

# RUNTASTIC



A group of four runners (three men and one woman) are captured in motion, running from left to right. They are wearing athletic gear: the lead man is in a black sleeveless shirt and leggings, the woman behind him is in a blue jacket and leggings, the man next is in a white t-shirt and shorts, and the woman at the back is in a black long-sleeve shirt and leggings. They are running on a paved surface in front of a large, light-colored stone wall. The image has a slightly desaturated, cinematic feel.

FEB 15, 2022

# Identity Access Management mit Ansible



**Name:** Alexander Lackner

**Info:** Infrastructure Engineer

RUNTASTIC

# **ABOUT ME**

# ALEXANDER LACKNER

- Seit März 2020 bei Runtastic
- Infrastructure Engineer
- Leidenschaft für Automation und Clouds
- Erfahrung mit Red Hat Produkten
  - Satellite, RHEL, Ansible Tower



**ALEXANDER LACKNER**  
Infrastructure Engineer

[alexander.lackner@runtastic.com](mailto:alexander.lackner@runtastic.com)

# **ABOUT RUNTASTIC**

A dark, low-key photograph of two runners in motion, likely on a track. The image is heavily shadowed, with the runners' forms emerging from the darkness. The text is overlaid in white, creating a strong contrast.

OUR MISSION

# THROUGH SPORT WE HAVE THE POWER TO CHANGE LIVES

BY ENGAGING AND EMPOWERING  
1 BILLION CONNECTED ATHLETES

RUNTASTIC

# RUNTASTIC

## BY THE NUMBERS



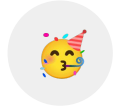
WE HAVE  
**4 FOUNDERS**



WE COME FROM  
**41 COUNTRIES**



USER REGISTRATIONS  
**182M**



WE ARE  
**12 YEARS OLD**



WE HAVE  
**3 OFFICES**



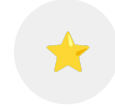
APP STORE DOWNLOADS  
**341M**



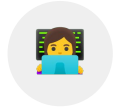
WE WERE PROFITABLE AFTER JUST  
**20 MONTHS**



OUR PRODUCTS ARE AVAILABLE IN  
**10 LANGUAGES**



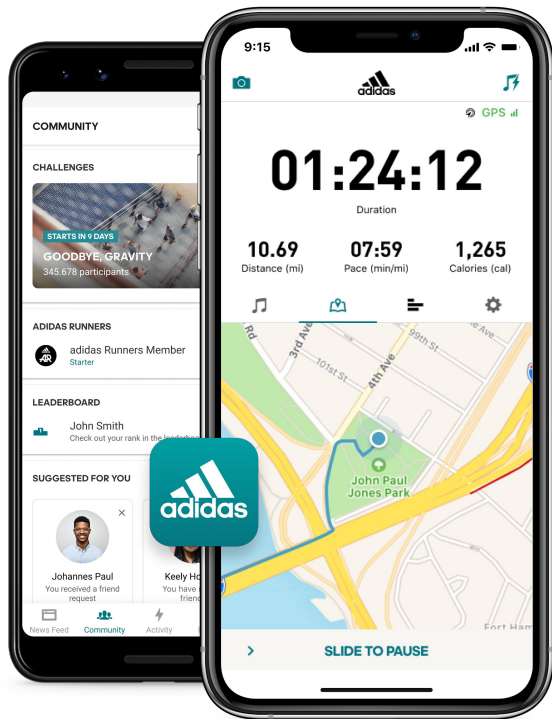
APP STORE RATING  
**4.66**



WE ARE  
**280 EMPLOYEES**



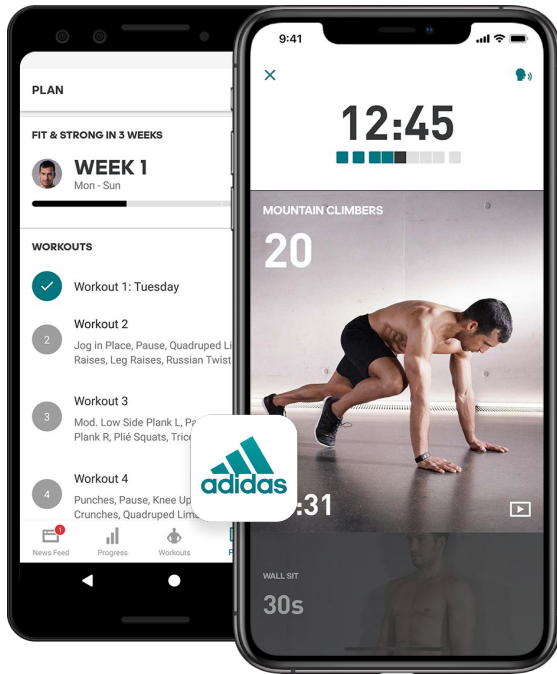
FOLLOWERS & FANS  
**5.7M**



**TRACK ACTIVITIES. BOOST PERFORMANCE.  
CELEBRATE SUCCESS.**

Record your workouts and review your statistics. Join challenges to get motivated – push your limits. Share your success with a global community and reach your goals with the adidas Running app.





**WORK OUT. BUILD STRENGTH. STAY ACTIVE & HEALTHY.**

Select muscle groups and create your own workout that fits your schedule. Join challenges: compare your activity to others and push yourself in new ways. Workout anywhere, any time with the adidas Training app.

# IDENTITY ACCESS MANAGEMENT (IAM)



- Viel **manueller** Aufwand mit **On- und Off-Boarding** von Mitarbeitern
  - Erstellung / Löschen von Benutzern
  - Vergabe von Berechtigungen
  - Aussenden von Informationen
- **Security** Aspekte 
  - Accounts von ehemaligen Usern werden vergessen



- **Automatisierung** des User Managements via **Ansible** 
  - Erstellen / Löschen von Benutzern und Gruppen
  - Vergeben von Berechtigungen
- **Challenges**
  - So gut wie keine Ansible Module für den Use-Case vorhanden
  - Noch kein Ansible Tower vorhanden

- User Daten als **.json** in **git** verwalten. Ein Folder pro User
- Ein **.json** für jede **Anwendung**, allgemeine Informationen in **general.json**

general.json

```
{
  "general": {
    "uid": "alextest",
    "firstname": "Alexander",
    "lastname": "Lackner Test",
    "email": "alexander.lackner@runtastic.com"
  }
}
```

github.json

```
{
  "github": {
    "username": "al-lac",
    "state": "absent",
    "role": "admin",
    "teams": [
      "Infrastructure"
    ]
  }
}
```

- Eine Role pro Applikation (GitHub, Slack, ...)
- Verwendung des **ansible.builtin.uri** Modules wo möglich
- Eigene Python Module für **Google Workspace** und **SCIM**

- **github\_manage\_users.yml**

```
- name: Manage GitHub users
  hosts: localhost
  tasks:
    - include_role:
        name: github_user
      vars:
        user_state: '{{ item.github.state | default("present") }}'
        user_properties:
          username: "{{ item.github.username }}"
          teams: "{{ item.github.teams | default([]) }}"
          role: "{{ item.github.role | default('member') }}"
        loop: "{{ user_details }}"
      when: item.github is defined
```

- Aufbau der github Role

 `create.yml` `delete.yml` `exists.yml` `main.yml` `manage_teams.yml` `update.yml`



- **github:** main.yml

```
---
- include_tasks: exists.yml

- include_tasks: create.yml
  when: user_state == "present" and github_user_exists.status == 404

- include_tasks: manage_teams.yml
  when: user_state == "present"

- include_tasks: update.yml
  when: user_state == "present" and github_user_exists.json.state == "active"

- include_tasks: delete.yml
  when: user_state == "absent" and github_user_exists.status == 200
```

- **github**: exists.yml

```
- name: "Check GitHub user {{ user_properties.username }}"
  ansible.builtin.uri:
    url: "{{ github_api_url }}/orgs/{{ github_api_org }}/memberships/{{user_properties.username}}"
    method: GET
    headers:
      Authorization: "Bearer {{ github_api_token }}"
    status_code:
      - 200
      - 404
  when: user_properties is defined
  register: github_user_exists
  no_log: true
```

- **github:** create.yml

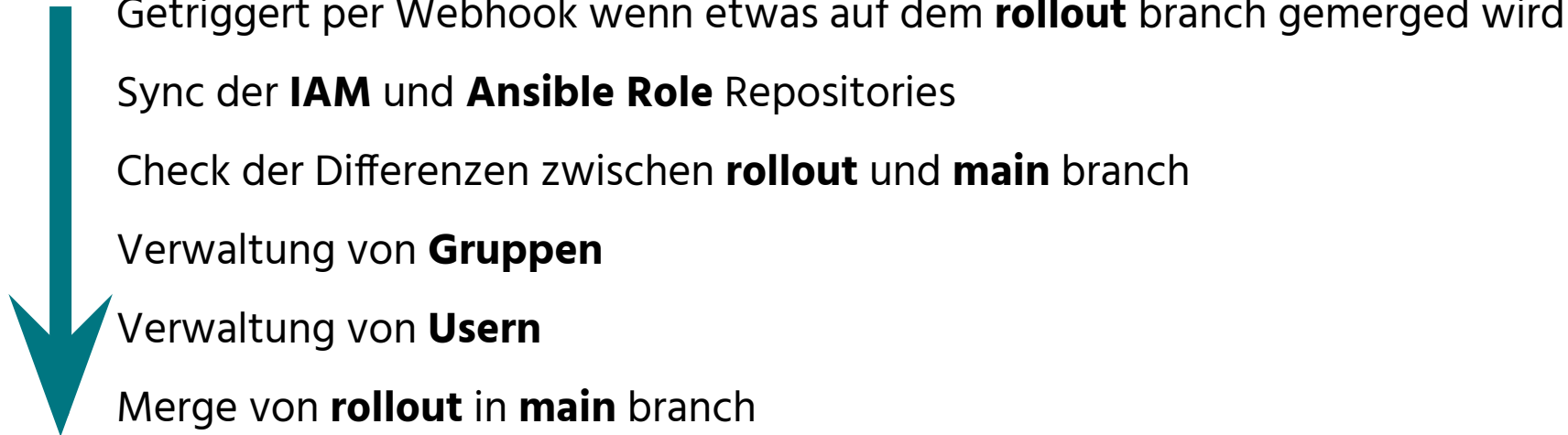
```
- name: "Add GitHub user {{ user_properties.username }} to GitHub Organization {{ github_api_org }}"
  ansible.builtin.uri:
    url: "{{ github_api_url }}/orgs/{{ github_api_org }}/memberships/{{user_properties.username}}"
    method: PUT
    headers:
      Authorization: "Bearer {{ github_api_token }}"
    body_format: json
    body:
      role: "{{ user_properties.role }}"
    status_code:
      - 200
  register: github_user_exists
  no_log: true
```

- Zwei Branches: **rollout** und **main**
- Differenzen zwischen den beiden werden als Extra Variables an die Ansible Roles mitgegeben: **users\_changed** / **groups\_changed**

- Konfiguriert via **Terraform** 
  - Team, Permissions, Job Templates, Credential Types, Workflows, ...
  - Mittels **restapi** provider
- **Secrets** und **Variablen** werden in unserer **Vault**  abgelegt

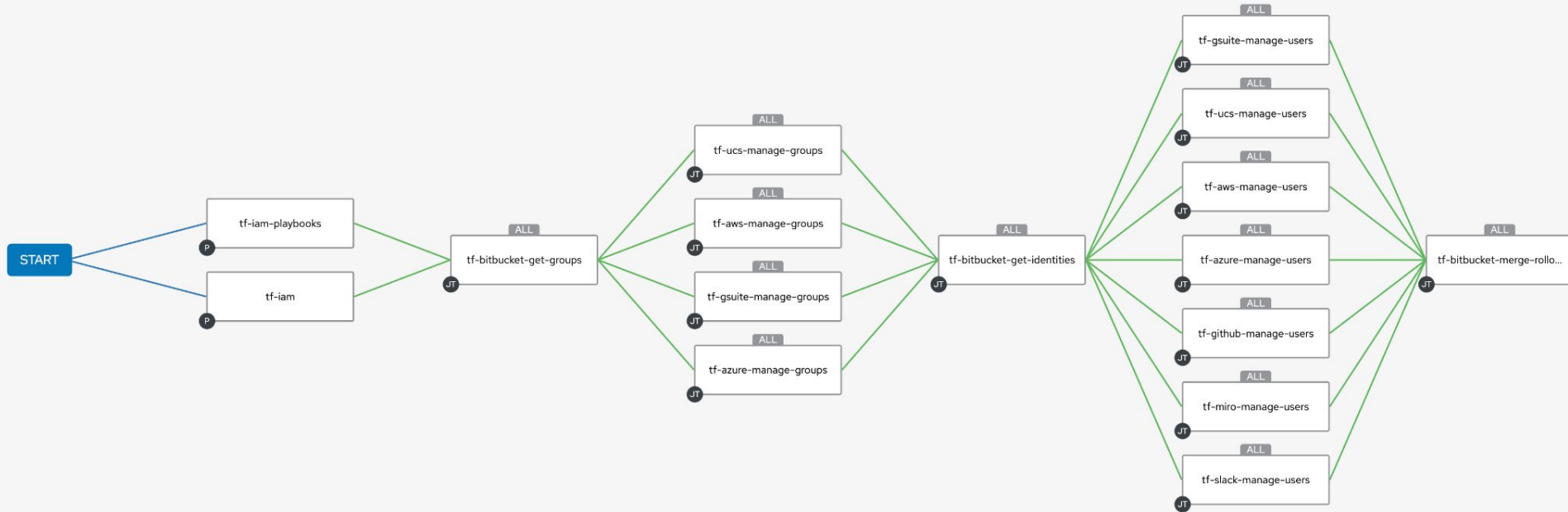
# ANSIBLE TOWER WORKFLOW

IAM



# ANSIBLE TOWER WORKFLOW

IAM



☐ **tf-0000-manage-users**

---

Activity





# ANSIBLE TOWER WORKFLOW

IAM

Name 

Status 

Type

> ☐ 6453 – tf-0000-manage-users

 Failed

Workflow Job



# ANSIBLE TOWER WORKFLOW

IAM

Name ↑

Status ↑

Type

> ☐ 6407 – tf-0000-manage-users

 Successful

Workflow Job



# ANSIBLE TOWER WORKFLOW

IAM



tf-bitbucket-merge\_torni\_update\_branches\_to\_rollout

Job Template

Activity



Organization

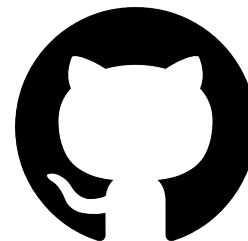
Runtastic

Auto-Merge von branches



# IMPLEMENTIERTE APPLIKATIONEN

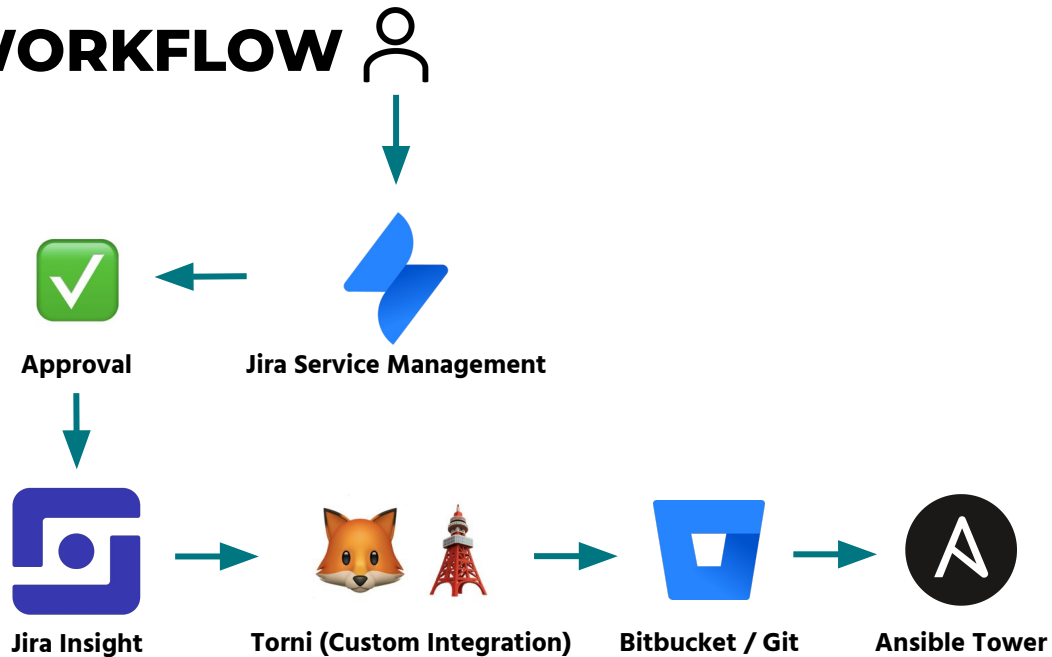
IAM



# **USER WORKFLOW**

# USER WORKFLOW

IAM



# USER WORKFLOW

JIRA SERVICE DESK 

IAM

**RUNTASTIC**

Requests 1 

 [Help Center](#) / [IT Support](#)

**Group or Email group change**

Take a look which groups you already have: [Group or Email group change](#)

Raise this request on behalf of

 Alexander Lackner

Team or User

 Alexander Lackner - allac

Team or user where you would like to change the group. You can only see teams, squads and its members where you are member to.

Action

Add

Approver

 Armin Deliomini - ard

Choose from this list Teamleads and Engineering Managers or HR

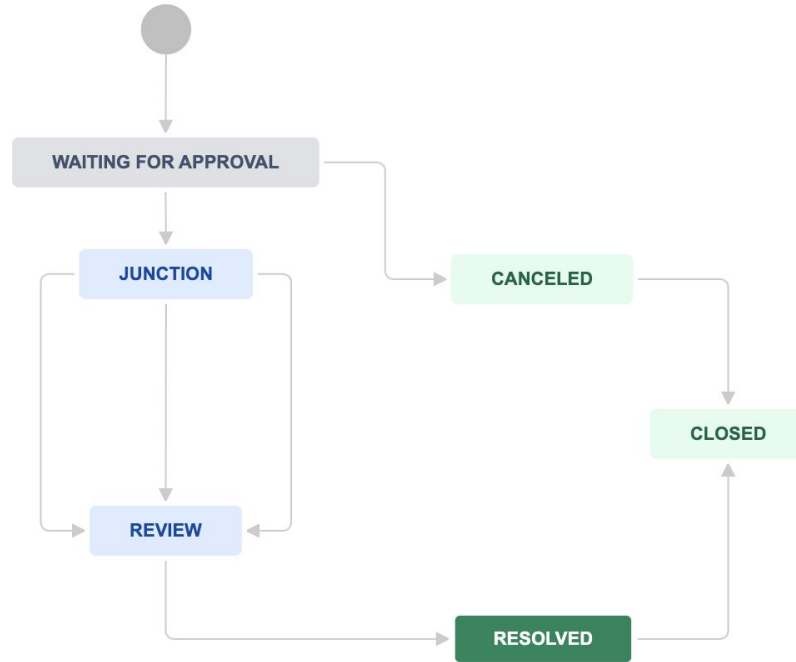
ITS Groups *(optional)*

 platform\_ios

# USER WORKFLOW

JIRA Workflow 

IAM





# USER WORKFLOW

JIRA Insight 

IAM

Human Relations / Employee / HR-441748

## Alexander Lackner



Edit



Comment

More ▾



Object Graph



### Details

Name



Groups

Job Title

Team



Alexander Lackner



platform\_ios



Domain Users

Infrastructure Engineer



Infrastructure

# USER WORKFLOW

IAM



Jira Insight



Torni (Custom Integration)



JSON



Bitbucket / Git

 platform\_ios  Domain Users

```
"groups": [  
  "CN=Domain Users,CN=Groups,DC=tst,DC=runlastic,DC=com",  
  "CN=platform_ios,CN=Groups,DC=tst,DC=runlastic,DC=com"  
],
```

# USER WORKFLOW

Bitbucket / Git 

IAM

```
1 1      {
2 2      "ucs": {
3 3          "password": "no initial password here",
4 4          "state": "present",
5 5          "groups": [
6 6      -      "CN=Domain Users,CN=Groups,DC=tst,DC=runtastic,DC=com"
7 7      +      "CN=Domain Users,CN=Groups,DC=tst,DC=runtastic,DC=com",
8 8      +      "CN=platform_ios,CN=Groups,DC=tst,DC=runtastic,DC=com"
9 9      ],
10 10     "networkAccess": true
11 11     }
12 12 }
```

# USER WORKFLOW

Ansible Tower 

IAM

☐ **tf-0000-manage-users**

Activity



Jira Ticket



Status:

**RESOLVED** (View Workflow)



Additional groups



Groups

☐ Select all

☐ Domain Users

☐ platform\_ios

ADD

REMOVE

**DEMO**



**FUTURE**



- Weitere Applikationen ergänzen
- Potentiell teile des Codes **Open Sourcen**
- Test von **async** für das schnellere Ausführen des Workflows



# SUMMARY





- **Vollautomatisierter** Workflow für IAM
- Integration von neuen Tools relativ **einfach** möglich
- Volle **Kontrolle** über den Code
- Manuelle Tasks werden auf ein **Minimum** reduziert
  - Mehr **Ressourcen** für andere Aufgaben
- Mehr **Sicherheit** - Accounts können nicht mehr vergessen werden

# SUMMARY

IAM

- **Entwickler** 

- Georg Gadinger alias **Foxy** 
- Peter Löffler
- Alexander Lackner
- Runtastic **Infrastructure** Team

**RUNTASTIC**

**THANK YOU**  
AND HAVE A GREAT DAY



Runtastic.com



**ALEXANDER LACKNER**  
Infrastructure Engineer

[alexander.lackner@runtastic.com](mailto:alexander.lackner@runtastic.com)

# Q&A

