

Setup twigs based discovery of your Azure Container Registry (ACR)

Overview

Twigs can help discover your Azure Container Registry and scan all container images in your ACR. Twigs requires you to login into your ACR to read your ACR contents. Also it requires that you perform “docker login” to be able to pull container images from your ACR for vulnerability scanning.

This document describes how you can create a service principal in Azure portal and use the same to discover your ACR using twigs.

Create service principal / app in Azure AD

- Login in to your Azure Portal
- Register app under Azure AD Tenant
 - Select Azure Directory
 - Select “App Registrations”
 - Select “New Registrations”
 - Specify “Name” and select appropriate value for “Supported account types” for your organization

[Home](#) > [Default Directory](#) >

Register an application

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

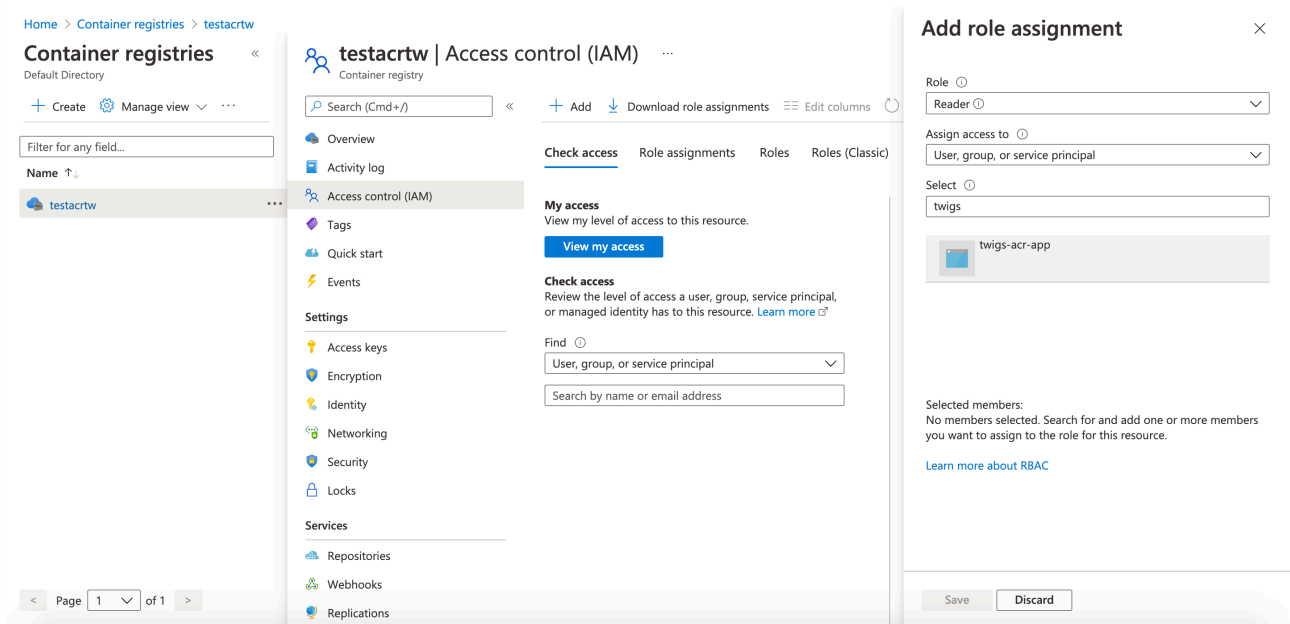
Register

- Click “Register”

Grant required roles to service principal / App

Assign required roles (Reader, AcrPull) to the service principal / App

- In Azure Portal, you need to select the level of scope you wish to assign to the application. You can set the scope at the level of the subscription, resource group, or resource. Here we have selected ACR resource.
- Select “Access Control (IAM)”
- Select “Add role assignment”
- Select Role as “Reader”
- Select the Service Principal / App that you created earlier and add it.



The screenshot shows the Azure Portal interface for a Container Registry resource named 'testactrw'. The 'Access control (IAM)' page is active, and the 'Add role assignment' dialog is open. The dialog shows the role 'Reader' assigned to the service principal 'twigs-acr-app'. The 'Selected members' section is empty, indicating no members have been selected for this role.

- Now similarly add role as “AcrPull” and save.

Create application secret for service principal / App

Create application secret for authentication

- In the Azure Portal select your Azure AD
- From “App Registrations”, select your application
- Select “Certificates & secrets”
- Select “Client secrets —> New client secret”
- Copy the value of the client secret, because you won’t be able to retrieve it later.



Home > Default Directory > twigs-acr-app

twigs-acr-app | Certificates & secrets

Search (Cmd+/)

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication
 - Certificates & secrets**
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators | Preview
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
------------	------------	---------	----

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	ID
sample secret	5/7/2022	[REDACTED]	[REDACTED]

Login as Service Principal / App on twigs box

This involves 3 steps as below:

1. Perform "az login" using the service principal as below:

```
az login --service-principal --username APP_ID --password PASSWORD --tenant TENANT_ID
```

2. Login into ACR using the command below:

```
az acr login --name MYREGISTRY
```

3. Perform docker login using the command below:

```
docker login MYREGISTRY.azurecr.io --username APP_ID --password PASSWORD
```

Run twigs

```
twigs -v acr --registry MYREGISTRY
```

Note you may want to add the above command to cron using "schedule" option in twigs.