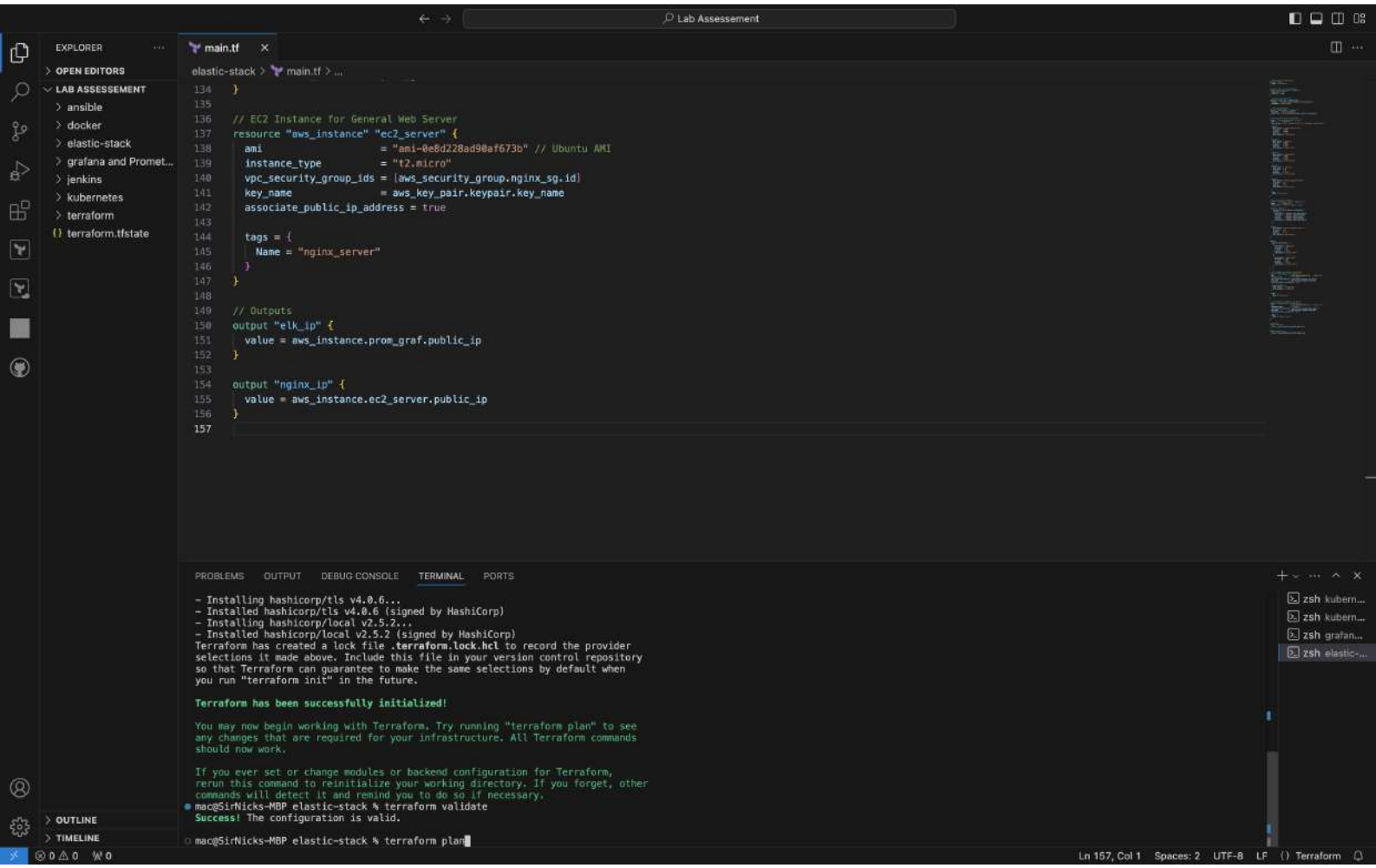
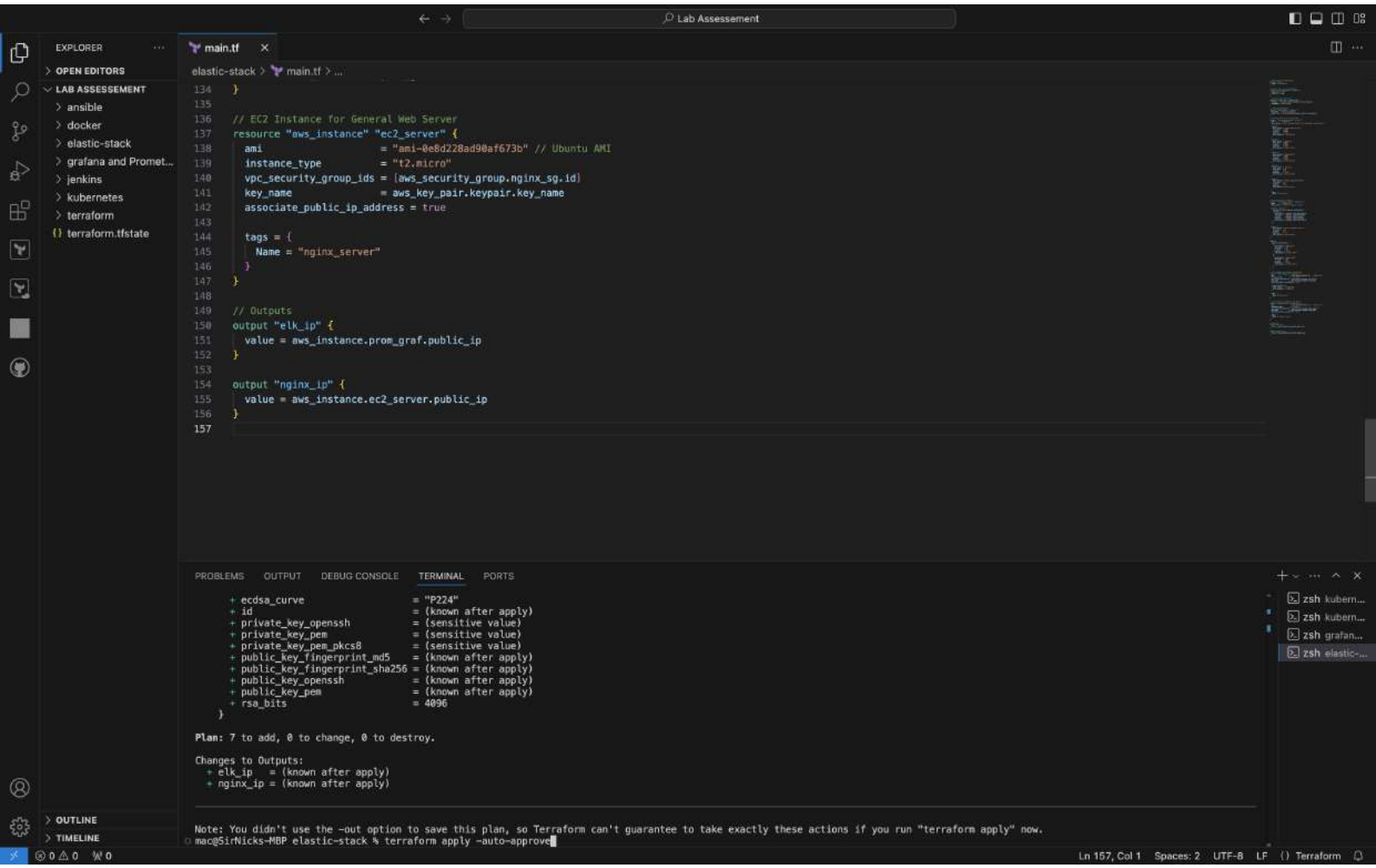
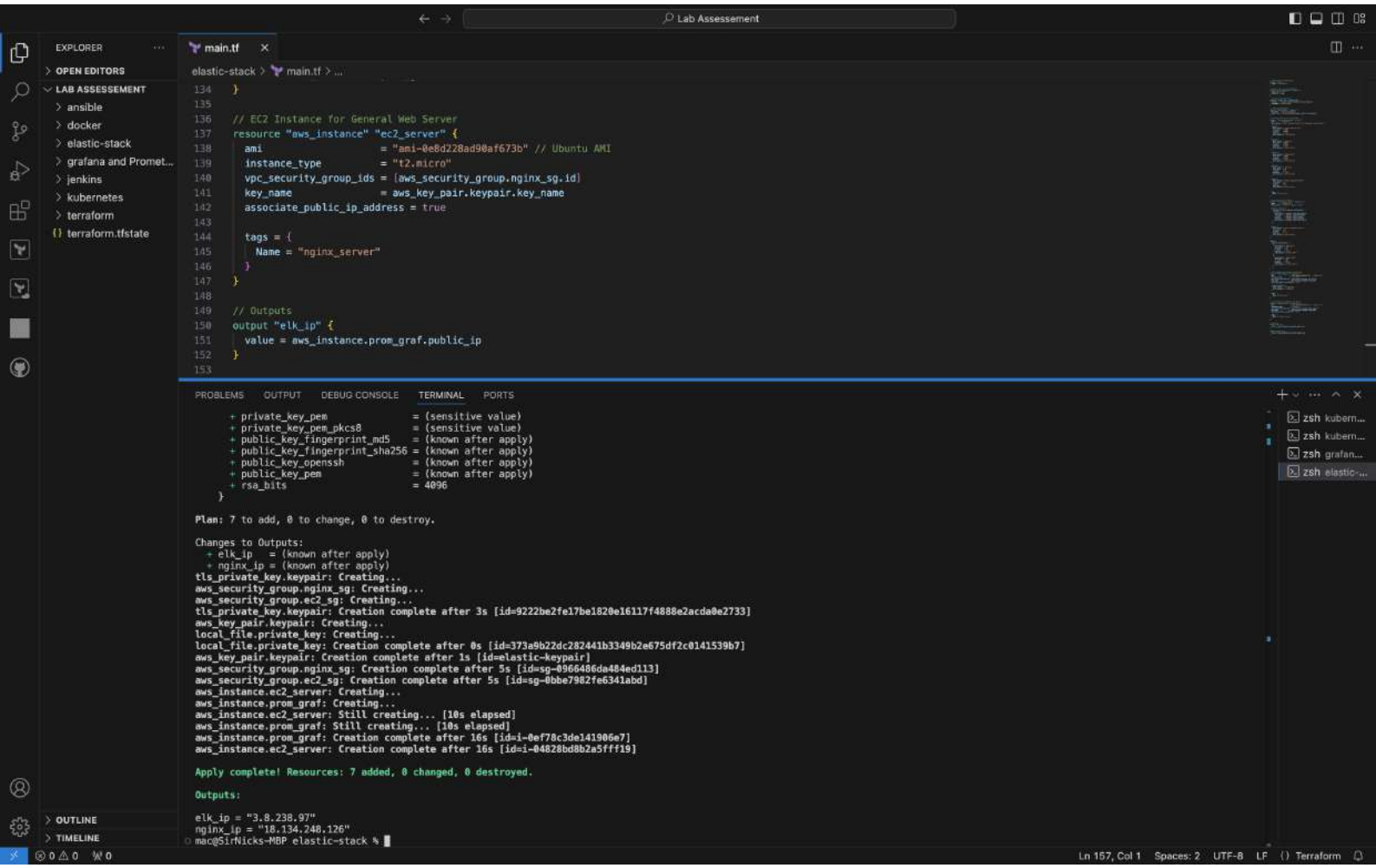
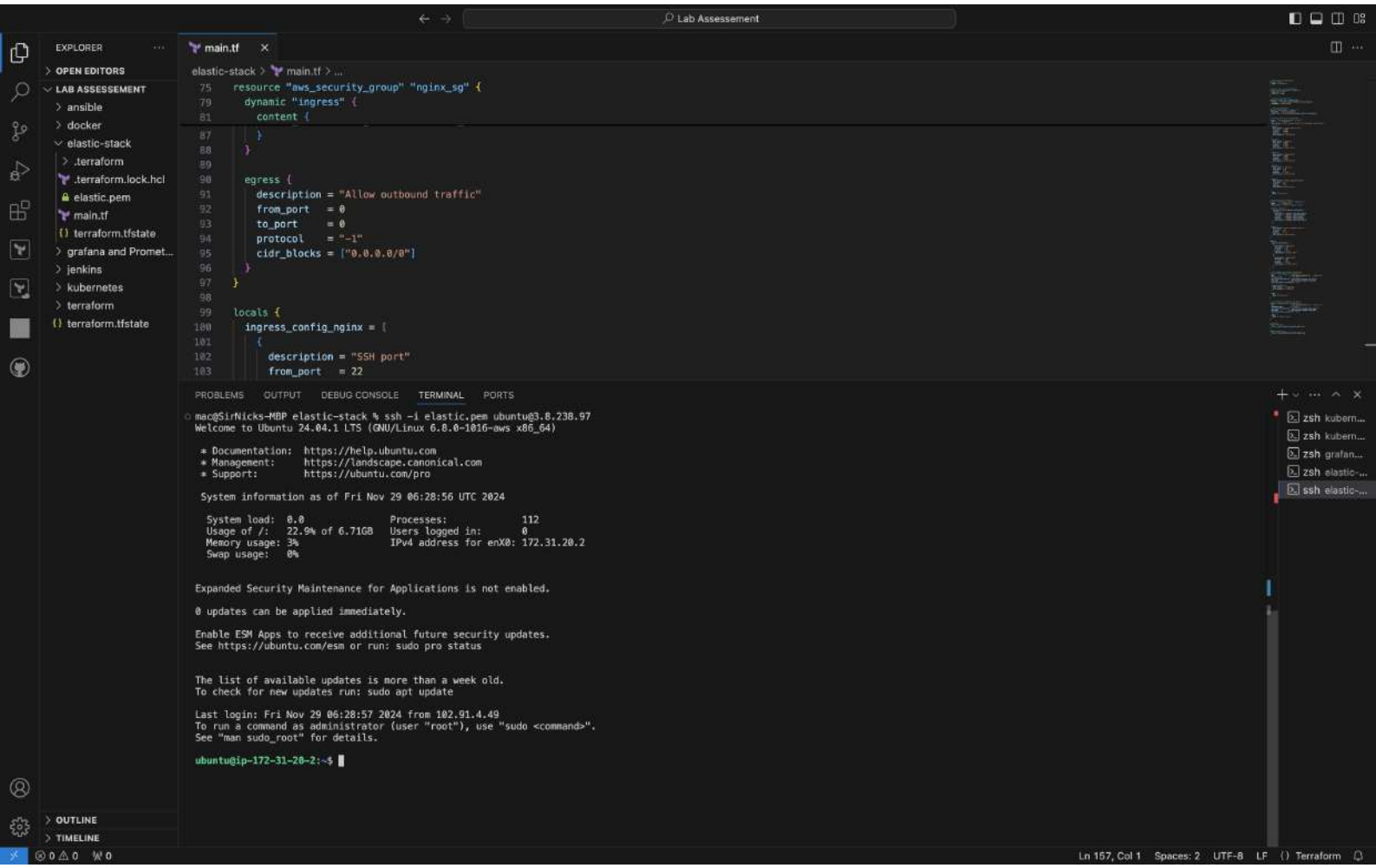
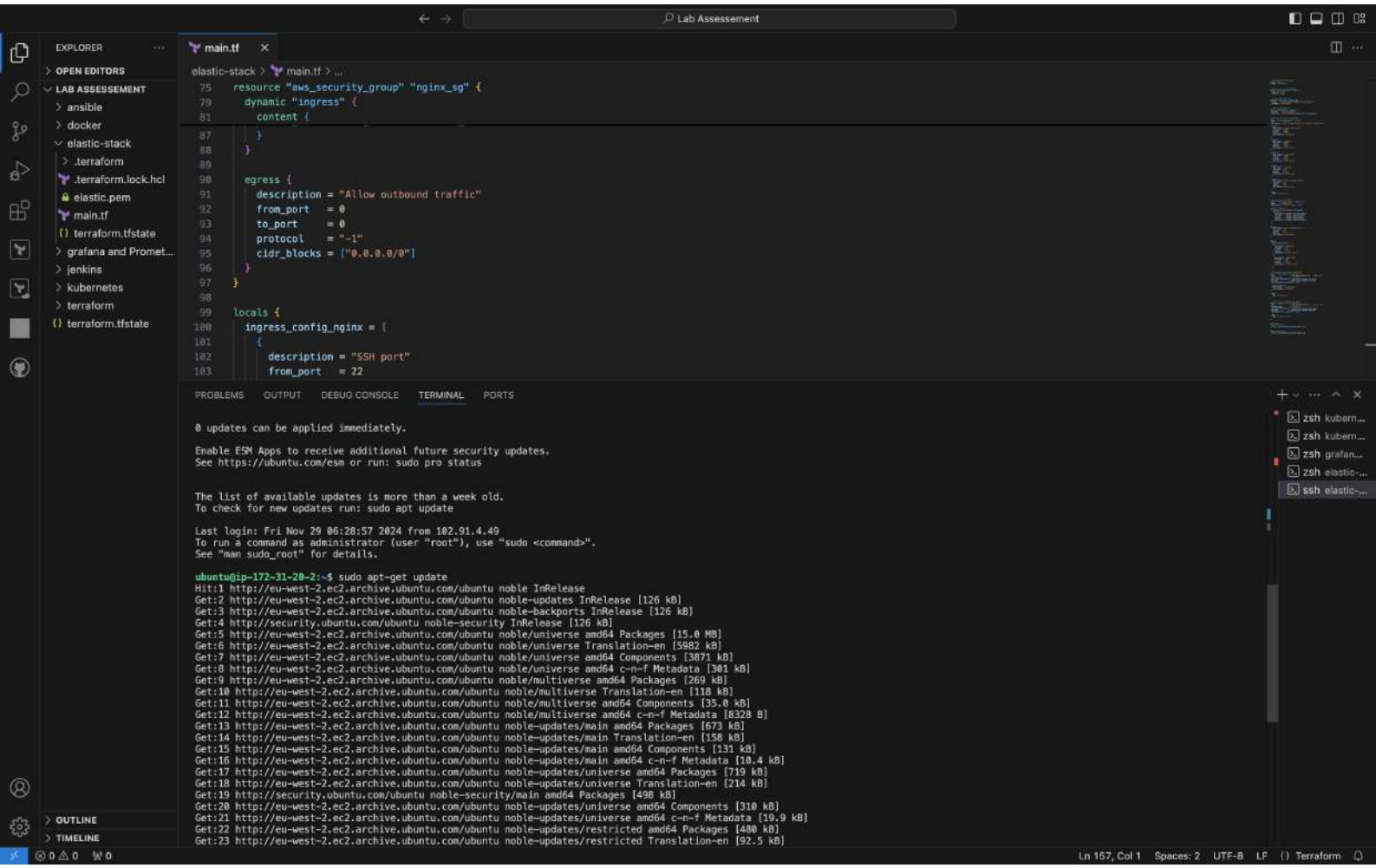
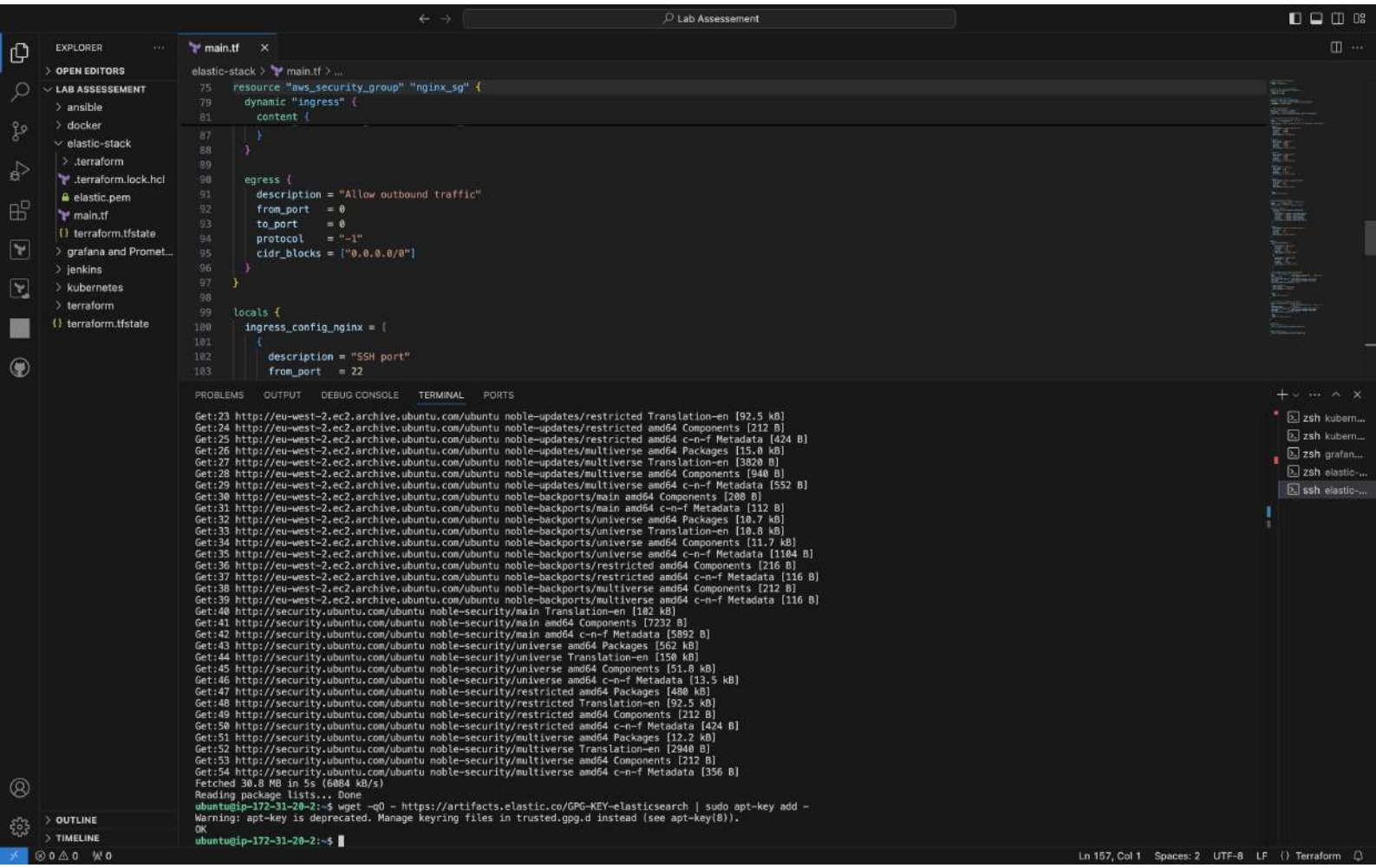

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
134 }
135
136 // EC2 Instance for General Web Server
137 resource "aws_instance" "ec2_server" {
138 ami = "ami-0e8d228ad90af673b" // Ubuntu AMI
139 instance_type = "t2.micro"
140 vpc_security_group_ids = [aws_security_group.nginx_sg.id]
141 key_name = aws_key_pair.keypair.key_name
142 associate_public_ip_address = true
143
144 tags = {
145 Name = "nginx_server"
146 }
147 }
148
149 // Outputs
150 output "elk_ip" {
151 value = aws_instance.prom_graf.public_ip
152 }
153
154 output "nginx_ip" {
155 value = aws_instance.ec2_server.public_ip
156 }
157
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
- Installing hashicorp/tls v4.0.6...
- Installed hashicorp/tls v4.0.6 (signed by HashiCorp)
- Installing hashicorp/local v2.5.2...
- Installed hashicorp/local v2.5.2 (signed by HashiCorp)
Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.
Terraform has been successfully initialized!
You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.
If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
mac@SirNicks-MBP elastic-stack % terraform validate
Success! The configuration is valid.
mac@SirNicks-MBP elastic-stack % terraform plan
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

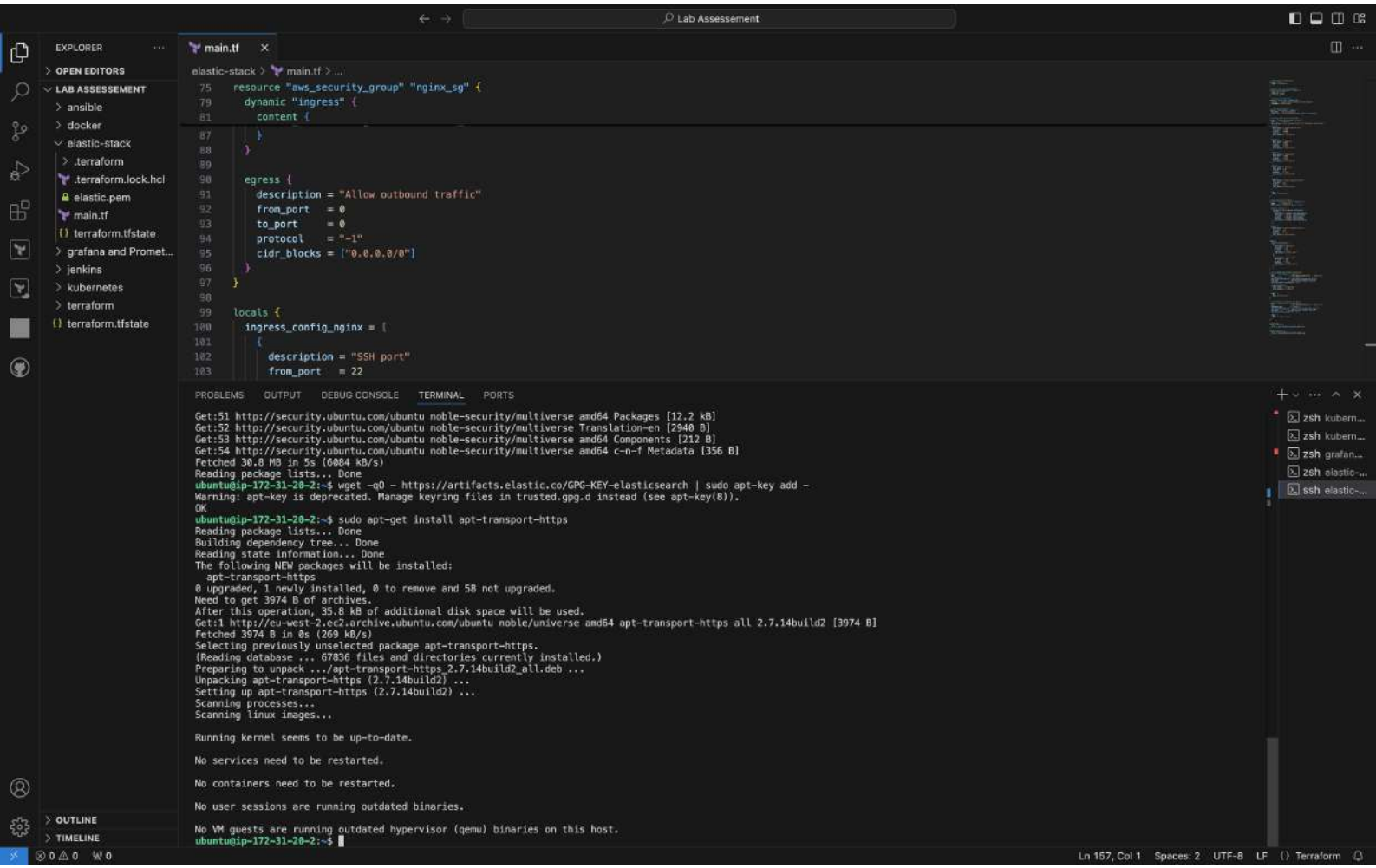

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
134 }
135
136 // EC2 Instance for General Web Server
137 resource "aws_instance" "ec2_server" {
138 ami = "ami-0e8d228ad90af673b" // Ubuntu AMI
139 instance_type = "t2.micro"
140 vpc_security_group_ids = [aws_security_group.nginx_sg.id]
141 key_name = aws_key_pair.keypair.key_name
142 associate_public_ip_address = true
143
144 tags = {
145 Name = "nginx_server"
146 }
147 }
148
149 // Outputs
150 output "elk_ip" {
151 value = aws_instance.prom_graf.public_ip
152 }
153
154 output "nginx_ip" {
155 value = aws_instance.ec2_server.public_ip
156 }
157
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
+ ecdsa_curve = "P224"
+ id = (known after apply)
+ private_key_openssh = (sensitive value)
+ private_key_pem = (sensitive value)
+ private_key_pem_pkcs8 = (sensitive value)
+ public_key_fingerprint_md5 = (known after apply)
+ public_key_fingerprint_sha256 = (known after apply)
+ public_key_openssh = (known after apply)
+ public_key_pem = (known after apply)
+ rsa_bits = 4096
}
Plan: 7 to add, 0 to change, 0 to destroy.
Changes to Outputs:
+ elk_ip = (known after apply)
+ nginx_ip = (known after apply)
Note: You didn't use the -out option to save this plan, so Terraform can't guarantee to take exactly these actions if you run "terraform apply" now.
mac@SirNicks-MBP elastic-stack % terraform apply -auto-approve
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

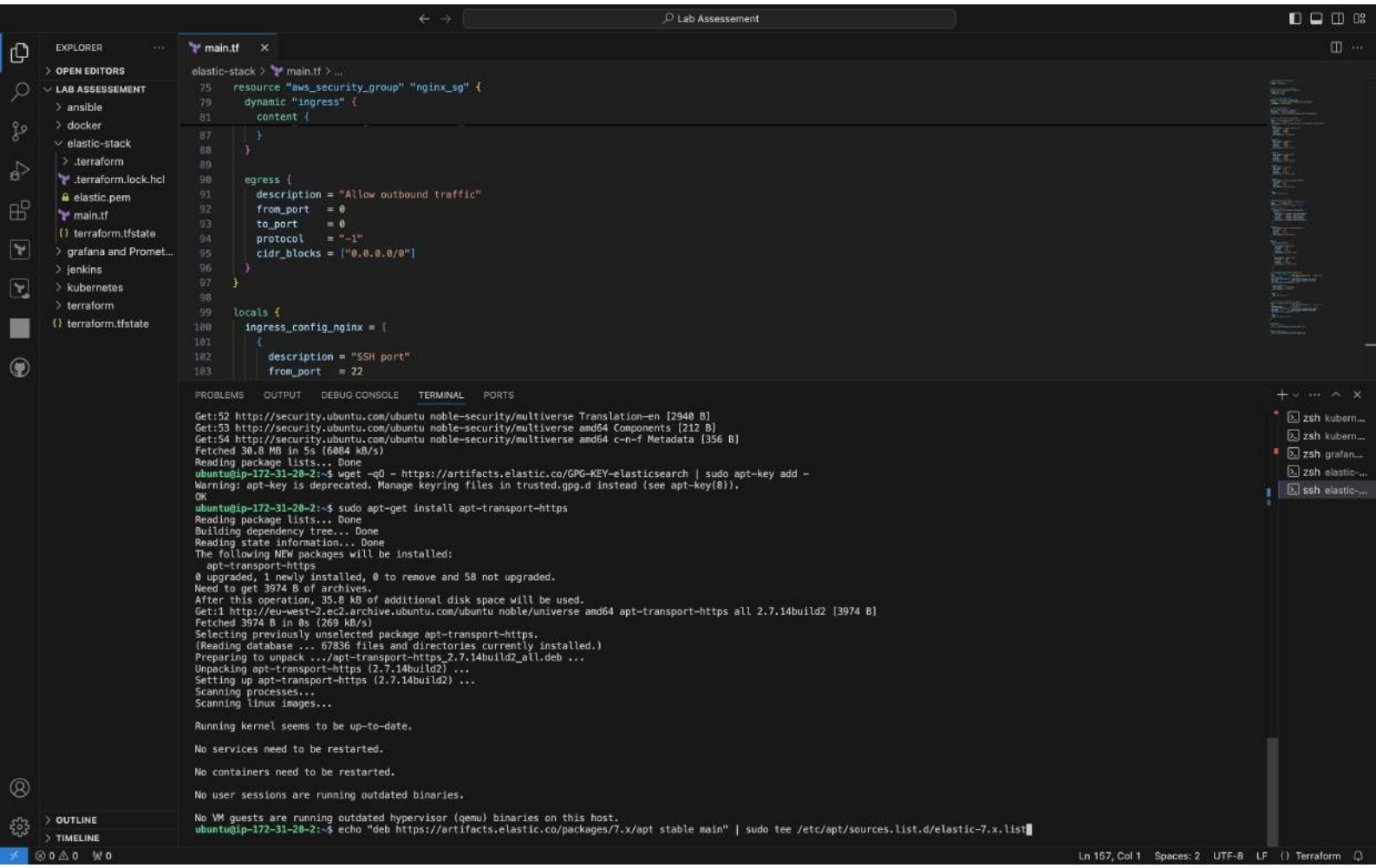

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
134 }
135
136 // EC2 Instance for General Web Server
137 resource "aws_instance" "ec2_server" {
138 ami = "ami-0e8d228ad90af673b" // Ubuntu AMI
139 instance_type = "t2.micro"
140 vpc_security_group_ids = [aws_security_group.nginx_sg.id]
141 key_name = aws_key_pair.keypair.key_name
142 associate_public_ip_address = true
143
144 tags = {
145 Name = "nginx_server"
146 }
147 }
148
149 // Outputs
150 output "elk_ip" {
151 value = aws_instance.prom_graf.public_ip
152 }
153
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
+ private_key_pem = (sensitive value)
+ private_key_pem_pkcs8 = (sensitive value)
+ public_key_fingerprint_md5 = (known after apply)
+ public_key_fingerprint_sha256 = (known after apply)
+ public_key_openssh = (known after apply)
+ public_key_pem = (known after apply)
+ rsa_bits = 4096
}
Plan: 7 to add, 0 to change, 0 to destroy.
Changes to Outputs:
+ elk_ip = (known after apply)
+ nginx_ip = (known after apply)
tls_private_key.keypair: Creating...
aws_security_group.nginx_sg: Creating...
aws_security_group.ec2_sg: Creating...
tls_private_key.keypair: Creation complete after 3s [id=9222be2fe17be1820e16117f4888e2acda0e2733]
aws_key_pair.keypair: Creating...
local_file.private_key: Creating...
local_file.private_key: Creation complete after 0s [id=373a9b22dc282441b3349b2e675df2c0141539b7]
aws_key_pair.keypair: Creation complete after 1s [id=elastic-keypair]
aws_security_group.nginx_sg: Creation complete after 5s [id=sg-0966486da484ed113]
aws_security_group.ec2_sg: Creation complete after 5s [id=sg-0bbe7982fe6341abd]
aws_instance.ec2_server: Creating...
aws_instance.prom_graf: Creating...
aws_instance.ec2_server: Still creating... [10s elapsed]
aws_instance.prom_graf: Still creating... [10s elapsed]
aws_instance.prom_graf: Creation complete after 16s [id=i-0ef78c3de141906e7]
aws_instance.ec2_server: Creation complete after 16s [id=i-04828bd8b2a5fff19]
Apply complete! Resources: 7 added, 0 changed, 0 destroyed.
Outputs:
elk_ip = "3.8.238.97"
nginx_ip = "18.134.248.126"
mac@SirNicks-MBP elastic-stack %
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

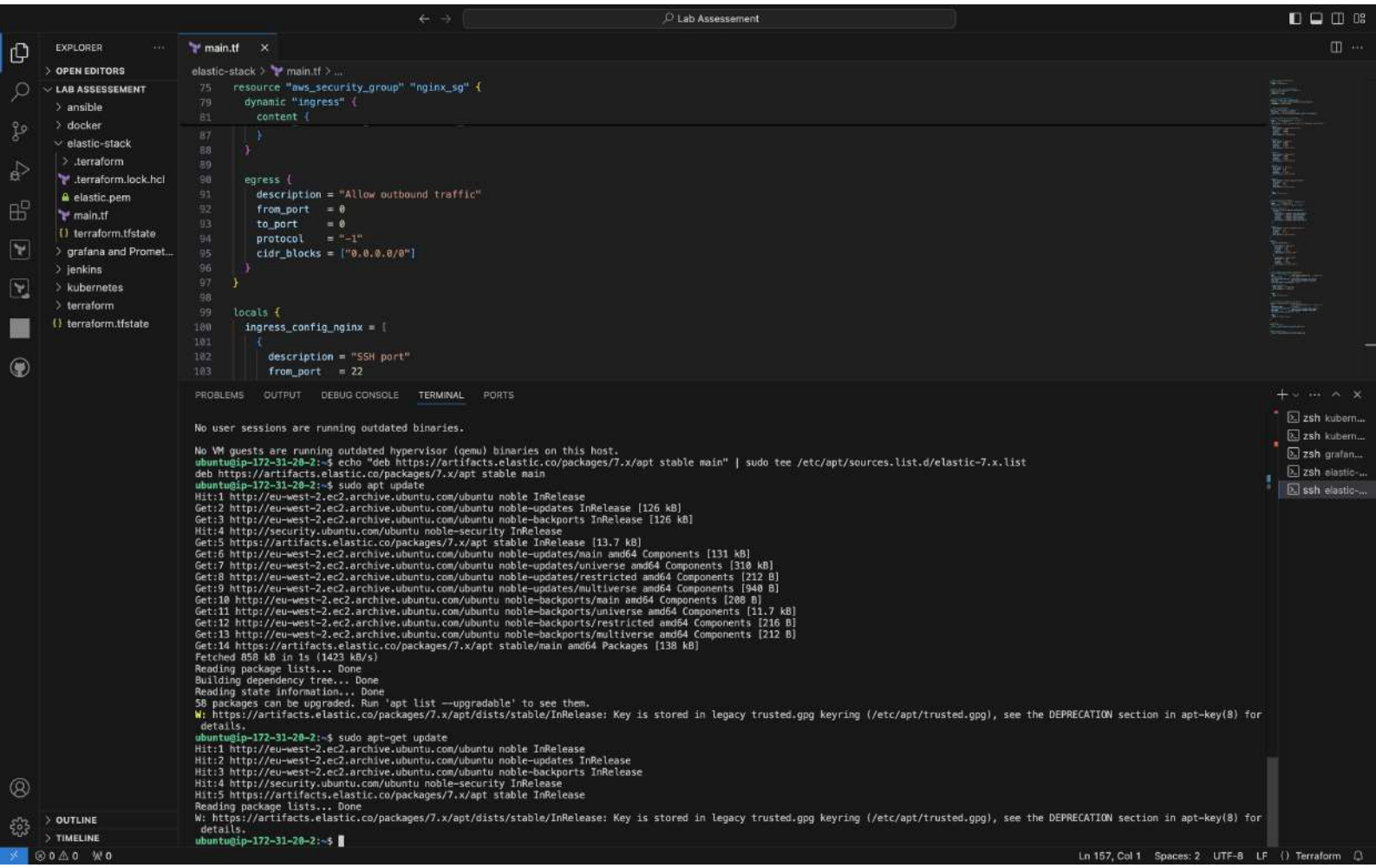

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
mac@SirNicks-MBP elastic-stack % ssh -i elastic.pem ubuntu@3.8.238.97
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Fri Nov 29 06:28:56 UTC 2024
System load: 0.0
Usage of /: 22.9% of 6.71GB
Memory usage: 3%
Swap usage: 0%
Processes: 112
Users logged in: 0
IPv4 address for enX0: 172.31.20.2
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Fri Nov 29 06:28:57 2024 from 102.91.4.49
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

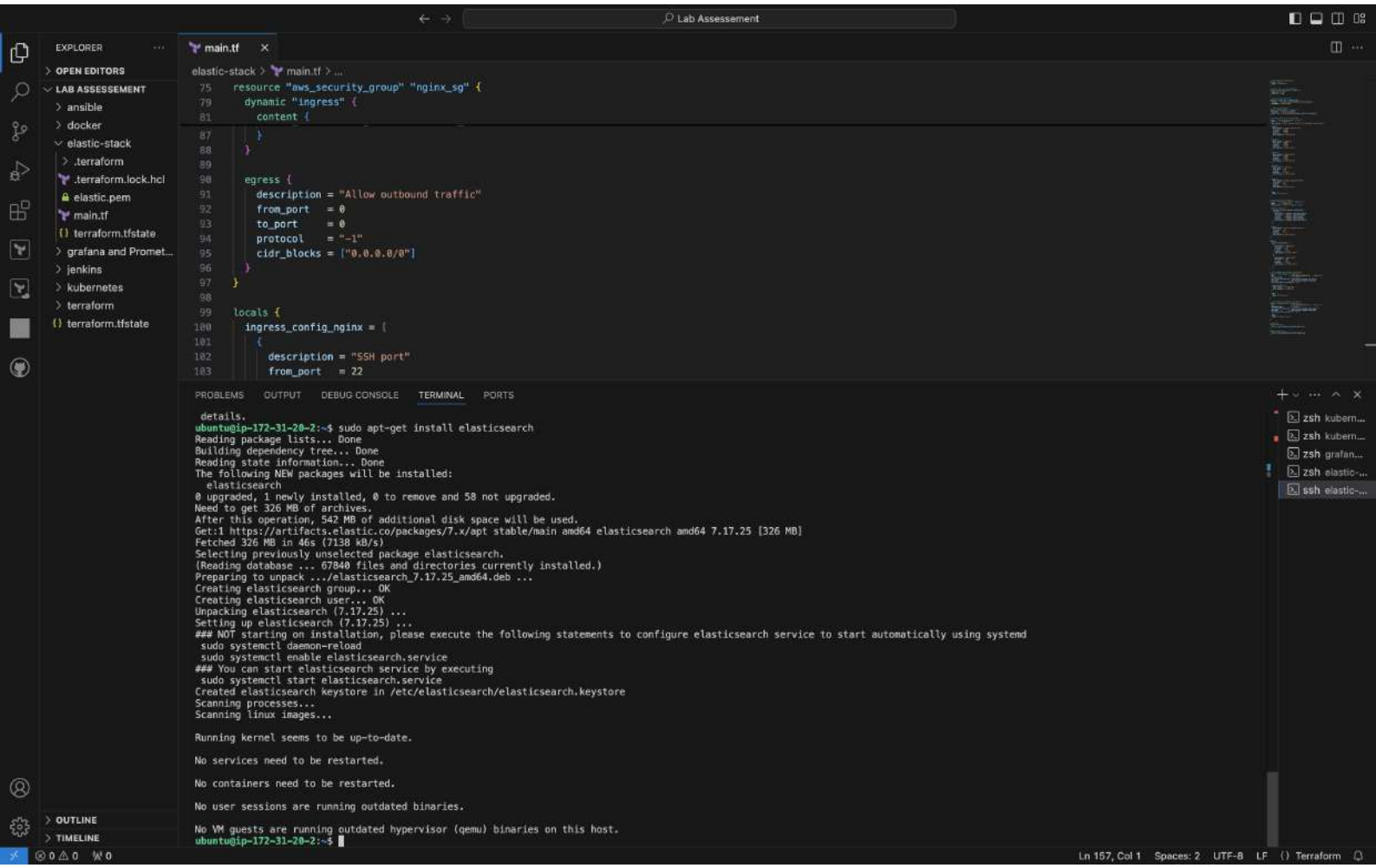

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Fri Nov 29 06:28:57 2024 from 102.91.4.49
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-20-2:~$ sudo apt-get update
Hit:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:11 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:12 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [673 kB]
Get:14 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [158 kB]
Get:15 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [131 kB]
Get:16 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [10.4 kB]
Get:17 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [719 kB]
Get:18 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [214 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [498 kB]
Get:20 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [310 kB]
Get:21 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [19.9 kB]
Get:22 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [480 kB]
Get:23 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [92.5 kB]
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

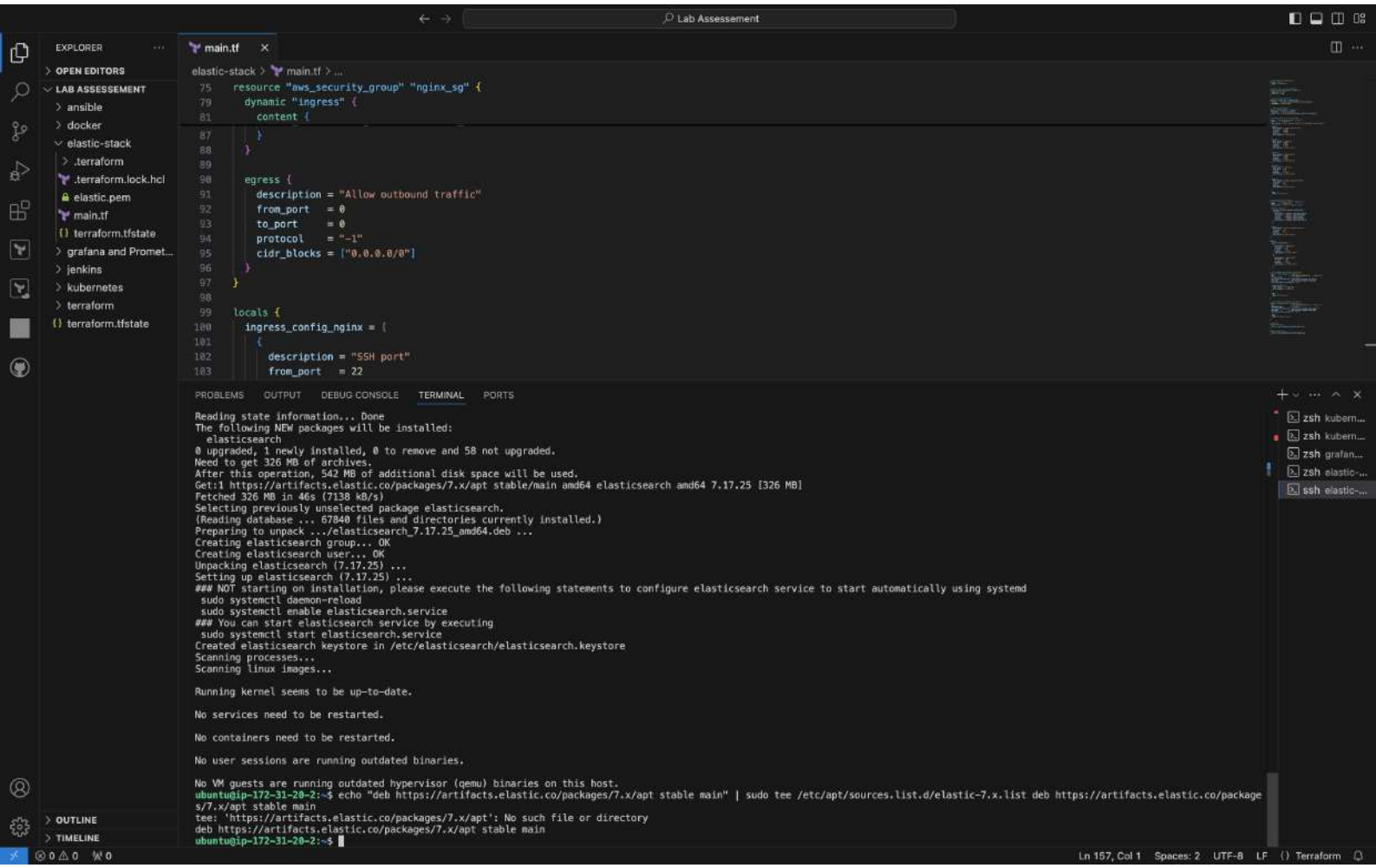

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Get:23 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [92.5 kB]
Get:24 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:25 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 c-n-f Metadata [424 B]
Get:26 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [15.0 kB]
Get:27 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3820 B]
Get:28 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:29 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [552 B]
Get:30 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:31 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:32 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [10.7 kB]
Get:33 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [10.8 kB]
Get:34 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.7 kB]
Get:35 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [1104 B]
Get:36 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:37 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:38 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:39 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:40 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [102 kB]
Get:41 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7232 B]
Get:42 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [5892 B]
Get:43 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [562 kB]
Get:44 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [150 kB]
Get:45 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.8 kB]
Get:46 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [13.5 kB]
Get:47 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [480 kB]
Get:48 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [92.5 kB]
Get:49 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:50 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 c-n-f Metadata [424 B]
Get:51 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [12.2 kB]
Get:52 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2940 B]
Get:53 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:54 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [356 B]
Fetched 30.8 MB in 5s (6084 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-20-2:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

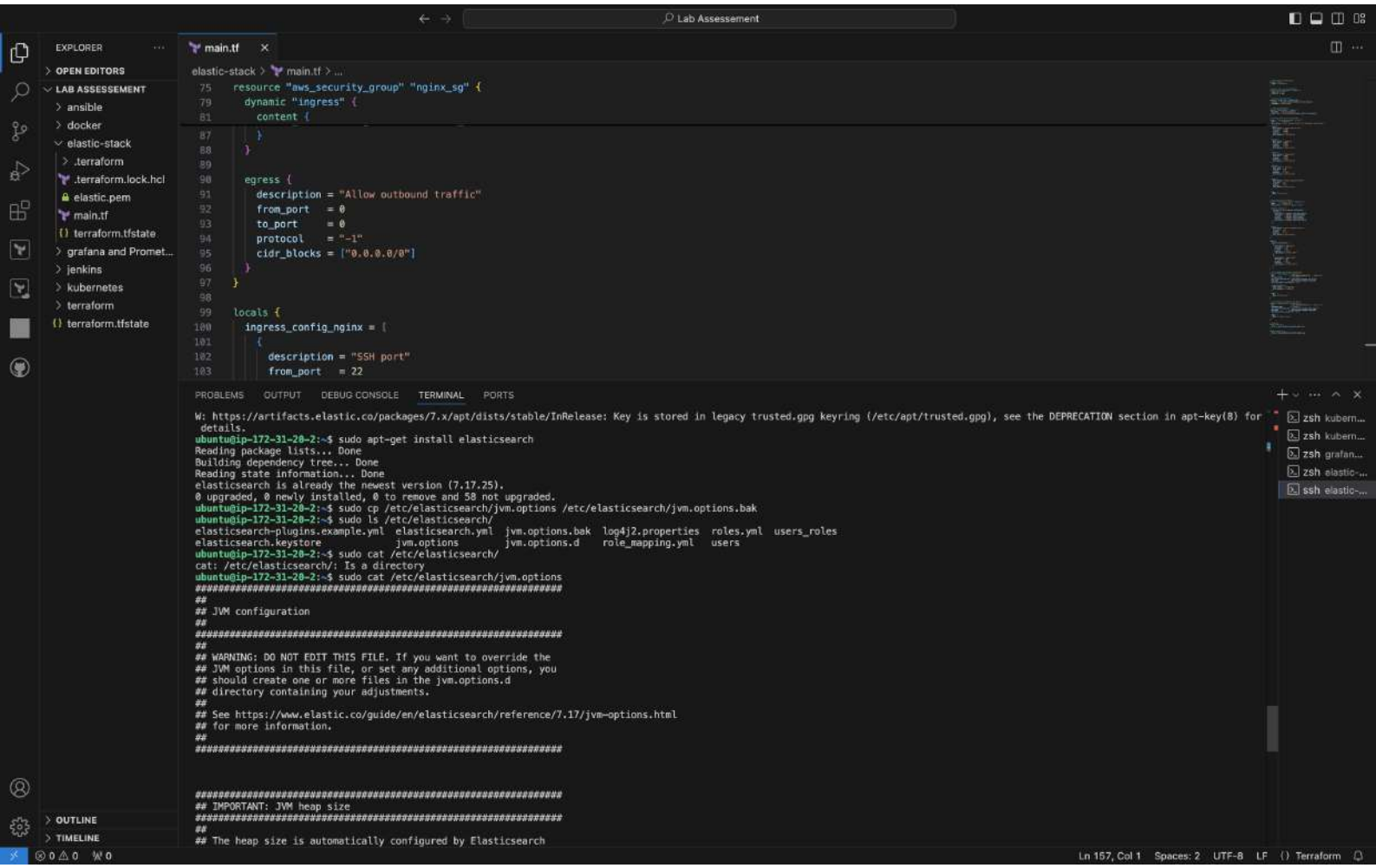

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Get:51 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [12.2 kB]
Get:52 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2940 B]
Get:53 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:54 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [356 B]
Fetched 30.8 MB in 5s (6084 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-20-2:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
ubuntu@ip-172-31-20-2:~$ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 3974 B of archives.
After this operation, 35.8 kB of additional disk space will be used.
Get:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3974 B]
Fetched 3974 B in 0s (269 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 67836 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.7.14build2_all.deb ...
Unpacking apt-transport-https (2.7.14build2) ...
Setting up apt-transport-https (2.7.14build2) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

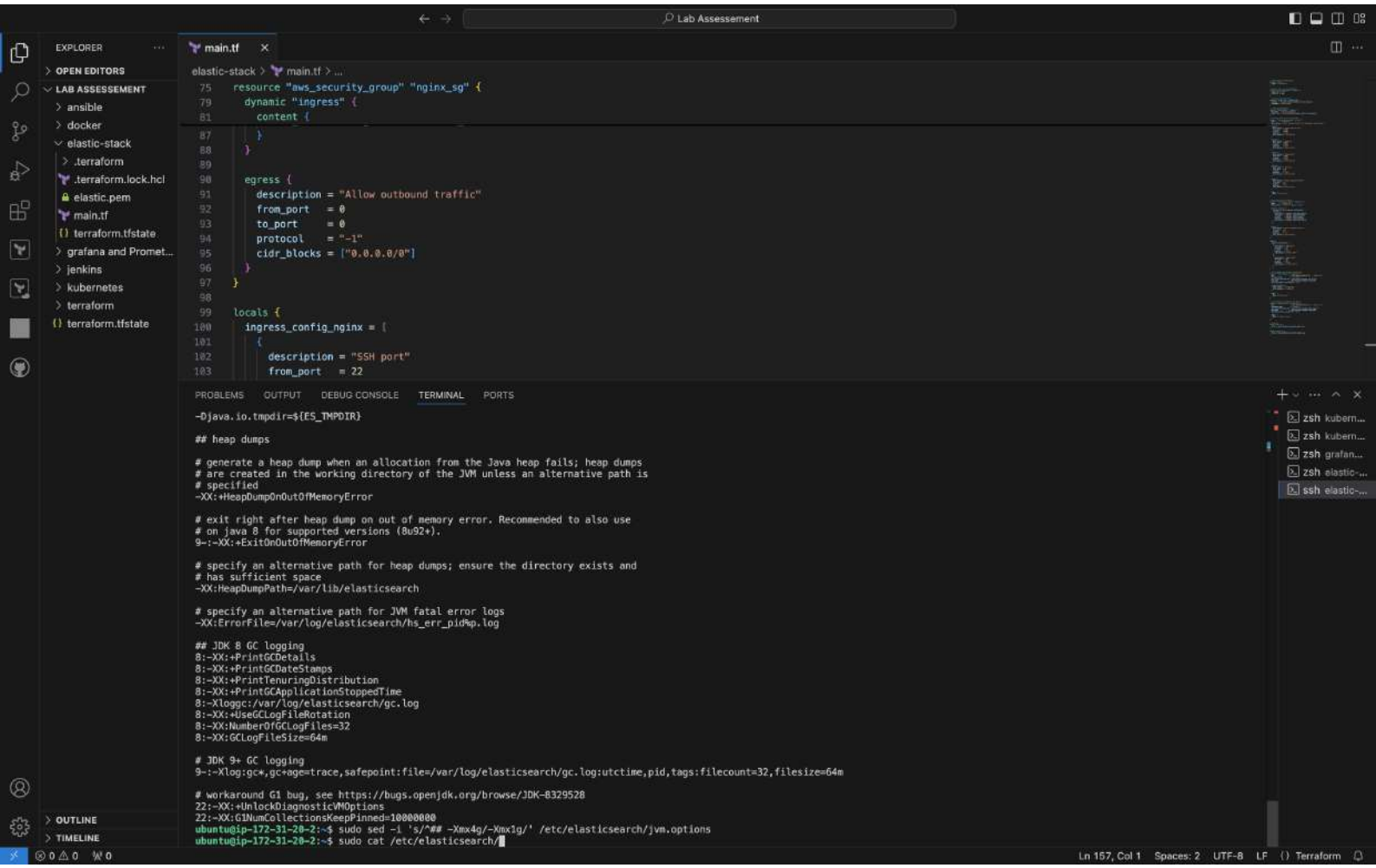

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Get:52 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2940 B]
Get:53 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:54 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [356 B]
Fetched 30.8 MB in 5s (6084 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-20-2:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
ubuntu@ip-172-31-20-2:~$ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 3974 B of archives.
After this operation, 35.8 kB of additional disk space will be used.
Get:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3974 B]
Fetched 3974 B in 0s (269 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 67836 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.7.14build2_all.deb ...
Unpacking apt-transport-https (2.7.14build2) ...
Setting up apt-transport-https (2.7.14build2) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

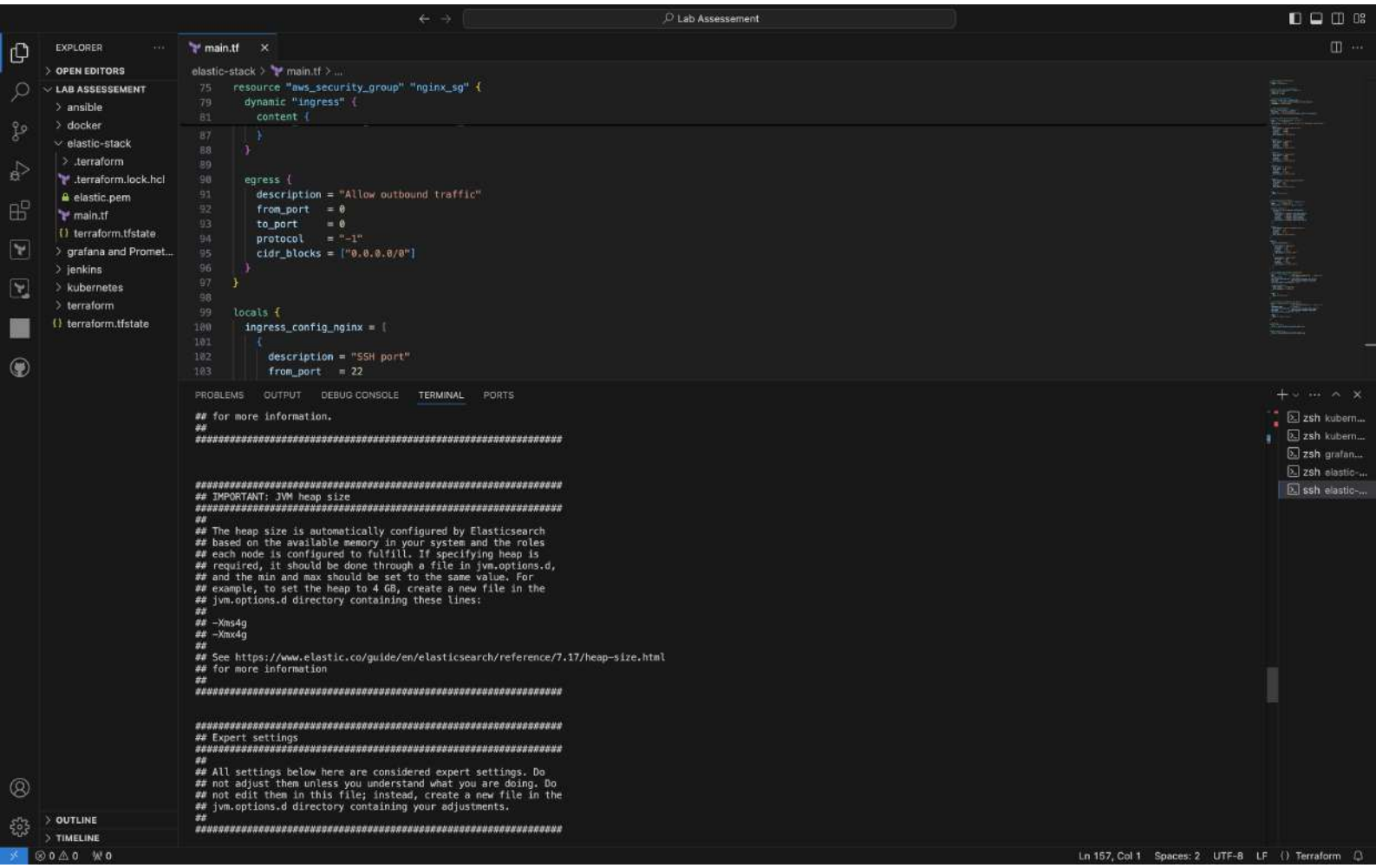

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
ubuntu@ip-172-31-20-2:~$ sudo apt update
Hit:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Get:6 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [131 kB]
Get:7 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [310 kB]
Get:8 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:9 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:10 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:11 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.7 kB]
Get:12 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:13 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Get:14 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [138 kB]
Fetched 858 kB in 1s (1423 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
58 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
ubuntu@ip-172-31-20-2:~$ sudo apt-get update
Hit:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:5 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Reading package lists... Done
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

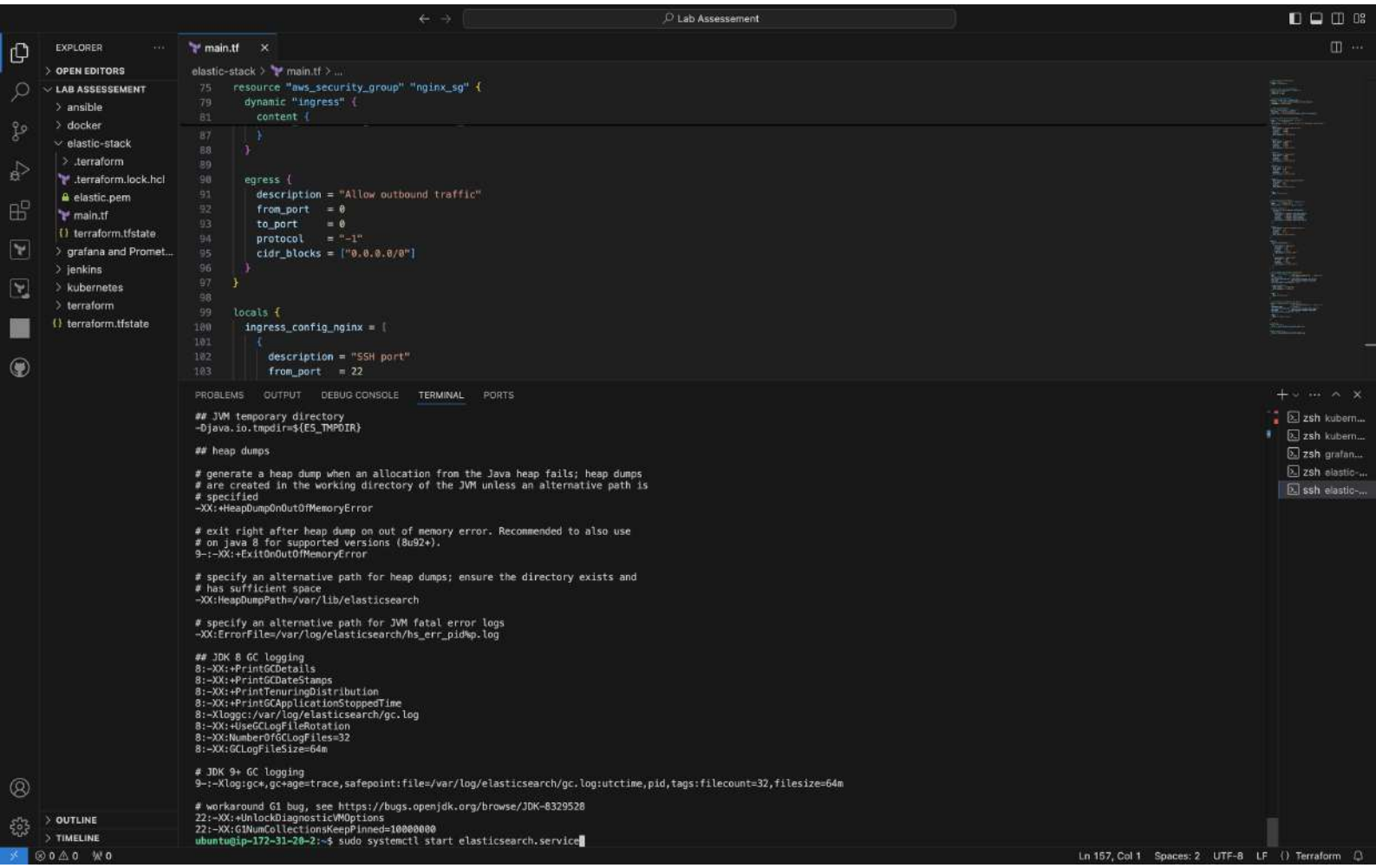

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
details.
ubuntu@ip-172-31-20-2:~$ sudo apt-get install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 326 MB of archives.
After this operation, 542 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17.25 [326 MB]
Fetched 326 MB in 46s (7138 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 67840 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.25_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.17.25) ...
Setting up elasticsearch (7.17.25) ...
NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

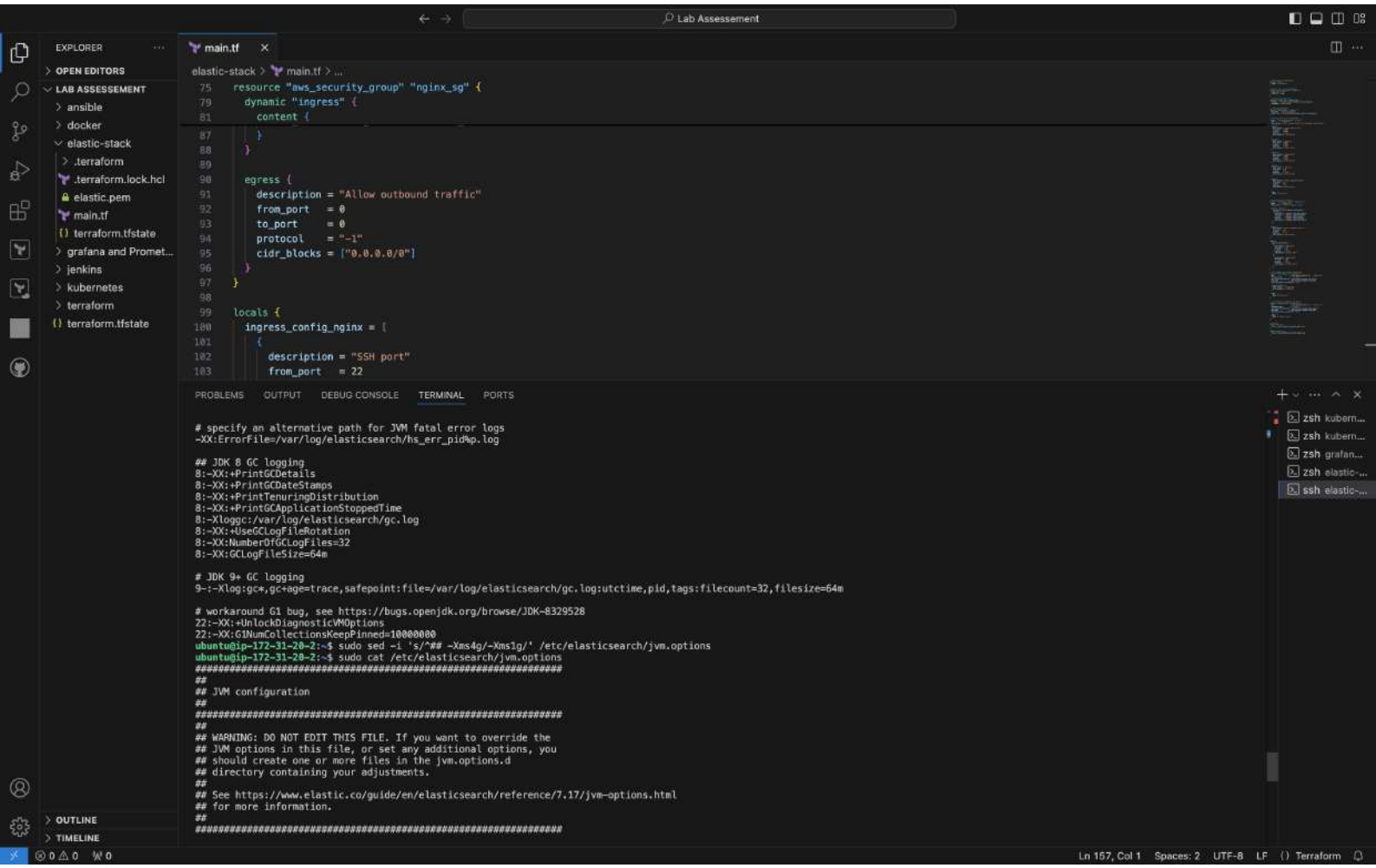

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Reading state information... Done
The following NEW packages will be installed:
elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 326 MB of archives.
After this operation, 542 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17.25 [326 MB]
Fetched 326 MB in 46s (7138 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 67840 files and directories currently installed.)
Preparing to unpack .../elasticsearch_7.17.25_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (7.17.25) ...
Setting up elasticsearch (7.17.25) ...
NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
Created elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list deb https://artifacts.elastic.co/packages/7.x/apt stable main
tee: 'https://artifacts.elastic.co/packages/7.x/apt': No such file or directory
deb https://artifacts.elastic.co/packages/7.x/apt stable main
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

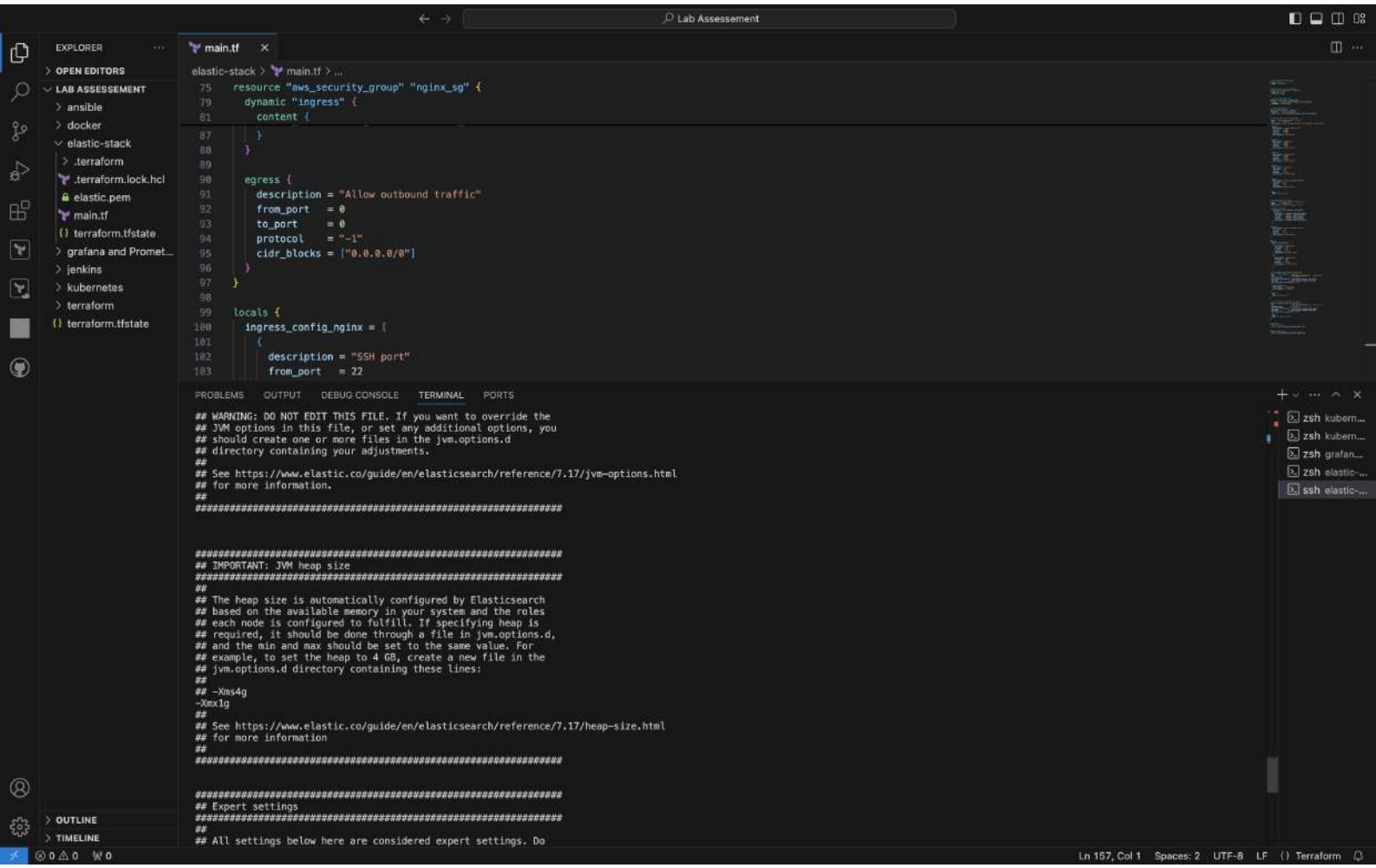

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
ubuntu@ip-172-31-20-2:~$ sudo apt-get install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
elasticsearch is already the newest version (7.17.25).
0 upgraded, 0 newly installed, 0 to remove and 58 not upgraded.
ubuntu@ip-172-31-20-2:~$ sudo cp /etc/elasticsearch/jvm.options /etc/elasticsearch/jvm.options.bak
ubuntu@ip-172-31-20-2:~$ sudo ls /etc/elasticsearch/
elasticsearch-plugins.example.yml elasticsearch.yml jvm.options.bak log4j2.properties roles.yml users_roles
elasticsearch.keystore jvm.options jvm.options.d role_mapping.yml users
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/elasticsearch/
cat: /etc/elasticsearch/: Is a directory
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/elasticsearch/jvm.options
JVM configuration
WARNING: DO NOT EDIT THIS FILE. If you want to override the
JVM options in this file, or set any additional options, you
should create one or more files in the jvm.options.d
directory containing your adjustments.
See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
for more information.
IMPORTANT: JVM heap size
The heap size is automatically configured by Elasticsearch
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

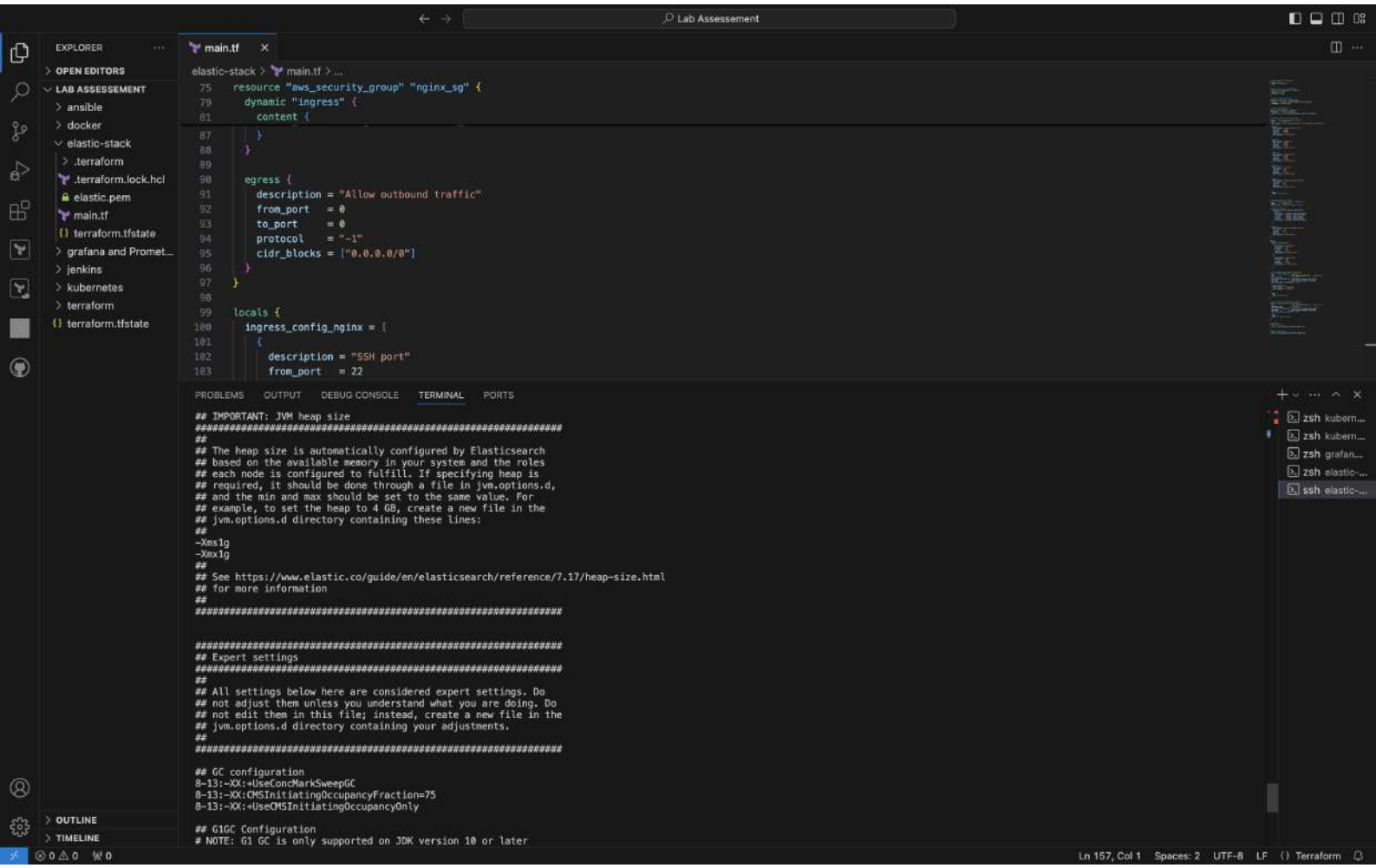

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
-Djava.io.tmpdir=${ES_TMPDIR}
heap dumps
generate a heap dump when an allocation from the Java heap fails; heap dumps
are created in the working directory of the JVM unless an alternative path is
specified
-XX:+HeapDumpOnOutOfMemoryError
exit right after heap dump on out of memory error. Recommended to also use
on java 8 for supported versions (8u92+).
9-:-XX:+ExitOnOutOfMemoryError
specify an alternative path for heap dumps; ensure the directory exists and
has sufficient space
-XX:HeapDumpPath=/var/lib/elasticsearch
specify an alternative path for JVM fatal error logs
-XX:ErrorFile=/var/log/elasticsearch/hs_err_pid%p.log
JDK 8 GC logging
8:-XX:+PrintGCDetails
8:-XX:+PrintGCDateStamps
8:-XX:+PrintTenuringDistribution
8:-XX:+PrintGCApplicationStoppedTime
8:-Xloggc:/var/log/elasticsearch/gc.log
8:-XX:+UseGCLogFileRotation
8:-XX:NumberOfGCLogFiles=32
8:-XX:GCLogFileSize=64m
JDK 9+ GC logging
9-:-Xlog:gc*,gc+age=trace,safepoint:file=/var/log/elasticsearch/gc.log:utctime,pid,tags:filecount=32,filesize=64m
workaround G1 bug, see https://bugs.openjdk.org/browse/JDK-8329528
22:-XX:+UnlockDiagnosticVMOptions
22:-XX:G1NumCollectionsKeepPinned=10000000
ubuntu@ip-172-31-20-2:~$ sudo sed -i 's/^## -Xmx4g/-Xmx1g/' /etc/elasticsearch/jvm.options
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/elasticsearch/
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

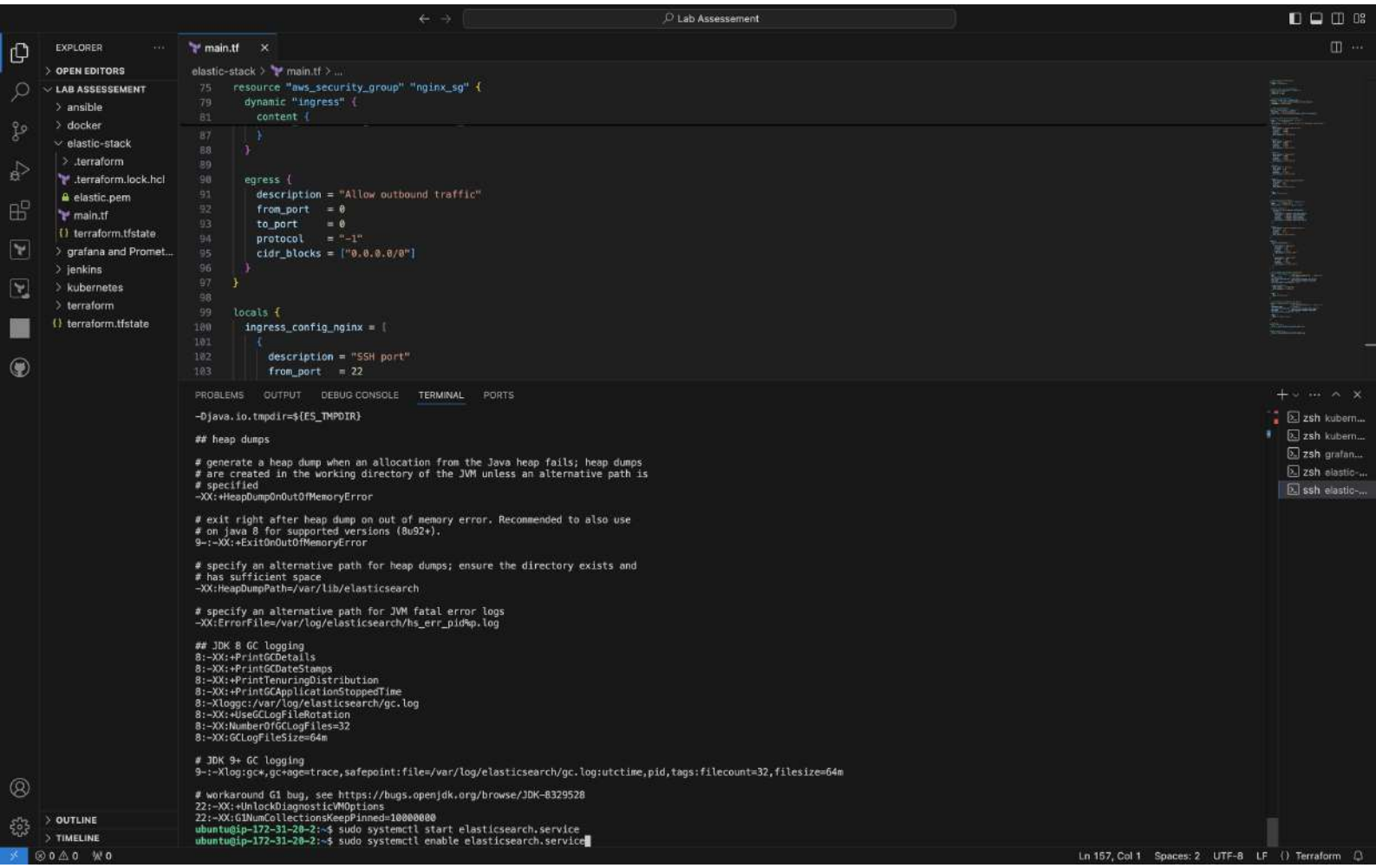

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
for more information.
##
IMPORTANT: JVM heap size
The heap size is automatically configured by Elasticsearch
based on the available memory in your system and the roles
each node is configured to fulfill. If specifying heap is
required, it should be done through a file in jvm.options.d,
and the min and max should be set to the same value. For
example, to set the heap to 4 GB, create a new file in the
jvm.options.d directory containing these lines:
-Xms4g
-Xmx4g
See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
for more information
Expert settings
All settings below here are considered expert settings. Do
not adjust them unless you understand what you are doing. Do
not edit them in this file; instead, create a new file in the
jvm.options.d directory containing your adjustments.
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

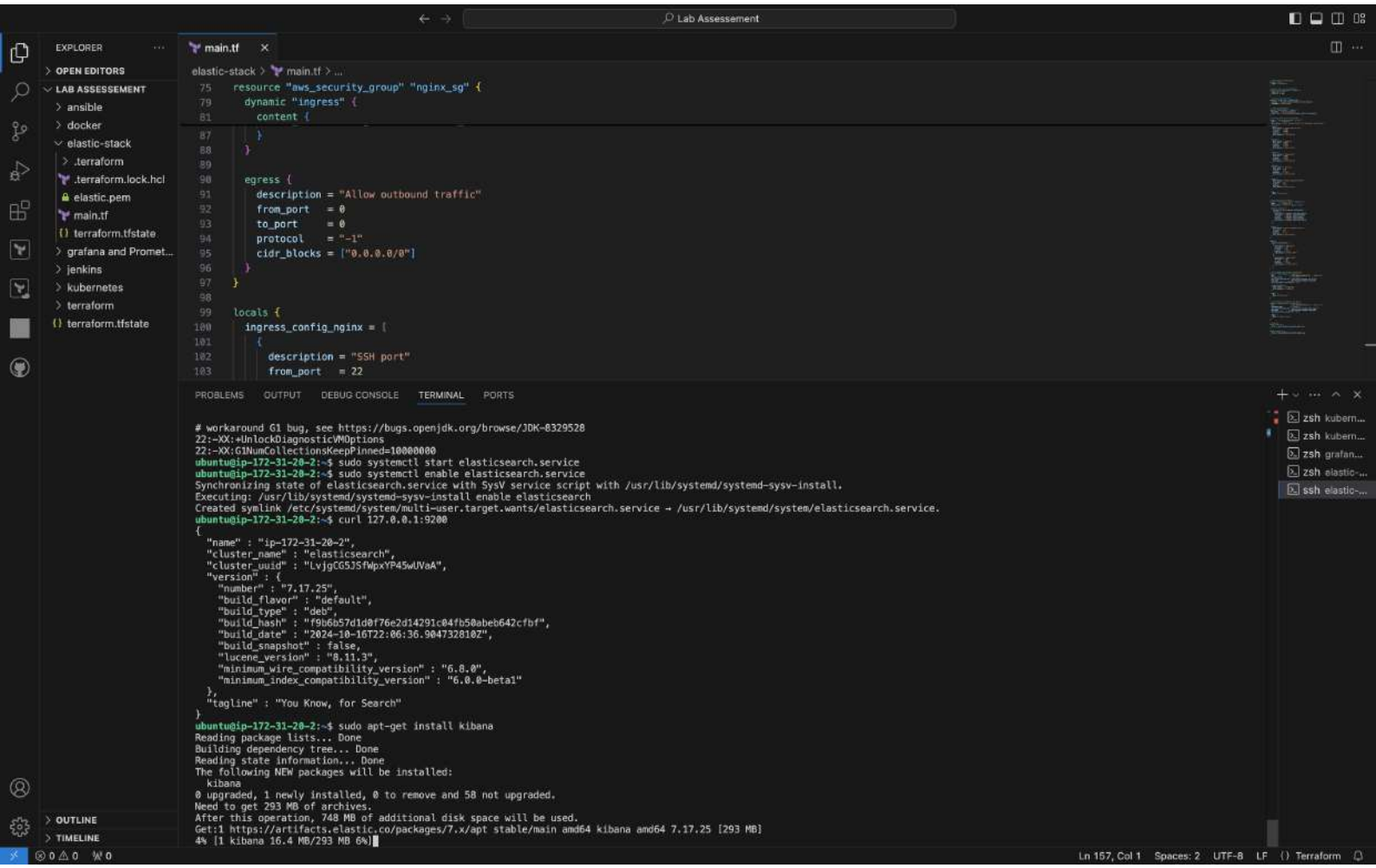

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
JVM temporary directory
-Djava.io.tmpdir=${ES_TMPDIR}
heap dumps
generate a heap dump when an allocation from the Java heap fails; heap dumps
are created in the working directory of the JVM unless an alternative path is
specified
-XX:+HeapDumpOnOutOfMemoryError
exit right after heap dump on out of memory error. Recommended to also use
on java 8 for supported versions (8u92+).
9-:-XX:+ExitOnOutOfMemoryError
specify an alternative path for heap dumps; ensure the directory exists and
has sufficient space
-XX:HeapDumpPath=/var/lib/elasticsearch
specify an alternative path for JVM fatal error logs
-XX:ErrorFile=/var/log/elasticsearch/hs_err_pid%p.log
JDK 8 GC logging
8:-XX:+PrintGCDetails
8:-XX:+PrintGCDateStamps
8:-XX:+PrintTenuringDistribution
8:-XX:+PrintGCApplicationStoppedTime
8:-Xloggc:/var/log/elasticsearch/gc.log
8:-XX:+UseGCLogFileRotation
8:-XX:NumberOfGCLogFiles=32
8:-XX:GCLogFileSize=64m
JDK 9+ GC logging
9-:-Xlog:gc*,gc+age=trace,safepoint:file=/var/log/elasticsearch/gc.log:utctime,pid,tags:filecount=32,filesize=64m
workaround G1 bug, see https://bugs.openjdk.org/browse/JDK-8329528
22:-XX:+UnlockDiagnosticVMOptions
22:-XX:G1NumCollectionsKeepPinned=10000000
ubuntu@ip-172-31-20-2:~$ sudo systemctl start elasticsearch.service
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

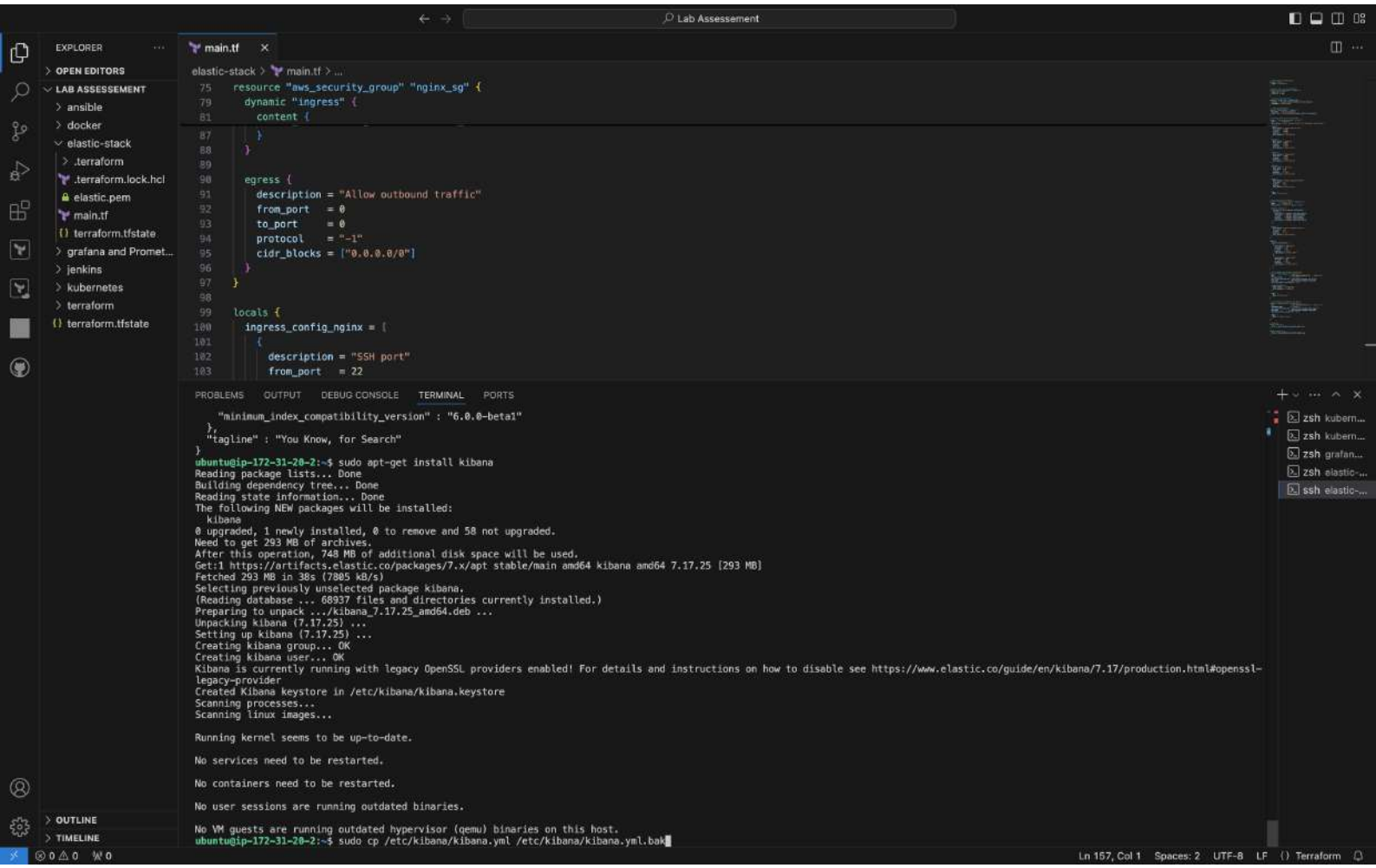

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
specify an alternative path for JVM fatal error logs
-XX:ErrorFile=/var/log/elasticsearch/hs_err_pid%p.log
JDK 8 GC logging
8:-XX:+PrintGCDetails
8:-XX:+PrintGCDateStamps
8:-XX:+PrintTenuringDistribution
8:-XX:+PrintGCApplicationStoppedTime
8:-Xloggc:/var/log/elasticsearch/gc.log
8:-XX:+UseGCLogFileRotation
8:-XX:NumberOfGCLogFiles=32
8:-XX:GCLogFileSize=64m
JDK 9+ GC logging
9-:-Xlog:gc*,gc+age=trace,safepoint:file=/var/log/elasticsearch/gc.log:utctime,pid,tags:filecount=32,filesize=64m
workaround G1 bug, see https://bugs.openjdk.org/browse/JDK-8329528
22:-XX:+UnlockDiagnosticVMOptions
22:-XX:G1NumCollectionsKeepPinned=10000000
ubuntu@ip-172-31-20-2:~$ sudo sed -i 's/^## -Xms4g/-Xms1g/' /etc/elasticsearch/jvm.options
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/elasticsearch/jvm.options
##
##
JVM configuration
##
##
##
WARNING: DO NOT EDIT THIS FILE. If you want to override the
JVM options in this file, or set any additional options, you
should create one or more files in the jvm.options.d
directory containing your adjustments.
##
See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
for more information.
##
##
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

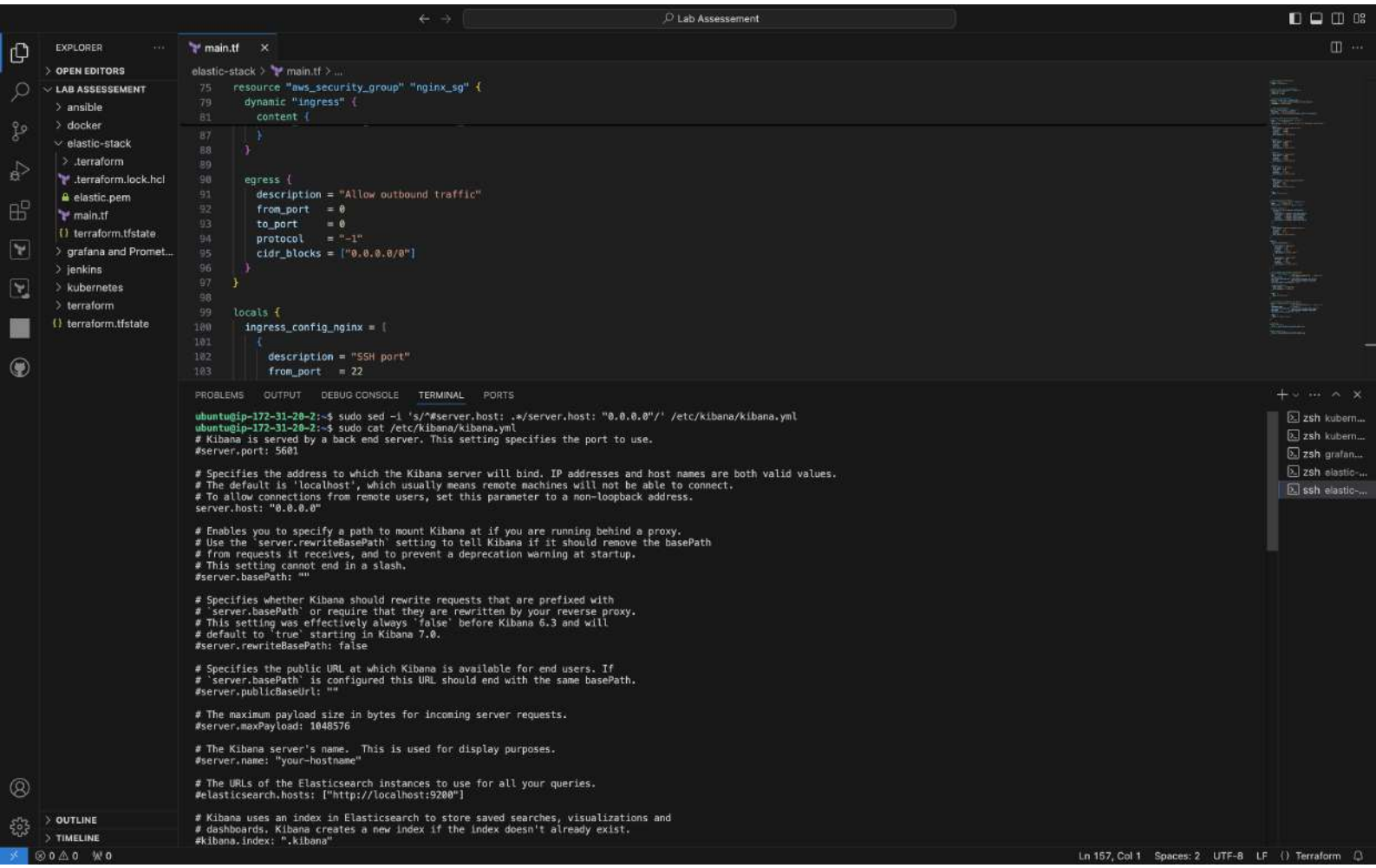

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
WARNING: DO NOT EDIT THIS FILE. If you want to override the
JVM options in this file, or set any additional options, you
should create one or more files in the jvm.options.d
directory containing your adjustments.
##
See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
for more information.
##
IMPORTANT: JVM heap size
The heap size is automatically configured by Elasticsearch
based on the available memory in your system and the roles
each node is configured to fulfill. If specifying heap is
required, it should be done through a file in jvm.options.d,
and the min and max should be set to the same value. For
example, to set the heap to 4 GB, create a new file in the
jvm.options.d directory containing these lines:
##
-Xms4g
-Xmx1g
##
See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
for more information
##
Expert settings
All settings below here are considered expert settings. Do
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

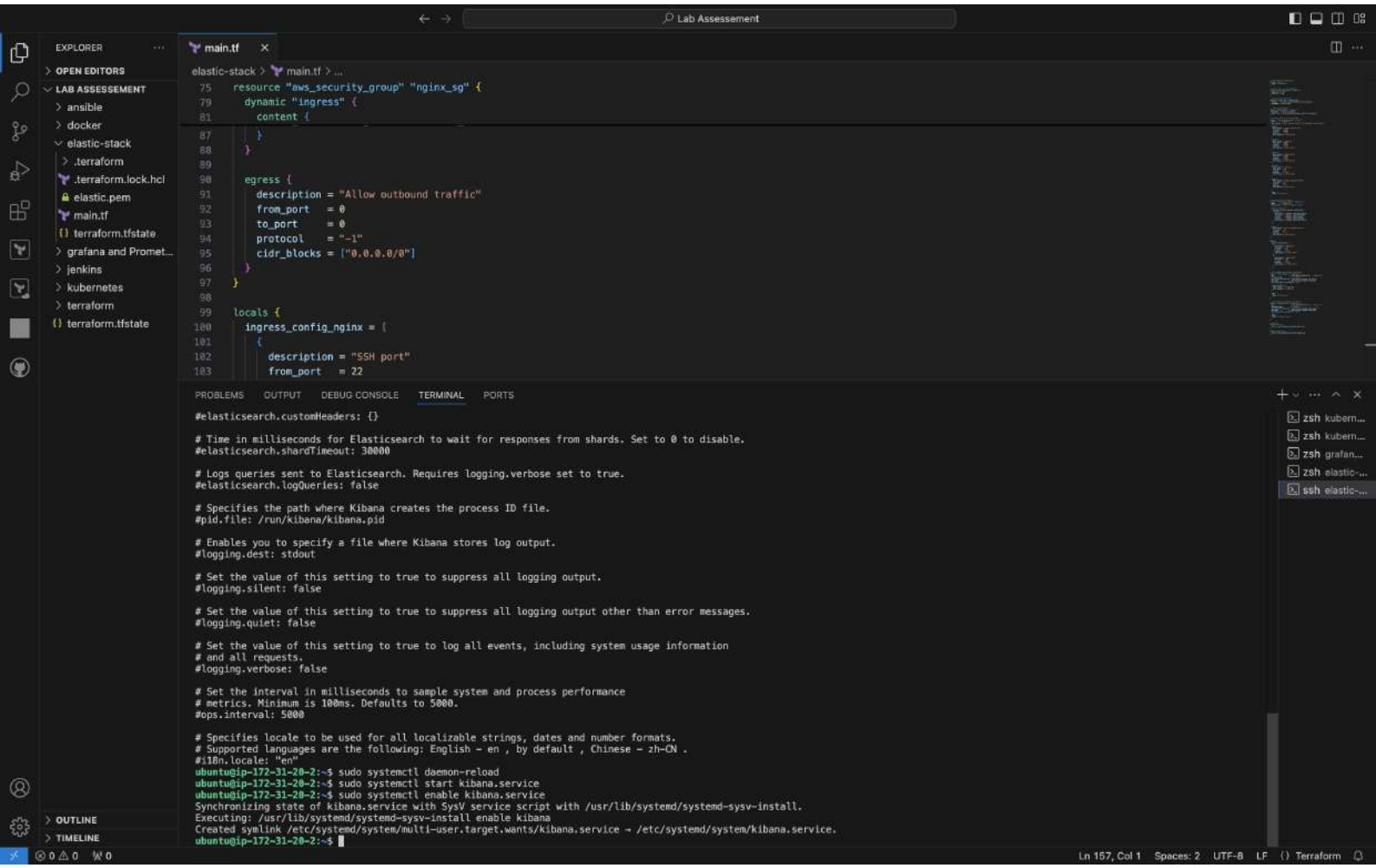

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
IMPORTANT: JVM heap size
The heap size is automatically configured by Elasticsearch
based on the available memory in your system and the roles
each node is configured to fulfill. If specifying heap is
required, it should be done through a file in jvm.options.d,
and the min and max should be set to the same value. For
example, to set the heap to 4 GB, create a new file in the
jvm.options.d directory containing these lines:
-Xms1g
-Xmx1g
See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
for more information
Expert settings
All settings below here are considered expert settings. Do
not adjust them unless you understand what you are doing. Do
not edit them in this file; instead, create a new file in the
jvm.options.d directory containing your adjustments.
GC configuration
8-13:-XX:+UseConcMarkSweepGC
8-13:-XX:CMSInitiatingOccupancyFraction=75
8-13:-XX:+UseCMSInitiatingOccupancyOnly
G1GC Configuration
NOTE: G1 GC is only supported on JDK version 10 or later
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
-Djava.io.tmpdir=${ES_TMPDIR}
heap dumps
generate a heap dump when an allocation from the Java heap fails; heap dumps
are created in the working directory of the JVM unless an alternative path is
specified
-XX:+HeapDumpOnOutOfMemoryError
exit right after heap dump on out of memory error. Recommended to also use
on java 8 for supported versions (8u92+).
9-:-XX:+ExitOnOutOfMemoryError
specify an alternative path for heap dumps; ensure the directory exists and
has sufficient space
-XX:HeapDumpPath=/var/lib/elasticsearch
specify an alternative path for JVM fatal error logs
-XX:ErrorFile=/var/log/elasticsearch/hs_err_pid%p.log
JDK 8 GC logging
8:-XX:+PrintGCDetails
8:-XX:+PrintGCDateStamps
8:-XX:+PrintTenuringDistribution
8:-XX:+PrintGCApplicationStoppedTime
8:-Xloggc:/var/log/elasticsearch/gc.log
8:-XX:+UseGCLogFileRotation
8:-XX:NumberOfGCLogFiles=32
8:-XX:GCLogFileSize=64m
JDK 9+ GC logging
9-:-Xlog:gc*,gc+age=trace,safepoint:file=/var/log/elasticsearch/gc.log:utctime,pid,tags:filecount=32,filesize=64m
workaround G1 bug, see https://bugs.openjdk.org/browse/JDK-8329528
22:-XX:+UnlockDiagnosticVMOptions
22:-XX:G1NumCollectionsKeepPinned=10000000
ubuntu@ip-172-31-20-2:~$ sudo systemctl start elasticsearch.service
ubuntu@ip-172-31-20-2:~$ sudo systemctl enable elasticsearch.service
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
workaround G1 bug, see https://bugs.openjdk.org/browse/JDK-8329528
22:-XX:+UnlockDiagnosticVMOptions
22:-XX:G1NumCollectionsKeepPinned=10000000
ubuntu@ip-172-31-20-2:~$ sudo systemctl start elasticsearch.service
ubuntu@ip-172-31-20-2:~$ sudo systemctl enable elasticsearch.service
Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
ubuntu@ip-172-31-20-2:~$ curl 127.0.0.1:9200
{
"name" : "ip-172-31-20-2",
"cluster_name" : "elasticsearch",
"cluster_uuid" : "LvjgCG5JSfWpxYP45wUVaA",
"version" : {
"number" : "7.17.25",
"build_flavor" : "default",
"build_type" : "deb",
"build_hash" : "f9b6b57d1d0f76e2d14291c04fb50abeb642cfbf",
"build_date" : "2024-10-16T22:06:36.904732810Z",
"build_snapshot" : false,
"lucene_version" : "8.11.3",
"minimum_wire_compatibility_version" : "6.8.0",
"minimum_index_compatibility_version" : "6.0.0-beta1"
},
"tagline" : "You Know, for Search"
}
ubuntu@ip-172-31-20-2:~$ sudo apt-get install kibana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
kibana
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 293 MB of archives.
After this operation, 748 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.25 [293 MB]
4% [1 kibana 16.4 MB/293 MB 6%]
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
"minimum_index_compatibility_version" : "6.0.0-beta1"
},
"tagline" : "You Know, for Search"
}
ubuntu@ip-172-31-20-2:~$ sudo apt-get install kibana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
kibana
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 293 MB of archives.
After this operation, 748 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.25 [293 MB]
Fetched 293 MB in 38s (7805 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 68937 files and directories currently installed.)
Preparing to unpack .../kibana_7.17.25_amd64.deb ...
Unpacking kibana (7.17.25) ...
Setting up kibana (7.17.25) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/7.17/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$ sudo cp /etc/kibana/kibana.yml /etc/kibana/kibana.yml.bak
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
ubuntu@ip-172-31-20-2:~$ sudo sed -i 's/^#server.host: .*/server.host: "0.0.0.0"/' /etc/kibana/kibana.yml
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/kibana/kibana.yml
Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601
Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
The default is 'localhost', which usually means remote machines will not be able to connect.
To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"
Enables you to specify a path to mount Kibana at if you are running behind a proxy.
Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
from requests it receives, and to prevent a deprecation warning at startup.
This setting cannot end in a slash.
#server.basePath: ""
Specifies whether Kibana should rewrite requests that are prefixed with
`server.basePath` or require that they are rewritten by your reverse proxy.
This setting was effectively always `false` before Kibana 6.3 and will
default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false
Specifies the public URL at which Kibana is available for end users. If
`server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""
The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576
The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"
The URLs of the Elasticsearch instances to use for all your queries.
#elasticsearch.hosts: ["http://localhost:9200"]
Kibana uses an index in Elasticsearch to store saved searches, visualizations and
dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
#elasticsearch.customHeaders: {}
Time in milliseconds for Elasticsearch to wait for responses from shards. Set to 0 to disable.
#elasticsearch.shardTimeout: 30000
Logs queries sent to Elasticsearch. Requires logging.verbose set to true.
#elasticsearch.logQueries: false
Specifies the path where Kibana creates the process ID file.
#pid.file: /run/kibana/kibana.pid
Enables you to specify a file where Kibana stores log output.
#logging.dest: stdout
Set the value of this setting to true to suppress all logging output.
#logging.silent: false
Set the value of this setting to true to suppress all logging output other than error messages.
#logging.quiet: false
Set the value of this setting to true to log all events, including system usage information
and all requests.
#logging.verbose: false
Set the interval in milliseconds to sample system and process performance
metrics. Minimum is 100ms. Defaults to 5000.
#ops.interval: 5000
Specifies locale to be used for all localizable strings, dates and number formats.
Supported languages are the following: English - en , by default , Chinese - zh-CN .
#i18n.locale: "en"
ubuntu@ip-172-31-20-2:~$ sudo systemctl daemon-reload
ubuntu@ip-172-31-20-2:~$ sudo systemctl start kibana.service
ubuntu@ip-172-31-20-2:~$ sudo systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

Not Secure 3.8.238.97:5601/app/home#/

inksnation | Xender Web Infinix | Free PSD | Digital... | Free Best Powerp... | Slack | graphics | F... | (277) Pinterest us... | Transparent Stars... | Inches to Pixels C... | The Making of a M... | All Bookmarks

Welcome to Elastic

Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and protect against security threats.

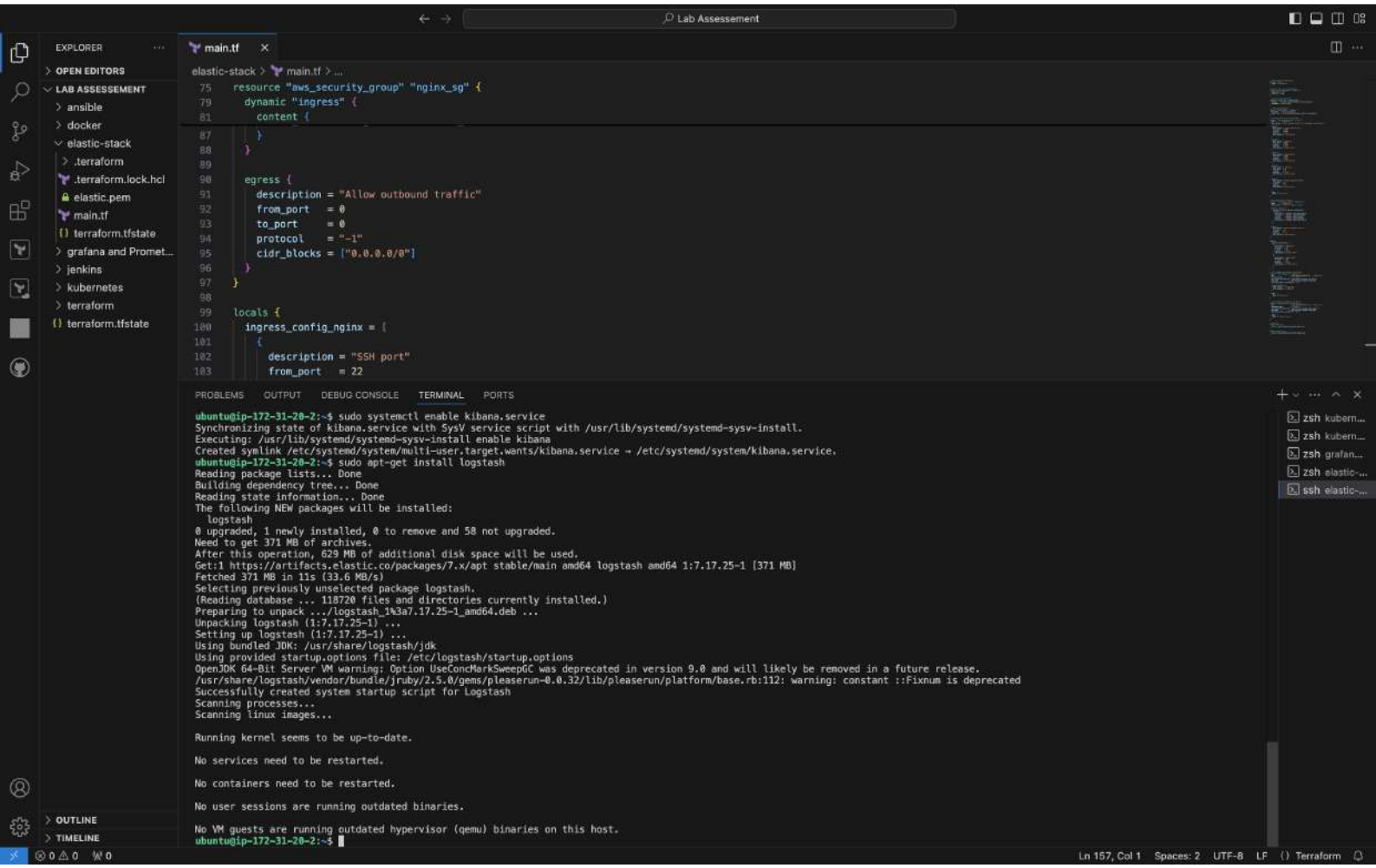
Add integrations | Explore on my own

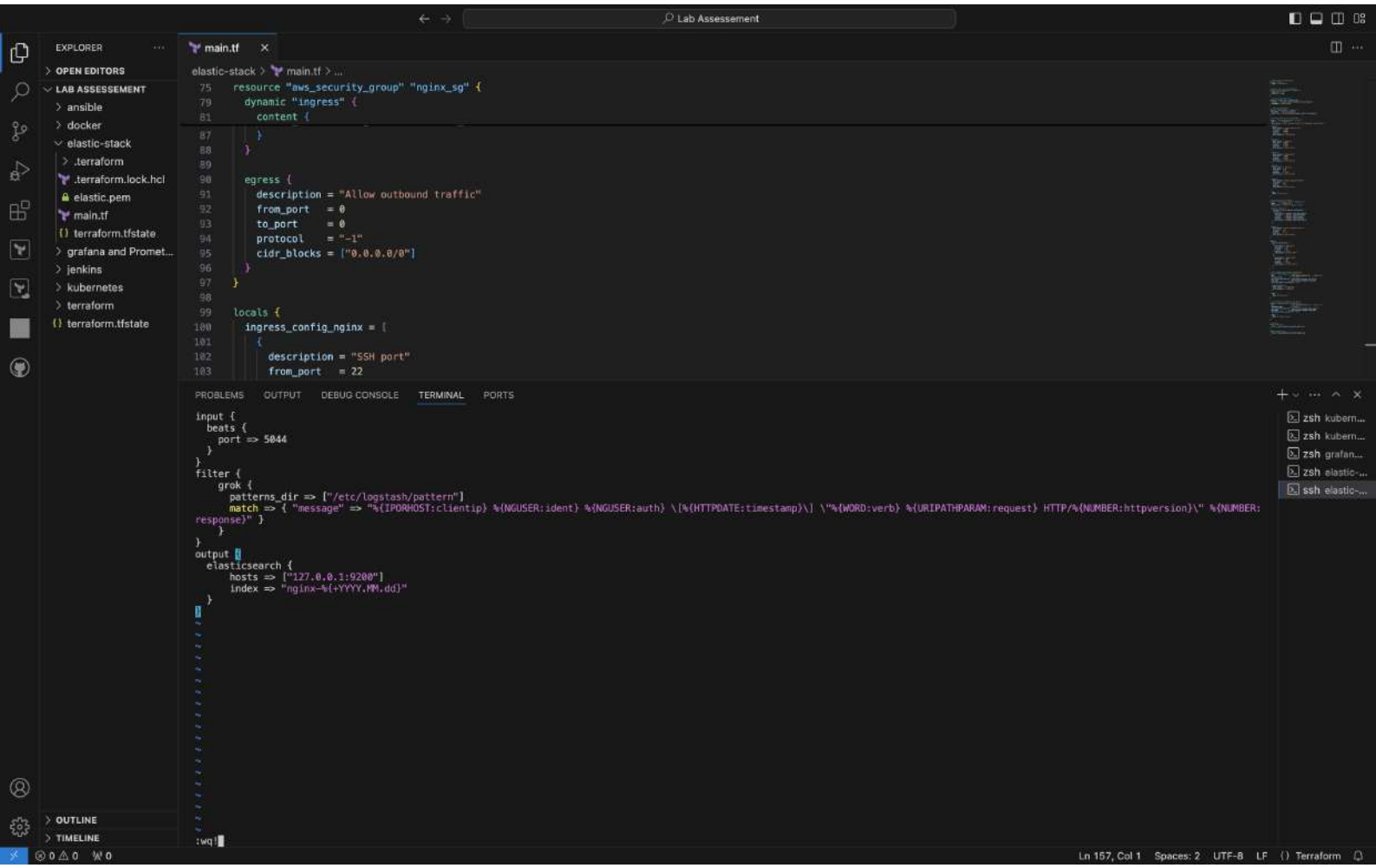
To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

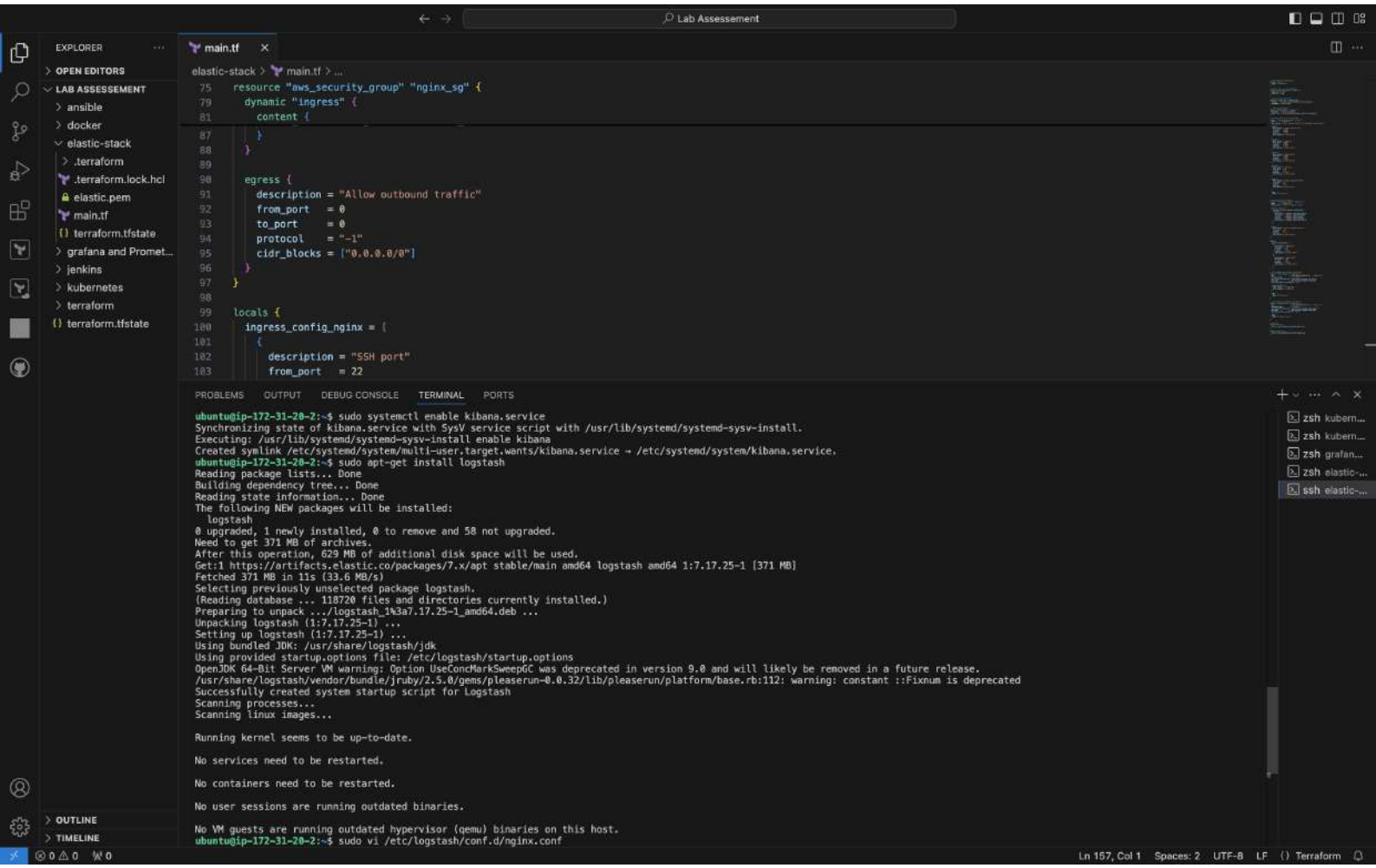
Configuration missing

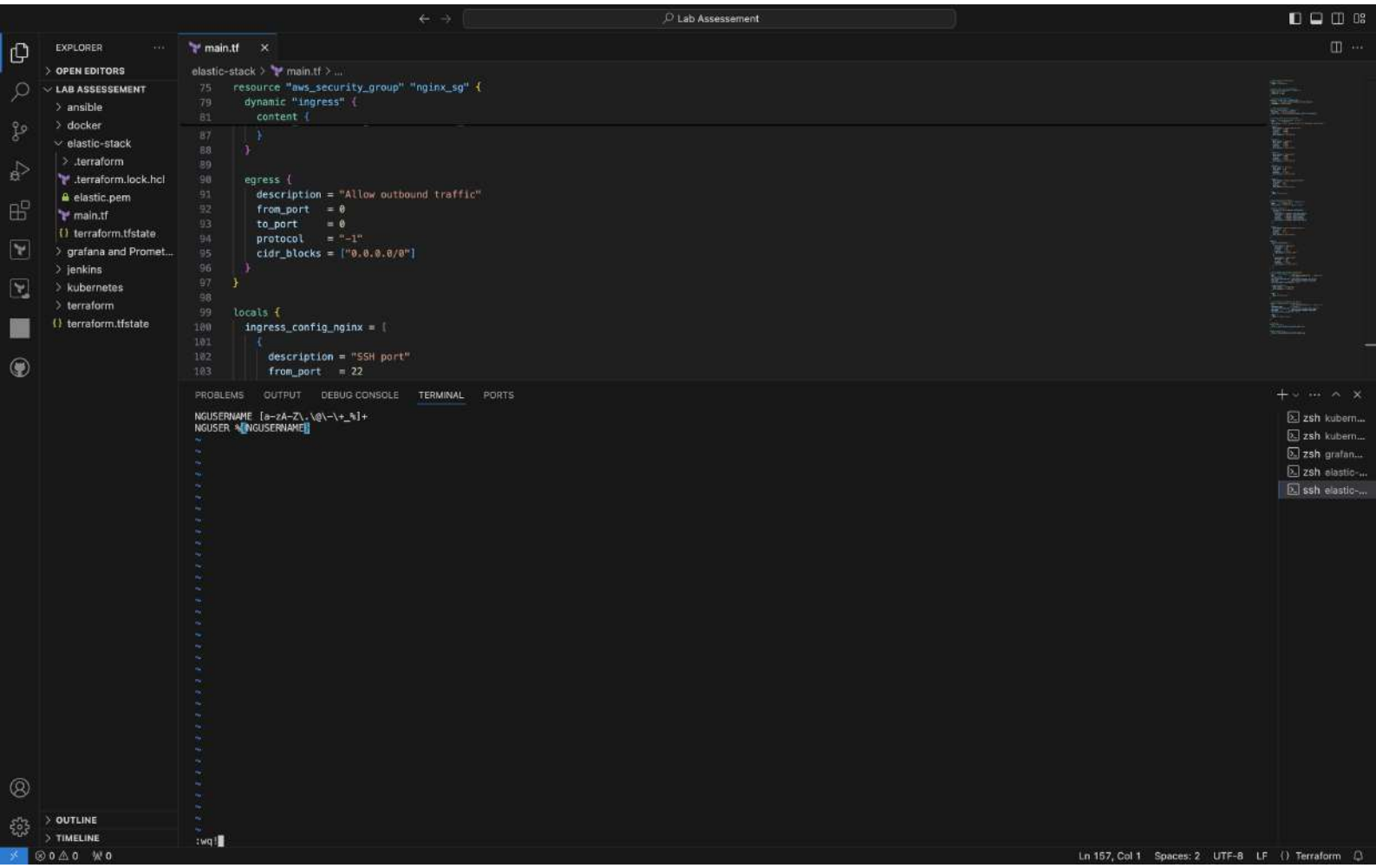
`server.publicBaseUrl` is missing and should be configured when running in a production environment. Some features may not behave correctly. See the documentation.

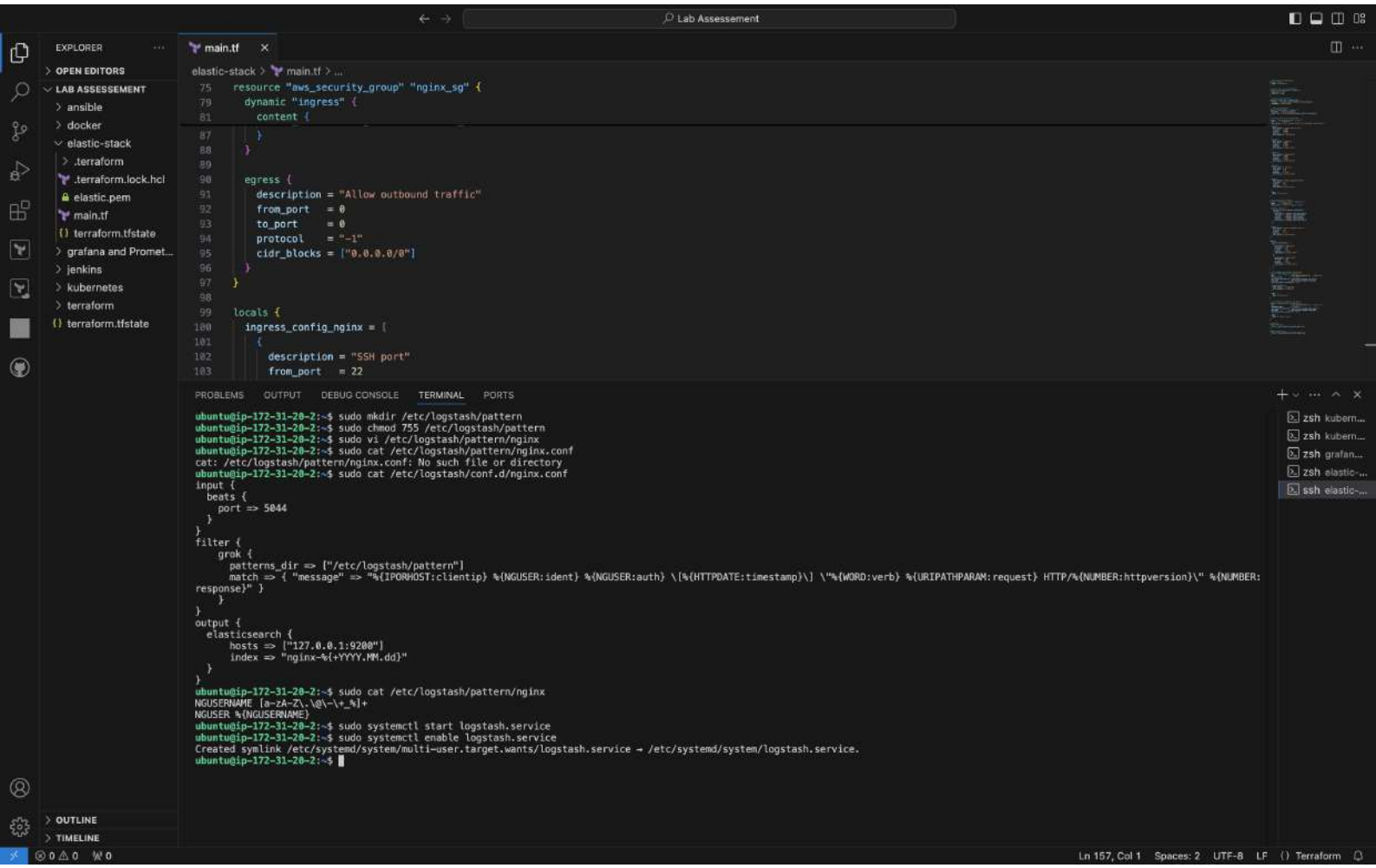
Mute warning

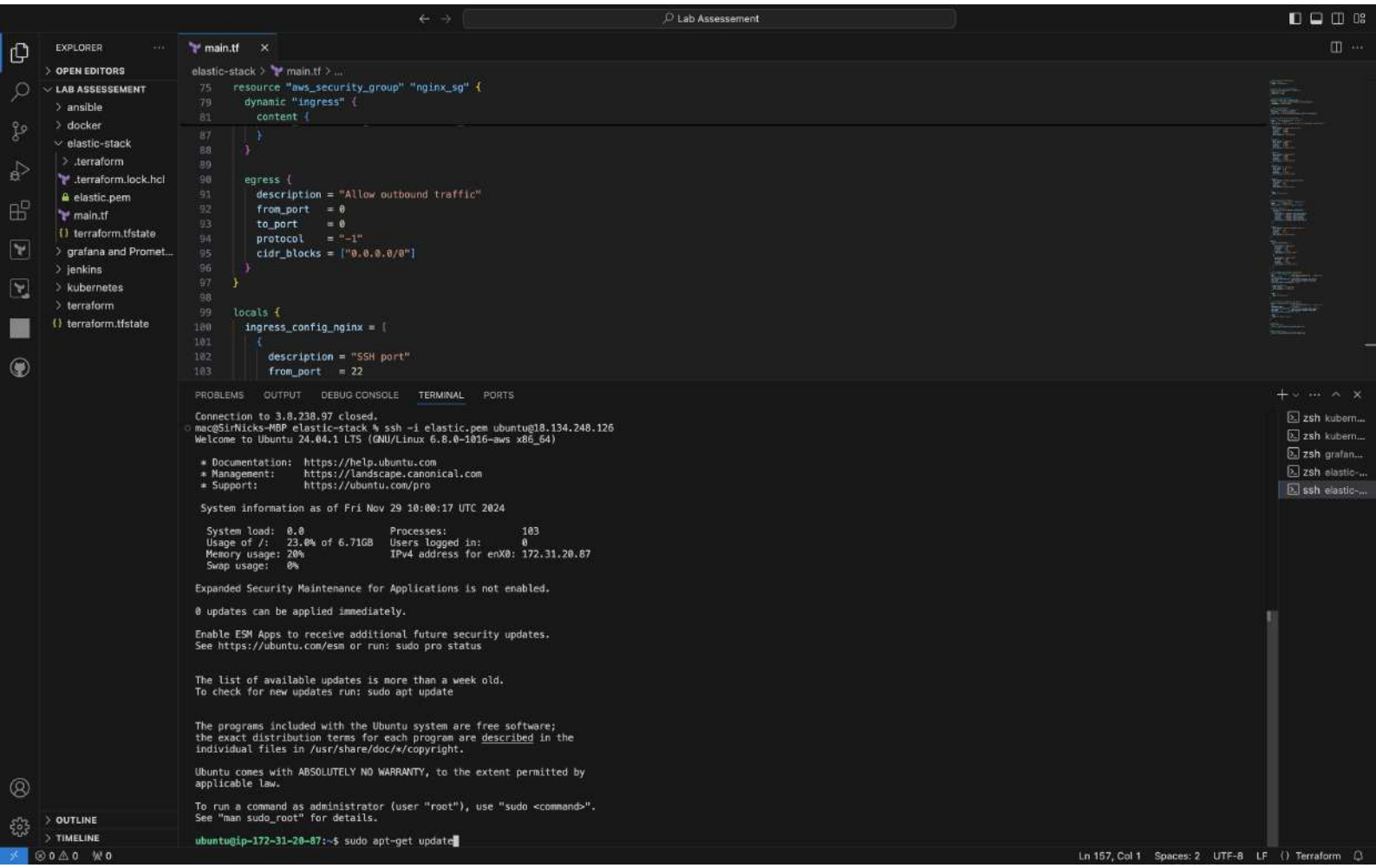

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
ubuntu@ip-172-31-20-2:~$ sudo systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
ubuntu@ip-172-31-20-2:~$ sudo apt-get install logstash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
logstash
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 371 MB of archives.
After this operation, 629 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash amd64 1:7.17.25-1 [371 MB]
Fetched 371 MB in 11s (33.6 MB/s)
Selecting previously unselected package logstash.
(Reading database ... 118720 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.17.25-1_amd64.deb ...
Unpacking logstash (1:7.17.25-1) ...
Setting up logstash (1:7.17.25-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

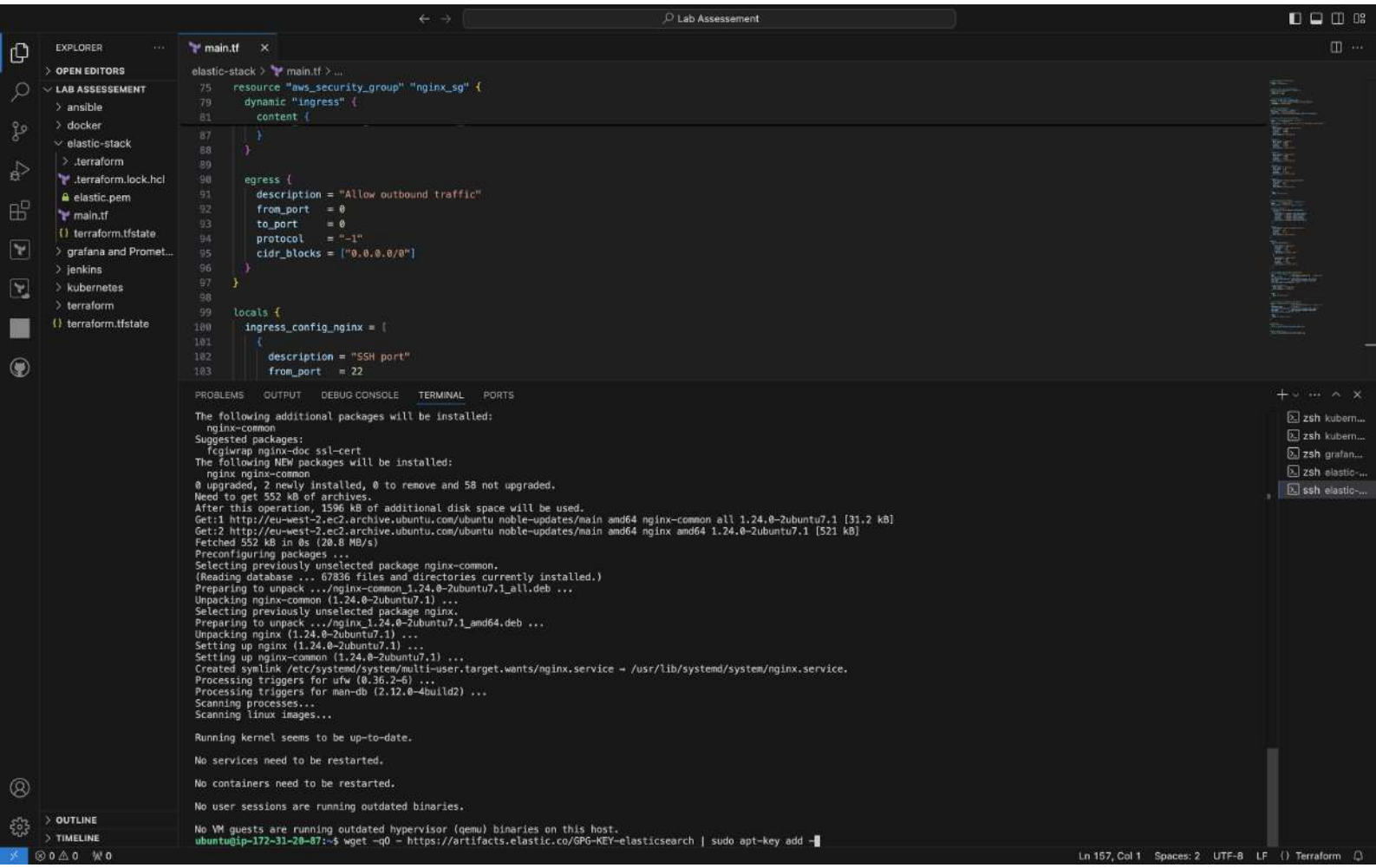

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
input {
beats {
port => 5044
}
}
filter {
grok {
patterns_dir => ["/etc/logstash/pattern"]
match => { "message" => "%{IPORHOST:clientip} %{NGUSER:ident} %{NGUSER:auth} \[%{HTTPDATE:timestamp}\] \"%{WORD:verb} %{URIPATHPARAM:request} HTTP/%{NUMBER:httpversion}\" %{NUMBER:
response}" }
}
}
output {
elasticsearch {
hosts => ["127.0.0.1:9200"]
index => "nginx-%{+YYYY.MM.dd}"
}
}
:wq!
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

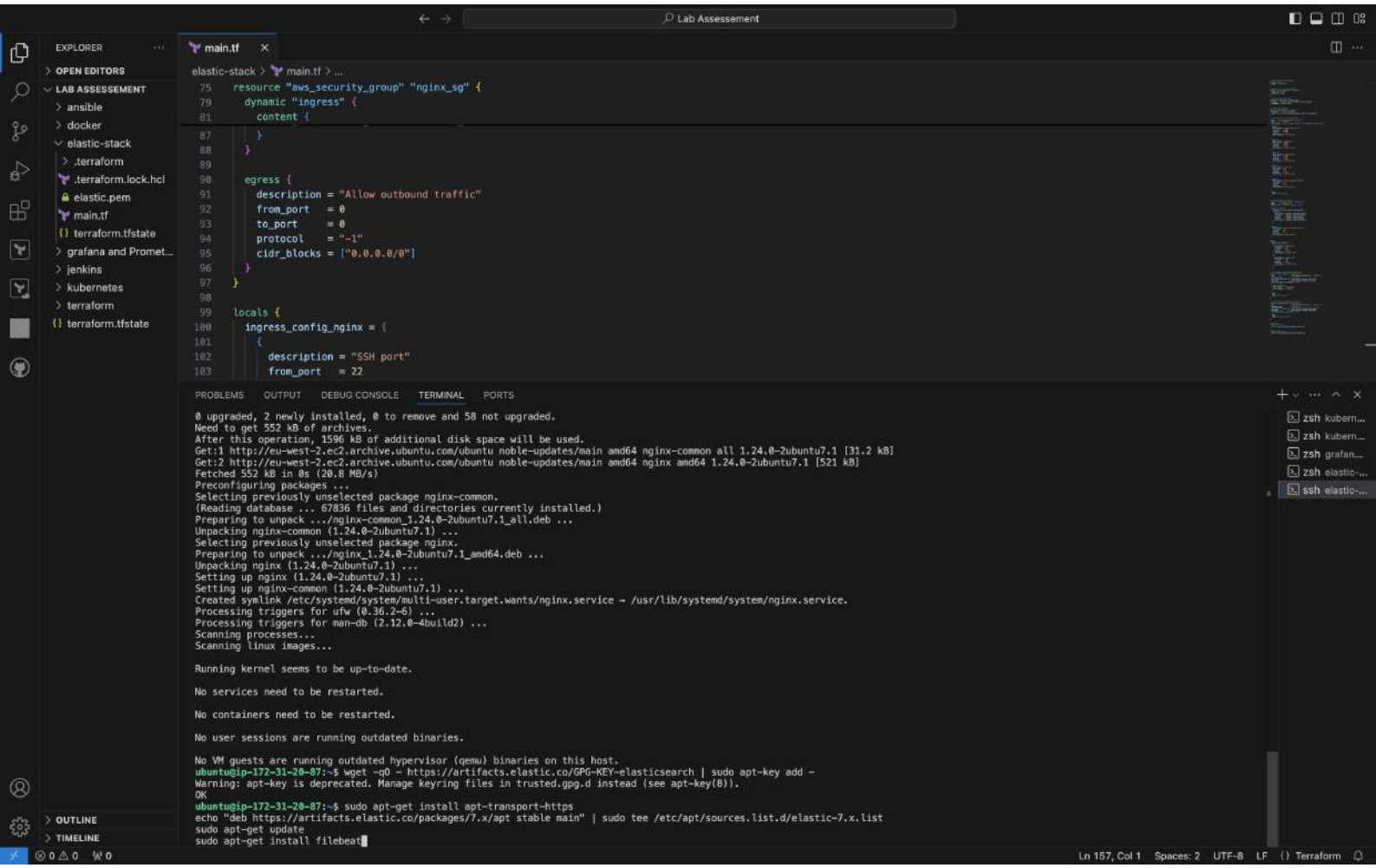

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
ubuntu@ip-172-31-20-2:~$ sudo systemctl enable kibana.service
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
ubuntu@ip-172-31-20-2:~$ sudo apt-get install logstash
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
logstash
0 upgraded, 1 newly installed, 0 to remove and 58 not upgraded.
Need to get 371 MB of archives.
After this operation, 629 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash amd64 1:7.17.25-1 [371 MB]
Fetched 371 MB in 11s (33.6 MB/s)
Selecting previously unselected package logstash.
(Reading database ... 118720 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.17.25-1_amd64.deb ...
Unpacking logstash (1:7.17.25-1) ...
Setting up logstash (1:7.17.25-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-2:~$ sudo vi /etc/logstash/conf.d/nginx.conf
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

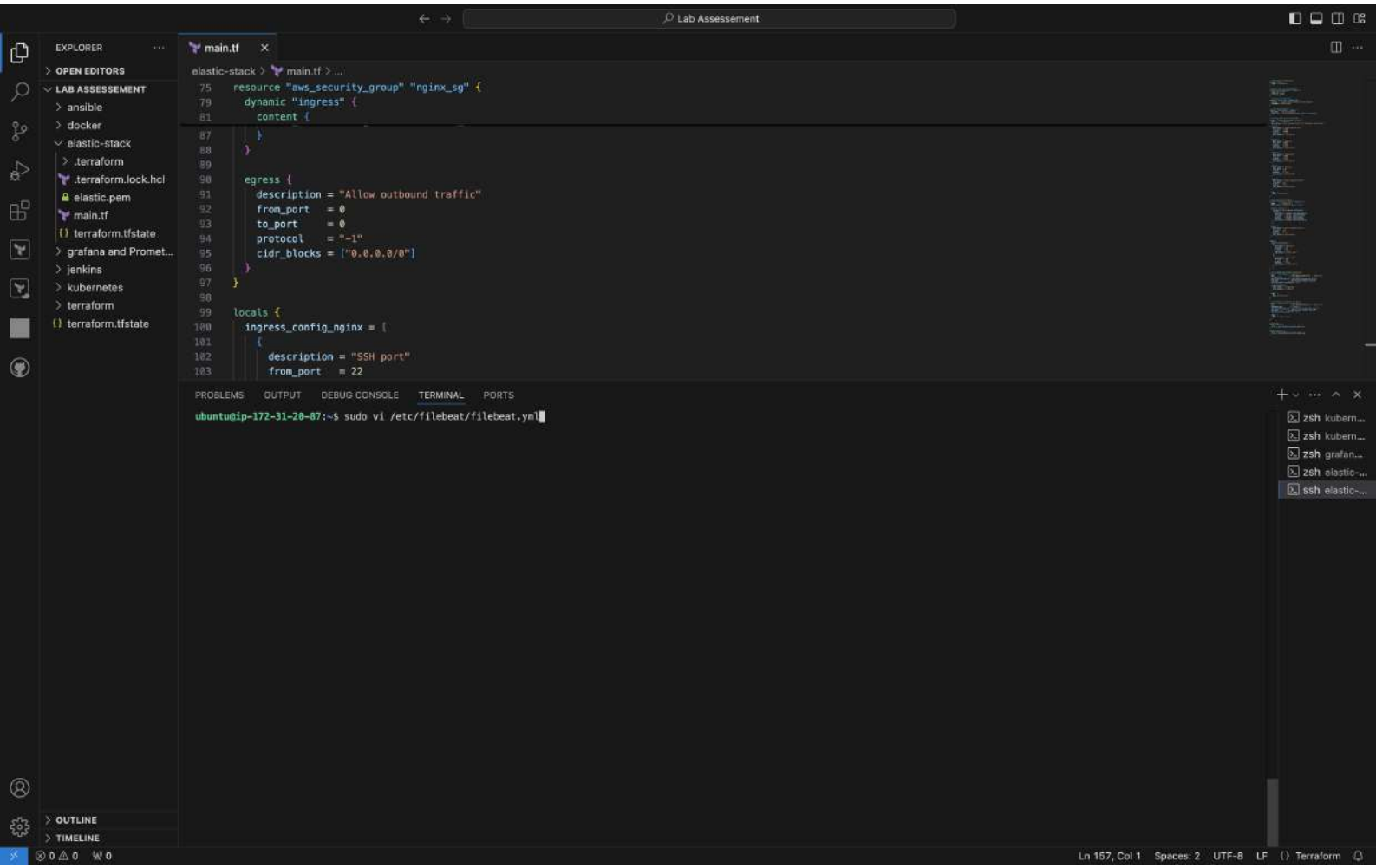

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
NGUSERNAME [a-zA-Z\.\@\-\+_%]+
NGUSER *(NGUSERNAME)
:wq!
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

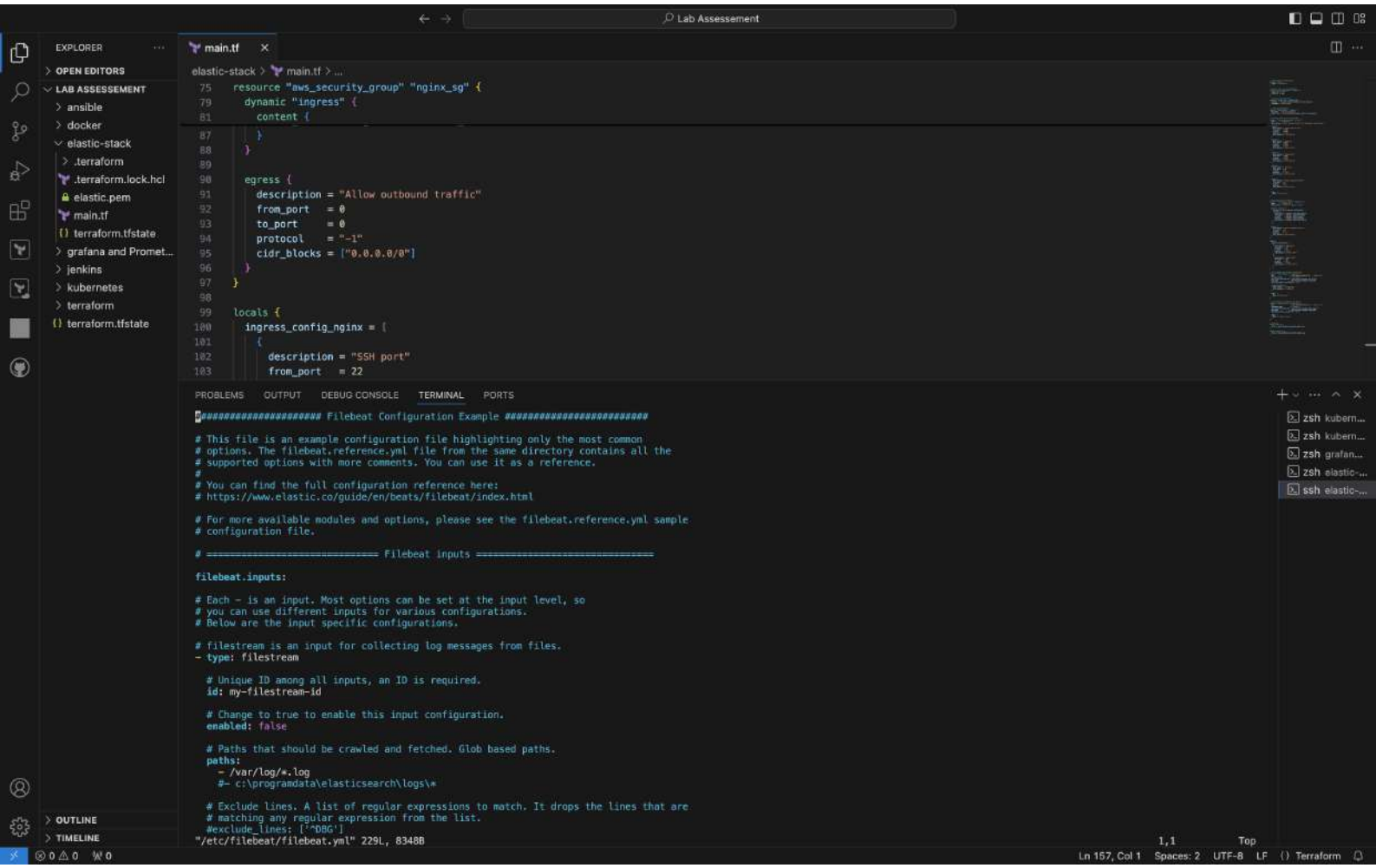

Lab Assessement
EXPLORER
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
main.tf
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
ubuntu@ip-172-31-20-2:~$ sudo mkdir /etc/logstash/pattern
ubuntu@ip-172-31-20-2:~$ sudo chmod 755 /etc/logstash/pattern
ubuntu@ip-172-31-20-2:~$ sudo vi /etc/logstash/pattern/nginx
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/logstash/pattern/nginx.conf
cat: /etc/logstash/pattern/nginx.conf: No such file or directory
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/logstash/conf.d/nginx.conf
input {
beats {
port => 5044
}
}
filter {
grok {
patterns_dir => ["/etc/logstash/pattern"]
match => { "message" => "%{IPORHOST:clientip} %{NGUSER:ident} %{NGUSER:auth} \[%{HTTPDATE:timestamp}\] \"%{WORD:verb} %{URIPATHPARAM:request} HTTP/%{NUMBER:httpversion}\" %{NUMBER:
response}" }
}
}
output {
elasticsearch {
hosts => ["127.0.0.1:9200"]
index => "nginx-%{+YYYY.MM.dd}"
}
}
ubuntu@ip-172-31-20-2:~$ sudo cat /etc/logstash/pattern/nginx
NGUSERNAME [a-zA-Z\.\@\-\+_%]+
NGUSER %{NGUSERNAME}
ubuntu@ip-172-31-20-2:~$ sudo systemctl start logstash.service
ubuntu@ip-172-31-20-2:~$ sudo systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /etc/systemd/system/logstash.service.
ubuntu@ip-172-31-20-2:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

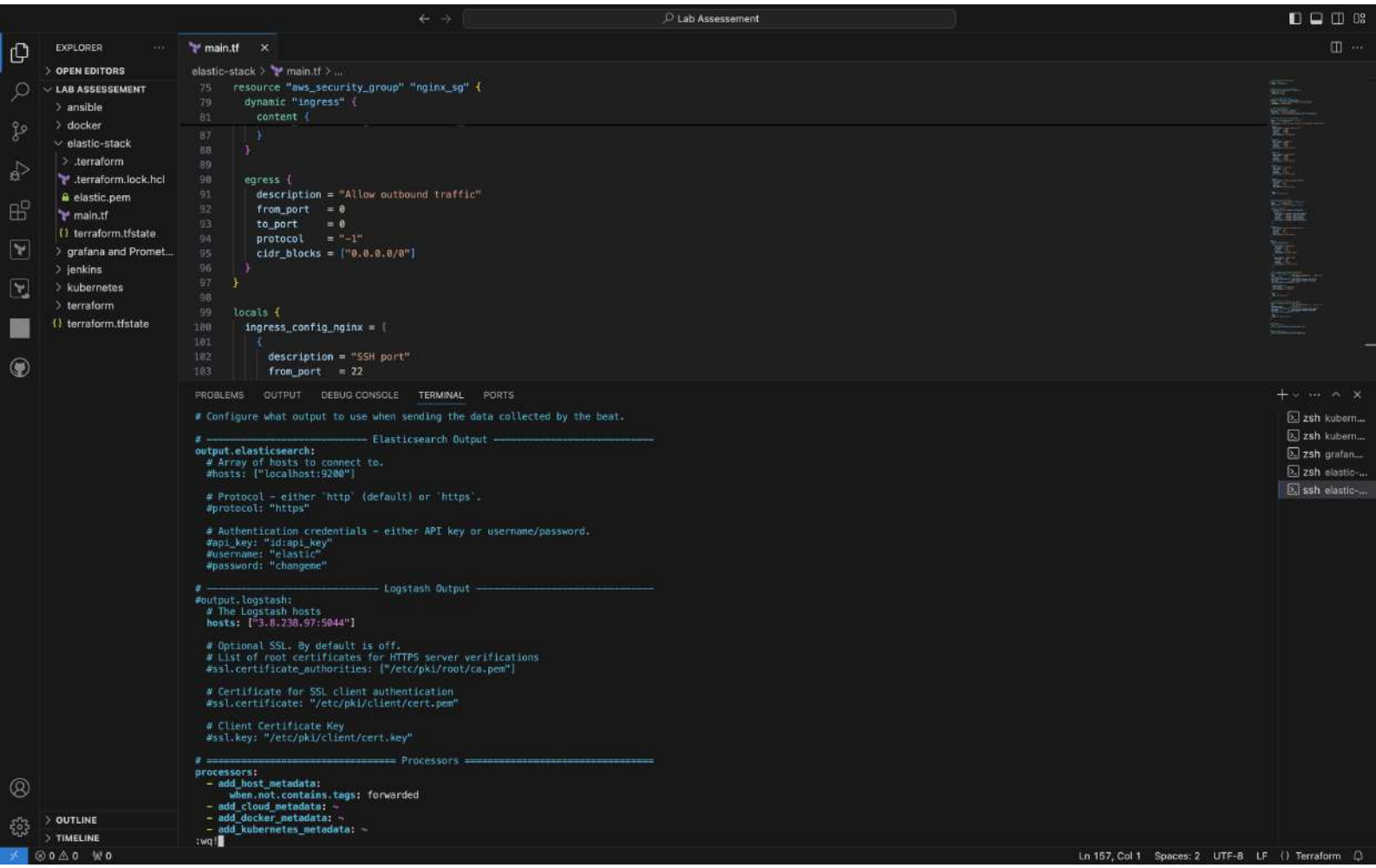

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Connection to 3.8.238.97 closed.
mac@SirNicks-MBP elastic-stack % ssh -i elastic.pem ubuntu@18.134.248.126
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Fri Nov 29 10:00:17 UTC 2024
System load: 0.0
Usage of /: 23.0% of 6.71GB
Memory usage: 20%
Swap usage: 0%
Processes: 103
Users logged in: 0
IPv4 address for enX0: 172.31.20.87
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
ubuntu@ip-172-31-20-87:~$ sudo apt-get update
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

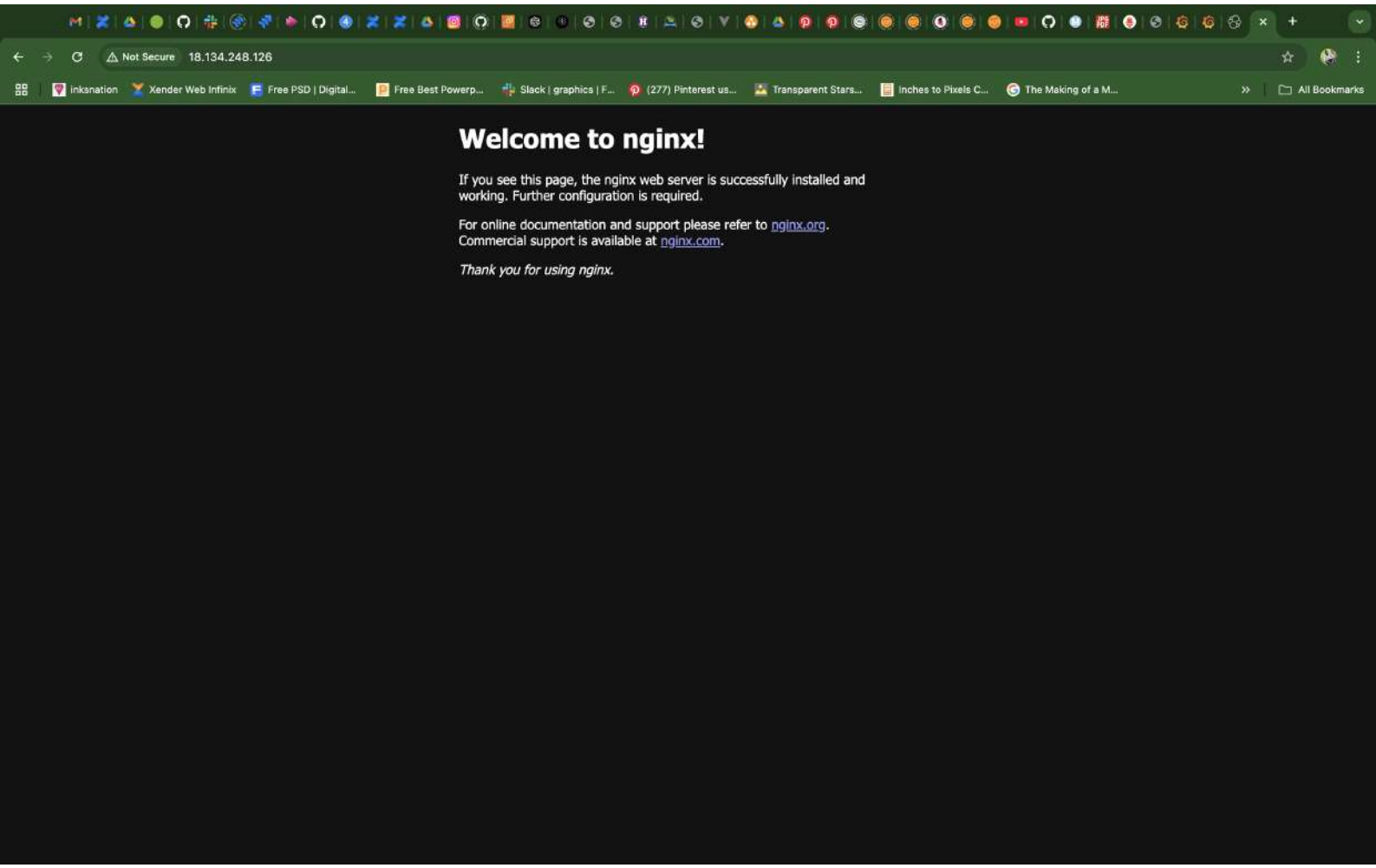

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
The following additional packages will be installed:
nginx-common
Suggested packages:
fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
nginx nginx-common
0 upgraded, 2 newly installed, 0 to remove and 58 not upgraded.
Need to get 552 kB of archives.
After this operation, 1596 kB of additional disk space will be used.
Get:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx-common all 1.24.0-2ubuntu7.1 [31.2 kB]
Get:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx amd64 1.24.0-2ubuntu7.1 [521 kB]
Fetched 552 kB in 0s (20.8 MB/s)
Preconfiguring packages ...
Selecting previously unselected package nginx-common.
(Reading database ... 67836 files and directories currently installed.)
Preparing to unpack .../nginx-common_1.24.0-2ubuntu7.1_all.deb ...
Unpacking nginx-common (1.24.0-2ubuntu7.1) ...
Selecting previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2ubuntu7.1_amd64.deb ...
Unpacking nginx (1.24.0-2ubuntu7.1) ...
Setting up nginx (1.24.0-2ubuntu7.1) ...
Setting up nginx-common (1.24.0-2ubuntu7.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-87:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

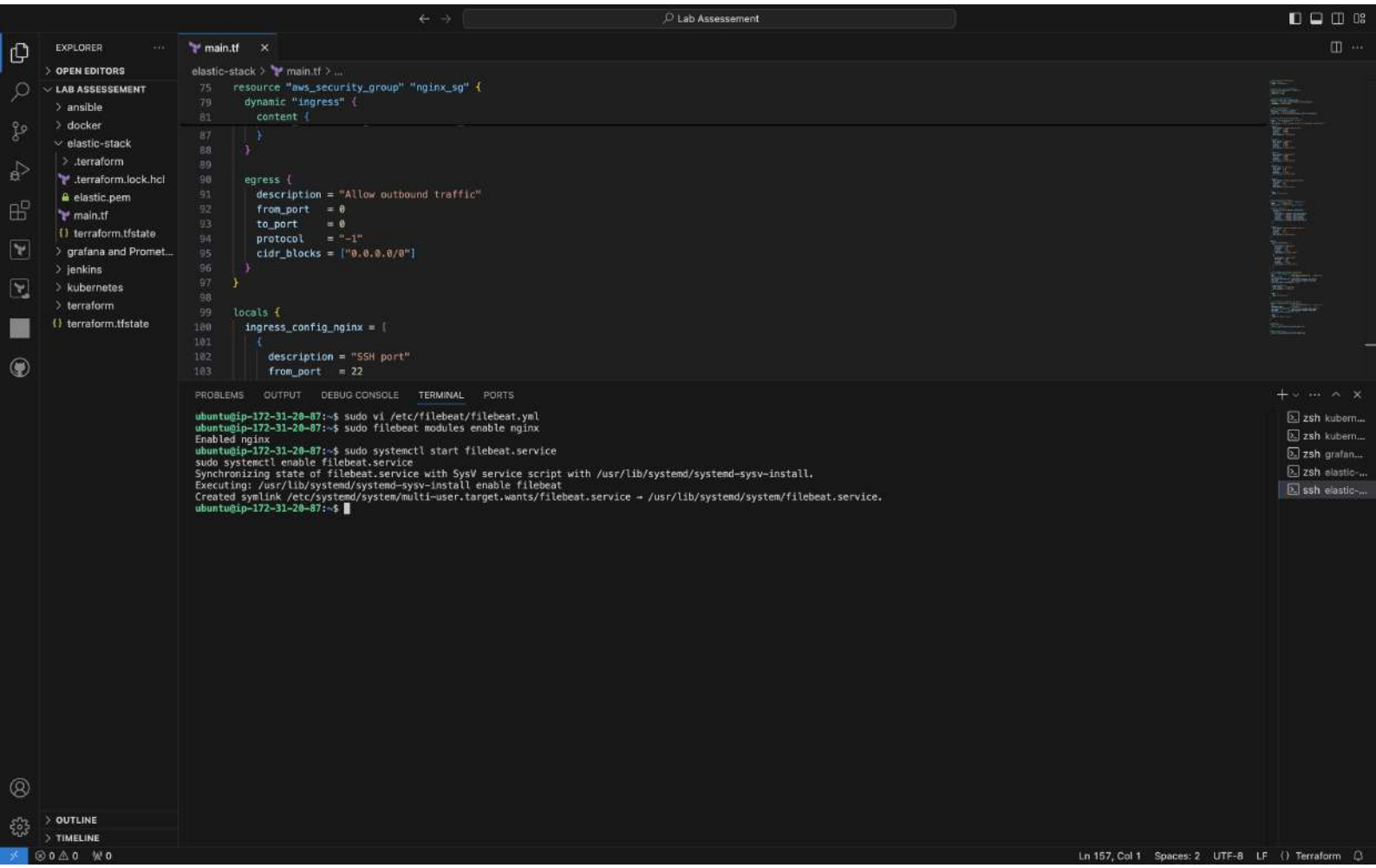

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
0 upgraded, 2 newly installed, 0 to remove and 58 not upgraded.
Need to get 552 kB of archives.
After this operation, 1596 kB of additional disk space will be used.
Get:1 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx-common all 1.24.0-2ubuntu7.1 [31.2 kB]
Get:2 http://eu-west-2.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx amd64 1.24.0-2ubuntu7.1 [521 kB]
Fetched 552 kB in 0s (20.8 MB/s)
Preconfiguring packages ...
Selecting previously unselected package nginx-common.
(Reading database ... 67836 files and directories currently installed.)
Preparing to unpack .../nginx-common_1.24.0-2ubuntu7.1_all.deb ...
Unpacking nginx-common (1.24.0-2ubuntu7.1) ...
Selecting previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2ubuntu7.1_amd64.deb ...
Unpacking nginx (1.24.0-2ubuntu7.1) ...
Setting up nginx (1.24.0-2ubuntu7.1) ...
Setting up nginx-common (1.24.0-2ubuntu7.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-87:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
ubuntu@ip-172-31-20-87:~$ sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
sudo apt-get update
sudo apt-get install filebeat
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

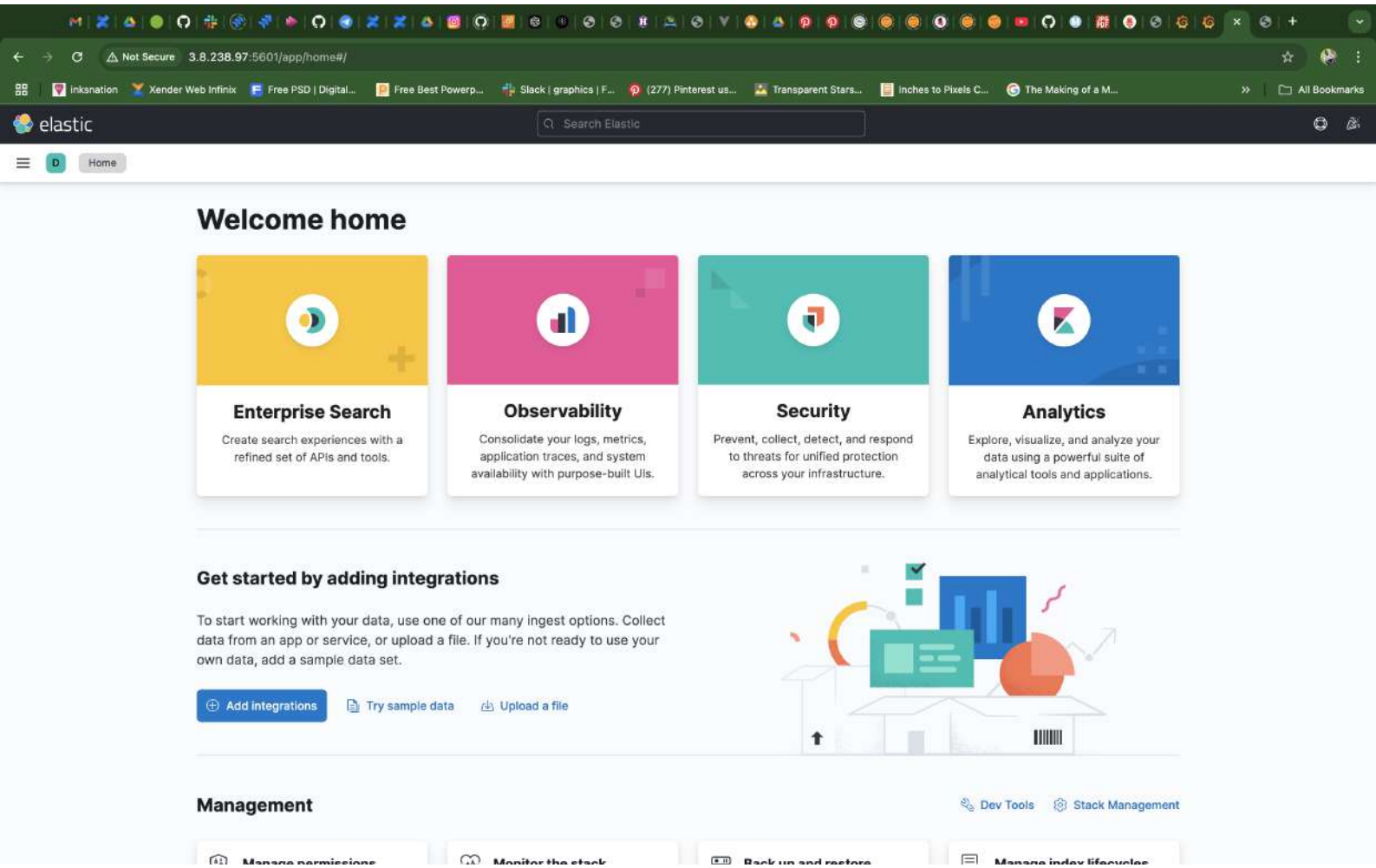

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
ubuntu@ip-172-31-20-87:~$ sudo vi /etc/filebeat/filebeat.yml
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

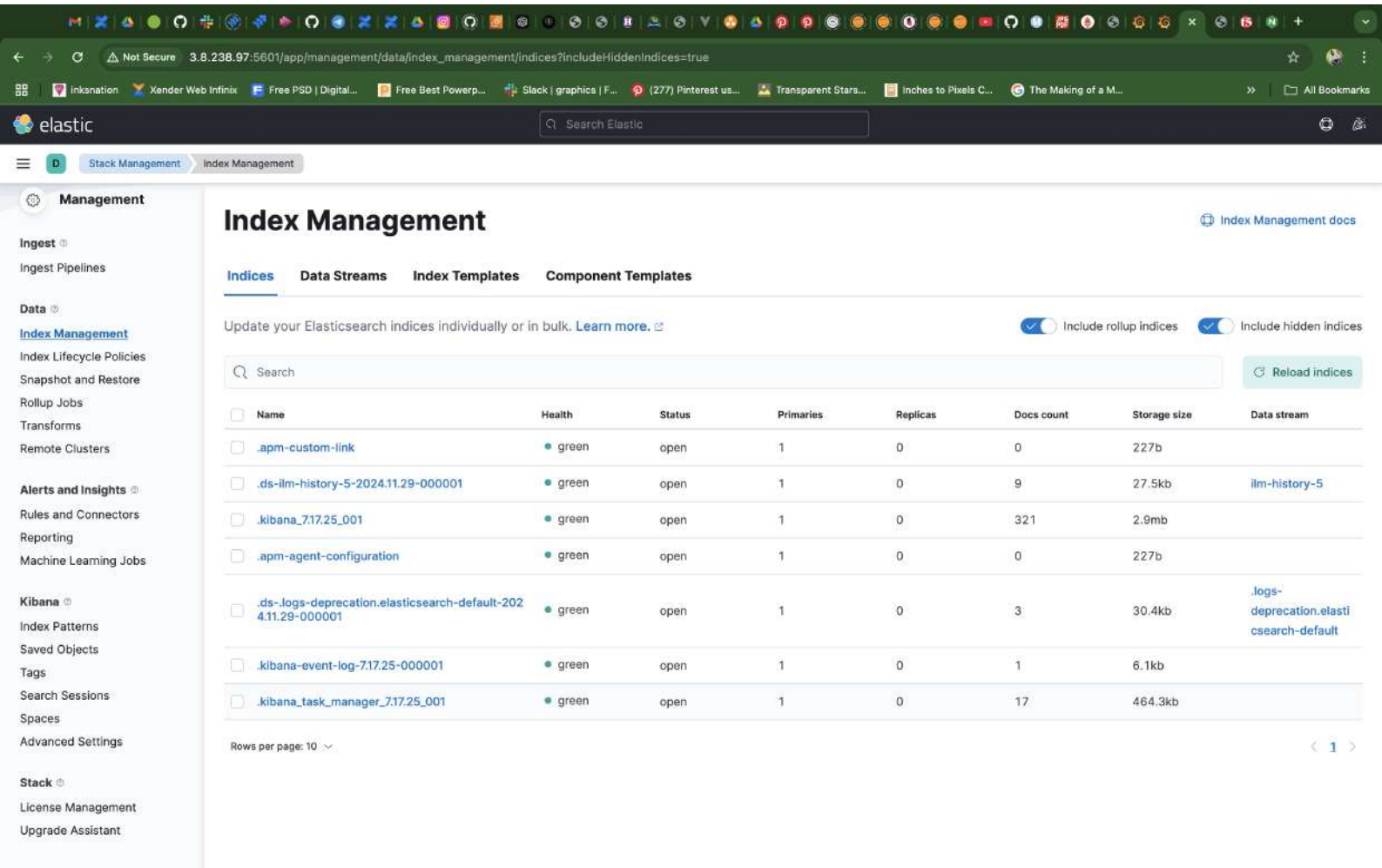

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
########## Filebeat Configuration Example ##########
This file is an example configuration file highlighting only the most common
options. The filebeat.reference.yml file from the same directory contains all the
supported options with more comments. You can use it as a reference.
#
You can find the full configuration reference here:
https://www.elastic.co/guide/en/beats/filebeat/index.html
For more available modules and options, please see the filebeat.reference.yml sample
configuration file.
============================== Filebeat inputs ===============================
filebeat.inputs:
Each - is an input. Most options can be set at the input level, so
you can use different inputs for various configurations.
Below are the input specific configurations.
filestream is an input for collecting log messages from files.
- type: filestream
Unique ID among all inputs, an ID is required.
id: my-filestream-id
Change to true to enable this input configuration.
enabled: false
Paths that should be crawled and fetched. Glob based paths.
paths:
- /var/log/*.log
#- c:\programdata\elasticsearch\logs*
Exclude lines. A list of regular expressions to match. It drops the lines that are
matching any regular expression from the list.
#exclude_lines: ['^DBG']
"/etc/filebeat/filebeat.yml" 229L, 8348B
1,1
Top
OUTLINE
TIMELINE
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform

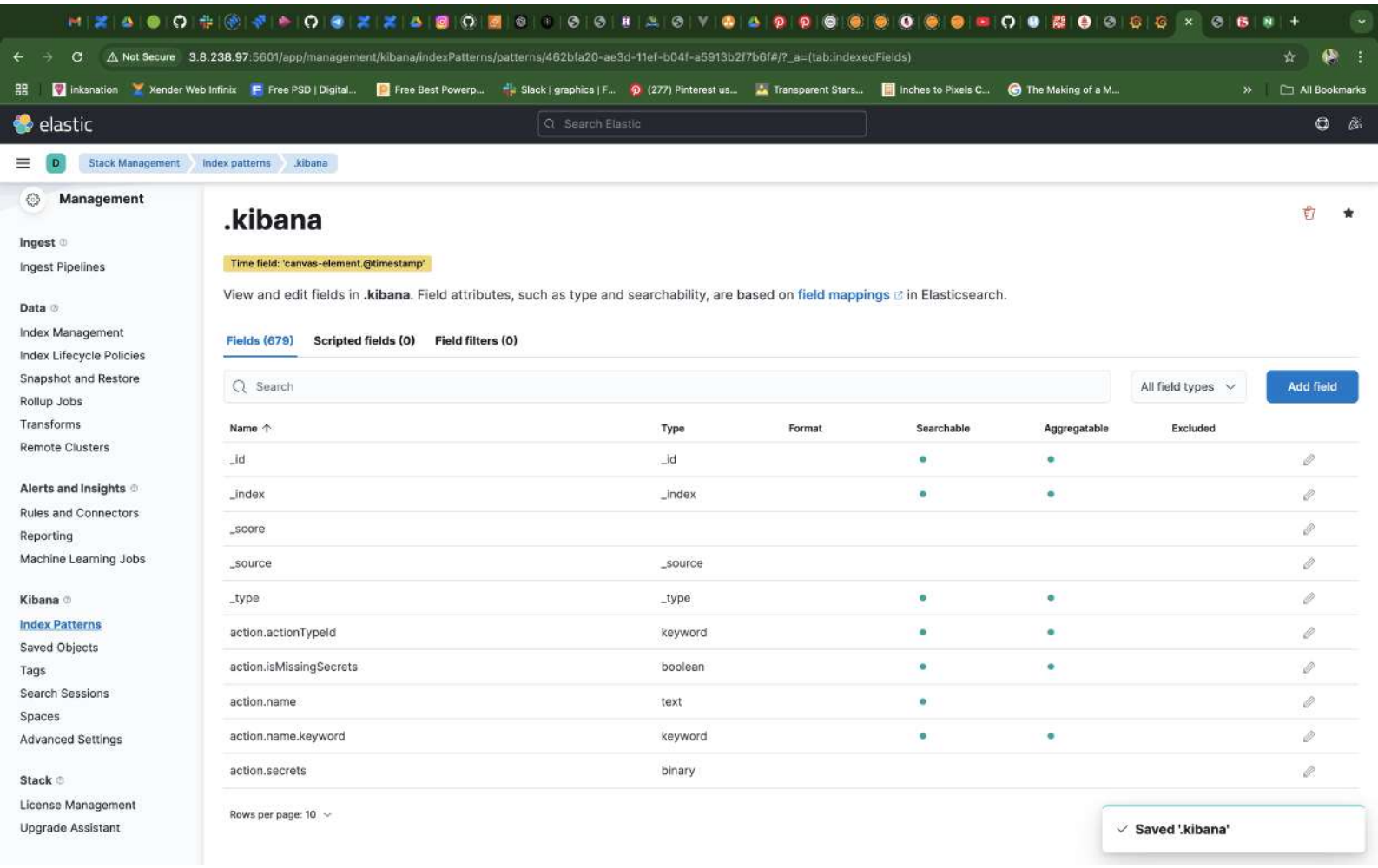

Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
Configure what output to use when sending the data collected by the beat.
---------------------------- Elasticsearch Output ----------------------------
output.elasticsearch:
Array of hosts to connect to.
#hosts: ["localhost:9200"]
Protocol - either `http` (default) or `https`.
#protocol: "https"
Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
#username: "elastic"
#password: "changeme"
------------------------------ Logstash Output -------------------------------
#output.logstash:
The Logstash hosts
hosts: ["3.8.230.97:5044"]
Optional SSL. By default is off.
List of root certificates for HTTPS server verifications
#ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]
Certificate for SSL client authentication
#ssl.certificate: "/etc/pki/client/cert.pem"
Client Certificate Key
#ssl.key: "/etc/pki/client/cert.key"
================================= Processors =================================
processors:
- add_host_metadata:
when.not.contains.tags: forwarded
- add_cloud_metadata: ~
- add_docker_metadata: ~
- add_kubernetes_metadata: ~
:wq!
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Not Secure
18.134.248.126
Inksnation
Xender Web Infinix
Free PSD | Digital...
Free Best Powerp...
Slack | graphics | F...
(277) Pinterest us...
Transparent Stars...
Inches to Pixels C...
The Making of a M...
All Bookmarks
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.


Lab Assessement
EXPLORER
main.tf
OPEN EDITORS
LAB ASSESSEMENT
ansible
docker
elastic-stack
.terraform
.terraform.lock.hcl
elastic.pem
main.tf
terraform.tfstate
grafana and Promet...
jenkins
kubernetes
terraform
terraform.tfstate
OUTLINE
TIMELINE
elastic-stack > main.tf > ...
resource "aws_security_group" "nginx_sg" {
dynamic "ingress" {
content {
}
}
egress {
description = "Allow outbound traffic"
from_port = 0
to_port = 0
protocol = "-1"
cidr_blocks = ["0.0.0.0/0"]
}
}
locals {
ingress_config_nginx = [
{
description = "SSH port"
from_port = 22
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
ubuntu@ip-172-31-20-87:~$ sudo vi /etc/filebeat/filebeat.yml
ubuntu@ip-172-31-20-87:~$ sudo filebeat modules enable nginx
Enabled nginx
ubuntu@ip-172-31-20-87:~$ sudo systemctl start filebeat.service
sudo systemctl enable filebeat.service
Synchronizing state of filebeat.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /usr/lib/systemd/system/filebeat.service.
ubuntu@ip-172-31-20-87:~$
zsh kubern...
zsh kubern...
zsh grafan...
zsh elastic-...
ssh elastic-...
Ln 157, Col 1
Spaces: 2
UTF-8
LF
Terraform


Not Secure 3.8.238.97:5601/app/home#/
elastic
Search Elastic
Home
Welcome home
Enterprise Search
Create search experiences with a refined set of APIs and tools.
Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.
Get started by adding integrations
To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.
Add integrations
Try sample data
Upload a file
Management
Dev Tools
Stack Management


Not Secure 3.8.238.97:5601/app/management/data/index_management/indices?includeHiddenIndices=true
elastic
Search Elastic
Stack Management
Index Management
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
Index Management
Index Management docs
Indices
Data Streams
Index Templates
Component Templates
Update your Elasticsearch indices individually or in bulk. Learn more.
Include rollup indices
Include hidden indices
Search
Reload indices
Name
Health
Status
Primaries
Replicas
Docs count
Storage size
Data stream
.apm-custom-link
green
open
1
0
0
227b
.ds-ilm-history-5-2024.11.29-000001
green
open
1
0
9
27.5kb
ilm-history-5
.kibana_7.17.25_001
green
open
1
0
321
2.9mb
.apm-agent-configuration
green
open
1
0
0
227b
.ds-.logs-deprecation.elasticsearch-default-2024.11.29-000001
green
open
1
0
3
30.4kb
.logs-deprecation.elasticsearch-default
.kibana-event-log-7.17.25-000001
green
open
1
0
1
6.1kb
.kibana_task_manager_7.17.25_001
green
open
1
0
17
464.3kb
Rows per page: 10
1


Not Secure 3.8.238.97:5601/app/management/kibana/indexPatterns/patterns/462bfa20-ae3d-11ef-b04f-a5913b2f7b6f#/?_a=(tab:indexedFields)
elastic
Search Elastic
Stack Management
Index patterns
.kibana
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Kibana
Index Patterns
Saved Objects
Tags
Search Sessions
Spaces
Advanced Settings
Stack
License Management
Upgrade Assistant
.kibana
Time field: 'canvas-element.@timestamp'
View and edit fields in .kibana. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.
Fields (679)
Scripted fields (0)
Field filters (0)
Search
All field types
Add field
Name
Type
Format
Searchable
Aggregatable
Excluded
_id
_index
_score
_source
_type
action.actionTypeId
action.isMissingSecrets
action.name
action.name.keyword
action.secrets
keyword
boolean
text
binary
Rows per page: 10
Saved '.kibana'