- Run `snyk monitor` to be notified about new related vulnerabilities.
- Run `snyk test` as part of your CI/test.


[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
v4.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0 --all-projects --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0...

Tested 17 dependencies for known issues, found 3 issues, 3 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade shelljs@0.8.4 to shelljs@0.8.5 to fix
  ✗ Improper Privilege Management [High
Severity][https://security.snyk.io/vuln/SNYK-JS-SHELLJS-2332187] in
shelljs@0.8.4
    introduced by shelljs@0.8.4


Issues with no direct upgrade or patch:
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-JS-MINIMATCH-3050818] in
minimatch@3.0.4
    introduced by shelljs@0.8.4 > glob@7.1.6 > minimatch@3.0.4
  This issue was fixed in versions: 3.0.5
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-JS-PATHPARSE-1077067] in path-
parse@1.0.6
    introduced by shelljs@0.8.4 > rechoir@0.6.2 > resolve@1.15.1 > path-
parse@1.0.6
  This issue was fixed in versions: 1.0.7
```

```
Organization:      code-mdh
Package manager:   npm
Target file:       package-lock.json
Project name:      terraform-generator
Open source:       no
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0
Licenses:          enabled


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
v3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0 --all-projects --detection-depth=3

Testing
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0...

Tested 16 dependencies for known issues, found 3 issues, 3 vulnerable
paths.


Issues to fix by upgrading:

  Upgrade shelljs@0.8.4 to shelljs@0.8.5 to fix
  ✗ Improper Privilege Management [High
Severity][https://security.snyk.io/vuln/SNYK-JS-SHELLJS-2332187] in
shelljs@0.8.4
    introduced by shelljs@0.8.4


Issues with no direct upgrade or patch:
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-JS-MINIMATCH-3050818] in
minimatch@3.0.4
    introduced by shelljs@0.8.4 > glob@7.1.6 > minimatch@3.0.4
  This issue was fixed in versions: 3.0.5
  ✗ Regular Expression Denial of Service (ReDoS) [Medium
Severity][https://security.snyk.io/vuln/SNYK-JS-PATHPARSE-1077067] in path-
parse@1.0.6
    introduced by shelljs@0.8.4 > rechoir@0.6.2 > resolve@1.15.1 > path-
parse@1.0.6
  This issue was fixed in versions: 1.0.7



Organization:      code-mdh
Package manager:   npm
Target file:       package-lock.json
Project name:      terraform-generator
Open source:       no
```

```
Project path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0
Licenses:          enabled


[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION 7.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION 6.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION v2.0.0
===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION v1.2
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC extra projects with Snyk manifest)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
v0.0.2 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
v0.0.1 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
```

```
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1 --all-projects --detection-depth=3
Failed to get dependencies for all 2 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION 2.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 4 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION 1.0.1
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2 --all-projects --detection-depth=3
Failed to get dependencies for all 2 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION v3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 2 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
```

```
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION v2.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 4 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION DEFAULT
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3 --all-projects --detection-depth=3
Failed to get dependencies for all 2 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION v7.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION v6.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 1 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4 --all-projects --detection-depth=3
Failed to get dependencies for all 10 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
```

```
something failed
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION v4.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 5 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION v3.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0 --all-projects --detection-depth=3
Failed to get dependencies for all 5 potential projects.
Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io
[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC tools with Snyk IaC)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== ansible VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0 --
detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/0
[Pipeline] echo
something failed
[Pipeline] echo
=============== ansible VERSION v2.0.0-0.1.alpha1 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v2.0.0
-0.1.alpha1
[Pipeline] echo
something failed
[Pipeline] echo
=============== ansible VERSION v1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0 -
-detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/ansible/v1.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1 --
detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/1
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION v1.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v1.0
.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== terraform VERSION v0.1.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
```

```
✓ Test completed.

Issues

Low Severity Issues: 183

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/connection.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/connection.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[db] > disable_api_termination
  File:    config/test-fixtures/dir-merge/two.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[db] > metadata_options
  File:    config/test-fixtures/dir-merge/two.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/provisioners.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/provisioners.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-bad-depends-on/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-bad-depends-on/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`
  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-bad-multi-resource/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-bad-multi-resource/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-count-below-zero/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-count-below-zero/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
```

```
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-count-zero/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-count-zero/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-dup-resource/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-dup-resource/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
```

```
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-output-bad-field/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-output-bad-field/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-unknown-resource-var-
output/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-unknown-resource-var-
output/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
```

```
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    config/test-fixtures/validate-unknown-resource-var/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[db] > disable_api_termination
  File:    config/test-fixtures/validate-unknown-resource-var/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    config/test-fixtures/validate-unknown-resource-var/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[db] > metadata_options
  File:    config/test-fixtures/validate-unknown-resource-var/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
```

```
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-cancel/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-cancel/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-cancel/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-cancel/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
```

```
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-compute/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-compute/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-compute/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-compute/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
```

```
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-destroy-outputs/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using 
Amazon
           EC2, you can enable termination protection for the instance. 
Without
           this setting enabled the instances can be terminated by 
accident.
           This setting should only be used for instances with high 
availability
           requirements. Enabling this may prevent IaC workflows from 
updating
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-destroy-outputs/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service 
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-destroy-outputs/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service 
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-destroy-outputs/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using 
Amazon
           EC2, you can enable termination protection for the instance. 
Without
           this setting enabled the instances can be terminated by 
accident.
           This setting should only be used for instances with high 
availability
           requirements. Enabling this may prevent IaC workflows from 
updating
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-destroy/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-destroy/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-destroy/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-destroy/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-error/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-error/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-error/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-error/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-idattr/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-idattr/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-minimal/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-minimal/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-minimal/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-minimal/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-output-multi-index/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-output-multi-index/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-output-multi-index/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-output-multi-index/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`
  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-output-multi/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-output-multi/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-output-multi/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-output-multi/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
```

```
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-output/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-output/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-output/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-output/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
```

```
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-compute/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-compute/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-compute/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-compute/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
```

```
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-conninfo/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-conninfo/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-conninfo/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-conninfo/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
```

```
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-fail/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-fail/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-fail/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-fail/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
```

```
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-provisioner-resource-ref/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-provisioner-resource-ref/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-taint/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-taint/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-unknown/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-unknown/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/apply-vars/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/apply-vars/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/apply-vars/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/apply-vars/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/graph-count/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/graph-count/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/graph-depends-on/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[db] > disable_api_termination
  File:    terraform/test-fixtures/graph-depends-on/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/graph-depends-on/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[db] > metadata_options
  File:    terraform/test-fixtures/graph-depends-on/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/graph-diff-destroy/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
```

```
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/graph-diff-destroy/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/graph-diff-destroy/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/graph-diff-destroy/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/graph-diff/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/graph-diff/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/new-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/new-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/new-graph-cycle/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
```

```
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/new-graph-cycle/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/new-graph-cycle/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/new-graph-cycle/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
```

```
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] Load balancer is internet facing
  Info:    Load balancer is internet facing. Increases attack vector
           reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-48
  Path:    resource > aws_elb[lb] > internal
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `internal` attribute to `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/new-provider-validate/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/new-provider-validate/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-computed/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-computed/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-computed/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-computed/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`
  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using 
Amazon
           EC2, you can enable termination protection for the instance. 
Without
           this setting enabled the instances can be terminated by 
accident.
           This setting should only be used for instances with high 
availability
           requirements. Enabling this may prevent IaC workflows from 
updating
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-count-dec/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using 
Amazon
           EC2, you can enable termination protection for the instance. 
Without
           this setting enabled the instances can be terminated by 
accident.
           This setting should only be used for instances with high 
availability
           requirements. Enabling this may prevent IaC workflows from 
updating
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-count-dec/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service 
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-count-dec/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service 
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-count-dec/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-count-inc/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-count-inc/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-count-inc/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-count-inc/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
```

```
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-count/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-count/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-count/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-count/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
```

```
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-destroy/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-destroy/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-destroy/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-destroy/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
```

```
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-diffvar/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-diffvar/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-diffvar/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-diffvar/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
```

```
           requirements. Enabling this may prevent IaC workflows from 
updating
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-empty/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using 
Amazon
           EC2, you can enable termination protection for the instance. 
Without
           this setting enabled the instances can be terminated by 
accident.
           This setting should only be used for instances with high 
availability
           requirements. Enabling this may prevent IaC workflows from 
updating
           the instance, for example terraform will not be able to 
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-empty/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service 
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-empty/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service 
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-empty/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using 
Amazon
           EC2, you can enable termination protection for the instance. 
Without
           this setting enabled the instances can be terminated by 
accident.
           This setting should only be used for instances with high 
availability
           requirements. Enabling this may prevent IaC workflows from 
updating
```

```
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-nil/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-nil/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-orphan/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-orphan/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-provider-init/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-provider-init/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/plan-taint/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/plan-taint/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/plan-taint/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/plan-taint/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/refresh-basic/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/refresh-basic/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/refresh-vars/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
```

```
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[db] > disable_api_termination
  File:    terraform/test-fixtures/refresh-vars/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/refresh-vars/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[db] > metadata_options
  File:    terraform/test-fixtures/refresh-vars/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[test] > disable_api_termination
  File:    terraform/test-fixtures/validate-bad-pc/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[test] > metadata_options
  File:    terraform/test-fixtures/validate-bad-pc/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[test] > disable_api_termination
  File:    terraform/test-fixtures/validate-bad-prov-conf/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[test] > metadata_options
  File:    terraform/test-fixtures/validate-bad-prov-conf/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[test] > disable_api_termination
  File:    terraform/test-fixtures/validate-bad-rc/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[test] > metadata_options
  File:    terraform/test-fixtures/validate-bad-rc/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`
  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/validate-bad-var/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/validate-bad-var/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/validate-bad-var/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/validate-bad-var/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[foo] > disable_api_termination
  File:    terraform/test-fixtures/validate-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[bar] > disable_api_termination
  File:    terraform/test-fixtures/validate-good/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[bar] > metadata_options
  File:    terraform/test-fixtures/validate-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[foo] > metadata_options
  File:    terraform/test-fixtures/validate-good/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
```

```
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/validate-required-var/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/validate-required-var/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/validate-self-ref-multi-all/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/validate-self-ref-multi-all/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
```

```
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/validate-self-ref-multi/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/validate-self-ref-multi/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

  [Low] EC2 API termination protection is not enabled
  Info:    To prevent instance from being accidentally terminated using
Amazon
           EC2, you can enable termination protection for the instance.
Without
           this setting enabled the instances can be terminated by
accident.
           This setting should only be used for instances with high
availability
           requirements. Enabling this may prevent IaC workflows from
updating
           the instance, for example terraform will not be able to
terminate the
           instance to update instance type
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AWS-426
  Path:    resource > aws_instance[web] > disable_api_termination
  File:    terraform/test-fixtures/validate-self-ref/main.tf
  Resolve: Set `disable_api_termination` attribute  with value `true`

  [Low] EC2 instance accepts IMDSv1
  Info:    Instance Metadata Service v2 is not enforced. Metadata service
may be
           vulnerable to reverse proxy/open firewall misconfigurations and
           server side request forgery attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-130
  Path:    resource > aws_instance[web] > metadata_options
  File:    terraform/test-fixtures/validate-self-ref/main.tf
  Resolve: Set `metadata_options.http_tokens` attribute to `required`

Medium Severity Issues: 91

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/connection.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[db] > root_block_device > encrypted
  File:    config/test-fixtures/dir-merge/two.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/provisioners.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-bad-depends-on/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-bad-multi-resource/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-count-below-zero/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That 
should
           someone gain unauthorized access to the data they would be able 
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-count-zero/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That 
should
           someone gain unauthorized access to the data they would be able 
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-dup-resource/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That 
should
           someone gain unauthorized access to the data they would be able 
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-output-bad-field/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That 
should
           someone gain unauthorized access to the data they would be able 
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-unknown-resource-var-
output/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That 
should
           someone gain unauthorized access to the data they would be able 
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    config/test-fixtures/validate-unknown-resource-var/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That 
should
           someone gain unauthorized access to the data they would be able 
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[db] > root_block_device > encrypted
  File:    config/test-fixtures/validate-unknown-resource-var/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-cancel/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-cancel/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-compute/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-compute/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-destroy-outputs/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-destroy-outputs/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-destroy/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-destroy/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-error/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-error/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-idattr/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-minimal/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-minimal/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-output-multi-index/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-output-multi-index/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-output-multi/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-output-multi/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-output/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-output/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-compute/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-compute/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-conninfo/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-conninfo/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-fail/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-fail/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-provisioner-resource-ref/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-taint/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-unknown/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-vars/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/apply-vars/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/graph-count/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/graph-depends-on/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[db] > root_block_device > encrypted
  File:    terraform/test-fixtures/graph-depends-on/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/graph-diff-destroy/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/graph-diff-destroy/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/graph-diff/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/new-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/new-graph-cycle/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/new-graph-cycle/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/new-pc-cache/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/new-provider-validate/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-computed/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-computed/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-count-dec/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-count-dec/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-count-inc/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-count-inc/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-count/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-count/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-destroy/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-destroy/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-diffvar/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-diffvar/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-empty/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-empty/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-nil/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-orphan/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-provider-init/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-taint/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/plan-taint/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/refresh-basic/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/refresh-vars/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[db] > root_block_device > encrypted
  File:    terraform/test-fixtures/refresh-vars/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[test] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-bad-pc/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[test] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-bad-prov-conf/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[test] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-bad-rc/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-bad-var/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-bad-var/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[bar] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[foo] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-good/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-required-var/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-self-ref-multi-all/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-self-ref-multi/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

  [Medium] Non-Encrypted root block device
  Info:    The root block device for ec2 instance is not encrypted. That
should
           someone gain unauthorized access to the data they would be able
to
           read the contents.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-53
  Path:    resource > aws_instance[web] > root_block_device > encrypted
  File:    terraform/test-fixtures/validate-self-ref/main.tf
  Resolve: Set `root_block_device.encrypted` attribute to `true`

Test Failures

  Failed to parse Terraform file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/basic.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/import.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/dir-basic/one.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/dir-basic/two.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/dir-merge/one.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/dir-override/one.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/dir-override/two.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/import/one.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/validate-good/main.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/validate-unknownthing/main.tf
```

```
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/validate-unknownvar/main.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/terraform/test-fixtures/graph-basic/main.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/terraform/test-fixtures/graph-cycle/main.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/terraform/test-fixtures/graph-provisioners/main.tf

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/terraform/test-fixtures/smc-uservars/main.tf

  Failed to parse JSON file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/terraform/v0.1
.0/config/test-fixtures/dir-override/foo_override.tf.json

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✓ Files without issues: 14
✗ Files with issues: 60
  Ignored issues: 0
  Total issues: 274 [ 0 critical, 0 high, 91 medium, 183 low ]

Tip: Re-run in debug mode to see more information: DEBUG=*snyk* <COMMAND>
If the issue persists contact support@snyk.io

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2 --
detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Failed to parse JSON file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/cspell.
json

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/kitchen
-tests/data_bags/users/adam.json
```

```
  Failed to parse YAML file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/2/omnibus
/kitchen.yml
[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION v18.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0 -
-detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Failed to parse JSON file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/c
spell.json

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/k
itchen-tests/data_bags/users/adam.json

  Failed to parse YAML file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v18.0.0/o
mnibus/kitchen.yml
[Pipeline] echo
something failed
[Pipeline] echo
=============== chef VERSION v17.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0 -
-detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Failed to parse JSON file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/c
spell.json

/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/k
itchen-tests/data_bags/users/adam.json

  Failed to parse YAML file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/chef/v17.0.0/o
mnibus/kitchen.yml
[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3 --
detection-depth=3
```

```
Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/3
[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION 8.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0 -
-detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/8.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== puppet VERSION 7.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0 -
-detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/puppet/7.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4 --
detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/4
[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION v2.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
--detection-depth=3
```

```
Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v2.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== vagrant VERSION v1.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
--detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/vagrant/v1.0.0
[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC scripts with Snyk IaC)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✔ Test completed.

Issues

Low Severity Issues: 6

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > runAsUser
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           resources > limits > memory
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > template > spec > containers[nginx] >
           livenessProbe
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > template > spec > containers[nginx] >
           imagePullPolicy
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           resources > limits > cpu
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > readOnlyRootFilesystem
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`
```

```
Medium Severity Issues: 3

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > runAsNonRoot
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > capabilities > drop
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > allowPrivilegeEscalation
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

High Severity Issues: 1

  [High] RoleBinding or ClusterRoleBinding is using a pre-defined role
  Info:    A RoleBinding or ClusterRoleBinding was found using one of the
           default user facing roles, `cluster-admin`, `admin`, `edit` or
           `view`. Using a default user facing role may be overly
permissive.
           For a ClusterRoleBinding this would be considered high severity.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-46
  Path:    [DocId: 0] > roleRef > name
  File:    kubernetes/examples/files/tiller-rbac.yml
  Resolve: Update roleRef.name to a specific role name with only the
necessary
           permissions

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk
```

```
✓ Files without issues: 0
✗ Files with issues: 2
  Ignored issues: 0
  Total issues: 10 [ 0 critical, 1 high, 3 medium, 6 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION 2.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/2.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✓ Test completed.

Issues

Low Severity Issues: 6

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > runAsUser
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           resources > limits > memory
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
```

```
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > template > spec > containers[nginx] >
           livenessProbe
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > template > spec > containers[nginx] >
           imagePullPolicy
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           resources > limits > cpu
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > readOnlyRootFilesystem
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

Medium Severity Issues: 3

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > runAsNonRoot
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > capabilities > drop
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > template > spec > containers[nginx]
>
           securityContext > allowPrivilegeEscalation
  File:    kubernetes/examples/files/nginx.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

High Severity Issues: 1

  [High] RoleBinding or ClusterRoleBinding is using a pre-defined role
  Info:    A RoleBinding or ClusterRoleBinding was found using one of the
           default user facing roles, `cluster-admin`, `admin`, `edit` or
           `view`. Using a default user facing role may be overly
permissive.
           For a ClusterRoleBinding this would be considered high severity.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-46
  Path:    [DocId: 0] > roleRef > name
  File:    kubernetes/examples/files/tiller-rbac.yml
  Resolve: Update roleRef.name to a specific role name with only the
necessary
           permissions

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✔ Files without issues: 0
✗ Files with issues: 2
  Ignored issues: 0
  Total issues: 10 [ 0 critical, 1 high, 3 medium, 6 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/geerlingguy/ansible-for-devops.git
VERSION 1.0 ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/ansibl
e-for-devops/1.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/1
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/3.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/iwf-web/vagrant-scripts.git VERSION
2.0.4 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/vagran
t-scripts/2.0.4
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/2
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
v4.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v4.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ahzhezhe/terraform-generator.git VERSION
v3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/terraf
orm-generator/v3.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION DEFAULT ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/3
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION 7.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/7.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible-
collections/community.general.git VERSION 6.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/commun
ity.general/6.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/4
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION v2.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v2.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/tropyx/NetBeansPuppet.git VERSION v1.2
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/scripts/NetBea
nsPuppet/v1.2
[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Scan of IaC extra projects with Snyk IaC)
[Pipeline] script
[Pipeline] {
[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✔ Test completed.

Issues
```

```
  No vulnerable paths were found!

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✓ Files without issues: 1
✗ Files with issues: 0
  Ignored issues: 0
  Total issues: 0 [ 0 critical, 0 high, 0 medium, 0 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
v0.0.2 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.2 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✓ Test completed.

Issues
  No vulnerable paths were found!

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✓ Files without issues: 1
✗ Files with issues: 0
  Ignored issues: 0
  Total issues: 0 [ 0 critical, 0 high, 0 medium, 0 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
=============== https://github.com/ricardozanini/soccer-stats.git VERSION
v0.0.1 ===================
[Pipeline] sh
```

```
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/soccer-
stats/v0.0.1 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✓ Test completed.

Issues
  No vulnerable paths were found!

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✓ Files without issues: 1
✗ Files with issues: 0
  Ignored issues: 0
  Total issues: 0 [ 0 critical, 0 high, 0 medium, 0 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION 2.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/2.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/ansible/ansible-runner.git VERSION 1.0.1
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/ansible-
runner/1.0.1
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/2 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✓ Test completed.

Issues

Low Severity Issues: 143

  [Low] API Management allows anonymous access to developer portal
  Info:    API Management allows anonymous access to developer portal.
Anonymous
           users can access your API documentation and specifications
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-504
  Path:    resource > azurerm_api_management[apim_service] > sign_in
  File:    examples/api-management/main.tf
  Resolve: Set a `sign_in.enabled` attribute set to `true`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[example] > purge_protection_enabled
  File:    examples/app-service-certificate/stored-in-keyvault/main.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
```

```
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/app-service-environment-v3/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/app-service/backup/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
```

```
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > securityContext > runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > containers[web] > resources > limits
>
           memory
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > containers[redis] > resources >
limits >
           memory
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > containers[redis] > livenessProbe
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > containers[web] > livenessProbe
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > containers[web] > imagePullPolicy
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > containers[redis] > imagePullPolicy
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > containers[web] > resources > limits
>
           cpu
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value
  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > containers[redis] > resources >
limits >
           cpu
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > securityContext >
readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
```

```
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/arckubernetes/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/azure-monitoring/data-collection-rule/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Ensure Diagnostic Setting captures appropriate categories
  Info:    Ensure Diagnostic Setting captures appropriate categories. Not
           capturing the diagnostic setting categories for appropriate
           management activities leads to missing important alerts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-552
  Path:    resource > azurerm_monitor_diagnostic_setting[example] > log
  File:    examples/azure-monitoring/eventhub_integration/main.tf
  Resolve: Set log blocks for the categories
           `Administrative`,`Alert`,`Policy`,`Security` with `enabled` set
to
           `true` for each

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/batch/basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[example] >
           os_profile_windows_config > provision_vm_agent
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
```

```
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[stor] > network_rules
  File:    examples/cdn/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/container-instance/subnet/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Geo replication for Azure Container Images disabled
  Info:    Geo replication for Azure Container Images disabled. Missing geo
           replication leads to reduced availability of container images
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-595
  Path:    resource > azurerm_container_registry[example] > georeplications
  File:    examples/container-registry/main.tf
  Resolve: Set a `georeplications` block within the resource, including a
valid
           `location` property

  [Low] CosmosDB account automatic failover disabled
  Info:    CosmosDB Account automatic failover disabled. Account will
experience
           loss of write availability for all the duration of the write
region
           outage
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-510
  Path:    resource > azurerm_cosmosdb_account[example] >
           enable_automatic_failover
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `enable_automatic_failover` attribute to `true`

  [Low] CosmosDB account automatic failover disabled
  Info:    CosmosDB Account automatic failover disabled. Account will
experience
           loss of write availability for all the duration of the write
region
           outage
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-510
  Path:    resource > azurerm_cosmosdb_account[example] >
           enable_automatic_failover
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `enable_automatic_failover` attribute to `true`

  [Low] Vault key expiration date not set
  Info:    Expiration date is not set for Azure Vault key. Key rotation
will not
           be enforced, which can lead to use of stale or compromised
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-173
  Path:    resource > azurerm_key_vault_key[example]
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `expiration_date` attribute to date in the future, with
format
           `YYYY-MM-DD'T'H:M:S'Z'`, e.g `2019-01-01T01:02:03Z`

  [Low] Data Factory not encrypted with customer managed key
  Info:    Data Factory is not using customer managed key to encrypt data.
Scope
           of use of the key cannot be controlled via access policies
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-514
  Path:    resource > azurerm_data_factory[target] >
customer_managed_key_id
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `customer_managed_key_id` attribute

  [Low] Data Factory not encrypted with customer managed key
  Info:    Data Factory is not using customer managed key to encrypt data.
Scope
           of use of the key cannot be controlled via access policies
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-514
  Path:    resource > azurerm_data_factory[host] > customer_managed_key_id
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `customer_managed_key_id` attribute
  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[test] > ddos_protection_plan
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/eventgrid/event-subscription/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example2] >
ddos_protection_plan
  File:    examples/eventhub/namespace-networkrulesets/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
```

```
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example1] >
ddos_protection_plan
  File:    examples/eventhub/namespace-networkrulesets/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`
  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext > runAsUser
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > resources > limits > memory
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > template > spec > containers[aci-helloworld]
>
           livenessProbe
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > template > spec > containers[aci-helloworld]
>
           imagePullPolicy
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > resources > limits > cpu
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value
  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext >
readOnlyRootFilesystem
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
```

```
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/monitoring-log-analytics/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/monitoring-log-analytics/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
```

```
          Cannot utilize network policies feature to provide network
          segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
          network_policy
  File:    examples/kubernetes/private-api-server/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
          cluster might prevent incident response based on crucial log or
          hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
          oms_agent
  File:    examples/kubernetes/private-api-server/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
          the network will not benefit from advanced DDoS protection
features
          such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
          Cannot utilize network policies feature to provide network
          segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
          network_policy
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
          cluster might prevent incident response based on crucial log or
          hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
          oms_agent
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
          Cannot utilize network policies feature to provide network
          segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
```

```
           network_policy
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[test] > purge_protection_enabled
  File:    examples/managed-disks/encrypted/1-dependencies.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Vault key expiration date not set
  Info:    Expiration date is not set for Azure Vault key. Key rotation
will not
           be enforced, which can lead to use of stale or compromised
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-173
  Path:    resource > azurerm_key_vault_key[test]
  File:    examples/managed-disks/encrypted/main.tf
  Resolve: Set `expiration_date` attribute to date in the future, with
format
           `YYYY-MM-DD'T'H:M:S'Z'`, e.g `2019-01-01T01:02:03Z`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/basic-with-assets/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example2] > network_rules
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/mssql/mssqlvm/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/nfsv3_volume_with_snapshot_policy/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/snapshot/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example_primary] >
           ddos_protection_plan
  File:    examples/netapp/volume_crr/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example_secondary] >
           ddos_protection_plan
  File:    examples/netapp/volume_crr/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/volume_from_snapshot/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/volume/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[main] > ddos_protection_plan
  File:    examples/orchestrated-vm-scale-set/automatic-vm-guest-
patching/main.t
           f
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[main] > ddos_protection_plan
  File:    examples/orchestrated-vm-scale-set/hotpatching-enabled/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/application-gateway/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/postgresql/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/private-dns-group/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/private-link-scope/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/private-link-service/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/recovery-services/site-recovery-zone-zone/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/recovery-services/site-recovery-zone-zone/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/basic/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/premium-with-clustering/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`
  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/standard/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Azure Search Service is not using system-assigned identities
  Info:    Azure Search Service is not using system-assigned identities.
The
           risk of improperly configured authentication as well as missing
           credentials rotation increases if not using managed identities
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-641
  Path:    resource > azurerm_search_service[example] > identity > type
  File:    examples/search/main.tf
  Resolve: Set `identity.type` to `SystemAssigned`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/service-fabric/windows-vmss-self-signed-certs/0-base.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/service-fabric/windows-vmss-self-signed-certs/0-base.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[example] > purge_protection_enabled
  File:    examples/service-fabric/windows-vmss-self-signed-certs/1-
keyvault.tf
```

```
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_sql_server[example]
  File:    examples/sql-azure/database/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[secondary]
  File:    examples/sql-azure/failover_group/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[example]
  File:    examples/sql-azure/failover_group/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Ensure Diagnostic Setting captures appropriate categories
  Info:    Ensure Diagnostic Setting captures appropriate categories. Not
           capturing the diagnostic setting categories for appropriate
           management activities leads to missing important alerts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-552
  Path:    resource > azurerm_monitor_diagnostic_setting[example] > log
  File:    examples/sql-azure/sql_auditing_eventhub/main.tf
  Resolve: Set log blocks for the categories
           `Administrative`,`Alert`,`Policy`,`Security` with `enabled` set
to
           `true` for each

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[example]
  File:    examples/sql-azure/sql_auditing_eventhub/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Ensure Diagnostic Setting captures appropriate categories
  Info:    Ensure Diagnostic Setting captures appropriate categories. Not
           capturing the diagnostic setting categories for appropriate
           management activities leads to missing important alerts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-552
  Path:    resource > azurerm_monitor_diagnostic_setting[example] > log
  File:    examples/sql-azure/sql_auditing_log_analytics/main.tf
  Resolve: Set log blocks for the categories
           `Administrative`,`Alert`,`Policy`,`Security` with `enabled` set
to
           `true` for each
  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[example]
  File:    examples/sql-azure/sql_auditing_log_analytics/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage_adls_acls/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage-account/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example2] > network_rules
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage-share/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/stream-analytics/basic-usage/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/stream-analytics/msi-auth/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/tfc-checks/app-service-app-usage/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[example] > purge_protection_enabled
  File:    examples/tfc-checks/app-service-certificate-expiry/main.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/tfc-checks/vm-power-state/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/basic/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/virtual-machine/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/vm-scale-set/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[azuvnet] >
ddos_protection_plan
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`
  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[vmjb] >
os_profile_windows_config
           > provision_vm_agent
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[vmserver] >
           os_profile_windows_config > provision_vm_agent
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[azusa] > network_rules
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/basic/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
```

```
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/multiple-subnets/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/network-interface-app-security-group-
associ
           ation/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/network-security-group/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[test] > ddos_protection_plan
  File:    examples/virtual-networks/private-link-service/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[second] >
ddos_protection_plan
  File:    examples/virtual-networks/virtual-network-peering/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
```

```
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[first] > ddos_protection_plan
  File:    examples/virtual-networks/virtual-network-peering/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

Medium Severity Issues: 102

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[example]
  File:    examples/app-service-certificate/stored-in-keyvault/main.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/app-service/backup/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/app-service/backup/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > securityContext > runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           capabilities > drop
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           capabilities > drop
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > securityContext >
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`
  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`
  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Ensure that RDP access is restricted from the internet
  Info:    Ensure that RDP access is restricted from the internet. Using
RDP
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-676
  Path:    resource > azurerm_network_security_group[example] >
security_rule >
           destination_port_range
  File:    examples/arckubernetes/main.tf
  Resolve: Remove `3389`, `*`, or any port range that covers `3389` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Ensure that SSH access is restricted from the internet
  Info:    Ensure that SSH access is restricted from the internet. Using
SSH
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-677
  Path:    resource > azurerm_network_security_group[example] >
security_rule >
           destination_port_range
  File:    examples/arckubernetes/main.tf
  Resolve: Remove `22`, `*`, or any port range that covers `22` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[example] >
security_rule >
           source_address_prefix
  File:    examples/arckubernetes/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/batch/basic/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/batch/basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] CDN Endpoint https not enforced
  Info:    CDN Endpoint https not enforced. The content could be
intercepted and
           manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-509
  Path:    resource > azurerm_cdn_endpoint[example] > is_http_allowed
  File:    examples/cdn/main.tf
  Resolve: Set `is_http_allowed` to `false`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[stor] >
account_replication_type
  File:    examples/cdn/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[stor] > min_tls_version
  File:    examples/cdn/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/failover/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/failover/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] Data Factory public access enabled
  Info:    The Azure Data Factory REST APIs are accessible from the
Internet.
           The REST APIs are subject to attacks from the public internet,
such
           as zero-day vulnerabilities and unauthorized access via lost
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-513
  Path:    resource > azurerm_data_factory[host] > public_network_enabled
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `public_network_enabled` to `false`

  [Medium] Data Factory public access enabled
  Info:    The Azure Data Factory REST APIs are accessible from the
Internet.
           The REST APIs are subject to attacks from the public internet,
such
           as zero-day vulnerabilities and unauthorized access via lost
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-513
  Path:    resource > azurerm_data_factory[target] > public_network_enabled
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `public_network_enabled` to `false`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/eventgrid/event-subscription/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/eventgrid/event-subscription/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[example] >
security_rule[0]
           > source_address_prefix
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`
  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[example] >
security_rule[3]
           > source_address_prefix
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext > runAsNonRoot
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext > capabilities >
drop
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext >
           allowPrivilegeEscalation
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`
  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/monitoring-log-analytics/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16
  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/private-api-server/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[test]
  File:    examples/managed-disks/encrypted/1-dependencies.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/basic-with-assets/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example2] > min_tls_version
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] WAF not enabled on application gateway
  Info:    WAF not enabled on application gateway. Application will not be
           protected using a Web Application Firewall
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-474
  Path:    resource > azurerm_application_gateway[example] >
waf_configuration
  File:    examples/private-endpoint/application-gateway/main.tf
  Resolve: Set `enabled` attribute to `true` within the `waf_configuration`
           block

  [Medium] App Gateway does not use OWASP 3.x rules
  Info:    App Gateway does not use OWASP 3.x rules. Out-of-date OWASP
rules
           might not protect as effectively as more recent rule sets
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-610
  Path:    resource > azurerm_application_gateway[example] >
waf_configuration
  File:    examples/private-endpoint/application-gateway/main.tf
  Resolve: Set `waf_configuration.rule_set_type` to `OWASP` and
           `waf_configuration.rule_set_version` to `3.1`

  [Medium] PostgreSQL server minimum TLS version 1.2
  Info:    PostgreSQL server minimum TLS version 1.2. An outdated TLS
version
           might lead to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-629
  Path:    resource > azurerm_postgresql_server[example]
  File:    examples/private-endpoint/postgresql/main.tf
  Resolve: Set `ssl_minimal_tls_version_enforced` to `TLS1_2`
  [Medium] PostgreSQL server minimum TLS version 1.2
  Info:    PostgreSQL server minimum TLS version 1.2. An outdated TLS
version
           might lead to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-629
  Path:    resource > azurerm_postgresql_server[example]
  File:    examples/private-endpoint/private-dns-group/main.tf
  Resolve: Set `ssl_minimal_tls_version_enforced` to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/recovery-services/site-recovery-zone-zone/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/recovery-services/site-recovery-zone-zone/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/basic/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/premium-with-clustering/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/service-fabric/windows-vmss-self-signed-certs/0-base.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[example]
  File:    examples/service-fabric/windows-vmss-self-signed-certs/1-
keyvault.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Service fabric does not use active directory authentication
  Info:    Service fabric does not use active directory authentication.
           Alternative certificate based authentication introduced
management
           overhead. Certificates are harder to revoke and rotate than
active
           directory membership
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-473
  Path:    resource > azurerm_service_fabric_cluster[example] >
           azure_active_directory
  File:    examples/service-fabric/windows-vmss-self-signed-certs/3-
servicefabri
           c.tf
  Resolve: Set an `azure_active_directory` block with the following
attributes,
           `tenant_id`, `cluster_application_id`, `client_application_id`

  [Medium] Windows VM scale set encryption at host disabled
  Info:    Windows VM scale set encryption at host disabled. Storage
devices
           attached to the VM will not be encrypted at rest
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-478
  Path:    resource > azurerm_windows_virtual_machine_scale_set[example] >
           encryption_at_host_enabled
  File:    examples/service-fabric/windows-vmss-self-signed-certs/3-
servicefabri
           c.tf
  Resolve: Set `encryption_at_host_enabled` attribute to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage_adls_acls/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`
  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage_adls_acls/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage-account/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage-account/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example2] >
           account_replication_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example2] > min_tls_version
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage-share/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage-share/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/stream-analytics/basic-usage/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/stream-analytics/basic-usage/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/stream-analytics/msi-auth/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/stream-analytics/msi-auth/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/tfc-checks/app-service-app-usage/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/tfc-checks/app-service-app-usage/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[example]
  File:    examples/tfc-checks/app-service-certificate-expiry/main.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[azusa] >
account_replication_type
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Ensure that RDP access is restricted from the internet
  Info:    Ensure that RDP access is restricted from the internet. Using
RDP
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-676
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           destination_port_range
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Remove `3389`, `*`, or any port range that covers `3389` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Ensure that SSH access is restricted from the internet
  Info:    Ensure that SSH access is restricted from the internet. Using
SSH
           over internet leaves your Azure Virtual Machines vulnerable to
brute
```

```
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-677
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           destination_port_range
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Remove `22`, `*`, or any port range that covers `22` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[azusa] > min_tls_version
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           source_address_prefix
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] Azure Network Security Rule allows public access
  Info:    That inbound traffic is allowed to a resource from any source
instead
           of a restricted range. That potentially everyone can access your
           resource
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-35
  Path:    resource > azurerm_network_security_rule[ssh] >
source_address_prefix
  File:    examples/virtual-networks/network-security-group/main.tf
  Resolve: Set `access` to `Deny` or `source_address_prefix` to specific IP
           range only, e.g. `192.168.1.0/24`

High Severity Issues: 17

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_linux_virtual_machine[example] >
admin_password
  File:    examples/arckubernetes/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Linux virtual machine has password authentication enabled
  Info:    Linux virtual machine has password authentication enabled.
Password
           authentication is less resistant to brute force and educated
guess
           attacks then SSH public key authentication
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-79
  Path:    resource > azurerm_linux_virtual_machine[example] >
           disable_password_authentication
  File:    examples/arckubernetes/main.tf
  Resolve: Set `disable_password_authentication` attribute to `true` or
remove
           the attribute

  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example] >
container_access_type
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `container_access_type` attribute to `private`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Linux virtual machine has password authentication enabled
  Info:    Linux virtual machine has password authentication enabled.
Password
           authentication is less resistant to brute force and educated
guess
           attacks then SSH public key authentication
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-79
  Path:    resource > azurerm_virtual_machine[example] >
os_profile_linux_config
```

```
           > disable_password_authentication
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `disable_password_authentication` attribute to `true` or
remove
           the attribute

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[test] > os_profile >
           admin_password
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/mssql/mssqlvm/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Azure Search service public network access enabled
  Info:    Azure Search service public network access enabled. Public
access to
           Azure Search exposes the service to unnecessary risks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-642
  Path:    resource > azurerm_search_service[example] >
           public_network_access_enabled
  File:    examples/search/main.tf
  Resolve: Set `public_network_access_enabled ` to `false`

  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example2] >
           container_access_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `container_access_type` attribute to `private`
  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example] >
container_access_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `container_access_type` attribute to `private`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[vmserver] > os_profile >
           admin_password
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[vmjb] > os_profile >
           admin_password
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_linux_virtual_machine[example] >
admin_password
  File:    examples/virtual-networks/network-interface-app-security-group-
associ
           ation/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Linux virtual machine has password authentication enabled
  Info:    Linux virtual machine has password authentication enabled.
Password
           authentication is less resistant to brute force and educated
guess
           attacks then SSH public key authentication
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-79
  Path:    resource > azurerm_linux_virtual_machine[example] >
           disable_password_authentication
  File:    examples/virtual-networks/network-interface-app-security-group-
associ
           ation/main.tf
  Resolve: Set `disable_password_authentication` attribute to `true` or
remove
           the attribute

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✔ Files without issues: 204
✗ Files with issues: 87
  Ignored issues: 0
  Total issues: 262 [ 0 critical, 17 high, 102 medium, 143 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION v3.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v3.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✔ Test completed.

Issues

Low Severity Issues: 191

  [Low] API Management allows anonymous access to developer portal
  Info:    API Management allows anonymous access to developer portal.
Anonymous
           users can access your API documentation and specifications
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-504
  Path:    resource > azurerm_api_management[apim_service] > sign_in
  File:    examples/api-management/main.tf
  Resolve: Set a `sign_in.enabled` attribute set to `true`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[example] > purge_protection_enabled
  File:    examples/app-service-certificate/stored-in-keyvault/main.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/app-service-environment-v3/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[test] > auth_settings
  File:    examples/app-service/backup/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[test] > identity
  File:    examples/app-service/backup/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[test] > client_cert_enabled
  File:    examples/app-service/backup/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[test] > site_config >
http2_enabled
  File:    examples/app-service/backup/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[test] > network_rules
  File:    examples/app-service/backup/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
```

```
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[test] > site_config >
           dotnet_framework_version
  File:    examples/app-service/backup/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > securityContext > runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence
```

```
  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > containers[web] > resources > limits
>
           memory
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > containers[redis] > resources >
limits >
           memory
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > containers[redis] > livenessProbe
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > containers[web] > livenessProbe
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > containers[web] > imagePullPolicy
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > containers[redis] > imagePullPolicy
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > containers[web] > resources > limits
>
           cpu
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > containers[redis] > resources >
limits >
           cpu
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > securityContext >
readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[main] > network_rules
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[main] > network_rules
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `identity` attribute
  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`
  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[example] > auth_settings
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[example] > identity
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[example] > client_cert_enabled
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[example] > site_config >
http2_enabled
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service does not use production level SKU
  Info:    App Service does not use production level SKU. Missing advanced
auto
           scale and traffic management features can cause stability issues
for
           production workload
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-613
  Path:    resource > azurerm_app_service_plan[main] > sku > tier
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `sku.tier` to `Standard` or higher

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service does not use production level SKU
  Info:    App Service does not use production level SKU. Missing advanced
auto
           scale and traffic management features can cause stability issues
for
           production workload
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-613
  Path:    resource > azurerm_app_service_plan[main] > sku > tier
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `sku.tier` to `Standard` or higher

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[example] > auth_settings
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[example] > identity
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[example] > client_cert_enabled
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[example] > site_config >
http2_enabled
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service does not use production level SKU
  Info:    App Service does not use production level SKU. Missing advanced
auto
           scale and traffic management features can cause stability issues
for
           production workload
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-613
  Path:    resource > azurerm_app_service_plan[main] > sku > tier
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `sku.tier` to `Standard` or higher

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest Java version
  Info:    Azure App Service is not running latest available Java version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-248
  Path:    resource > azurerm_app_service[main] > site_config >
java_version
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `site_config.java_version` attribute to `11`

  [Low] Ensure Diagnostic Setting captures appropriate categories
  Info:    Ensure Diagnostic Setting captures appropriate categories. Not
           capturing the diagnostic setting categories for appropriate
           management activities leads to missing important alerts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-552
  Path:    resource > azurerm_monitor_diagnostic_setting[example] > log
  File:    examples/azure-monitoring/eventhub_integration/main.tf
  Resolve: Set log blocks for the categories
           `Administrative`,`Alert`,`Policy`,`Security` with `enabled` set
to
           `true` for each

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/batch/basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[example] >
           os_profile_windows_config > provision_vm_agent
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[stor] > network_rules
  File:    examples/cdn/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/container-instance/network-profile/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Geo replication for Azure Container Images disabled
  Info:    Geo replication for Azure Container Images disabled. Missing geo
           replication leads to reduced availability of container images
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-595
  Path:    resource > azurerm_container_registry[example] > georeplications
  File:    examples/container-registry/main.tf
  Resolve: Set a `georeplications` block within the resource, including a
valid
```

```
           `location` property

  [Low] CosmosDB account automatic failover disabled
  Info:    CosmosDB Account automatic failover disabled. Account will
experience
           loss of write availability for all the duration of the write
region
           outage
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-510
  Path:    resource > azurerm_cosmosdb_account[example] >
           enable_automatic_failover
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `enable_automatic_failover` attribute to `true`

  [Low] CosmosDB account automatic failover disabled
  Info:    CosmosDB Account automatic failover disabled. Account will
experience
           loss of write availability for all the duration of the write
region
           outage
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-510
  Path:    resource > azurerm_cosmosdb_account[example] >
           enable_automatic_failover
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `enable_automatic_failover` attribute to `true`

  [Low] Vault key expiration date not set
  Info:    Expiration date is not set for Azure Vault key. Key rotation
will not
           be enforced, which can lead to use of stale or compromised
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-173
  Path:    resource > azurerm_key_vault_key[example]
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `expiration_date` attribute to date in the future, with
format
           `YYYY-MM-DD'T'H:M:S'Z'`, e.g `2019-01-01T01:02:03Z`

  [Low] Data Factory not encrypted with customer managed key
  Info:    Data Factory is not using customer managed key to encrypt data.
Scope
           of use of the key cannot be controlled via access policies
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-514
  Path:    resource > azurerm_data_factory[target] >
customer_managed_key_id
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `customer_managed_key_id` attribute

  [Low] Data Factory not encrypted with customer managed key
  Info:    Data Factory is not using customer managed key to encrypt data.
Scope
           of use of the key cannot be controlled via access policies
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-514
  Path:    resource > azurerm_data_factory[host] > customer_managed_key_id
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `customer_managed_key_id` attribute

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
```

```
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[test] > ddos_protection_plan
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/eventgrid/event-subscription/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
```

```
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext > runAsUser
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > resources > limits > memory
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > template > spec > containers[aci-helloworld]
>
           livenessProbe
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > template > spec > containers[aci-helloworld]
>
           imagePullPolicy
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > resources > limits > cpu
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext >
readOnlyRootFilesystem
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/monitoring-log-analytics/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/monitoring-log-analytics/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/private-api-server/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/private-api-server/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Kubernetes Dashboard enabled
  Info:    AKS Kubernetes Dashboard enabled. Increases attack vectors of
           kubernetes cluster
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-177
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           kube_dashboard
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `addon_profile.kube_dashboard` attribute to `false`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[test] > purge_protection_enabled
  File:    examples/managed-disks/encrypted/1-dependencies.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`
  [Low] Vault key expiration date not set
  Info:    Expiration date is not set for Azure Vault key. Key rotation
will not
           be enforced, which can lead to use of stale or compromised
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-173
  Path:    resource > azurerm_key_vault_key[test]
  File:    examples/managed-disks/encrypted/main.tf
  Resolve: Set `expiration_date` attribute to date in the future, with
format
           `YYYY-MM-DD'T'H:M:S'Z'`, e.g `2019-01-01T01:02:03Z`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/basic-with-assets/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example2] > network_rules
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/mssql/mssqlvm/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/nfsv3_volume_with_snapshot_policy/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/snapshot/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example_primary] >
           ddos_protection_plan
  File:    examples/netapp/volume_crr/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example_secondary] >
           ddos_protection_plan
  File:    examples/netapp/volume_crr/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/volume_from_snapshot/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/volume/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[main] > ddos_protection_plan
  File:    examples/orchestrated-vm-scale-set/automatic-vm-guest-
patching/main.t
           f
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[main] > ddos_protection_plan
  File:    examples/orchestrated-vm-scale-set/hotpatching-enabled/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/application-gateway/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] CosmosDB account automatic failover disabled
  Info:    CosmosDB Account automatic failover disabled. Account will
experience
           loss of write availability for all the duration of the write
region
           outage
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-510
  Path:    resource > azurerm_cosmosdb_account[example] >
           enable_automatic_failover
  File:    examples/private-endpoint/cosmos-db/main.tf
  Resolve: Set `enable_automatic_failover` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/cosmos-db/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/postgresql/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/private-dns-group/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private-endpoint/private-link-service/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/basic/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
```

```
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/premium-with-clustering/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/standard/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Azure Search Service is not using system-assigned identities
  Info:    Azure Search Service is not using system-assigned identities.
The
           risk of improperly configured authentication as well as missing
           credentials rotation increases if not using managed identities
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-641
  Path:    resource > azurerm_search_service[example] > identity > type
  File:    examples/search/main.tf
  Resolve: Set `identity.type` to `SystemAssigned`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/service-fabric/windows-vmss-self-signed-certs/0-base.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/service-fabric/windows-vmss-self-signed-certs/0-base.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
```

```
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[example] > purge_protection_enabled
  File:    examples/service-fabric/windows-vmss-self-signed-certs/1-
keyvault.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_sql_server[example]
  File:    examples/sql-azure/database/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[secondary]
  File:    examples/sql-azure/failover_group/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[example]
  File:    examples/sql-azure/failover_group/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Ensure Diagnostic Setting captures appropriate categories
  Info:    Ensure Diagnostic Setting captures appropriate categories. Not
           capturing the diagnostic setting categories for appropriate
           management activities leads to missing important alerts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-552
  Path:    resource > azurerm_monitor_diagnostic_setting[example] > log
  File:    examples/sql-azure/sql_auditing_eventhub/main.tf
  Resolve: Set log blocks for the categories
           `Administrative`,`Alert`,`Policy`,`Security` with `enabled` set
to
           `true` for each

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[example]
  File:    examples/sql-azure/sql_auditing_eventhub/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Ensure Diagnostic Setting captures appropriate categories
  Info:    Ensure Diagnostic Setting captures appropriate categories. Not
           capturing the diagnostic setting categories for appropriate
           management activities leads to missing important alerts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-552
  Path:    resource > azurerm_monitor_diagnostic_setting[example] > log
  File:    examples/sql-azure/sql_auditing_log_analytics/main.tf
  Resolve: Set log blocks for the categories
           `Administrative`,`Alert`,`Policy`,`Security` with `enabled` set
to
           `true` for each

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_mssql_server[example]
  File:    examples/sql-azure/sql_auditing_log_analytics/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage_adls_acls/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage-account/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
```

```
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example2] > network_rules
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/storage/storage-share/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/stream-analytics/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/basic/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/virtual-machine/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/vm-scale-set/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[azuvnet] >
ddos_protection_plan
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[vmjb] >
os_profile_windows_config
           > provision_vm_agent
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[vmserver] >
           os_profile_windows_config > provision_vm_agent
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[azusa] > network_rules
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
```

```
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/basic/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/multiple-subnets/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/network-interface-app-security-group-
associ
           ation/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/network-security-group/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[test] > ddos_protection_plan
  File:    examples/virtual-networks/private-link-service/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
```

```
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[second] >
ddos_protection_plan
  File:    examples/virtual-networks/virtual-network-peering/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[first] > ddos_protection_plan
  File:    examples/virtual-networks/virtual-network-peering/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

Medium Severity Issues: 129

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[example]
  File:    examples/app-service-certificate/stored-in-keyvault/main.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[test] > sku > capacity
  File:    examples/app-service/backup/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[test] >
account_replication_type
  File:    examples/app-service/backup/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[test] > https_only
  File:    examples/app-service/backup/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[test] > min_tls_version
  File:    examples/app-service/backup/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > securityContext > runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           capabilities > drop
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           capabilities > drop
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > securityContext >
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium]  Function App does not enforce HTTPS
  Info:    Function App does not enforce use of HTTPS connections, users
can
           access via HTTP. The connection and transmitted data could be
           intercepted and manipulated
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-500
  Path:    resource > azurerm_function_app[main] > https_only
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Function App built-in authentication disabled
  Info:    Function App built-in authentication disabled. Users will not be
able
           to use Azure Active Directory for authentication in their
Function
           App
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-501
  Path:    resource > azurerm_function_app[main] > auth_settings > enabled
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[main] >
account_replication_type
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[main] > min_tls_version
  File:    examples/app-service/function-azure-RBAC-role-assignment/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium]  Function App does not enforce HTTPS
  Info:    Function App does not enforce use of HTTPS connections, users
can
           access via HTTP. The connection and transmitted data could be
           intercepted and manipulated
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-500
  Path:    resource > azurerm_function_app[main] > https_only
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Function App built-in authentication disabled
  Info:    Function App built-in authentication disabled. Users will not be
able
           to use Azure Active Directory for authentication in their
Function
           App
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-501
  Path:    resource > azurerm_function_app[main] > auth_settings > enabled
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more
  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[main] >
account_replication_type
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[main] > min_tls_version
  File:    examples/app-service/function-basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium]  Function App does not enforce HTTPS
  Info:    Function App does not enforce use of HTTPS connections, users
can
           access via HTTP. The connection and transmitted data could be
           intercepted and manipulated
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-500
  Path:    resource > azurerm_function_app[example] > https_only
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Function App built-in authentication disabled
  Info:    Function App built-in authentication disabled. Users will not be
able
           to use Azure Active Directory for authentication in their
Function
           App
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-501
  Path:    resource > azurerm_function_app[example] > auth_settings >
enabled
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[example] > sku > capacity
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`
  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/app-service/function-python/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[example] > sku > capacity
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[example] > https_only
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[example] > sku > capacity
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[example] > https_only
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
```

```
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/batch/basic/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/batch/basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] CDN Endpoint https not enforced
  Info:    CDN Endpoint https not enforced. The content could be
intercepted and
           manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-509
  Path:    resource > azurerm_cdn_endpoint[example] > is_http_allowed
  File:    examples/cdn/main.tf
  Resolve: Set `is_http_allowed` to `false`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[stor] >
account_replication_type
  File:    examples/cdn/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[stor] > min_tls_version
  File:    examples/cdn/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`
  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/customer-managed-key/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/failover/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/failover/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] Data Factory public access enabled
  Info:    The Azure Data Factory REST APIs are accessible from the
Internet.
           The REST APIs are subject to attacks from the public internet,
such
           as zero-day vulnerabilities and unauthorized access via lost
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-513
  Path:    resource > azurerm_data_factory[host] > public_network_enabled
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `public_network_enabled` to `false`

  [Medium] Data Factory public access enabled
  Info:    The Azure Data Factory REST APIs are accessible from the
Internet.
           The REST APIs are subject to attacks from the public internet,
such
           as zero-day vulnerabilities and unauthorized access via lost
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-513
  Path:    resource > azurerm_data_factory[target] > public_network_enabled
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `public_network_enabled` to `false`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/eventgrid/event-subscription/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/eventgrid/event-subscription/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[example] >
security_rule[0]
           > source_address_prefix
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[example] >
security_rule[3]
           > source_address_prefix
  File:    examples/hdinsight/enterprise-security-package/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/aci_connector_linux/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext > runAsNonRoot
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext > capabilities >
drop
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > template > spec >
           containers[aci-helloworld] > securityContext >
           allowPrivilegeEscalation
  File:    examples/kubernetes/aci_connector_linux/virtual-node.yaml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/basic-cluster/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/egress-with-udr-azure-cni/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/egress-with-udr-kubenet/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/monitoring-log-analytics/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/network-policy-calico/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/nodes-on-internal-network/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/private-api-server/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/public-ip/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/spot-node-pool/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[test]
  File:    examples/managed-disks/encrypted/1-dependencies.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/basic-with-assets/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`
  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example2] > min_tls_version
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] WAF not enabled on application gateway
  Info:    WAF not enabled on application gateway. Application will not be
           protected using a Web Application Firewall
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-474
  Path:    resource > azurerm_application_gateway[example] >
waf_configuration
  File:    examples/private-endpoint/application-gateway/main.tf
  Resolve: Set `enabled` attribute to `true` within the `waf_configuration`
           block

  [Medium] App Gateway does not use OWASP 3.x rules
  Info:    App Gateway does not use OWASP 3.x rules. Out-of-date OWASP
rules
           might not protect as effectively as more recent rule sets
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-610
  Path:    resource > azurerm_application_gateway[example] >
waf_configuration
  File:    examples/private-endpoint/application-gateway/main.tf
  Resolve: Set `waf_configuration.rule_set_type` to `OWASP` and
           `waf_configuration.rule_set_version` to `3.1`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/private-endpoint/cosmos-db/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/private-endpoint/cosmos-db/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`
  [Medium] PostgreSQL server minimum TLS version 1.2
  Info:    PostgreSQL server minimum TLS version 1.2. An outdated TLS
version
           might lead to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-629
  Path:    resource > azurerm_postgresql_server[example]
  File:    examples/private-endpoint/postgresql/main.tf
  Resolve: Set `ssl_minimal_tls_version_enforced` to `TLS1_2`

  [Medium] PostgreSQL server minimum TLS version 1.2
  Info:    PostgreSQL server minimum TLS version 1.2. An outdated TLS
version
           might lead to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-629
  Path:    resource > azurerm_postgresql_server[example]
  File:    examples/private-endpoint/private-dns-group/main.tf
  Resolve: Set `ssl_minimal_tls_version_enforced` to `TLS1_2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/basic/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/premium-with-clustering/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/service-fabric/windows-vmss-self-signed-certs/0-base.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[example]
  File:    examples/service-fabric/windows-vmss-self-signed-certs/1-
keyvault.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Service fabric does not use active directory authentication
  Info:    Service fabric does not use active directory authentication.
           Alternative certificate based authentication introduced
management
           overhead. Certificates are harder to revoke and rotate than
active
           directory membership
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-473
  Path:    resource > azurerm_service_fabric_cluster[example] >
           azure_active_directory
  File:    examples/service-fabric/windows-vmss-self-signed-certs/3-
servicefabri
           c.tf
  Resolve: Set an `azure_active_directory` block with the following
attributes,
           `tenant_id`, `cluster_application_id`, `client_application_id`

  [Medium] Windows VM scale set encryption at host disabled
  Info:    Windows VM scale set encryption at host disabled. Storage
devices
           attached to the VM will not be encrypted at rest
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-478
  Path:    resource > azurerm_windows_virtual_machine_scale_set[example] >
           encryption_at_host_enabled
  File:    examples/service-fabric/windows-vmss-self-signed-certs/3-
servicefabri
           c.tf
  Resolve: Set `encryption_at_host_enabled` attribute to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage_adls_acls/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage_adls_acls/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage-account/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage-account/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example2] >
           account_replication_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example2] > min_tls_version
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/storage/storage-share/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/storage/storage-share/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/stream-analytics/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/stream-analytics/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[azusa] >
account_replication_type
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Ensure that RDP access is restricted from the internet
  Info:    Ensure that RDP access is restricted from the internet. Using
RDP
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-676
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           destination_port_range
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Remove `3389`, `*`, or any port range that covers `3389` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Ensure that SSH access is restricted from the internet
  Info:    Ensure that SSH access is restricted from the internet. Using
SSH
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-677
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           destination_port_range
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Remove `22`, `*`, or any port range that covers `22` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[azusa] > min_tls_version
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           source_address_prefix
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] Azure Network Security Rule allows public access
  Info:    That inbound traffic is allowed to a resource from any source
instead
           of a restricted range. That potentially everyone can access your
           resource
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-35
  Path:    resource > azurerm_network_security_rule[ssh] >
source_address_prefix
  File:    examples/virtual-networks/network-security-group/main.tf
  Resolve: Set `access` to `Deny` or `source_address_prefix` to specific IP
           range only, e.g. `192.168.1.0/24`

High Severity Issues: 28

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[test] > site_config > ftps_state
  File:    examples/app-service/backup/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`
  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[example] > site_config >
ftps_state
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[example] > site_config >
ftps_state
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example] >
container_access_type
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `container_access_type` attribute to `private`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
```

```
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Linux virtual machine has password authentication enabled
  Info:    Linux virtual machine has password authentication enabled.
Password
           authentication is less resistant to brute force and educated
guess
           attacks then SSH public key authentication
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-79
  Path:    resource > azurerm_virtual_machine[example] >
os_profile_linux_config
           > disable_password_authentication
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `disable_password_authentication` attribute to `true` or
remove
           the attribute

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[test] > os_profile >
           admin_password
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/data-factory/shared-self-hosted/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/mssql/mssqlvm/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Azure Search service public network access enabled
  Info:    Azure Search service public network access enabled. Public
access to
           Azure Search exposes the service to unnecessary risks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-642
  Path:    resource > azurerm_search_service[example] >
           public_network_access_enabled
  File:    examples/search/main.tf
  Resolve: Set `public_network_access_enabled ` to `false`

  [High] Public access level for storage containers & blobs is enabled
  Info:    Public access level for storage containers & blobs is enabled.
Client
           has unauthorized read access to storage container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-535
  Path:    resource > azurerm_storage_account[example2] >
           allow_blob_public_access
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `allow_blob_public_access` to `false`

  [High] Public access level for storage containers & blobs is enabled
  Info:    Public access level for storage containers & blobs is enabled.
Client
           has unauthorized read access to storage container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-535
  Path:    resource > azurerm_storage_account[example] >
           allow_blob_public_access
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `allow_blob_public_access` to `false`

  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example2] >
           container_access_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `container_access_type` attribute to `private`

  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example] >
container_access_type
  File:    examples/storage/storage-container/main.tf
  Resolve: Set `container_access_type` attribute to `private`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[vmserver] > os_profile >
           admin_password
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication
  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[vmjb] > os_profile >
           admin_password
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_linux_virtual_machine[example] >
admin_password
  File:    examples/virtual-networks/network-interface-app-security-group-
associ
           ation/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Linux virtual machine has password authentication enabled
  Info:    Linux virtual machine has password authentication enabled.
Password
           authentication is less resistant to brute force and educated
guess
           attacks then SSH public key authentication
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-79
  Path:    resource > azurerm_linux_virtual_machine[example] >
           disable_password_authentication
  File:    examples/virtual-networks/network-interface-app-security-group-
associ
           ation/main.tf
  Resolve: Set `disable_password_authentication` attribute to `true` or
remove
           the attribute

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✓ Files without issues: 181
✗ Files with issues: 89
  Ignored issues: 0
  Total issues: 348 [ 0 critical, 28 high, 129 medium, 191 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
```

```
something failed
[Pipeline] echo
=============== https://github.com/hashicorp/terraform-provider-azurerm.git
VERSION v2.0.0 ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/terrafor
m-provider-azurerm/v2.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
✓ Test completed.

Issues

Low Severity Issues: 125

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[example] > purge_protection_enabled
  File:    examples/app-service-certificate/stored-in-keyvault/main.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[test] > auth_settings
  File:    examples/app-service/backup/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[test] > identity
  File:    examples/app-service/backup/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[test] > client_cert_enabled
  File:    examples/app-service/backup/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[test] > site_config >
http2_enabled
  File:    examples/app-service/backup/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`
  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[test] > network_rules
  File:    examples/app-service/backup/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[test] > site_config >
           dotnet_framework_version
  File:    examples/app-service/backup/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
```

```
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > securityContext > runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container's or Pod's  UID could clash with host's UID
  Info:    `runAsUser` value is set to low UID. UID of the container
processes
           could clash with host's UIDs and lead to unintentional
authorization
           bypass
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-11
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           runAsUser
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsUser` value to greater or equal than
           10'000. SecurityContext can be set on both `pod` and `container`
           level. If both are set, then the container level takes
precedence

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > containers[web] > resources > limits
>
           memory
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without memory limit
  Info:    Memory limit is not defined. Containers without memory limits
are
           more likely to be terminated when the node runs out of memory
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-4
  Path:    [DocId: 0] > input > spec > containers[redis] > resources >
limits >
           memory
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `resources.limits.memory` value

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > containers[redis] > livenessProbe
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container is running without liveness probe
  Info:    Liveness probe is not defined. Kubernetes will not be able to
detect
           if application is able to service requests, and will not restart
           unhealthy pods
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-41
  Path:    [DocId: 0] > spec > containers[web] > livenessProbe
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `livenessProbe` attribute

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > containers[web] > imagePullPolicy
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container could be running with outdated image
  Info:    The image policy does not prevent image reuse. The container may
run
           with outdated or unauthorized image
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-42
  Path:    [DocId: 0] > spec > containers[redis] > imagePullPolicy
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `imagePullPolicy` attribute to `Always`

  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > containers[web] > resources > limits
>
           cpu
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value
  [Low] Container has no CPU limit
  Info:    Container has no CPU limit. CPU limits can prevent containers
from
           consuming valuable compute time for no benefit (e.g. inefficient
           code) that might lead to unnecessary costs. It is advisable to
also
           configure CPU requests to ensure application stability.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-5
  Path:    [DocId: 0] > input > spec > containers[redis] > resources >
limits >
           cpu
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `resources.limits.cpu` field with required CPU limit value

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > securityContext >
readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] Container or Pod is running with writable root filesystem
  Info:    `readOnlyRootFilesystem` attribute is not set to `true`.
Compromised
           process could abuse writable root filesystem to elevate
privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-8
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           readOnlyRootFilesystem
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.readOnlyRootFilesystem` to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[example] > auth_settings
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[example] > identity
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[example] > client_cert_enabled
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[example] > site_config >
http2_enabled
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service does not use production level SKU
  Info:    App Service does not use production level SKU. Missing advanced
auto
           scale and traffic management features can cause stability issues
for
           production workload
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-613
  Path:    resource > azurerm_app_service_plan[main] > sku > tier
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `sku.tier` to `Standard` or higher

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service does not use production level SKU
  Info:    App Service does not use production level SKU. Missing advanced
auto
           scale and traffic management features can cause stability issues
for
           production workload
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-613
  Path:    resource > azurerm_app_service_plan[main] > sku > tier
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `sku.tier` to `Standard` or higher

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest .Net version
  Info:    Azure App Service is not running latest available .Net version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-245
  Path:    resource > azurerm_app_service[main] > site_config >
           dotnet_framework_version
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `site_config.dotnet_framework_version` attribute to `v5.0`

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[example] > auth_settings
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[example] > identity
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[example] > client_cert_enabled
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[example] > site_config >
http2_enabled
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service does not use production level SKU
  Info:    App Service does not use production level SKU. Missing advanced
auto
           scale and traffic management features can cause stability issues
for
           production workload
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-613
  Path:    resource > azurerm_app_service_plan[main] > sku > tier
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `sku.tier` to `Standard` or higher

  [Low] App Service authentication disabled
  Info:    Azure App Service authentication is not enabled. Service may be
           accessible without authorization
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-160
  Path:    resource > azurerm_app_service[main] > auth_settings
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `auth_settings.enabled` attribute to `true`

  [Low] App Service identity missing
  Info:    App Service identity missing. Authentication and authorization
will
           not be possible via Microsoft Identity platform
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-161
  Path:    resource > azurerm_app_service[main] > identity
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `identity` attribute

  [Low] App Service mutual TLS disabled
  Info:    App Service mutual TLS disabled. Clients without authorized
           certificate may be allowed to connect to the application
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-162
  Path:    resource > azurerm_app_service[main] > client_cert_enabled
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `client_cert_enabled` attribute to `true`

  [Low] App Service HTTP/2 disabled
  Info:    HTTP/2 is not enabled on the App Service. No security impact.
           Provides performance improvement.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-163
  Path:    resource > azurerm_app_service[main] > site_config >
http2_enabled
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `site_config.http2_enabled` attribute to `true`

  [Low] App Service not running latest Java version
  Info:    Azure App Service is not running latest available Java version.
           Application cannot benefit from latest security improvements to
           runtime engine
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-248
  Path:    resource > azurerm_app_service[main] > site_config >
java_version
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `site_config.java_version` attribute to `11`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
```

```
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/batch/basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[example] >
           os_profile_windows_config > provision_vm_agent
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`
  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[stor] > network_rules
  File:    examples/cdn/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Geo replication for Azure Container Images disabled
  Info:    Geo replication for Azure Container Images disabled. Missing geo
           replication leads to reduced availability of container images
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-595
  Path:    resource > azurerm_container_registry[example] > georeplications
  File:    examples/container-registry/main.tf
  Resolve: Set a `georeplications` block within the resource, including a
valid
           `location` property

  [Low] CosmosDB account automatic failover disabled
  Info:    CosmosDB Account automatic failover disabled. Account will
experience
           loss of write availability for all the duration of the write
region
           outage
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-510
  Path:    resource > azurerm_cosmosdb_account[example] >
           enable_automatic_failover
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `enable_automatic_failover` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[test] > ddos_protection_plan
  File:    examples/kubernetes/advanced-networking-calico-policy/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[test] > addon_profile >
           oms_agent
  File:    examples/kubernetes/advanced-networking-calico-policy/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/advanced-networking-multiple-
agentpool/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/advanced-networking-multiple-
agentpool/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/advanced-networking-multiple-
agentpool/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`
  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/kubernetes/advanced-networking/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/advanced-networking/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/advanced-networking/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/basic/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/basic/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/monitoring/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/role-based-access-control-azuread/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/role-based-access-control-azuread/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] AKS Network Policies disabled
  Info:    Azure Kubernetes Service cluster has network policies disabled.
           Cannot utilize network policies feature to provide network
           segmentation between services
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-176
  Path:    resource > azurerm_kubernetes_cluster[example] > network_profile
>
           network_policy
  File:    examples/kubernetes/role-based-access-control/main.tf
  Resolve: Set `network_profile.network_policy` attribute to `azure` or
`calico`

  [Low] Container Insights is disabled for AKS
  Info:    Container Insights is disabled for AKS. No insight into an AKS
           cluster might prevent incident response based on crucial log or
           hardware utilization information
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-82
  Path:    resource > azurerm_kubernetes_cluster[example] > addon_profile >
           oms_agent
  File:    examples/kubernetes/role-based-access-control/main.tf
  Resolve: Set `addon_profile.oms_agent.enabled` attribute to `true`

  [Low] Key Vault accidental purge prevention disabled
  Info:    Key Vault accidental purge prevention disabled. Accidentally
purged
           key material will not recoverable
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-175
  Path:    resource > azurerm_key_vault[test] > purge_protection_enabled
  File:    examples/managed-disks/encrypted/1-dependencies.tf
  Resolve: Set `purge_protection_enabled` attribute to `true`

  [Low] Vault key expiration date not set
  Info:    Expiration date is not set for Azure Vault key. Key rotation
will not
           be enforced, which can lead to use of stale or compromised
           credentials
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-173
  Path:    resource > azurerm_key_vault_key[test]
  File:    examples/managed-disks/encrypted/main.tf
  Resolve: Set `expiration_date` attribute to date in the future, with
format
           `YYYY-MM-DD'T'H:M:S'Z'`, e.g `2019-01-01T01:02:03Z`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/basic/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
```

```
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example2] > network_rules
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/snapshot/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/netapp/volume/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/private_endpoint/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/basic/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/premium-with-clustering/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Redis Cache backup disabled
  Info:    Redis Cache backup disabled. In the event of hardware failure or
           other disasters, data may be lost. Note this is only available
to
           Premium Service Tier Caches (SKUs)
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-518
  Path:    resource > azurerm_redis_cache[example] > redis_configuration
  File:    examples/redis-cache/standard/main.tf
  Resolve: Set `rdb_backup_enabled` to `true`

  [Low] Azure Search Service is not using system-assigned identities
  Info:    Azure Search Service is not using system-assigned identities.
The
           risk of improperly configured authentication as well as missing
           credentials rotation increases if not using managed identities
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-641
  Path:    resource > azurerm_search_service[example] > identity > type
  File:    examples/search/main.tf
  Resolve: Set `identity.type` to `SystemAssigned`

  [Low] Azure SQL server extended auditing is disabled
  Info:    Azure SQL server extended auditing is disabled. Audit records
may not
           be available during investigation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-167
  Path:    resource > azurerm_sql_server[example]
  File:    examples/sql-azure/database/main.tf
  Resolve: Set `extended_auditing_policy` attribute

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[example] > network_rules
  File:    examples/stream-analytics/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/basic/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/virtual-machine/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Traffic Manager insecure probing protocol
  Info:    Traffic Manager insecure probing protocol. HTTPS-based
monitoring
           improves security and increases accuracy of health probes
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-650
  Path:    resource > azurerm_traffic_manager_profile[example] >
monitor_config
           > protocol
  File:    examples/traffic-manager/vm-scale-set/main.tf
  Resolve: Set `properties.monitorConfig.protocol` to `HTTPS`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[azuvnet] >
ddos_protection_plan
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[vmjb] >
os_profile_windows_config
           > provision_vm_agent
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] VM Agent is not provisioned automatically for Windows
  Info:    VM Agent is not provisioned automatically for Windows. VM Agent
           reduces management overhead by enabling straightforward
bootstrapping
           of monitoring and configuration of guest OS
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-667
  Path:    resource > azurerm_virtual_machine[vmserver] >
           os_profile_windows_config > provision_vm_agent
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `os_profile_windows_config.provision_vm_agent` to `true`

  [Low] Trusted Microsoft Service access to storage account is disabled
  Info:    Network access bypass for Trusted Microsoft Services is not
enabled
           on the storage account. Trusted network services cannot be
           whitelisted via network rules. When any network rule is
configured,
           the trusted services will not be able to access the storage
account.
           Note, by default there is no network rule configured.
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-172
  Path:    resource > azurerm_storage_account[azusa] > network_rules
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `network_rules.bypass` attribute to `['Azure Services'].
Ensure
           to add appropriate rules for your application alongside the
proposed
           remediation step. Setting this remediation without any other
rules
           will block all network access to the storage account except for
           Microsoft Trusted Services.`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/basic/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`
  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/multiple-subnets/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[example] >
ddos_protection_plan
  File:    examples/virtual-networks/network-security-group/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[test] > ddos_protection_plan
  File:    examples/virtual-networks/private-link-service/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[second] >
ddos_protection_plan
  File:    examples/virtual-networks/virtual-network-peering/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

  [Low] Virtual Network DDoS protection plan disabled
  Info:    Virtual Network DDoS protection plan disabled. Services deployed
in
           the network will not benefit from advanced DDoS protection
features
           such as attack alerting and analytics
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-516
  Path:    resource > azurerm_virtual_network[first] > ddos_protection_plan
  File:    examples/virtual-networks/virtual-network-peering/main.tf
  Resolve: Set `ddos_protection_plan.enable` attribute to `true`

Medium Severity Issues: 77

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[example]
  File:    examples/app-service-certificate/stored-in-keyvault/main.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[test] > sku > capacity
  File:    examples/app-service/backup/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[test] >
account_replication_type
  File:    examples/app-service/backup/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[test] > https_only
  File:    examples/app-service/backup/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[test] > min_tls_version
  File:    examples/app-service/backup/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `https_only` attribute to `true`
  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > securityContext > runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container or Pod is running without root user control
  Info:    Container or Pod is running without root user control. Container
or
           Pod could be running with full administrative privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-10
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           runAsNonRoot
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.runAsNonRoot` to `true`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           capabilities > drop
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container does not drop all default capabilities
  Info:    All default capabilities are not explicitly dropped. Containers
are
           running with potentially unnecessary privileges
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-6
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
           capabilities > drop
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Add `ALL` to `securityContext.capabilities.drop` list, and add
only
           required capabilities in `securityContext.capabilities.add`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > securityContext >
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > containers[redis] > securityContext
>
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Container or Pod is running without privilege escalation control
  Info:    `allowPrivilegeEscalation` attribute is not set to `false`.
Processes
           could elevate current privileges via known vectors, for example
SUID
           binaries
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-K8S-9
  Path:    [DocId: 0] > input > spec > containers[web] > securityContext >
```

```
           allowPrivilegeEscalation
  File:    examples/app-service/docker-kubernetes/kubernetes.yml
  Resolve: Set `securityContext.allowPrivilegeEscalation` to `false`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[example] > sku > capacity
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[example] > https_only
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
```

```
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] App Service remote debugging enabled
  Info:    App Service remote debugging enabled. Leaving remote debugging
           enabled might increase exposure to unnecessary risk
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-619
  Path:    resource > azurerm_app_service[main] > site_config >
           remote_debugging_enabled
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `site_config.remote_debugging_enabled` to `false`, or remove
the
           `remote_debugging_enabled` property

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[example] > sku > capacity
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[example] > https_only
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `https_only` attribute to `true`
  [Medium] Use two or more App Service Plan instances
  Info:    Use two or more App Service Plan instances. A single App Service
Plan
           instance increases the risk of application unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-618
  Path:    resource > azurerm_app_service_plan[main] > sku > capacity
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `sku.capacity` to `2` or more

  [Medium] Azure App Service allows HTTP traffic
  Info:    Azure App Service allows HTTP traffic. The HTTP content could be
           intercepted and manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-144
  Path:    resource > azurerm_app_service[main] > https_only
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `https_only` attribute to `true`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/batch/basic/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/batch/basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] CDN Endpoint https not enforced
  Info:    CDN Endpoint https not enforced. The content could be
intercepted and
           manipulated in transit
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-509
  Path:    resource > azurerm_cdn_endpoint[example] > is_http_allowed
  File:    examples/cdn/main.tf
  Resolve: Set `is_http_allowed` to `false`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[stor] >
account_replication_type
  File:    examples/cdn/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[stor] > min_tls_version
  File:    examples/cdn/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/container-instance/volume-mount/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/basic/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] CosmosDB account public network access enabled
  Info:    CosmosDB account public network access enabled. Databases under
the
           account may be accessible by anyone on the Internet
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-511
  Path:    resource > azurerm_cosmosdb_account[example] >
           public_network_access_enabled
  File:    examples/cosmos-db/failover/main.tf
  Resolve: Set `public_network_access_enabled` attribute to `false`

  [Medium] Restrict user access to data operations in Azure Cosmos DB
  Info:    Restrict user access to data operations in Azure Cosmos DB.
Account
           key-based write access to account data exposes sensitive
           configuration options to non-administrative accounts
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-621
  Path:    resource > azurerm_cosmosdb_account[example] >
           access_key_metadata_writes_enabled
  File:    examples/cosmos-db/failover/main.tf
  Resolve: Set `access_key_metadata_writes_enabled` to `false`

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[test] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/advanced-networking-calico-policy/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/advanced-networking-multiple-
agentpool/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/advanced-networking/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/basic/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/monitoring/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/role-based-access-control-azuread/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] API Server allows public access
  Info:    The Kubernetes API server could be accessible by anyone.
Increases
           attack vector reachability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-81
  Path:    resource > azurerm_kubernetes_cluster[example] >
           api_server_authorized_ip_ranges
  File:    examples/kubernetes/role-based-access-control/main.tf
  Resolve: Set `api_server_authorized_ip_ranges` attribute to specific
range
           e.g. 10.0.0.0/16

  [Medium] Key Vault purge protection is disabled
  Info:    Key Vault purge protection is disabled. Accidentally purged
vaults
           and vault items are not recoverable and might lead to data loss
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-624
  Path:    resource > azurerm_key_vault[test]
  File:    examples/managed-disks/encrypted/1-dependencies.tf
  Resolve: Set `purge_protection_enabled` to `true`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/basic/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example2] > min_tls_version
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/media-services/multiple-storage-accounts/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/basic/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/redis-cache/premium-with-backup/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Redis Cache minimum TLS version
  Info:    Redis Cache minimum TLS version. An outdated TLS version might
lead
           to data leakage or manipulation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-633
  Path:    resource > azurerm_redis_cache[example]
  File:    examples/redis-cache/premium-with-clustering/main.tf
  Resolve: Set `minimum_tls_version` to `1.2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
```

```
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[example] >
           account_replication_type
  File:    examples/stream-analytics/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[example] > min_tls_version
  File:    examples/stream-analytics/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Storage Account geo-replication disabled
  Info:    Storage Account geo-replication disabled. Data might be exposed
to
           the risk of loss or unavailability
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-649
  Path:    resource > azurerm_storage_account[azusa] >
account_replication_type
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `sku.name` to either `GRS`,`RAGRS`,`GZRS` or `RAGZRS`

  [Medium] Ensure that RDP access is restricted from the internet
  Info:    Ensure that RDP access is restricted from the internet. Using
RDP
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-676
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           destination_port_range
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Remove `3389`, `*`, or any port range that covers `3389` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Ensure that SSH access is restricted from the internet
  Info:    Ensure that SSH access is restricted from the internet. Using
SSH
           over internet leaves your Azure Virtual Machines vulnerable to
brute
           force attacks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-677
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           destination_port_range
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Remove `22`, `*`, or any port range that covers `22` from
           `security_rule.destination_port_range` when
'security_rule.access' is
           set to `allow`

  [Medium] Storage Account does not enforce latest TLS
  Info:    Azure Storage Account does not enforce latest TLS version. Older
           cipher suites could be vulnerable to hijacking and information
           disclosure
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-149
  Path:    resource > azurerm_storage_account[azusa] > min_tls_version
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `min_tls_version` attribute to `TLS1_2`

  [Medium] Azure Network Security Group allows public access
  Info:    Azure Network Security Group allows public access. Public access
to
           all resources behind the network security group
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-33
  Path:    resource > azurerm_network_security_group[azunsgjb] >
security_rule >
           source_address_prefix
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `source_address_prefix` attribute to specific IP range only,
e.g.
           `192.168.1.0/24`

  [Medium] Azure Network Security Rule allows public access
  Info:    That inbound traffic is allowed to a resource from any source
instead
           of a restricted range. That potentially everyone can access your
           resource
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-35
  Path:    resource > azurerm_network_security_rule[ssh] >
source_address_prefix
  File:    examples/virtual-networks/network-security-group/main.tf
  Resolve: Set `access` to `Deny` or `source_address_prefix` to specific IP
           range only, e.g. `192.168.1.0/24`

High Severity Issues: 19

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[test] > site_config > ftps_state
  File:    examples/app-service/backup/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-authentication/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-basic/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-compose/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/docker-kubernetes/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/linux-authentication/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/linux-basic/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/linux-nodejs/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[example] > site_config >
ftps_state
  File:    examples/app-service/linux-php/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/windows-authentication/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/windows-basic/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[example] > site_config >
ftps_state
  File:    examples/app-service/windows-container/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] App Service allows FTP deployments
  Info:    App Service allows FTP deployments. FTP is a plain-text protocol
that
           is vulnerable to manipulation and eavesdropping
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-533
  Path:    resource > azurerm_app_service[main] > site_config > ftps_state
  File:    examples/app-service/windows-java/main.tf
  Resolve: Set `ftps_state` to `FtpsOnly` or `Disabled`

  [High] Storage container allows public access
  Info:    Azure Storage Container allows public access. Potentially anyone
can
           access data stored in container or blob
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-181
  Path:    resource > azurerm_storage_container[example] >
container_access_type
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `container_access_type` attribute to `private`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[example] > os_profile >
           admin_password
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Linux virtual machine has password authentication enabled
  Info:    Linux virtual machine has password authentication enabled.
Password
           authentication is less resistant to brute force and educated
guess
           attacks then SSH public key authentication
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-79
  Path:    resource > azurerm_virtual_machine[example] >
os_profile_linux_config
```

```
           > disable_password_authentication
  File:    examples/batch/custom-image/main.tf
  Resolve: Set `disable_password_authentication` attribute to `true` or
remove
           the attribute

  [High] Azure Search service public network access enabled
  Info:    Azure Search service public network access enabled. Public
access to
           Azure Search exposes the service to unnecessary risks
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-AZURE-642
  Path:    resource > azurerm_search_service[example] >
           public_network_access_enabled
  File:    examples/search/main.tf
  Resolve: Set `public_network_access_enabled ` to `false`

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[vmserver] > os_profile >
           admin_password
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

  [High] Virtual machine is configured with password authentication for
admin
  Info:    Administrative password has been set in configuration file. The
           secret value will be readable to anyone with access to VCS,
which can
           lead to unauthorized data disclosure or privilege escalation
  Rule:    https://security.snyk.io/rules/cloud/SNYK-CC-TF-263
  Path:    resource > azurerm_virtual_machine[vmjb] > os_profile >
           admin_password
  File:    examples/virtual-networks/azure-firewall/main.tf
  Resolve: Set `admin_ssh_key` attribute instead of password authentication

-------------------------------------------------------

Test Summary

  Organization: code-mdh
  Project name: componentsevotestingsnyk

✓ Files without issues: 123
✗ Files with issues: 52
  Ignored issues: 0
  Total issues: 221 [ 0 critical, 19 high, 77 medium, 125 low ]

-------------------------------------------------------

Tip

  New: Share your test results in the Snyk Web UI with the option --report

[Pipeline] echo
something failed
[Pipeline] echo
```

```
=============== https://github.com/chef/cookstyle.git VERSION DEFAULT
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Failed to parse JSON file
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/3/cspell.json
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION v7.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v7.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/chef/cookstyle.git VERSION v6.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/cookstyl
e/v6.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION
DEFAULT ===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
```

```
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/4
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION v4.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v4.0.0
[Pipeline] echo
something failed
[Pipeline] echo
=============== https://github.com/pulumi/pulumi-datadog.git VERSION v3.0.0
===================
[Pipeline] sh
+ sudo -su aicha.war /usr/local/bin/snyk iac test
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0 --detection-depth=3

Snyk Infrastructure as Code

- Snyk testing Infrastructure as Code configuration issues.
  Could not find any valid IaC files
  Path:
/Users/aicha.war/.jenkins/workspace/componentsevotestingsnyk/extra/pulumi-
datadog/v3.0.0
[Pipeline] echo
something failed
[Pipeline] }
[Pipeline] // script
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```