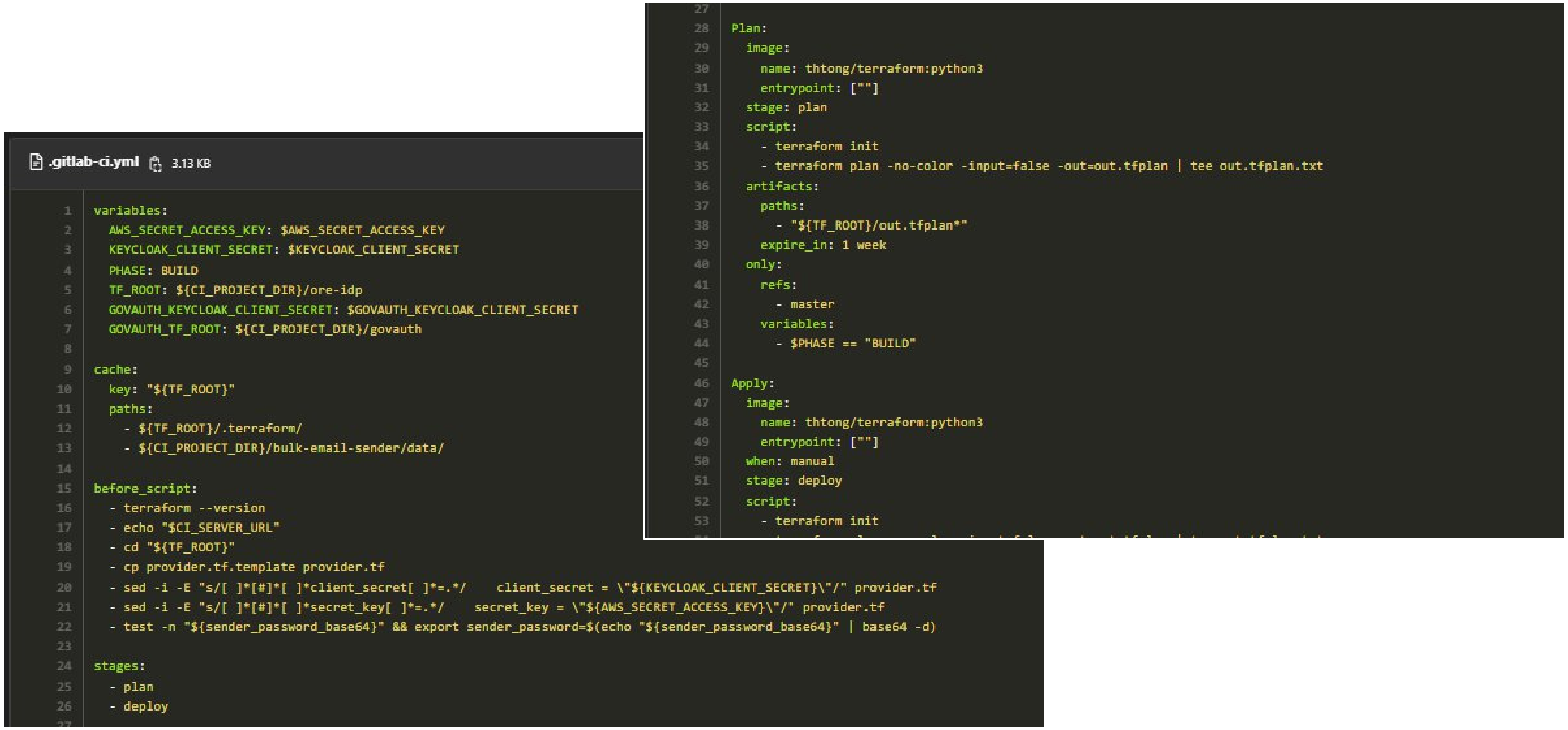
Orchestrated Repository for the Enterprise

Automation Work-flows for On-boarding

These slides describe how the implementation of automation can result in more streamlined system management and governance over time for the ORE. By reducing bottlenecks on services and staff, automation simplifies the overall system life-cycle.

Example CI/CD work-flow definition

ORE leverages CI/CD pipelines to efficiently coordinate regular administrative tasks, such as user on-boarding.

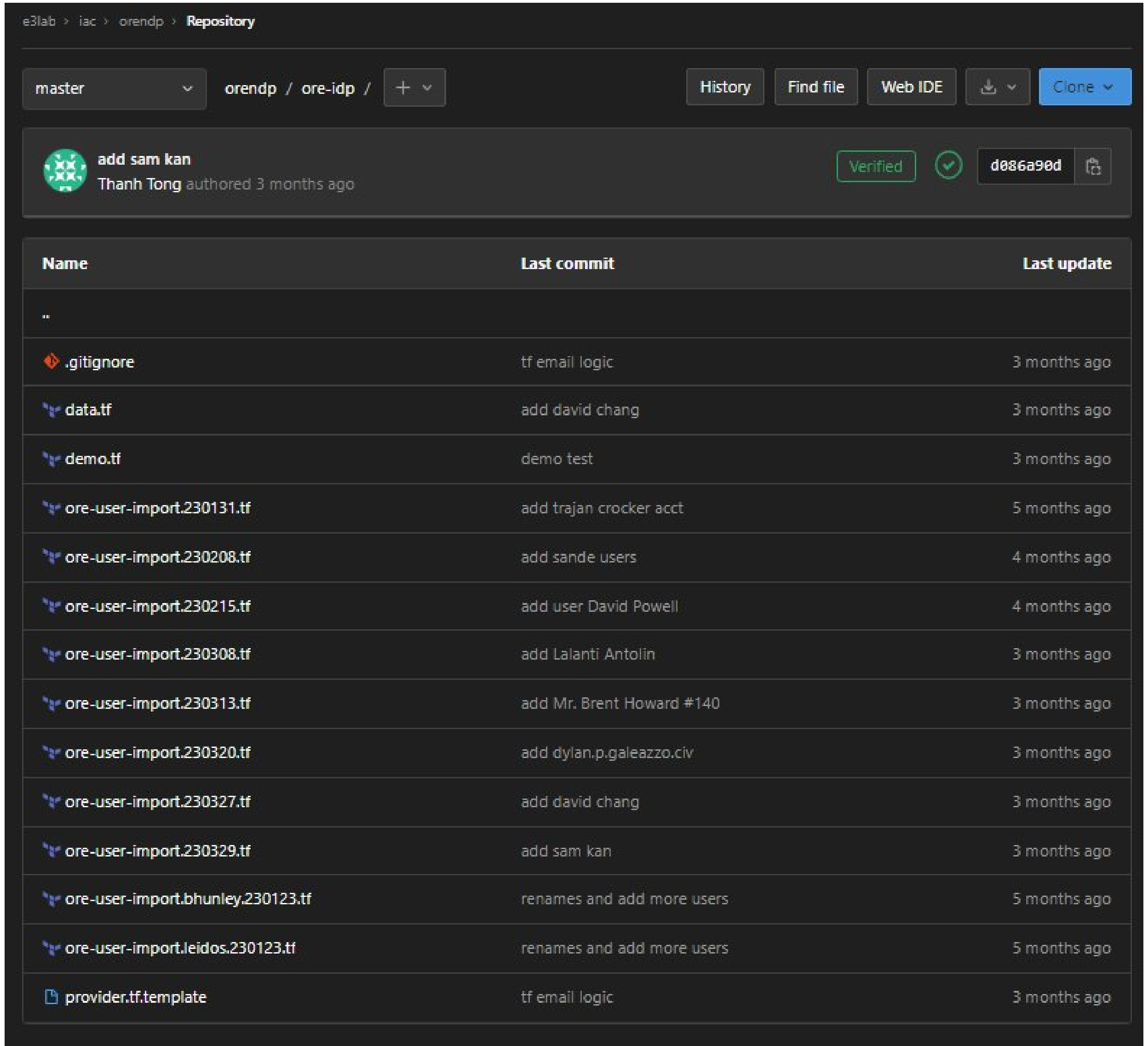


```yaml
variables:
  AWS_SECRET_ACCESS_KEY: $AWS_SECRET_ACCESS_KEY
  KEYCLOAK_CLIENT_SECRET: $KEYCLOAK_CLIENT_SECRET
  PHASE: BUILD
  TF_ROOT: ${CI_PROJECT_DIR}/ore-idp
  GOVAUTH_KEYCLOAK_CLIENT_SECRET: $GOVAUTH_KEYCLOAK_CLIENT_SECRET
  GOVAUTH_TF_ROOT: ${CI_PROJECT_DIR}/govauth

cache:
  key: "${TF_ROOT}"
  paths:
    - ${TF_ROOT}/.terraform/
    - ${CI_PROJECT_DIR}/bulk-email-sender/data/

before_script:
  - terraform --version
  - echo "$CI_SERVER_URL"
  - cd "${TF_ROOT}"
  - cp provider.tf.template provider.tf
  - sed -i -E "s/[ ]*[#]*[ ]*client_secret[ ]*=.*/    client_secret = \"${KEYCLOAK_CLIENT_SECRET}\"/" provider.tf
  - sed -i -E "s/[ ]*[#]*[ ]*secret_key[ ]*=.*/    secret_key = \"${AWS_SECRET_ACCESS_KEY}\"/" provider.tf
  - test -n "${sender_password_base64}" && export sender_password=$(echo "${sender_password_base64}" | base64 -d)

stages:
  - plan
  - deploy
```

```yaml

Plan:
  image:
    name: thtong/terraform:python3
    entrypoint: [""]
  stage: plan
  script:
    - terraform init
    - terraform plan -no-color -input=false -out=out.tfplan | tee out.tfplan.txt
  artifacts:
    paths:
      - "${TF_ROOT}/out.tfplan*"
    expire_in: 1 week
  only:
    refs:
      - master
    variables:
      - $PHASE == "BUILD"

Apply:
  image:
    name: thtong/terraform:python3
    entrypoint: [""]
  when: manual
  stage: deploy
  script:
    - terraform init
```

ORE IaC definitions in git repository

Changes are encoded in source code using Infrastructure as Code (IaC) to enable review and approval processes. This approach also facilitates version control, enabling future reviews and the ability to roll back changes if necessary.



add sam kan
Thanh Tong authored 3 months ago
d086a90d

Name	Last commit	Last update
..		
.gitignore	tf email logic	3 months ago
data.tf	add david chang	3 months ago
demo.tf	demo test	3 months ago
ore-user-import.230131.tf	add trajan crocker acct	5 months ago
ore-user-import.230208.tf	add sande users	4 months ago
ore-user-import.230215.tf	add user David Powell	4 months ago
ore-user-import.230308.tf	add Lalanti Antolin	3 months ago
ore-user-import.230313.tf	add Mr. Brent Howard #140	3 months ago
ore-user-import.230320.tf	add dylan.p.galeazzo.civ	3 months ago
ore-user-import.230327.tf	add david chang	3 months ago
ore-user-import.230329.tf	add sam kan	3 months ago
ore-user-import.bhunley.230123.tf	renames and add more users	5 months ago
ore-user-import.leidos.230123.tf	renames and add more users	5 months ago
provider.tf.template	tf email logic	3 months ago

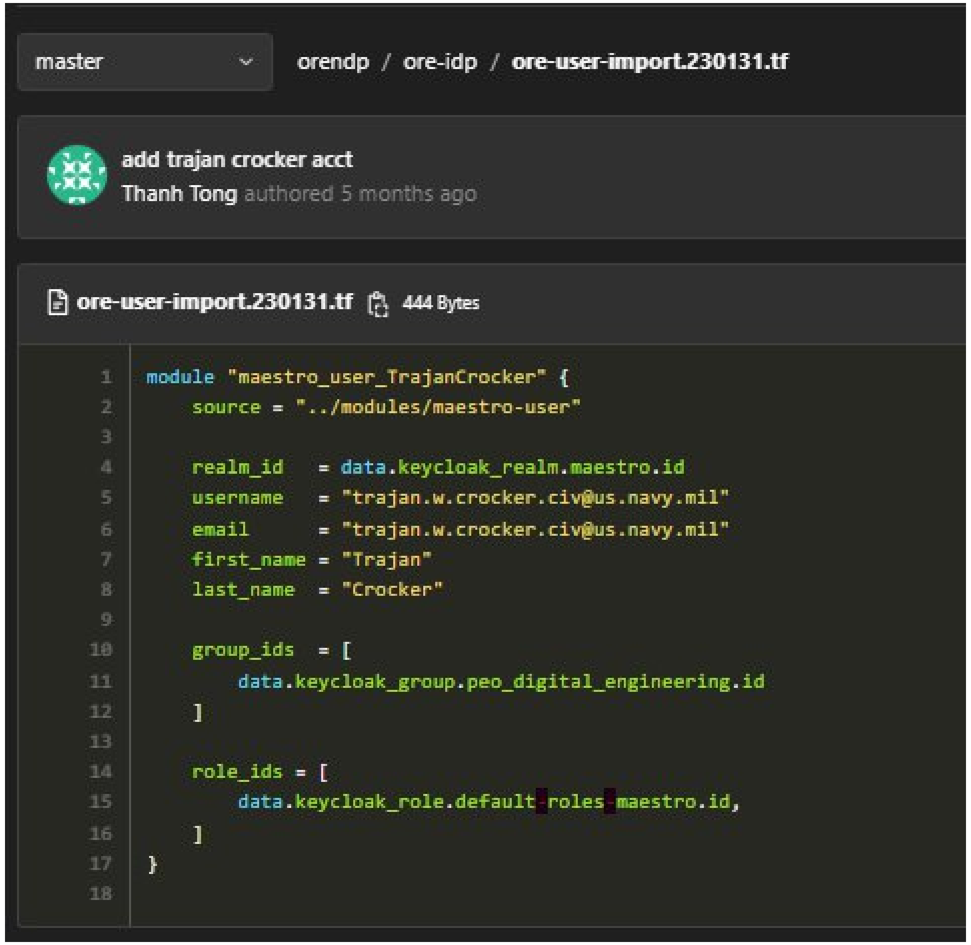
Example declarative IaC for an ORE user

This example declares a specific user account should exist in the ORE. It describes the following information about the user:

–Name and email

–ORE tenant

–Role



master
orendp / ore-idp / ore-user-import.230131.tf

add trajan crocker acct

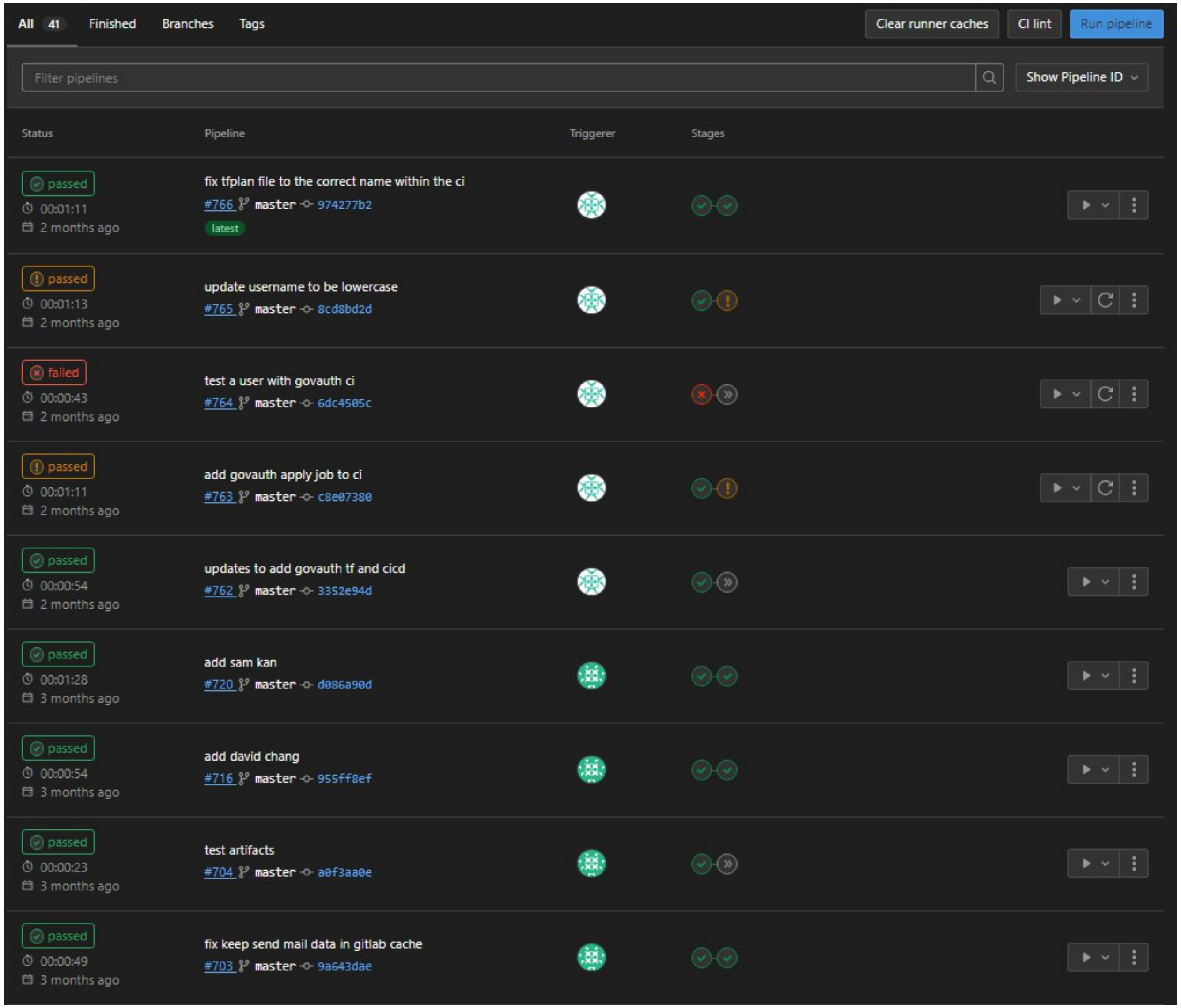
Thanh Tong authored 5 months ago

ore-user-import.230131.tf
444 Bytes

```
module "maestro_user_TrajanCrocker" {
    source = "../modules/maestro-user"

    realm_id   = data.keycloak_realm.maestro.id
    username   = "trajan.w.crocker.civ@us.navy.mil"
    email      = "trajan.w.crocker.civ@us.navy.mil"
    first_name = "Trajan"
    last_name  = "Crocker"

    group_ids  = [
        data.keycloak_group.peo_digital_engineering.id
    ]

    role_ids = [
        data.keycloak_role.default-roles-maestro.id,
    ]
}

```

CI pipeline job status

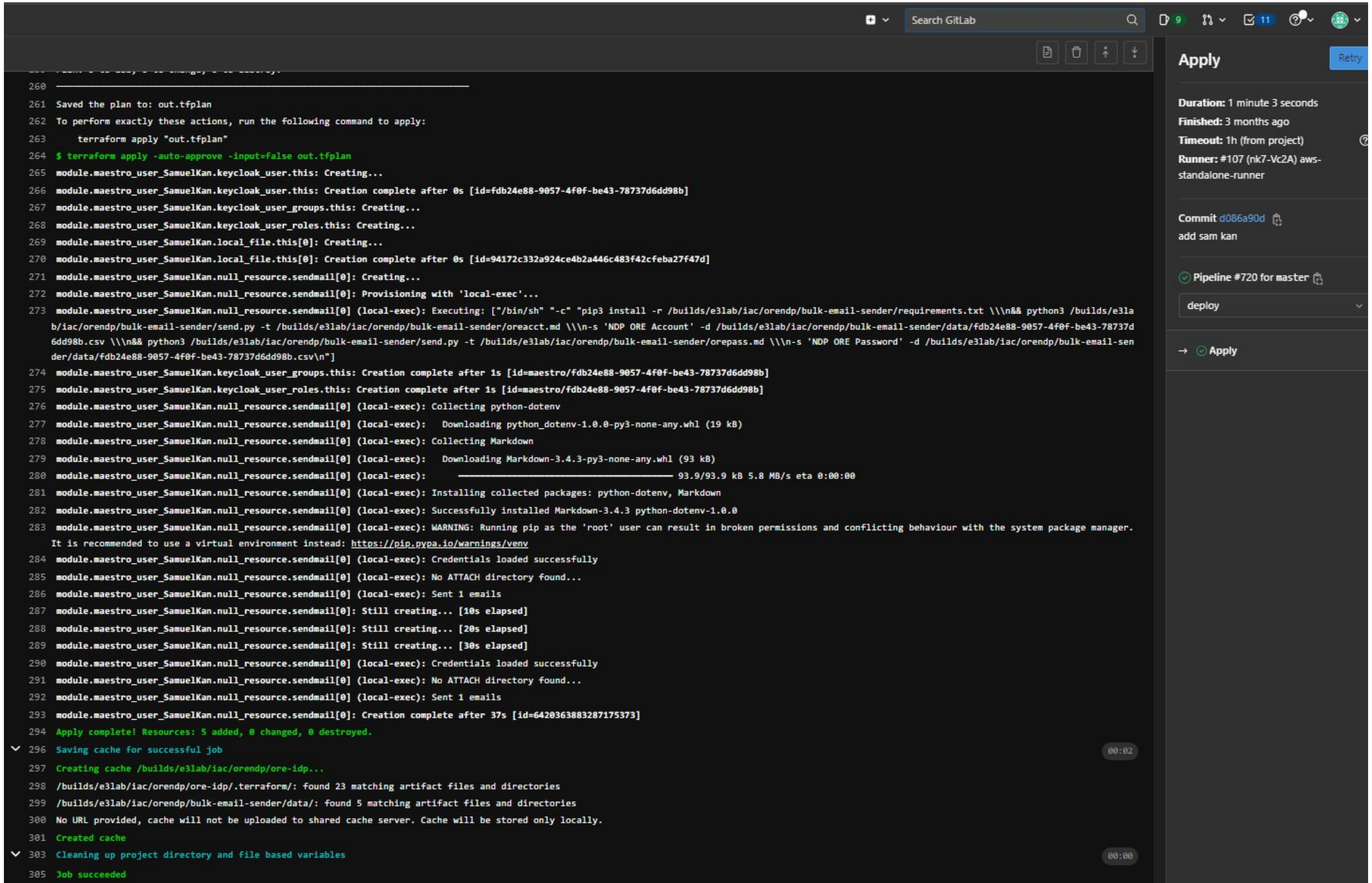
After the Infrastructure as Code (IaC) is approved, the CI pipeline is triggered to update the ORE to the intended outcome. A status report is generated each time the pipeline is executed and can be accessed and reviewed by authorized personnel.



Status	Pipeline	Triggerer	Stages
passed 00:01:11 2 months ago	fix tfplan file to the correct name within the ci #766 master 974277b2 latest		✓ ✓
! passed 00:01:13 2 months ago	update username to be lowercase #765 master 8cd8bd2d		✓ !
✗ failed 00:00:43 2 months ago	test a user with govauth ci #764 master 6dc4505c		✗ »
! passed 00:01:11 2 months ago	add govauth apply job to ci #763 master c8e07380		✓ !
✓ passed 00:00:54 2 months ago	updates to add govauth tf and cicd #762 master 3352e94d		✓ »
✓ passed 00:01:28 3 months ago	add sam kan #720 master d086a90d		✓ ✓
✓ passed 00:00:54 3 months ago	add david chang #716 master 955ff8ef		✓ ✓
✓ passed 00:00:23 3 months ago	test artifacts #704 master a0f3aa0e		✓ »
✓ passed 00:00:49 3 months ago	fix keep send mail data in gitlab cache #703 master 9a643dae		✓ ✓

Example result of CI job running

The CI result provides a comprehensive, step-by-step breakdown of the applied changes. This includes details such as user provisioning and the successful delivery of an on-boarding email to the user.



```
Plan: 5 to add, 0 to change, 0 to destroy.
────────────────────────────────────────────────────────────────────────────
Saved the plan to: out.tfplan
To perform exactly these actions, run the following command to apply:
    terraform apply "out.tfplan"
$ terraform apply -auto-approve -input=false out.tfplan
module.maestro_user_SamuelKan.keycloak_user.this: Creating...
module.maestro_user_SamuelKan.keycloak_user.this: Creation complete after 0s [id=fdb24e88-9057-4f0f-be43-78737d6dd98b]
module.maestro_user_SamuelKan.keycloak_user_groups.this: Creating...
module.maestro_user_SamuelKan.keycloak_user_roles.this: Creating...
module.maestro_user_SamuelKan.local_file.this[0]: Creating...
module.maestro_user_SamuelKan.local_file.this[0]: Creation complete after 0s [id=94172c332a924ce4b2a446c483f42cfeba27f47d]
module.maestro_user_SamuelKan.null_resource.sendmail[0]: Creating...
module.maestro_user_SamuelKan.null_resource.sendmail[0]: Provisioning with 'local-exec'...
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Executing: ["/bin/sh" "-c" "pip3 install -r /builds/e3lab/iac/orendp/bulk-email-sender/requirements.txt \\\n&& python3 /builds/e3la
b/iac/orendp/bulk-email-sender/send.py -t /builds/e3lab/iac/orendp/bulk-email-sender/oreacct.md \\\n-s 'NDP ORE Account' -d /builds/e3lab/iac/orendp/bulk-email-sender/data/fdb24e88-9057-4f0f-be43-78737d
6dd98b.csv \\\n&& python3 /builds/e3lab/iac/orendp/bulk-email-sender/send.py -t /builds/e3lab/iac/orendp/bulk-email-sender/orepass.md \\\n-s 'NDP ORE Password' -d /builds/e3lab/iac/orendp/bulk-email-sen
der/data/fdb24e88-9057-4f0f-be43-78737d6dd98b.csv\n"]
module.maestro_user_SamuelKan.keycloak_user_groups.this: Creation complete after 1s [id=maestro/fdb24e88-9057-4f0f-be43-78737d6dd98b]
module.maestro_user_SamuelKan.keycloak_user_roles.this: Creation complete after 1s [id=maestro/fdb24e88-9057-4f0f-be43-78737d6dd98b]
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Collecting python-dotenv
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec):   Downloading python_dotenv-1.0.0-py3-none-any.whl (19 kB)
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Collecting Markdown
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec):   Downloading Markdown-3.4.3-py3-none-any.whl (93 kB)
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec):      ──────────────────────────────────────── 93.9/93.9 kB 5.8 MB/s eta 0:00:00
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Installing collected packages: python-dotenv, Markdown
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Successfully installed Markdown-3.4.3 python-dotenv-1.0.0
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager.
It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Credentials loaded successfully
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): No ATTACH directory found...
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Sent 1 emails
module.maestro_user_SamuelKan.null_resource.sendmail[0]: Still creating... [10s elapsed]
module.maestro_user_SamuelKan.null_resource.sendmail[0]: Still creating... [20s elapsed]
module.maestro_user_SamuelKan.null_resource.sendmail[0]: Still creating... [30s elapsed]
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Credentials loaded successfully
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): No ATTACH directory found...
module.maestro_user_SamuelKan.null_resource.sendmail[0] (local-exec): Sent 1 emails
module.maestro_user_SamuelKan.null_resource.sendmail[0]: Creation complete after 37s [id=6420363883287175373]
Apply complete! Resources: 5 added, 0 changed, 0 destroyed.
Saving cache for successful job                                                                          00:02
Creating cache /builds/e3lab/iac/orendp/ore-idp...
/builds/e3lab/iac/orendp/ore-idp/.terraform/: found 23 matching artifact files and directories
/builds/e3lab/iac/orendp/bulk-email-sender/data/: found 5 matching artifact files and directories
No URL provided, cache will not be uploaded to shared cache server. Cache will be stored only locally.
Created cache
Cleaning up project directory and file based variables                                                    00:00
Job succeeded
```

Apply

Duration: 1 minute 3 seconds
Finished: 3 months ago
Timeout: 1h (from project)
Runner: #107 (nk7-Vc2A) aws-standalone-runner

Commit d086a90d
add sam kan

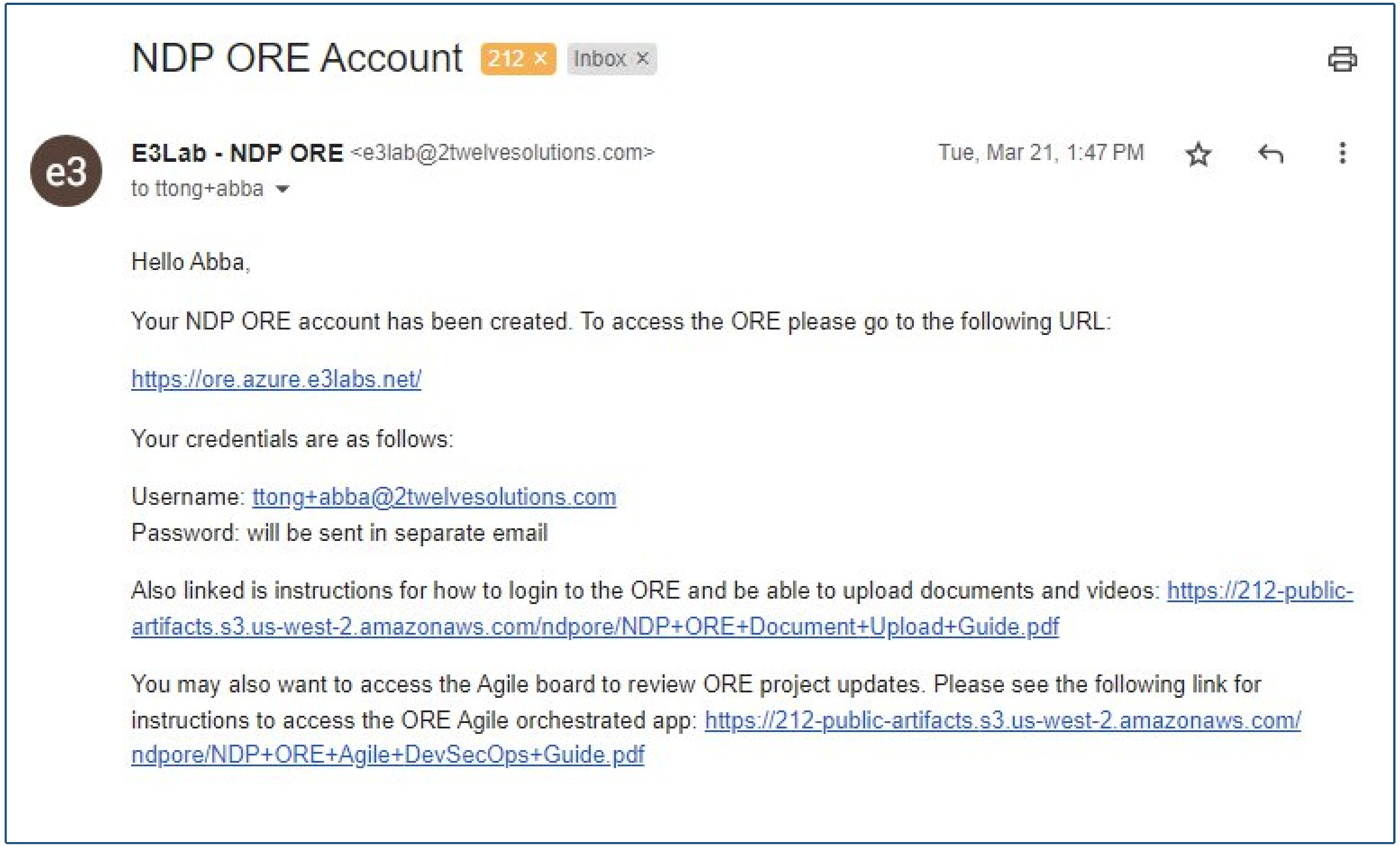
Pipeline #720 for master

deploy

→ Apply

Example of account created email generated through CI/CD work-flow

The on-boarding email, generated by the CI/CD process and sent to the user, contains all the essential account information and documentation required to begin using the ORE.



NDP ORE Account 212 × Inbox ×

E3Lab - NDP ORE <e3lab@2twelvesolutions.com> Tue, Mar 21, 1:47 PM

to ttong+abba

Hello Abba,

Your NDP ORE account has been created. To access the ORE please go to the following URL:

https://ore.azure.e3labs.net/

Your credentials are as follows:

Username: ttong+abba@2twelvesolutions.com
Password: will be sent in separate email

Also linked is instructions for how to login to the ORE and be able to upload documents and videos: https://212-public-artifacts.s3.us-west-2.amazonaws.com/ndpore/NDP+ORE+Document+Upload+Guide.pdf

You may also want to access the Agile board to review ORE project updates. Please see the following link for instructions to access the ORE Agile orchestrated app: https://212-public-artifacts.s3.us-west-2.amazonaws.com/ndpore/NDP+ORE+Agile+DevSecOps+Guide.pdf