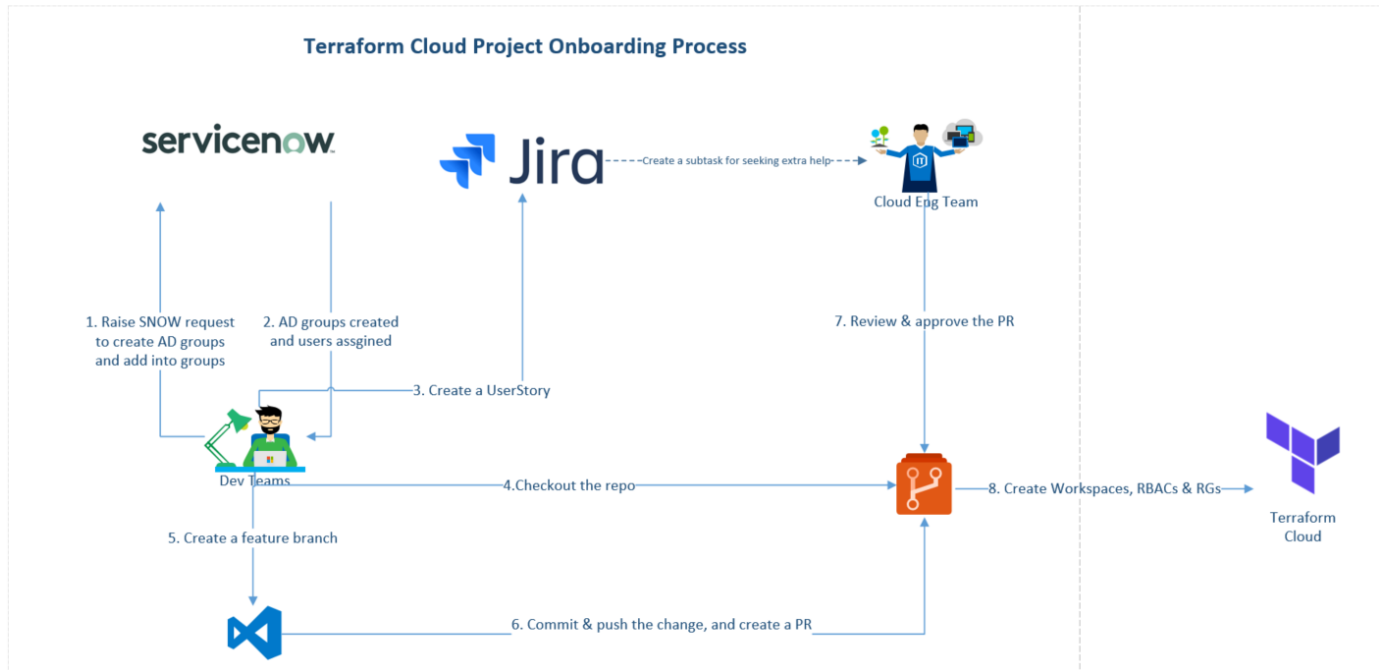


# Terraform Access for Cloud v1.2



12 May 2022

[Terraform Access for Cloud v1.2.wmv](#)

## Instructions

**Step 1:** Create Essential AD group & Access On-boarding Project Repo:

**a.** Raise a SNOw ticket to create AD groups and add members [https://tal.service-now.com/tal\\_portal/tal\\_portal?id=sc\\_cat\\_item&sys\\_id=52c0e85b4f02d2002255c61f0310c71a](https://tal.service-now.com/tal_portal/tal_portal?id=sc_cat_item&sys_id=52c0e85b4f02d2002255c61f0310c71a). AD group naming standards: **tf-<businessunit>-<projectname>-<prod/nonprod>-rw** (Note: This ad group should be in **lower & kebab** case only. No Camel case or other characters eg: **tf-group-myproject-nonprod-rw**)  
**FYI:** AD Groups ServiceNOW request

⚠ Please make sure you have this AD group ready before you create the Terraform workspace

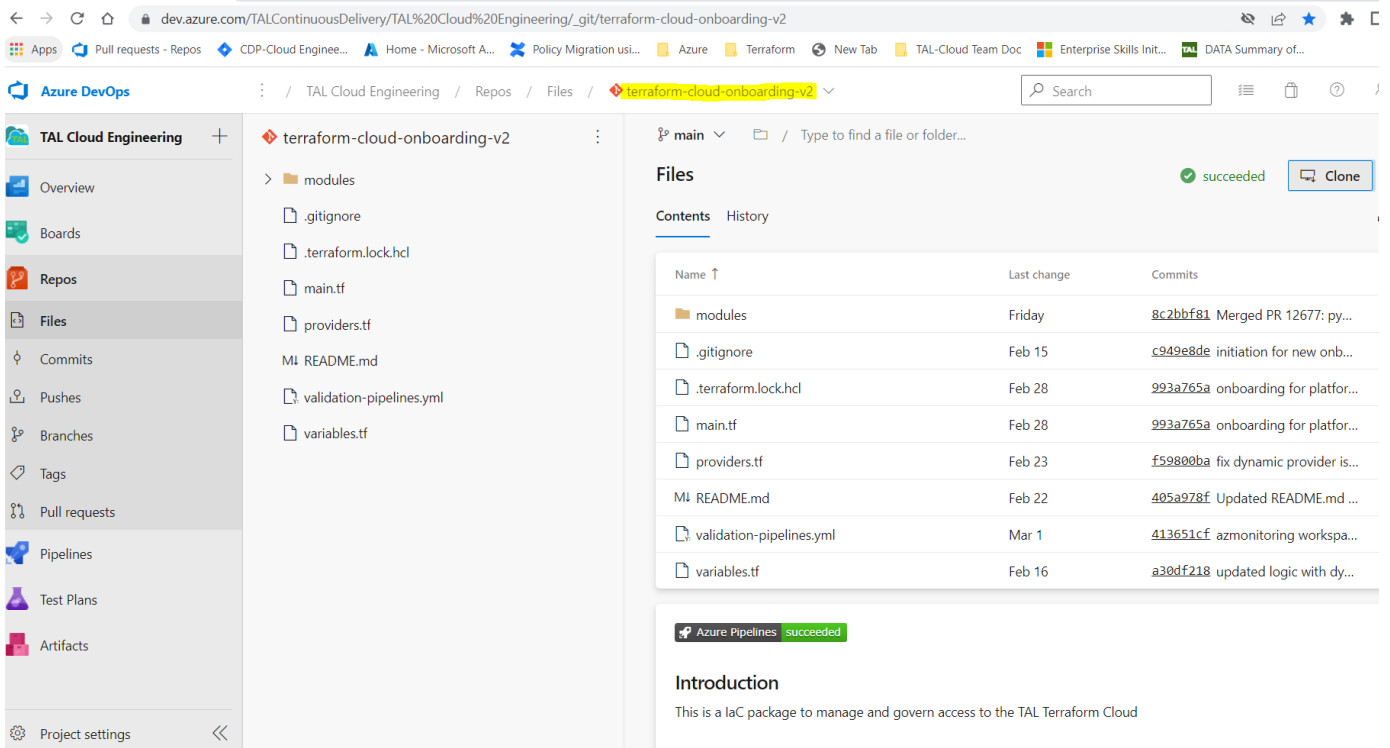
⚠ Please don't re-use the old ones (if you have to, please check with Cloud Team)

⚠ On this stage, you still don't have the access to Terraform Workspace. Login Terraform Cloud platform, you will get errors. For more information, please refer to [How to access your workspace in TAL Terraform Cloud](#)

*For Cloud team:* Please don't create the AD groups from the Azure portal which is not synced with On-Prem AD and having the source as "Cloud" (AD Groups synced from On-Premise AD will be having their "Source" as "Windows server AD")

**b.** Raise a request to add yourself to **.uTAL-TF-onboarding**, so that you can access this repo. Refer to this page [AD Groups ServiceNOW request](#) Then you should be able to see this repo on Azure DevOps portal as below [https://dev.azure.com/TALContinuousDelivery/TAL Cloud Engineering/\\_git/terraform-cloud-onboarding-v2](https://dev.azure.com/TALContinuousDelivery/TAL Cloud Engineering/_git/terraform-cloud-onboarding-v2)

⚠ If you don't have the access to Azure DevOps, please check with Cloud Team to change your access from stakeholder to basic (normally basic access is enough) or VS professional (You need to raise a ServiceNow request to get your manager's approval for the license which is quite expensive). FYI about the access level: <https://docs.microsoft.com/en-us/azure/devops/organizations/security/access-levels?view=azure-devops>



## Step 2: Azure DevOps Project

For the Azure DevOps Project which will be used for your projects (it will be filled in the <azuredevops\_projects> as the screenshot below)

```
module "appsecantapi" {
  source      = "../../project-core"
  organization = var.organization
  tal_workspaces = [
    Debanjan Basu, 6 months ago | 3 authors (hkanakamedala and others)
    {
      # <<projectname>>-<<workspacenumber>>
      workspace_name = "${local.project_name}-001"
      project_name   = local.project_name
      hkanakamedala, 6 months ago | 1 author (hkanakamedala)
      tal_environments = [{
        environment_name = "nonprod"
        location         = "australiaeast"
      }]
      additional_environments = []
      azuredevops_projects   = ["TAL.CD.AppSec"]
      description             = "Workspace for the ${local.project_name} project"
    }
  ]
}
```

- If you need to create a new one, please refer to [Azure DevOps - Create A New Project Request](#) to raise a request. For the AD groups used for this DevOps project giving people different access for this project, please refer to [Azure DevOps Projects Access](#);
- if you already have one, just put the name there;
- If leave it empty, by default, the project will be <TAL Cloud Engineering>.

**Step 3:** Create a userstory on Jira board of CDP-Cloud Engineering & Services, assign to yourself (This is for tracking all the details of the Terraform workspace)

Epics to use:

Platform	PI15	PI-16	PI-17
Digital	<a href="#">+ DIGPLAT-771</a> - Digital Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-763</a> - Digital Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-816</a> - Digital Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Claims	<a href="#">+ DIGPLAT-768</a> - Claims Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-760</a> - Claims Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-817</a> - Claims Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Data	<a href="#">+ DIGPLAT-769</a> - Data Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-761</a> - Data Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-818</a> - Data Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Direct	<a href="#">+ DIGPLAT-786</a> - Direct Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-785</a> - Direct Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-819</a> - Direct Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Group	<a href="#">+ DIGPLAT-767</a> - Group Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-759</a> - Group Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-820</a> - Group Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Investment	<a href="#">+ DIGPLAT-813</a> - Investment Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-814</a> - Investment Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-821</a> - Investment Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Retail	<a href="#">+ DIGPLAT-770</a> - Retail Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-762</a> - Retail Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-822</a> - Retail Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>
Finance	<a href="#">+ DIGPLAT-787</a> - Finance Platform Cloud Services/Support Unplanned (PI-15) <b>RELEASED</b>	<a href="#">+ DIGPLAT-784</a> - Finance Platform Cloud Services/Support Unplanned (PI-16) <b>IN PROGRESS</b>	<a href="#">+ DIGPLAT-823</a> - Finance Platform Cloud Services/Support Unplanned (PI-17) <b>OPEN</b>

Here is one example:

TALCLOUD-56 / TALCLOUD-66 ← copy the id

## Create iol3 terraform workspace

[Attach](#) [Create subtask](#) [Link issue](#) [Show draw.io Diagrams Panel](#)

Description

Normal text ▼ **B** *I* ... A ▼ ☰ ☷ [Link](#) [Image](#) [@](#) [Emoji](#) [Grid](#) [Code](#) [Info](#) [+](#) ▼

1. Project Name: IOL 3.0
2. AD groups: tf-iol3-ro, tf-iol3-rw
3. Environments: dev1, dev2, dev3, dev4, sys1, sys2, sys3, sys4, uat, pre-prod, prod
4. <7 mandatory Tags for resource group>

1  
← put down all details


[Save](#) [Cancel](#)

Acceptance Criteria

<none>

Business Benefit

None



Pro tip: press **M** to comment

Note: If you need help and don't understand the process, please create a subtask and assign it to a cloud engineer

**⚠ Move to step 4 only after AD groups/Azure DevOps Project are created.**

If an AD group from one of the previous modules will be reused, Terraform Apply will throw errors.

If the required AD groups and Azure DevOps are not created, Terraform Apply will throw errors..

**Step 4:** Clone terraform-cloud-onboarding-v2 repo in your VS code. (You have to be added into .uTAL-TF-onboarding in Step 1.)

```
git clone https://TALContinuousDelivery@dev.azure.com
/TALContinuousDelivery/TAL%20Cloud%20Engineering/_git/terraform-cloud-
onboarding-v2
```

**⚠** If you already in the AD group <.uTAL-TF-onboarding> while got authentication error. Please check this page. <https://docs.microsoft.com/en-us/azure/devops/repos/git/auth-overview?view=azure-devops>

**Step 5:** Create a feature branch with the UserStory ID and project name as below, then work on your branch

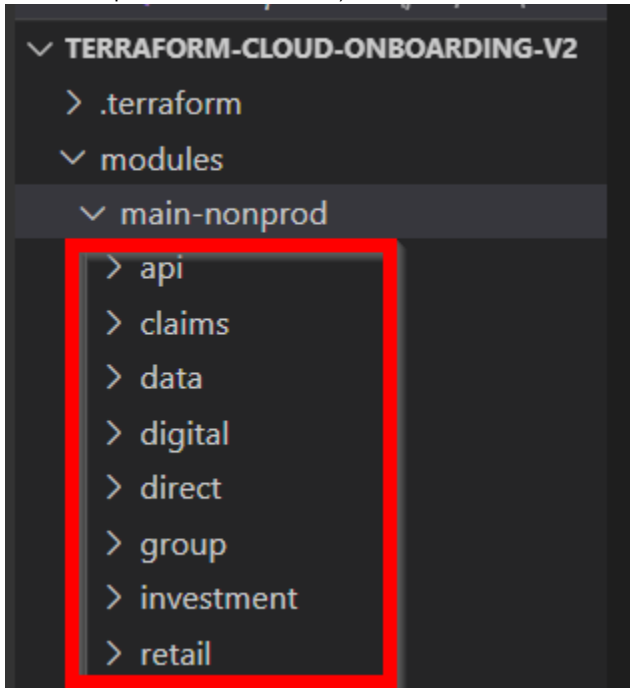
```
twang@L012GJQG MINGW64 /c/terraform-cloud-onboarding (main)
$ git status
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean
copied ID project name
twang@L012GJQG MINGW64 /c/terraform-cloud-onboarding (main)
$ git branch feature/talcloud66-create-iol3
```

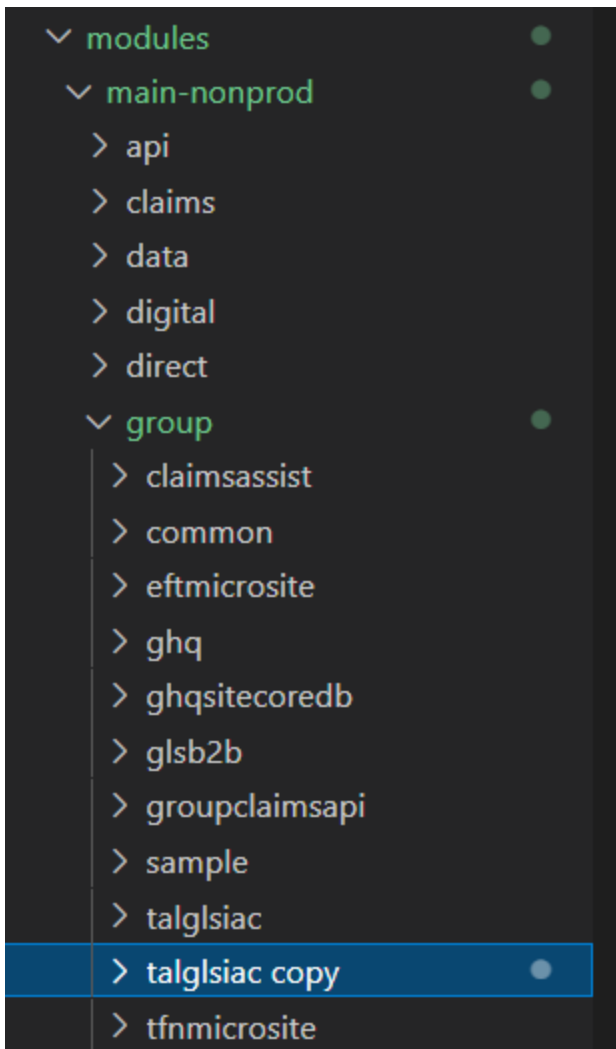
**Sep 6:** Create the Terraform Workspace

Copy any existing similar project and reconfigure the settings (Project name has to be **lowercased**.)

1. Go to modules main-nonprod or main-prod or main-sandbox (depends on your project env) business unit your project belongs to (eg: Groups or retail or claims etc)



2. Find one project and copy then paste in the same env folder. or copy and paste the sample folder . For example: My project is similar to talgsiac project, So I copy it then paste it as below.



3. Update your folder name (Project name has to be **lowercased**.) reconfigure the settings as below. Only update the [main.tf](#) file inside your folder.

☀ The checklist for updates (Please don't tick them on this page)

- ☒ Update the module name
- ☒ Update the workspace\_name if need
- ☒ Update the env and location
- ☒ Update the DevOps Project name (optional)
- ☐ Update the tags (Please check with your team if you don't know)
- ☒ Update the project\_teams if need
- ☒ Is everything in lower & kebab case ?
- ☒ Do not hard code ad group in the main.tf. If you want to hardcode, consult Cloud Engineering staff
- ☒ Do you want to have a working directory as a folder "terraform" ? By default, all the main.tf etc files will be inside folder "terraform".

1. foldername and module name should be the same

2. terraform cloud workspace name will be created using this Eg: group-ghq-preprod-syd

3. RG name will be create using this Eg: ghq-preprodsyd-rg

4. Location where resource Group will be create Only australiaeast or australianoutheast

5. if true, RG name will be create using this Eg: ghq-preprodsyd-001

6. Add more code blocks like these, if more terraform workspaces and resource groups are needed

7. if multiple resource groups required, add more of these blocks in the list

```

12
13 module "ghq" {
14     source = "../../../../../project-core"
15     tal_workspaces = [
16         #Add or remove workspace as per your requirements
17         {
18             # <<projectname>>-<<workspacename>>
19             workspace_name = "${local.project_name}-preprod-syd"
20             project_name = local.project_name
21             tal_environments = [
22                 {
23                     environment_name = "preprodsyd"
24                     location = "australiaeast"
25                     numeric_prefix = false
26                 }
27             ]
28             additional_environments = []
29             azuredevops_projects = ["TAL.GLS.GroupHub"]
30             description = "Workspace for the ${local.project_name} project"
31         },
32         # <<projectname>>-<<workspacename>>
33         {
34             workspace_name = "${local.project_name}-preprod-mel"
35             project_name = local.project_name
36             tal_environments = [
37                 {
38                     environment_name = "preprodmel"
39                     location = "australiasoutheast"
40                     numeric_prefix = false
41                 }
42             ]
43             additional_environments = []
44             azuredevops_projects = ["TAL.GLS.GroupHub"]
45             description = "Workspace for the ${local.project_name} project"
46         }
47     ],
48     project_teams = [
49         {
50             team_name = "tf-${var.business_unit_name}-${local.project_name}-nonprod-rw"
51             write_access = true
52             /* uncomment the line below if an AD group from other modules have to be repurposed for this module */
53             #reuse_adgroup = true
54         }
55     ]
56 }

```

4. Update the below mandatory Tags with valid values. Follow this link to validate if your tags exists

7 Mandatory Tags with allowed values as Azure Policies will not allow new tag values

```

290     numeric_prefix = false
291 }
292 ]
293 additional_environments = []
294 azuredevops_projects = ["TAL.GLS.GroupHub"]
295 description = "Workspace for the ${local.project_name} project"
296 }
297 ]
298 # Common tags to be assigned to all resources. Change the values <> accordingly
299 # ashekar2, last month | 2 authors (cgundeboina and others)
300 tags = {
301     platform = "group"
302     team-pod = "group-partner-services"
303     environment = "prod"
304     infra-app = "application"
305     application-service = "group-ghq-website"
306     business-service = "group-life-systems"
307     data-classification = "confidential"
308 }
309 project_teams = [

```

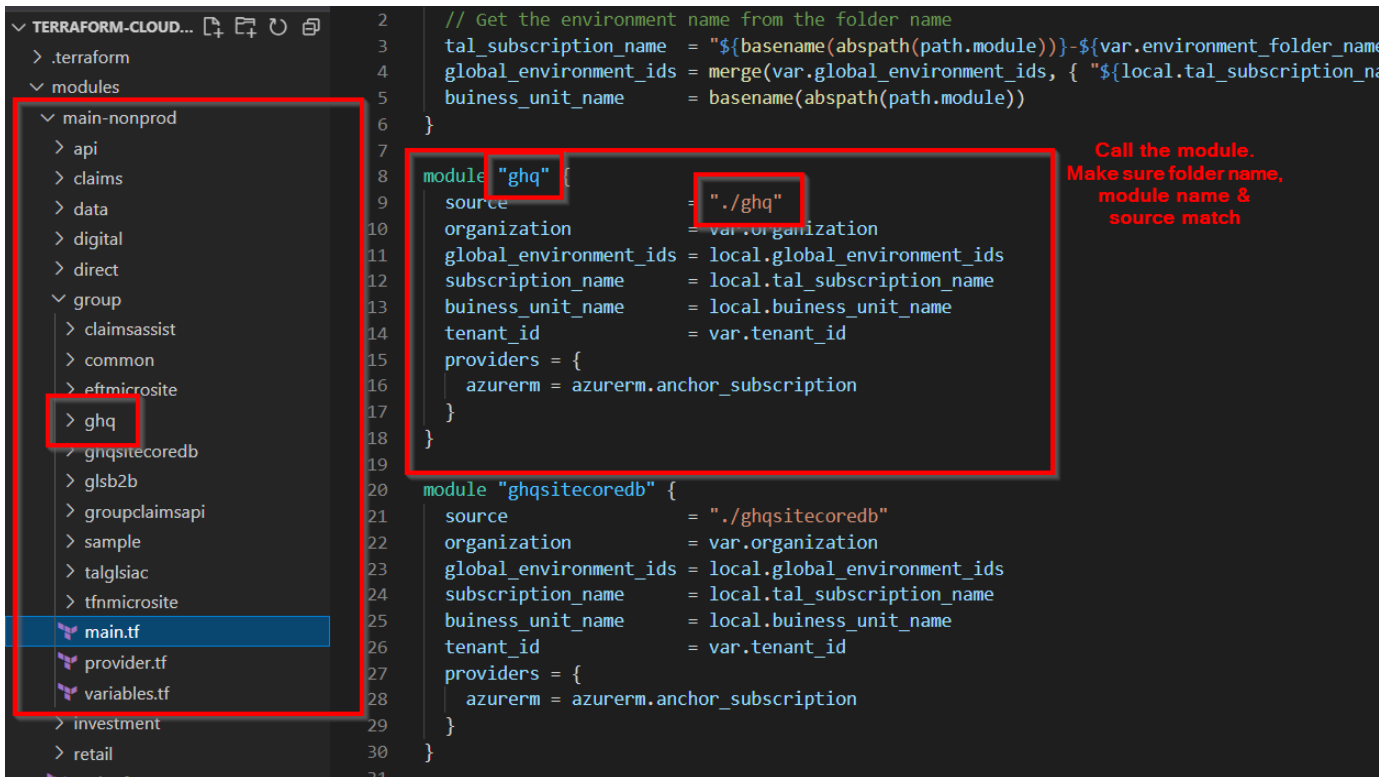
⚠ Make sure the team\_name is the same as the AD groups as Step 1.

```

project_teams = [
{
    team_name = "tf-${var.business_unit_name}-${local.project_name}-nonprod-rw"
    write_access = true
    /* uncomment the line below if an AD group from other modules have to be repurposed for this module */
    #reuse_adgroup = true
}
]

```

4. Update the main.tf file under the business unit folders to call your module as below.



⚠ Please make sure your folder name is the same as the module name for right reference.

☀ For providing Azure DevOps project name, auto generated SPN will be applied as service connection in the DevOps project.

**Step 7:** Commit and push the feature branch

**Step 8:** Make a Pull Request and put Cloud Team as reviewer

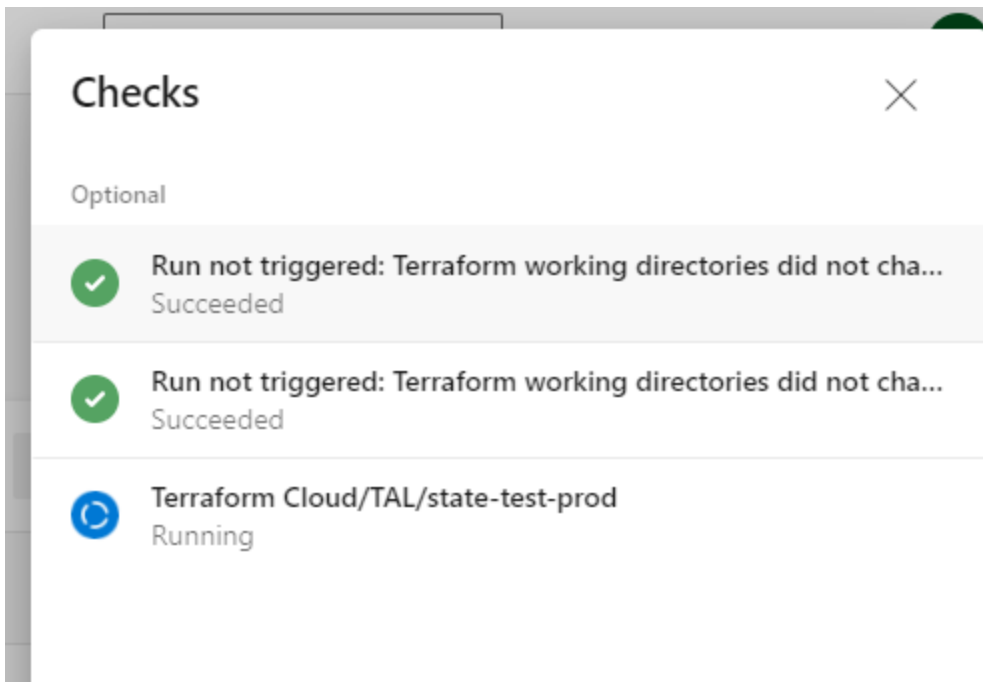
#### **For Cloud Team:**

There are 4 workspaces based on the environment as below.

onboarding-v2-nonprod	✓ Applied	TALContinuousDelivery/TAL Cloud Engineering/terraform-cloud-onboarding-v2	17 hours ago
onboarding-v2-platform	✓ Applied	TALContinuousDelivery/TAL Cloud Engineering/terraform-cloud-onboarding-v2	16 hours ago
onboarding-v2-prod	✓ Planned and finished	TALContinuousDelivery/TAL Cloud Engineering/terraform-cloud-onboarding-v2	20 hours ago
onboarding-v2-sandbox	✓ Applied	TALContinuousDelivery/TAL Cloud Engineering/terraform-cloud-onboarding-v2	a month ago

When complete the PR, you will see something similar as below screenshot. As long as the right workspace is triggered and planned with no error, it is good to go.

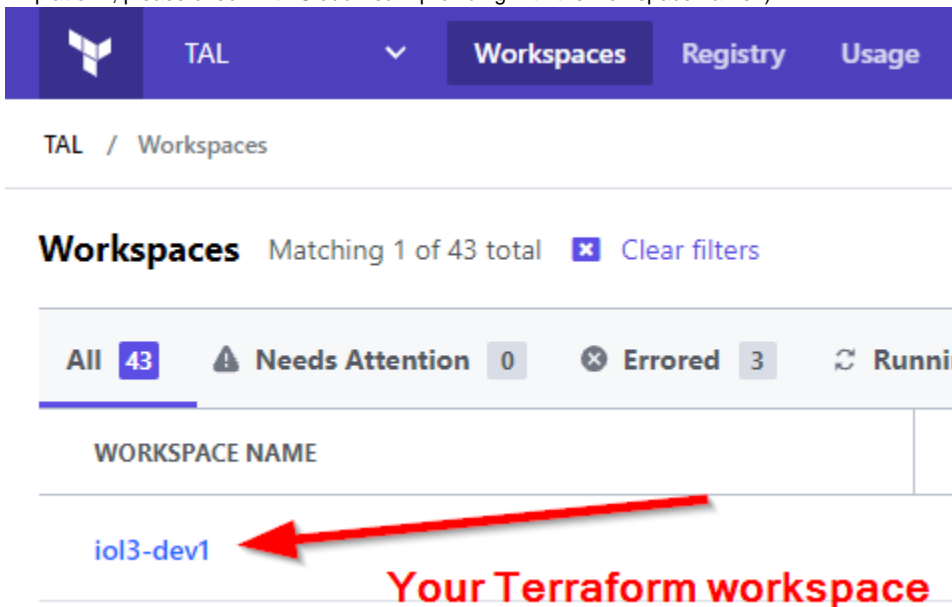




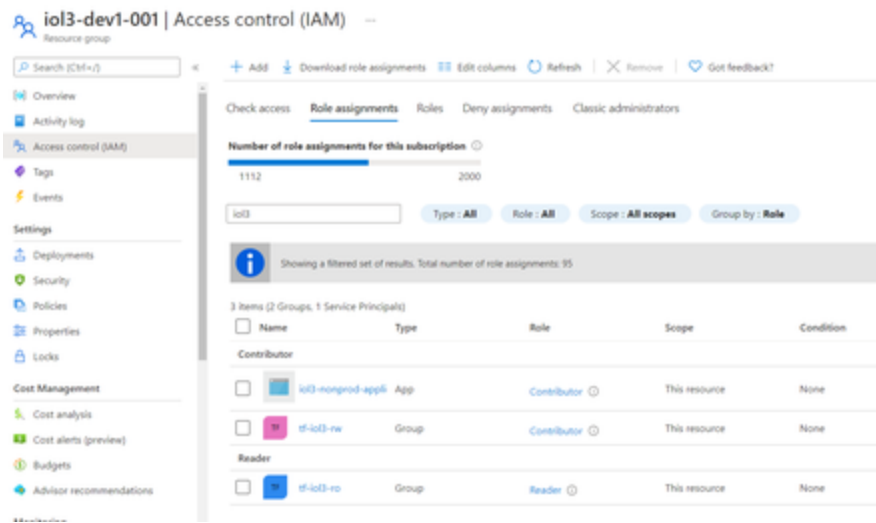
**Step 9:** Double check you have all the resources and access

After cloud engineers review and approve the PR, the workspace(s), RG(s), SPN(s) and RBAC(s) will be created automatically. Double check your access one by one as below.

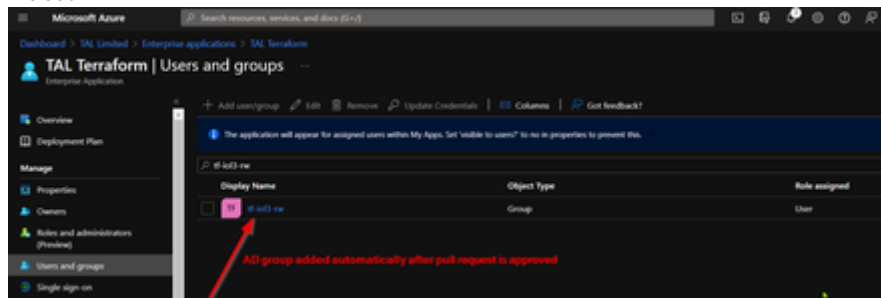
- Sign in with SSO to access Terraform Cloud Platform, for more information, please refer to [How to access your workspace in TAL Terraform Cloud](#) (⚠️ Please log out then SSO sign in again.)
- You can find your Terraform workspace by searching the module name as below. (⚠️ If you still cannot see it on your Terraform Cloud platform, please check with Cloud Team providing with the workspace name. )



- You can search module name on Azure Portal to find all the RGs you created



- AD group (*tf-<projectname>-<prod/nonprod>-rw*) will be added automatically to TAL Terraform Enterprise application, which grants access to workspaces in terraform cloud.



**Step 10:** If you have all the access and the projects are ready to use, then please close the Jira ticket.



1. Cloud Eng team has no authority in creating/manipulating AD groups.
2. Cloud Engineers are approachable on Teams Channel (Terraform Cloud) for further enquiries and feedback.

#### Related articles

- [Terraform Access for Cloud v1.2](#)
- [Terraform Cloud Access](#)