Cloud Village

Azure DevOps Security

Viktor Gazdag

WhoAmI

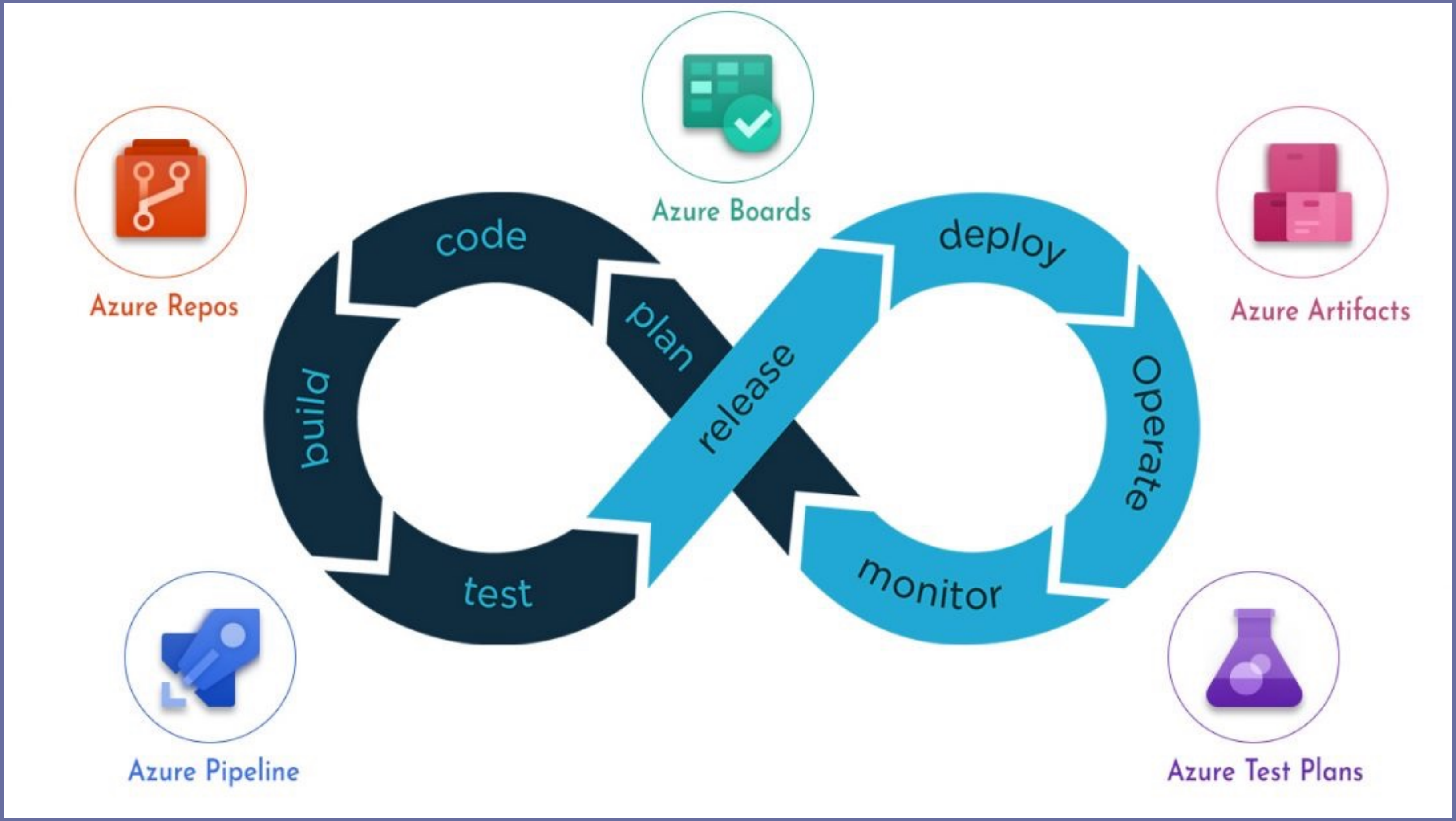
- Managing Security Consultant at NCC Group
- Cloud and CI/CD Security
- Azure DevOps Certification (AZ-400)
- 2019 Jenkins Security MVP
- Multiple Responsible Disclosure (Jenkins, Nexus, Sonatype, JetBrains)
- Black Hat USA 2022 RCE-as-a-Service

Azure DevOps

- “Azure DevOps is a Software as a service (SaaS) platform from Microsoft that provides an end-to-end DevOps toolchain for developing and deploying software.” - Microsoft

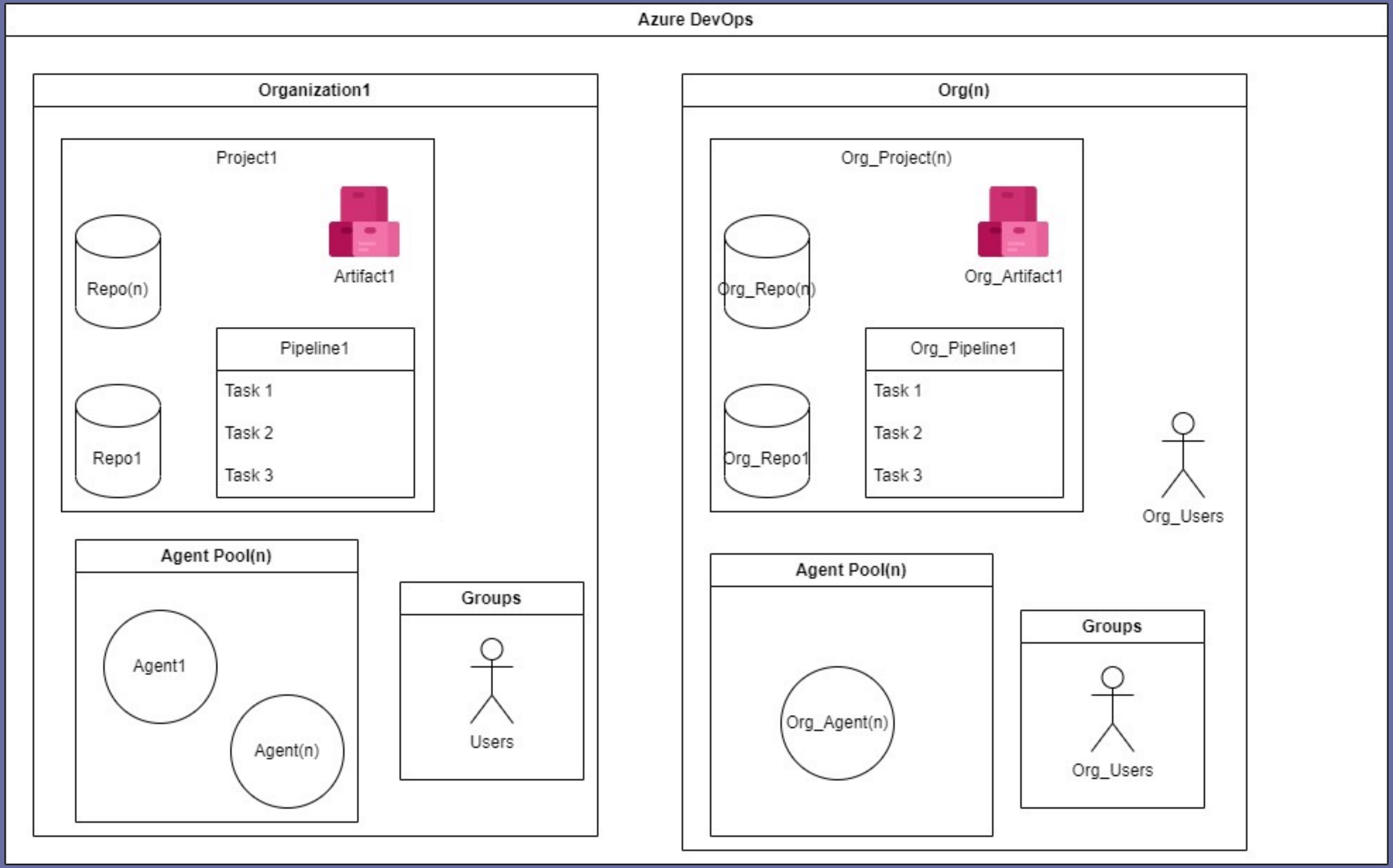
Azure DevOps - ADO

Cloud Village



Azure DevOps

Cloud Village



Related Services

Cloud Village

- DevTest Lab
- Dev Box
- Azure AD Integration (AAD)
- Defender for DevOps
- Key Vault

Cloud DevOps Security

Cloud Village

- Security ***in*** the pipeline
- Security ***of*** the pipeline
- Security around the pipeline*

Authentication

Cloud Village

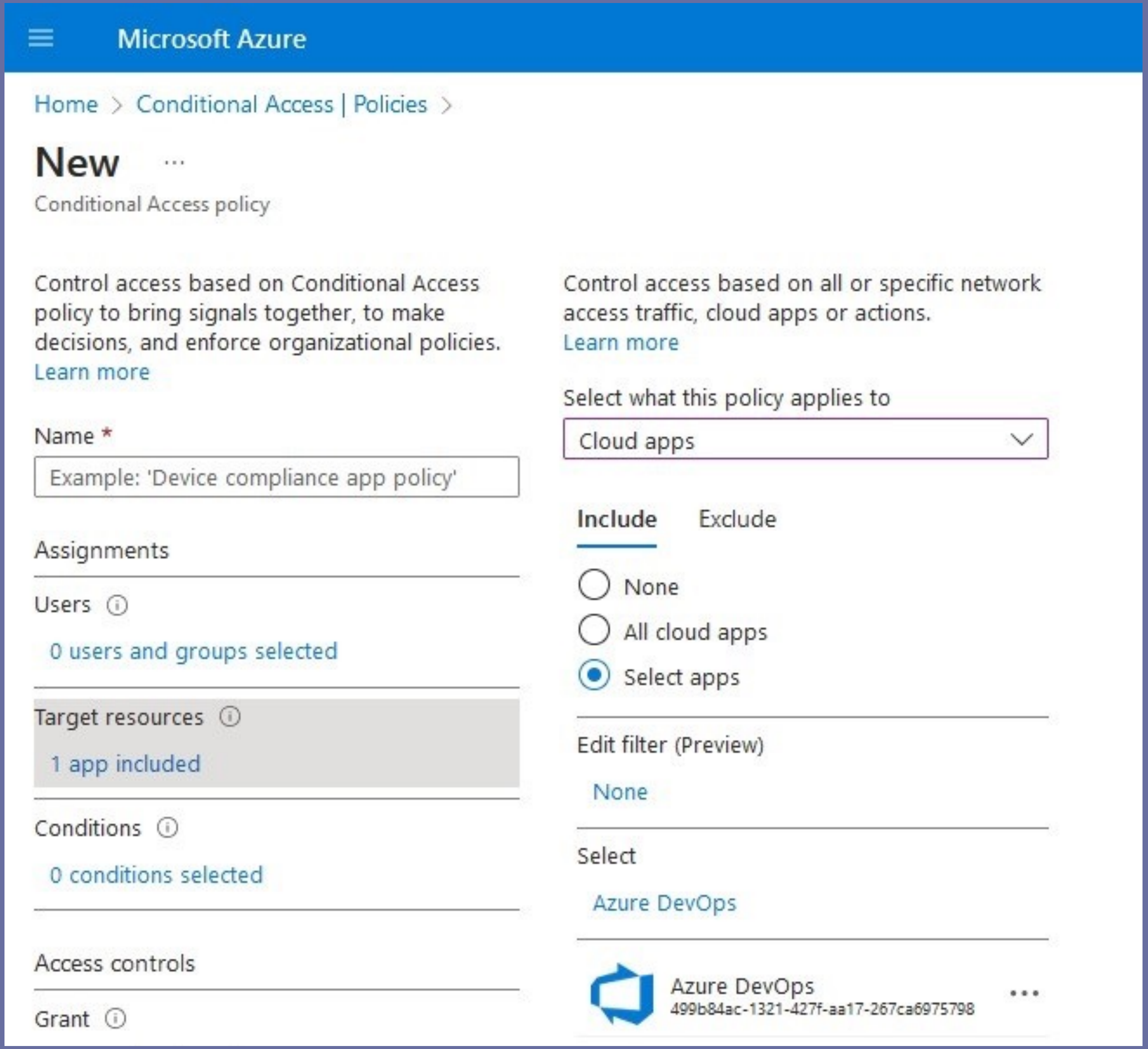
- https://dev.azure.com/YourOrgName/
- Azure AD Integration
- Conditional Access Policy (CA)

Authentication

- Password Spray
- Password Brute-Force
- Unauthorized Access

Authentication

Cloud Village



Microsoft Azure

Home > Conditional Access | Policies >

New ···

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users ⓘ

0 users and groups selected

Target resources ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

Control access based on all or specific network access traffic, cloud apps or actions. Learn more

Select what this policy applies to

Cloud apps

Include | Exclude

○ None
○ All cloud apps
● Select apps

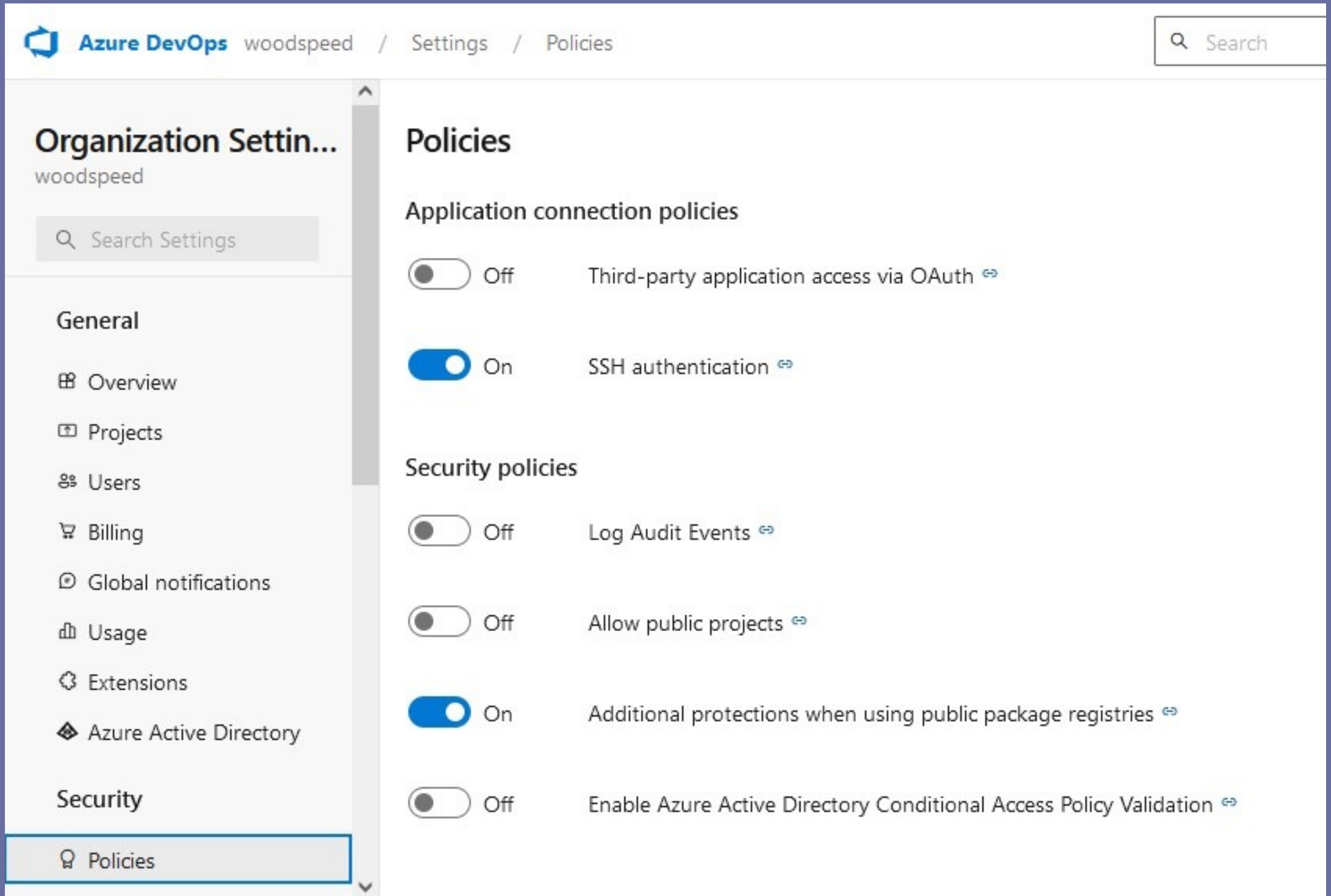
Edit filter (Preview)

None

Select

Azure DevOps

Azure DevOps
499b84ac-1321-427f-aa17-267ca6975798 ···



Azure DevOps woodspeed / Settings / Policies

Search

Organization Settin...
woodspeed

Search Settings

General
- Overview
- Projects
- Users
- Billing
- Global notifications
- Usage
- Extensions
- Azure Active Directory

Security
- Policies

Policies

Application connection policies

Off	Third-party application access via OAuth
On	SSH authentication

Security policies

Off	Log Audit Events
Off	Allow public projects
On	Additional protections when using public package registries
Off	Enable Azure Active Directory Conditional Access Policy Validation

Authorization

- Security: Project, Pipeline, Repo, Agent, Secret, Feed
- Privilege Identity Management (PIM)
- Azure DevOps Administrator

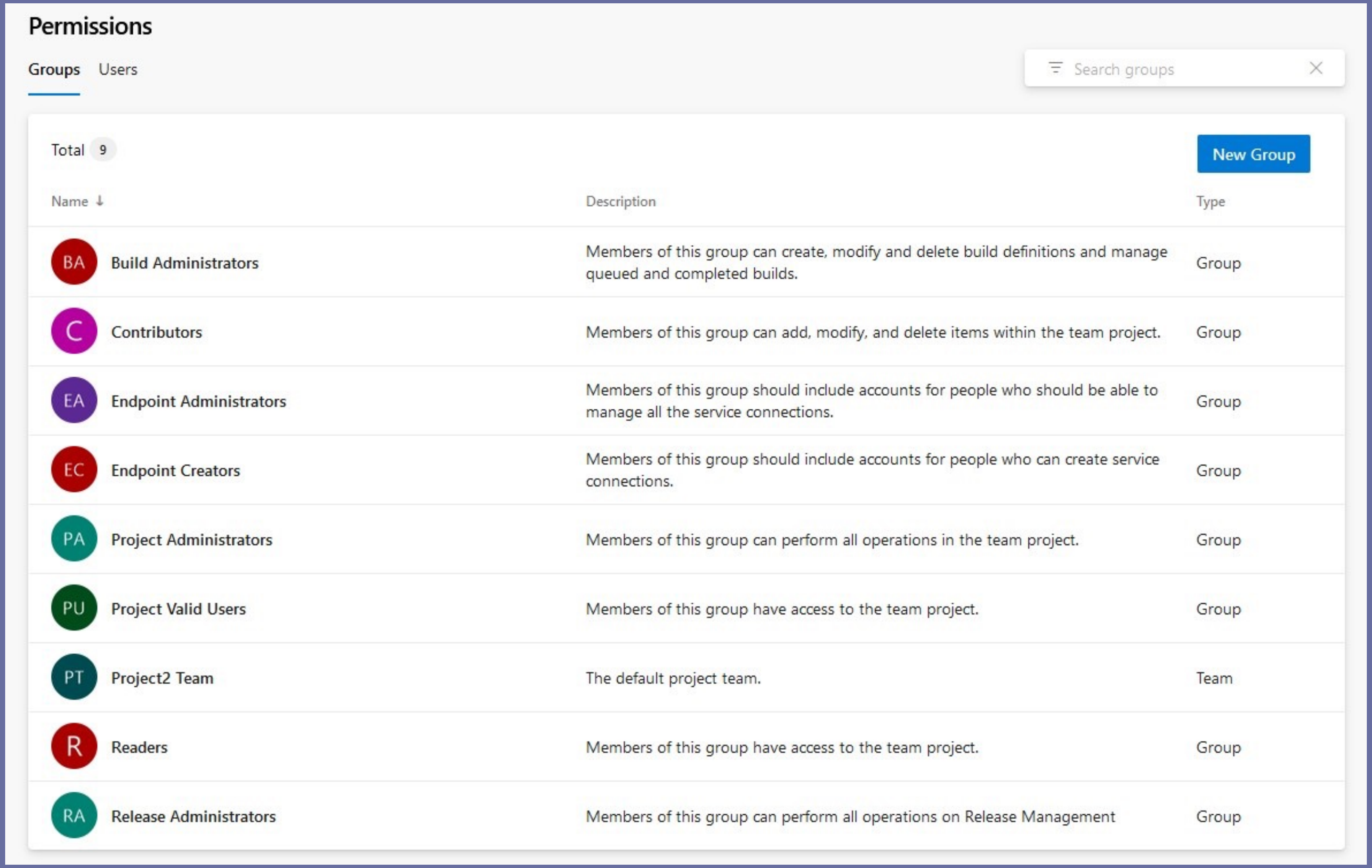
Authorization

Cloud Village

- Unauthorized Access (User, Pipeline, Repo, Agent)
- Privilege Escalation
- Malicious Code Injection
- Steal Code

Authorization

Cloud Village



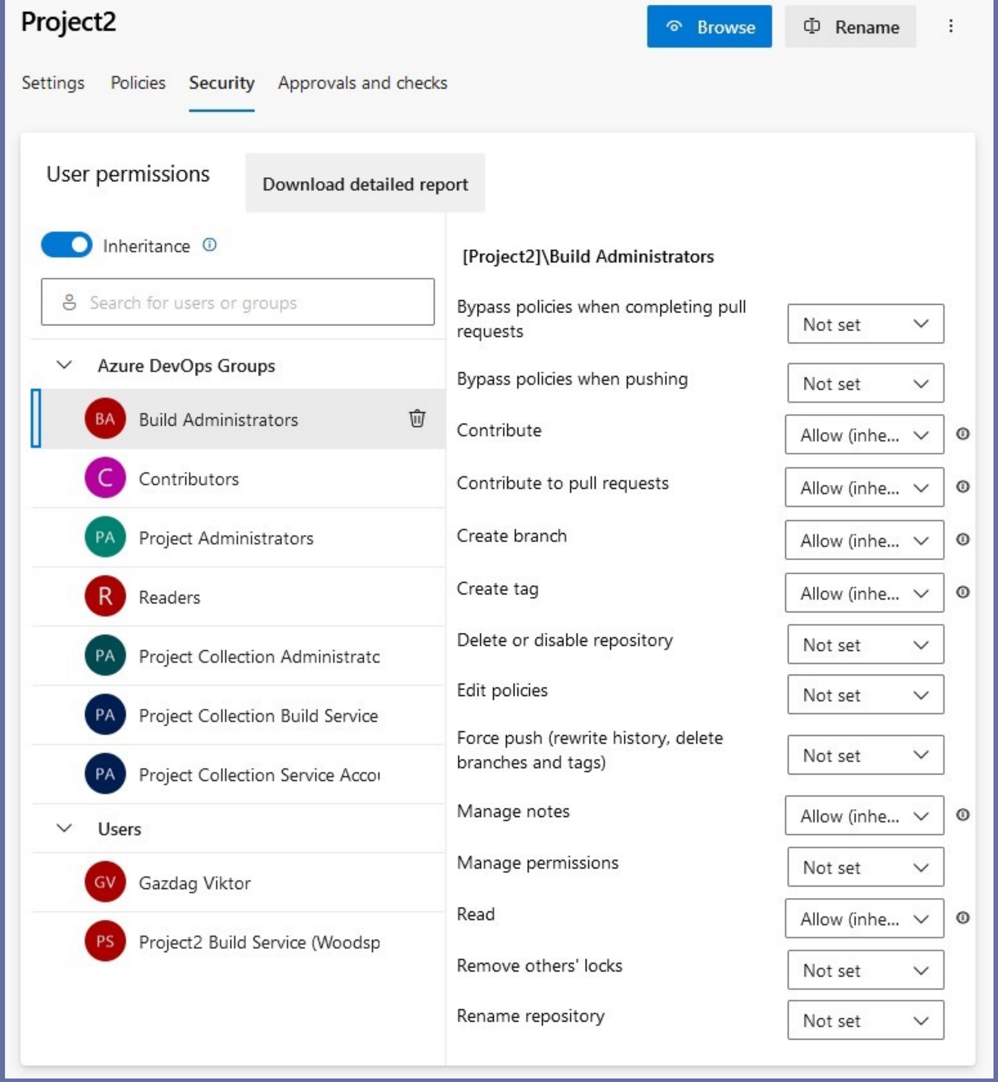
Permissions

Total 9

Name ↓	Description	Type
BA Build Administrators	Members of this group can create, modify and delete build definitions and manage queued and completed builds.	Group
C Contributors	Members of this group can add, modify, and delete items within the team project.	Group
EA Endpoint Administrators	Members of this group should include accounts for people who should be able to manage all the service connections.	Group
EC Endpoint Creators	Members of this group should include accounts for people who can create service connections.	Group
PA Project Administrators	Members of this group can perform all operations in the team project.	Group
PU Project Valid Users	Members of this group have access to the team project.	Group
PT Project2 Team	The default project team.	Team
R Readers	Members of this group have access to the team project.	Group
RA Release Administrators	Members of this group can perform all operations on Release Management	Group

Authorization

Cloud Village



Project2

Browse Rename

Settings Policies Security Approvals and checks

User permissions

Download detailed report

Inheritance

Search for users or groups

Azure DevOps Groups

- BA Build Administrators
- C Contributors
- PA Project Administrators
- R Readers
- PA Project Collection Administratc
- PA Project Collection Build Service
- PA Project Collection Service Accoı

Users

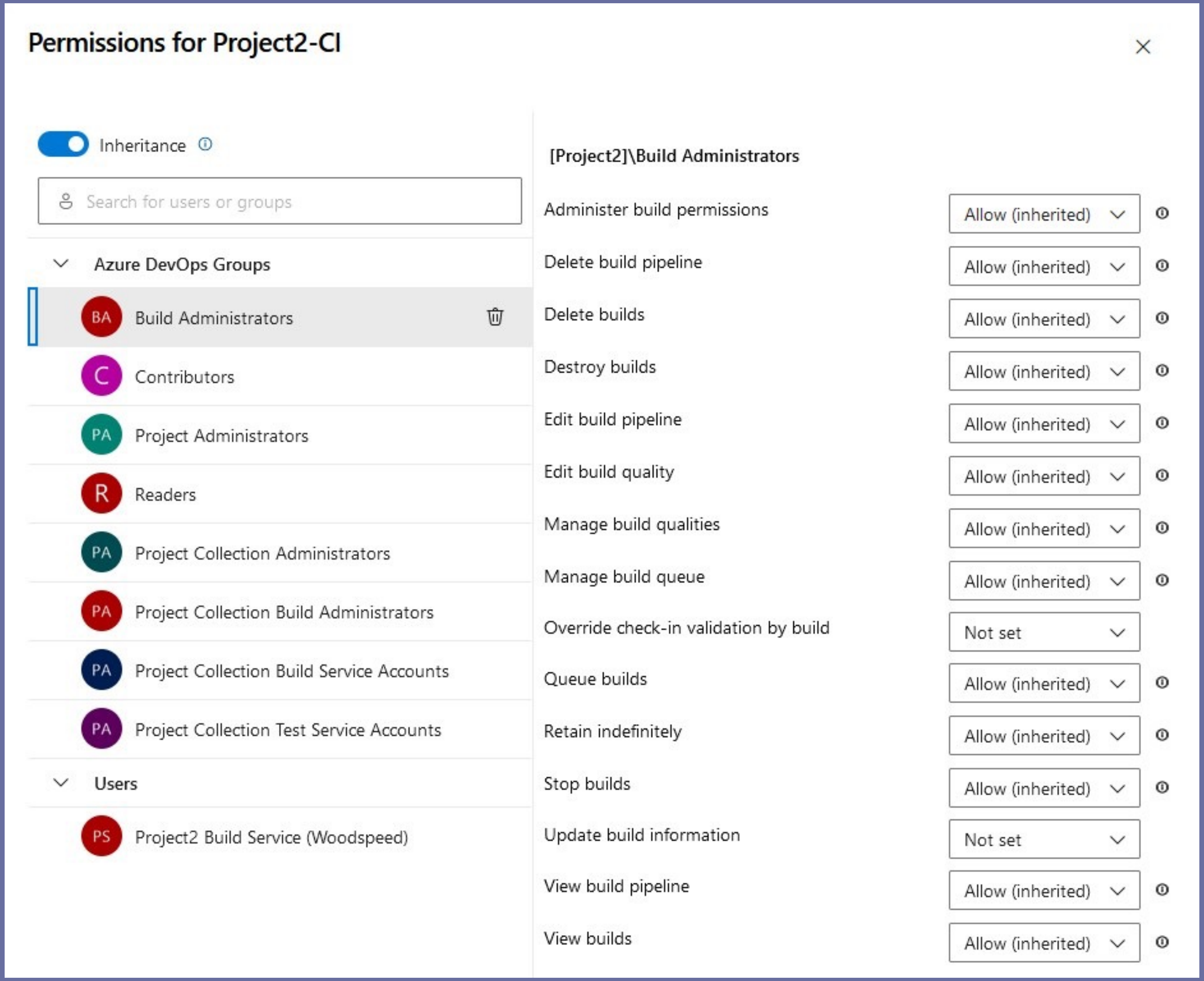
- GV Gazdag Viktor
- PS Project2 Build Service (Woodsp

[Project2]\Build Administrators

Bypass policies when completing pull requests	Not set
Bypass policies when pushing	Not set
Contribute	Allow (inhe...
Contribute to pull requests	Allow (inhe...
Create branch	Allow (inhe...
Create tag	Allow (inhe...
Delete or disable repository	Not set
Edit policies	Not set
Force push (rewrite history, delete branches and tags)	Not set
Manage notes	Allow (inhe...
Manage permissions	Not set
Read	Allow (inhe...
Remove others' locks	Not set
Rename repository	Not set

Authorization

Cloud Village



Permissions for Project2-CI

Inheritance

Search for users or groups

Azure DevOps Groups

- BA Build Administrators
- C Contributors
- PA Project Administrators
- R Readers
- PA Project Collection Administrators
- PA Project Collection Build Administrators
- PA Project Collection Build Service Accounts
- PA Project Collection Test Service Accounts

Users

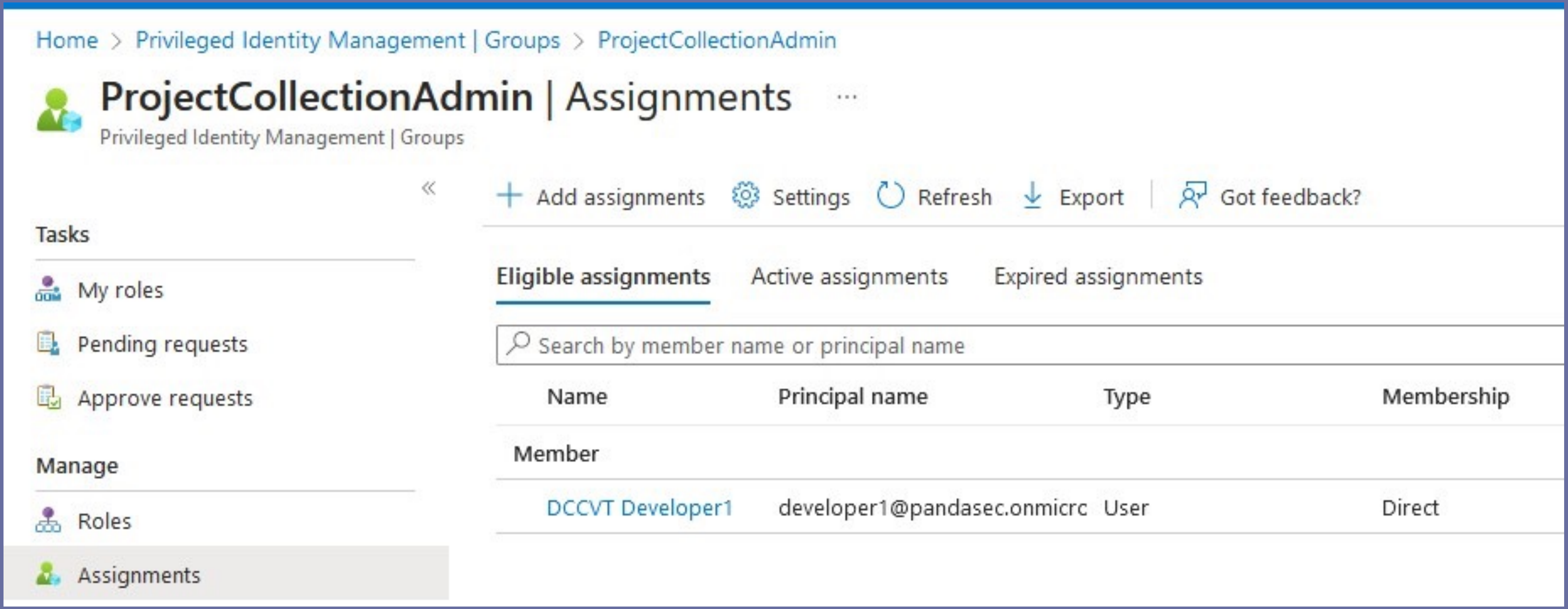
- PS Project2 Build Service (Woodspeed)

[Project2]\Build Administrators

Administer build permissions	Allow (inherited)
Delete build pipeline	Allow (inherited)
Delete builds	Allow (inherited)
Destroy builds	Allow (inherited)
Edit build pipeline	Allow (inherited)
Edit build quality	Allow (inherited)
Manage build qualities	Allow (inherited)
Manage build queue	Allow (inherited)
Override check-in validation by build	Not set
Queue builds	Allow (inherited)
Retain indefinitely	Allow (inherited)
Stop builds	Allow (inherited)
Update build information	Not set
View build pipeline	Allow (inherited)
View builds	Allow (inherited)

Authorization

Cloud Village



Home > Privileged Identity Management | Groups > ProjectCollectionAdmin

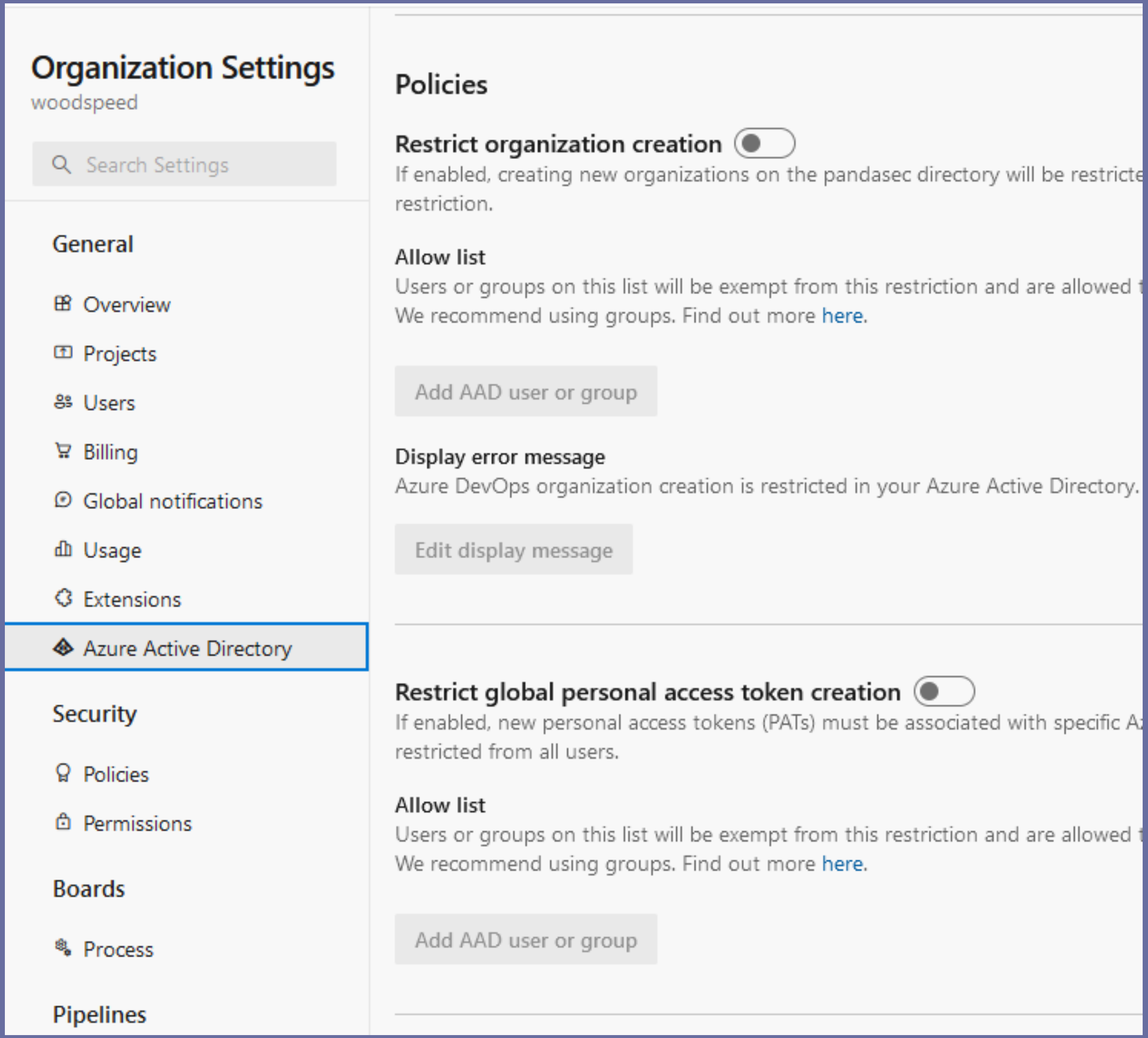
ProjectCollectionAdmin | Assignments

Privileged Identity Management | Groups

Name	Principal name	Type	Membership
Member			
DCCVT Developer1	developer1@pandasec.onmicrc	User	Direct

Authorization

Cloud Village



Organization Settings

woodspeed

Search Settings

General

- Overview
- Projects
- Users
- Billing
- Global notifications
- Usage
- Extensions
- Azure Active Directory

Security

- Policies
- Permissions

Boards

- Process

Pipelines

Policies

Restrict organization creation

If enabled, creating new organizations on the pandasec directory will be restricte restriction.

Allow list

Users or groups on this list will be exempt from this restriction and are allowed t We recommend using groups. Find out more here.

Add AAD user or group

Display error message

Azure DevOps organization creation is restricted in your Azure Active Directory.

Edit display message

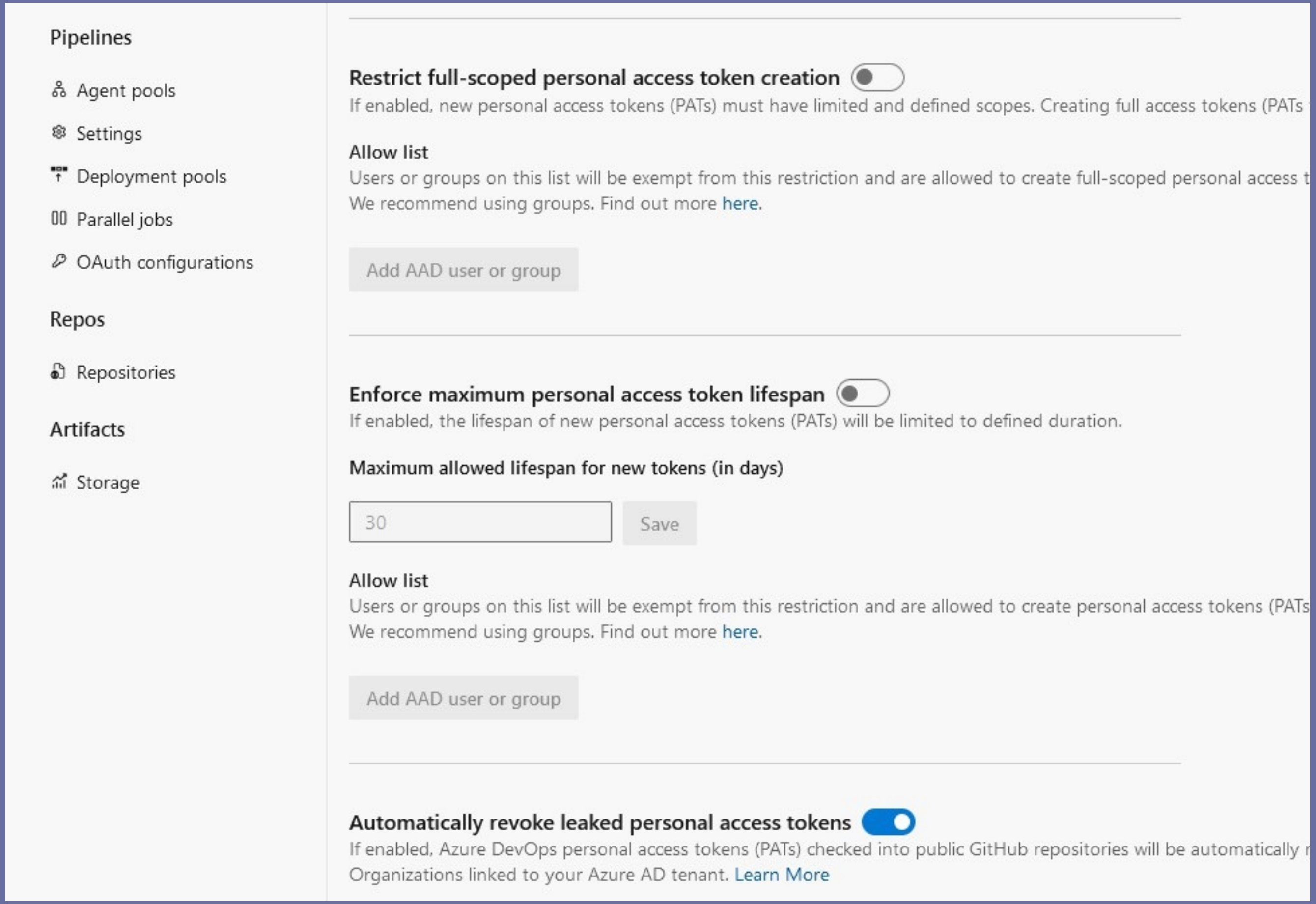
Restrict global personal access token creation

If enabled, new personal access tokens (PATs) must be associated with specific A restricted from all users.

Allow list

Users or groups on this list will be exempt from this restriction and are allowed t We recommend using groups. Find out more here.

Add AAD user or group



Pipelines

- Agent pools
- Settings
- Deployment pools
- Parallel jobs
- OAuth configurations

Repos

- Repositories

Artifacts

- Storage

Restrict full-scoped personal access token creation

If enabled, new personal access tokens (PATs) must have limited and defined scopes. Creating full access tokens (PATs

Allow list

Users or groups on this list will be exempt from this restriction and are allowed to create full-scoped personal access t We recommend using groups. Find out more here.

Add AAD user or group

Enforce maximum personal access token lifespan

If enabled, the lifespan of new personal access tokens (PATs) will be limited to defined duration.

Maximum allowed lifespan for new tokens (in days)

30 Save

Allow list

Users or groups on this list will be exempt from this restriction and are allowed to create personal access tokens (PATs We recommend using groups. Find out more here.

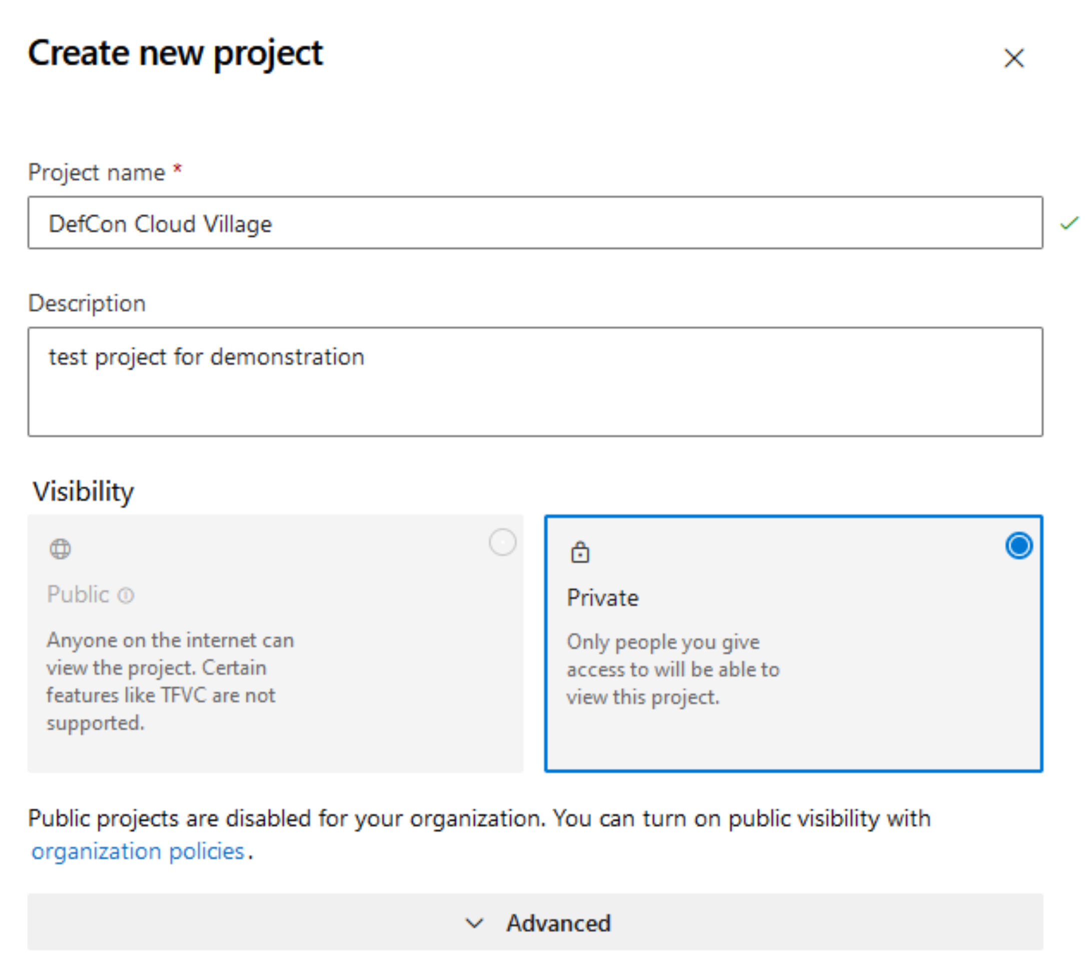
Add AAD user or group

Automatically revoke leaked personal access tokens

If enabled, Azure DevOps personal access tokens (PATs) checked into public GitHub repositories will be automatically r Organizations linked to your Azure AD tenant. Learn More

Project Visibility

Cloud Village



Create new project

Project name *

DefCon Cloud Village

Description

test project for demonstration

Visibility

○ Public

Anyone on the internet can view the project. Certain features like TFVC are not supported.

● Private

Only people you give access to will be able to view this project.

Public projects are disabled for your organization. You can turn on public visibility with organization policies.

Repos

- Unknown Changes
- Unauthorized Changes
- Backdoor Code
- Code Stealing
- Over Permissive Privilege

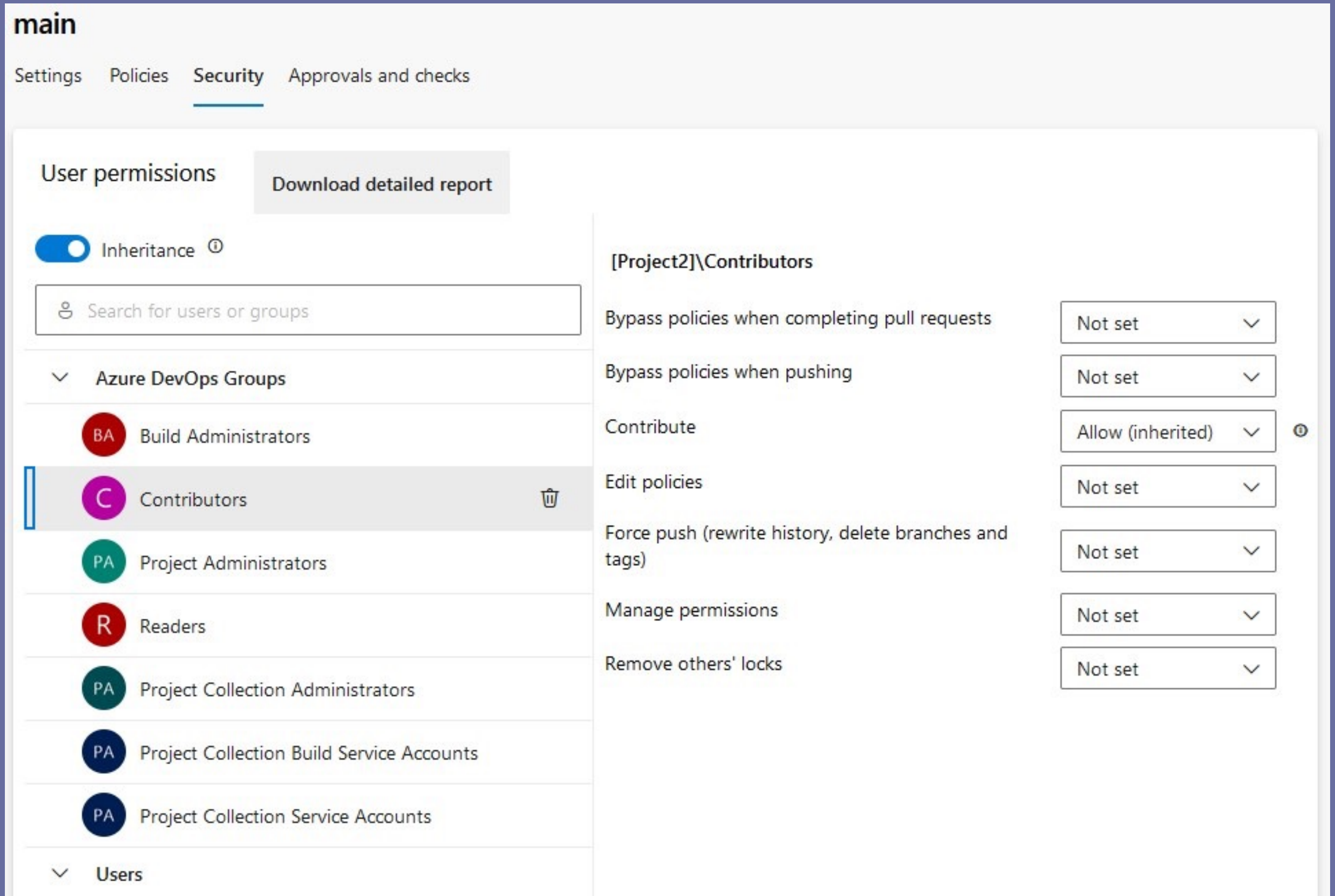
Repos

Cloud Village

- Security
- Pipeline Access
- Commit Author Email Validation
- Create Branch

Repos

Cloud Village



main

User permissions

Azure DevOps Groups

- BA Build Administrators
- C Contributors
- PA Project Administrators
- R Readers
- PA Project Collection Administrators
- PA Project Collection Build Service Accounts
- PA Project Collection Service Accounts

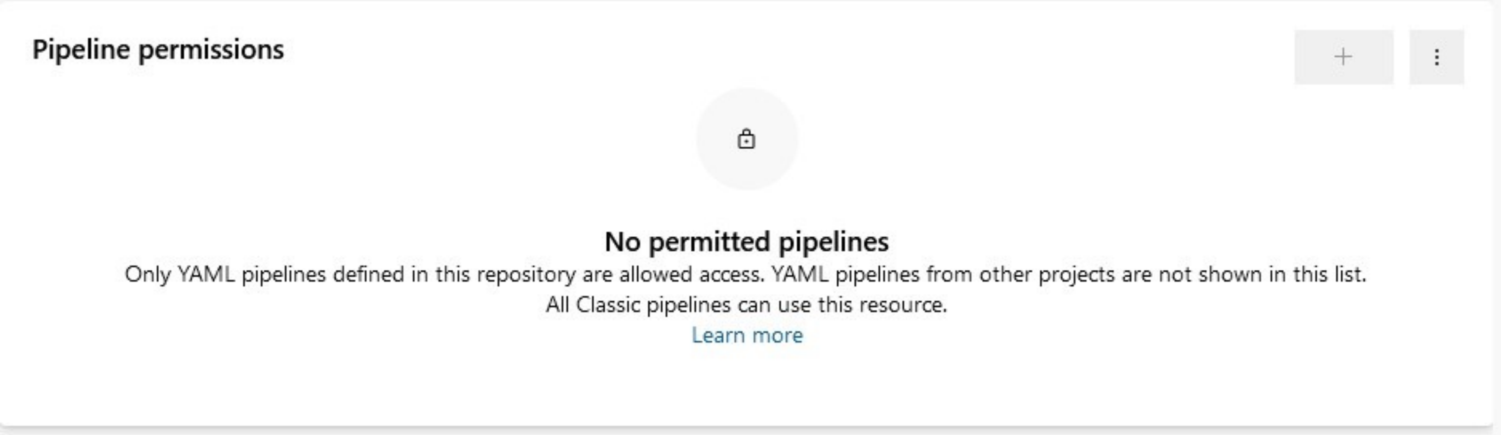
Users

[Project2]\Contributors

Bypass policies when completing pull requests	Not set
Bypass policies when pushing	Not set
Contribute	Allow (inherited)
Edit policies	Not set
Force push (rewrite history, delete branches and tags)	Not set
Manage permissions	Not set
Remove others' locks	Not set

Repos

Cloud Village



Pipeline permissions

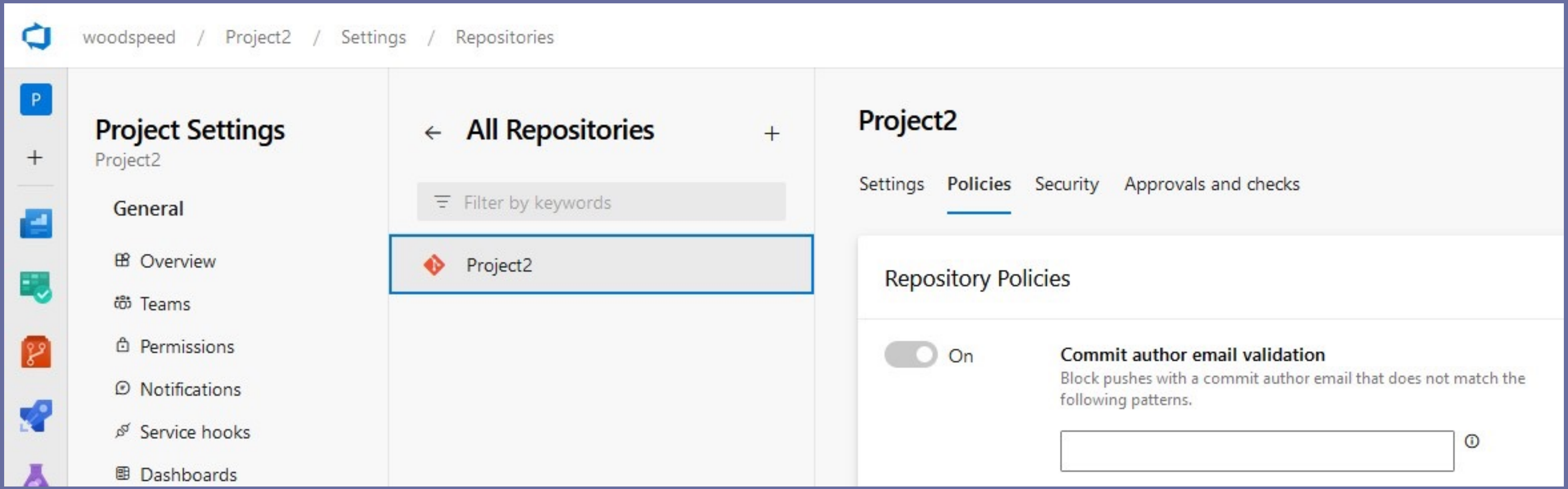
No permitted pipelines

Only YAML pipelines defined in this repository are allowed access. YAML pipelines from other projects are not shown in this list.
All Classic pipelines can use this resource.

Learn more

Repos

Cloud Village



woodspeed / Project2 / Settings / Repositories

Project Settings
Project2

General

← All Repositories +

Project2

Project2

Repository Policies

On **Commit author email validation**
Block pushes with a commit author email that does not match the following patterns.

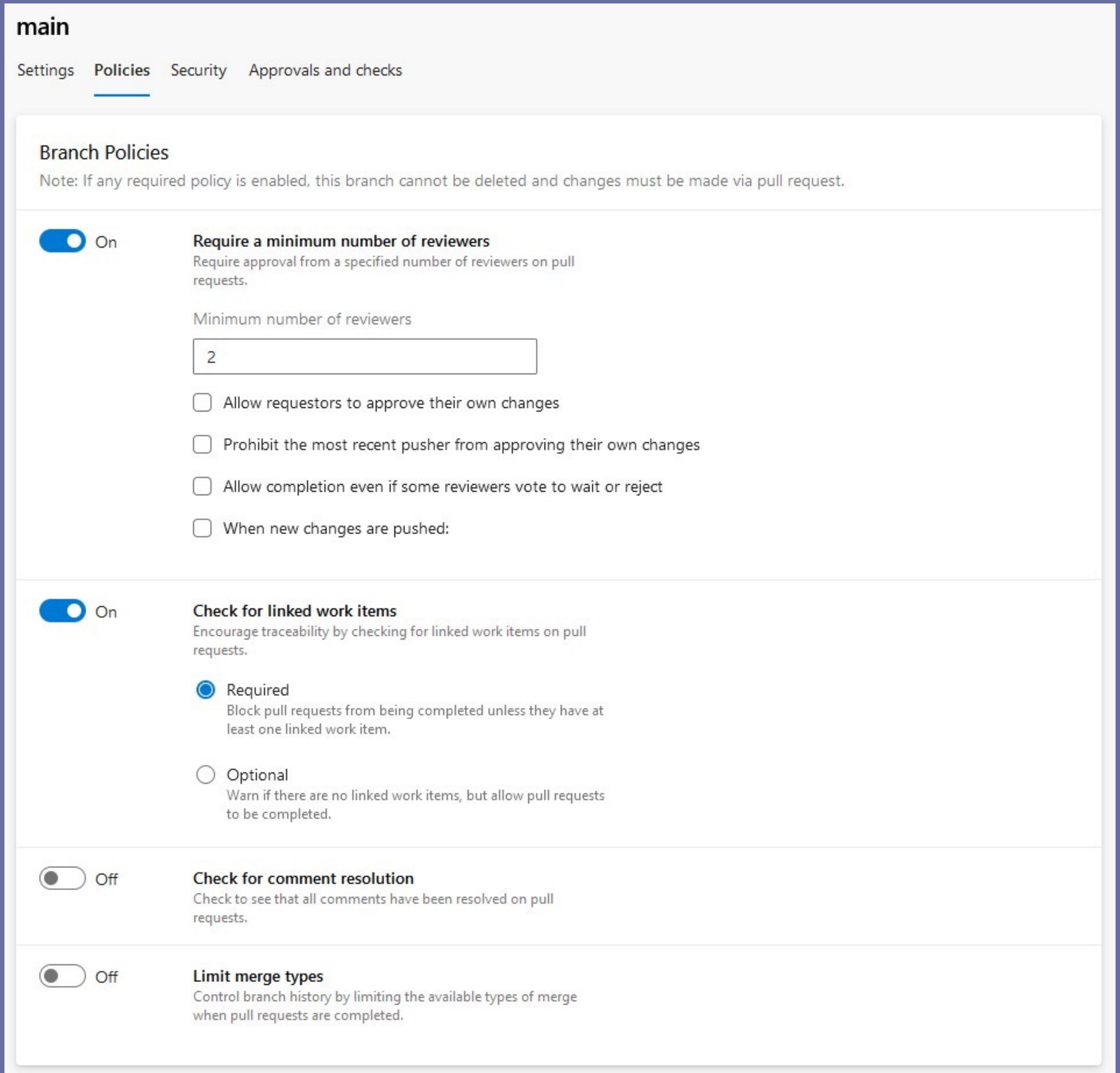
Branch

Cloud Village

- PR Reviewers
- Linked Work Items
- Branch Control

Branch

Cloud Village



main

Branch Policies

Note: If any required policy is enabled, this branch cannot be deleted and changes must be made via pull request.

On **Require a minimum number of reviewers**
Require approval from a specified number of reviewers on pull requests.

Minimum number of reviewers: 2

□ Allow requestors to approve their own changes

□ Prohibit the most recent pusher from approving their own changes

□ Allow completion even if some reviewers vote to wait or reject

□ When new changes are pushed:

On **Check for linked work items**
Encourage traceability by checking for linked work items on pull requests.

● Required
Block pull requests from being completed unless they have at least one linked work item.

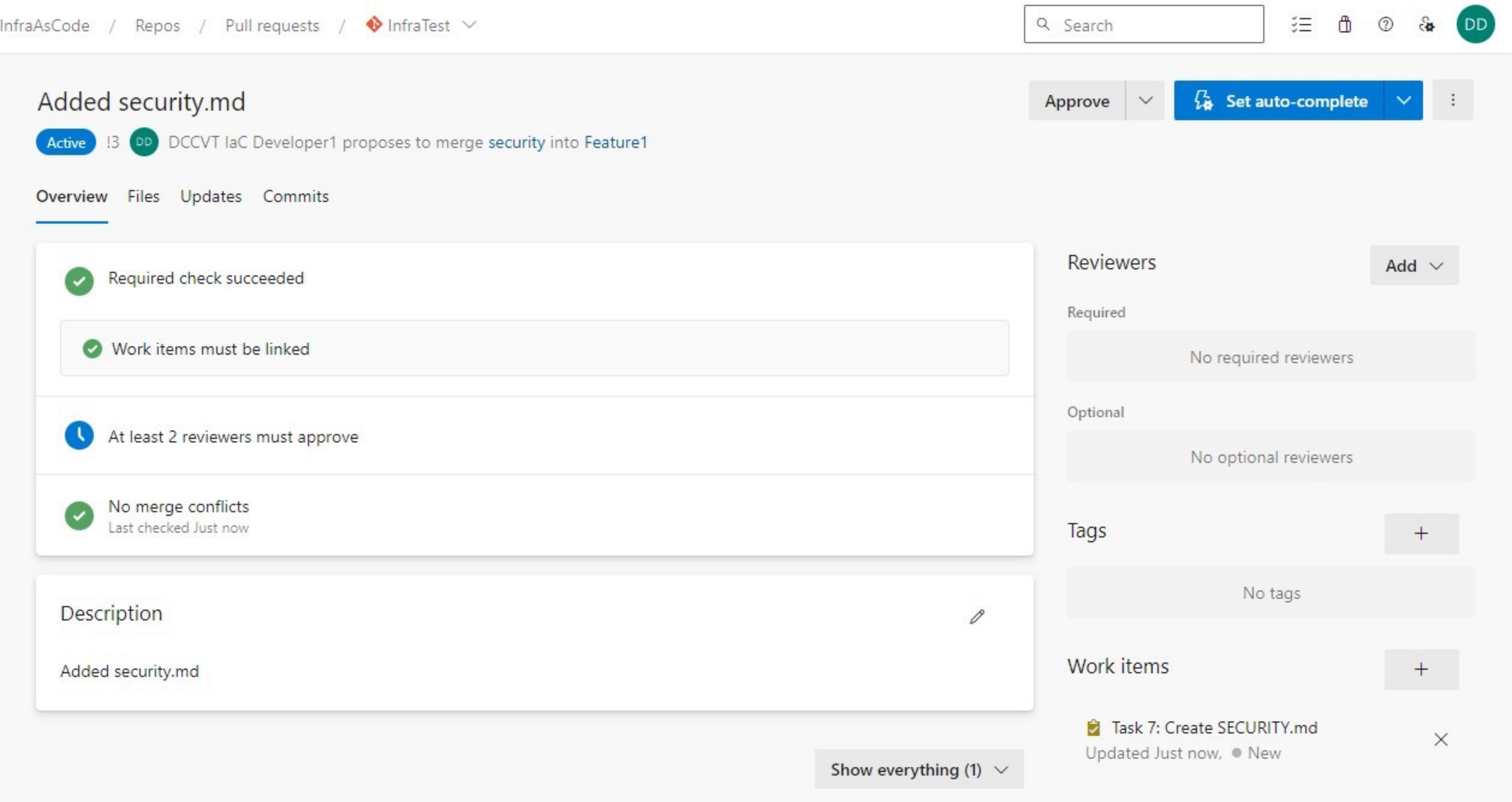
○ Optional
Warn if there are no linked work items, but allow pull requests to be completed.

Off **Check for comment resolution**
Check to see that all comments have been resolved on pull requests.

Off **Limit merge types**
Control branch history by limiting the available types of merge when pull requests are completed.

Branch

Cloud Village



Added security.md

Active !3 DD DCCVT IaC Developer1 proposes to merge security into Feature1

✓ Required check succeeded

✓ Work items must be linked

At least 2 reviewers must approve

✓ No merge conflicts
Last checked Just now

Description

Added security.md

Reviewers

Required

No required reviewers

Optional

No optional reviewers

Tags

No tags

Work items

Task 7: Create SECURITY.md
Updated Just now, ● New

Pipelines

Cloud Village

- Build vs Release
- Classic vs YAML
- Classic Build Disabled

Pipelines

Cloud Village

- Argument Injection
- Privilege Escalation
- Data Exfiltration
- Auto Build
- Out of Business Hours Build
- Introduce Malicious Step

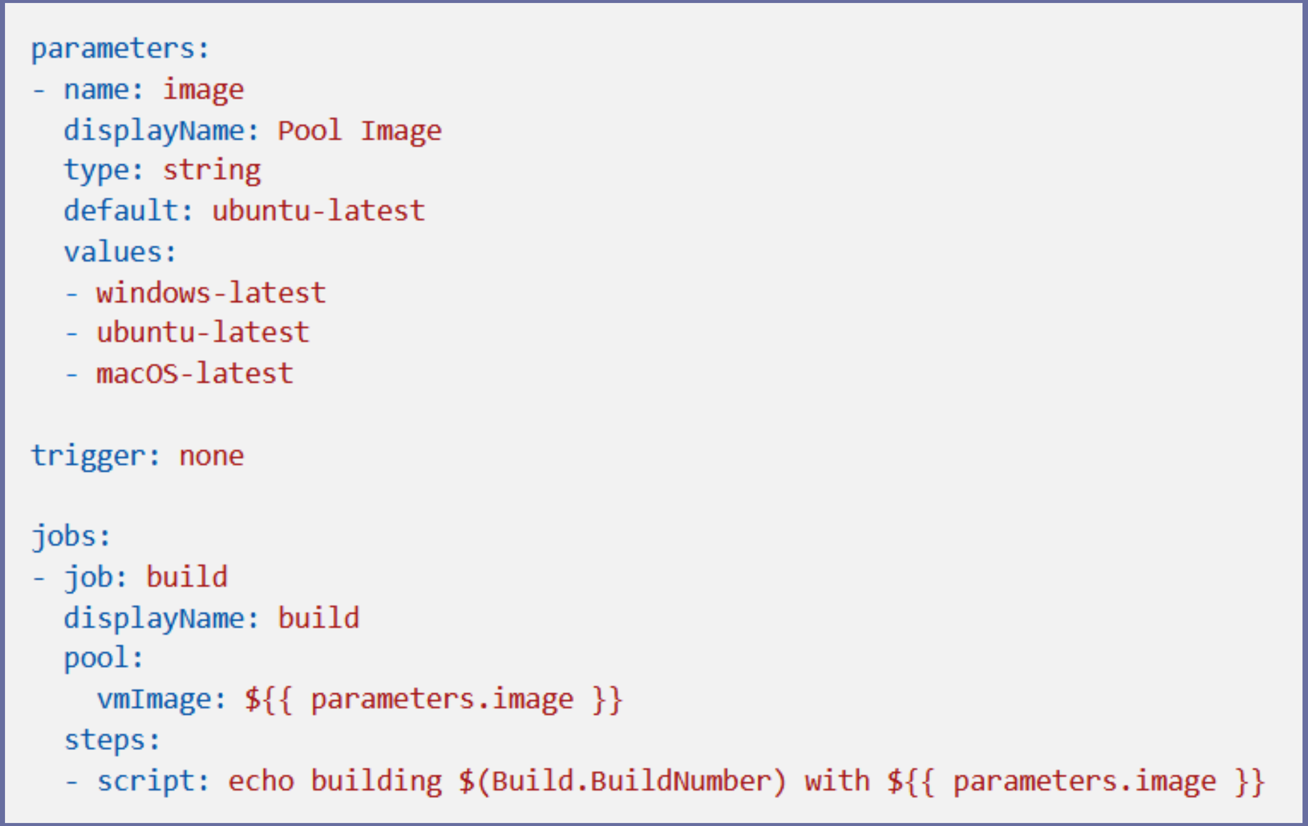
Pipelines

Cloud Village

- Runtime Parameter
- Approvals
- Manual Validation/Intervention
- Branch Control
- Business Hours

Pipelines

- Runtime Parameter



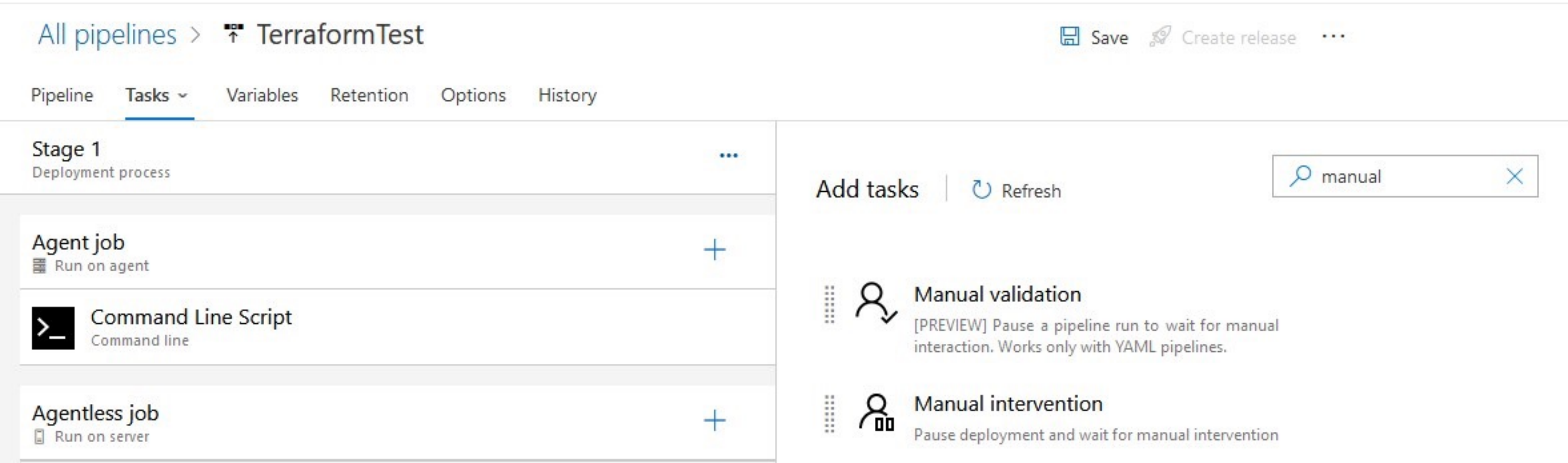
```yaml
parameters:
- name: image
  displayName: Pool Image
  type: string
  default: ubuntu-latest
  values:
  - windows-latest
  - ubuntu-latest
  - macOS-latest

trigger: none

jobs:
- job: build
  displayName: build
  pool:
    vmImage: ${{ parameters.image }}
  steps:
  - script: echo building $(Build.BuildNumber) with ${{ parameters.image }}
```

Pipelines

Cloud Village



All pipelines > TerraformTest

Save · Create release · ···

Pipeline · Tasks · Variables · Retention · Options · History

Stage 1
Deployment process

Agent job
Run on agent

Command Line Script
Command line

Agentless job
Run on server

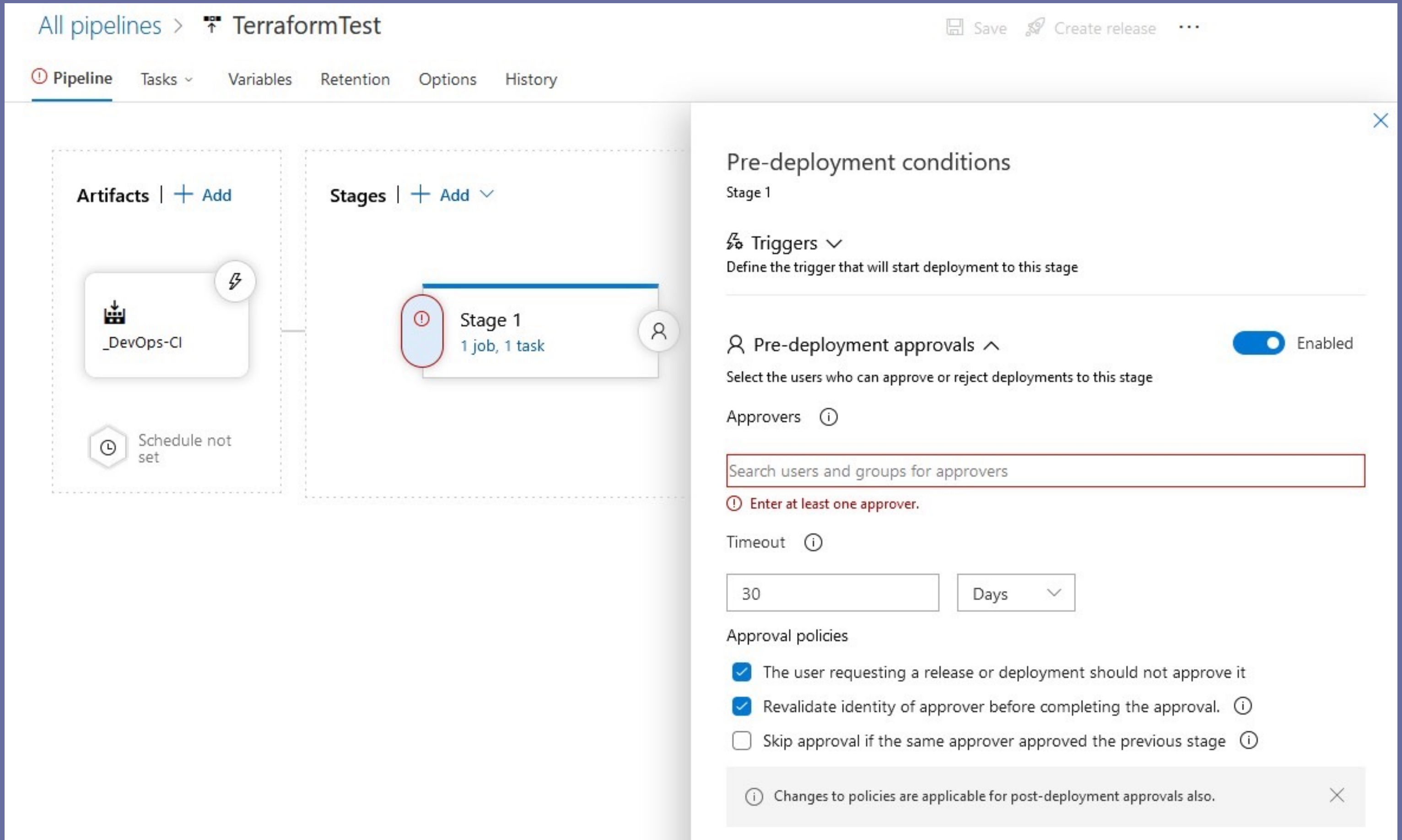
Add tasks · Refresh · manual

Manual validation
[PREVIEW] Pause a pipeline run to wait for manual interaction. Works only with YAML pipelines.

Manual intervention
Pause deployment and wait for manual intervention

Pipelines

Cloud Village



Pre-deployment conditions

Stage 1

Triggers

Define the trigger that will start deployment to this stage

Pre-deployment approvals ● Enabled

Select the users who can approve or reject deployments to this stage

Approvers

Search users and groups for approvers

Enter at least one approver.

Timeout

30 Days

Approval policies

☑ The user requesting a release or deployment should not approve it

☑ Revalidate identity of approver before completing the approval.

□ Skip approval if the same approver approved the previous stage

Changes to policies are applicable for post-deployment approvals also.

Secrets

- Library->Variable Groups (Secret, File)
- Permission for Group/Pipeline/Agent/User
- Key Vault Integration with Auditing

Secrets

- GitOps != store base64 encoded secret in Git

- Secret removed, but still in history, also needs rotation

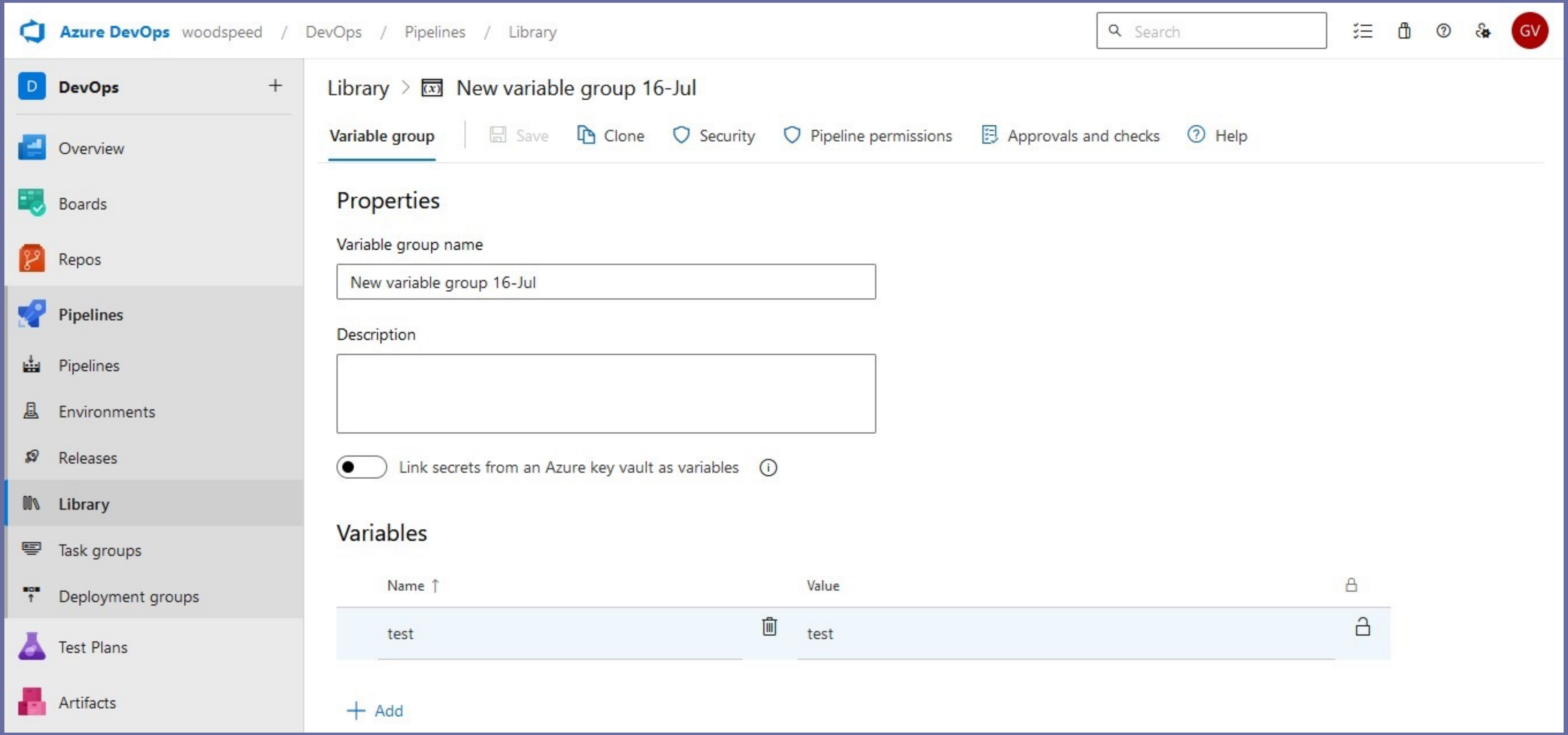
Secrets

Cloud Village

- Read Secrets
- Access Environments/Services
- Privilege Escalation

Secrets

Cloud Village



Properties

Variable group name: New variable group 16-Jul

Description:

○ Link secrets from an Azure key vault as variables

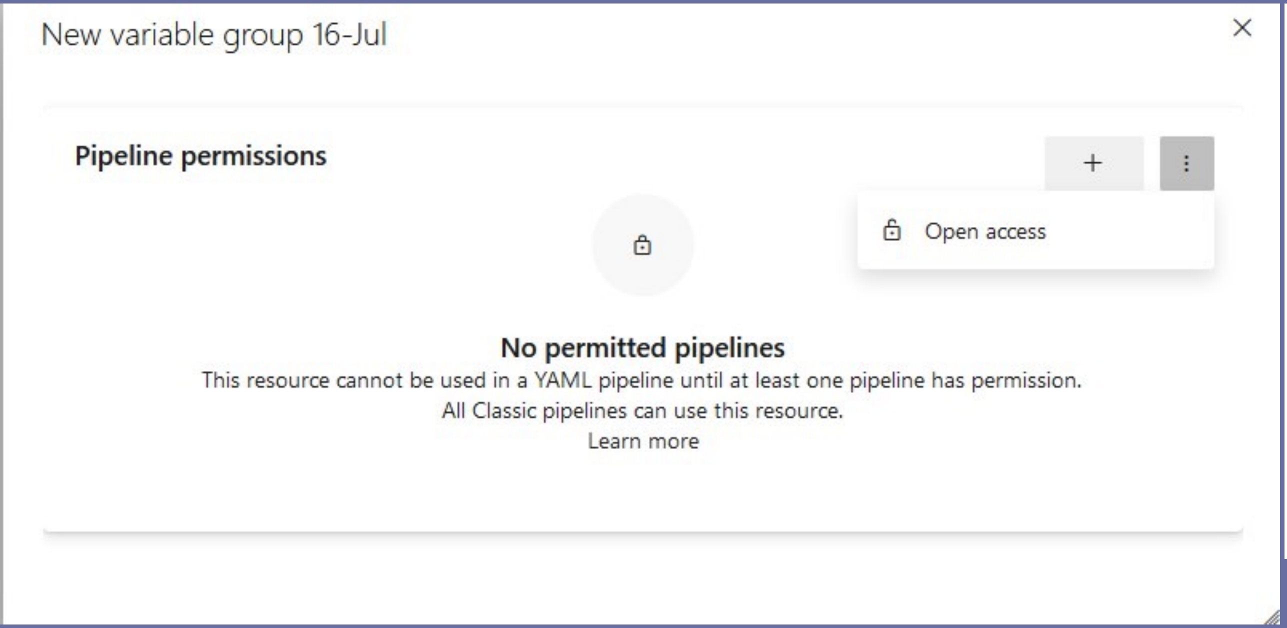
Variables

Name ↑	Value
test	test

+ Add

Secrets

Cloud Village

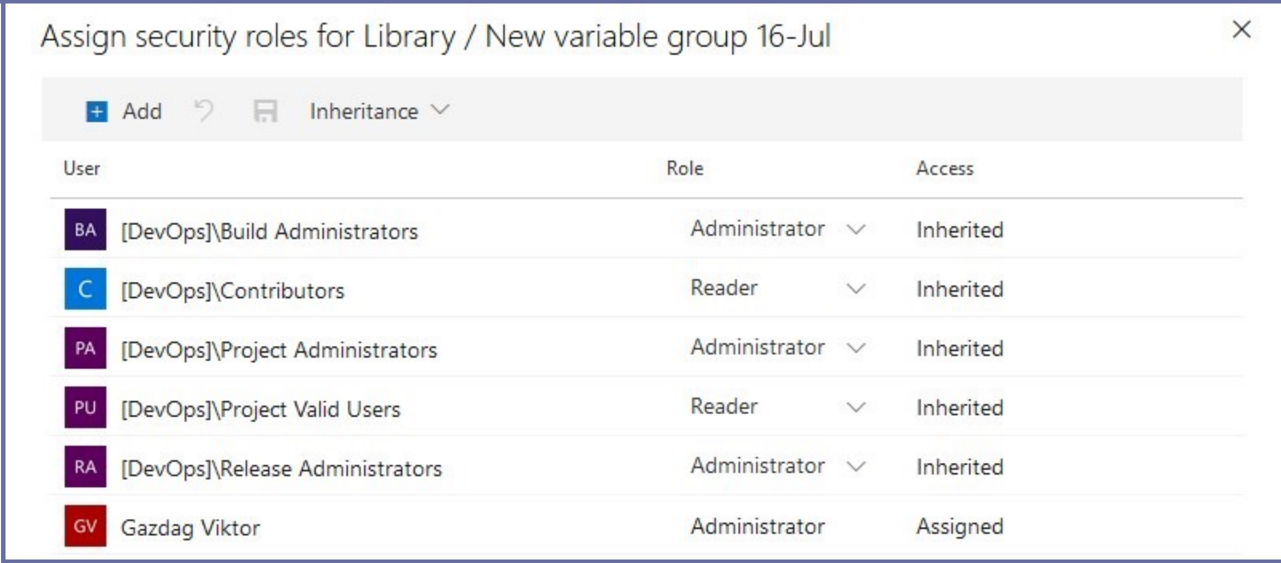


New variable group 16-Jul

Pipeline permissions

No permitted pipelines

This resource cannot be used in a YAML pipeline until at least one pipeline has permission.
All Classic pipelines can use this resource.
Learn more



Assign security roles for Library / New variable group 16-Jul

User	Role	Access
BA [DevOps]\Build Administrators	Administrator	Inherited
C [DevOps]\Contributors	Reader	Inherited
PA [DevOps]\Project Administrators	Administrator	Inherited
PU [DevOps]\Project Valid Users	Reader	Inherited
RA [DevOps]\Release Administrators	Administrator	Inherited
GV Gazdag Viktor	Administrator	Assigned

Agents

Cloud Village

- Agent Pool
- Hosted vs Self-Hosted (443 TCP, PAT)

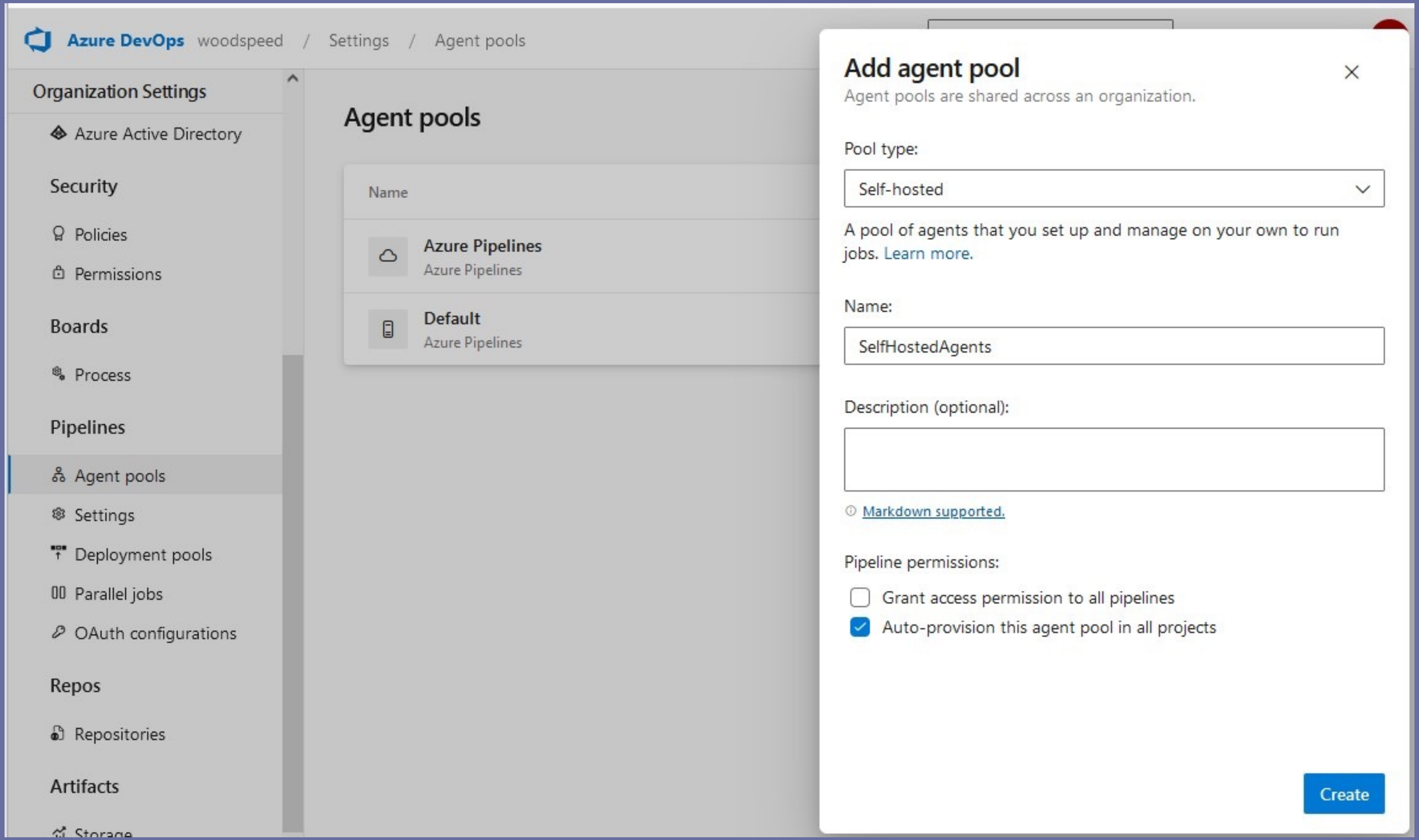
- Decommission and Hardening
- Pipeline Access, No Share
- Permission
- Update the Agent

Agents

- Stealing Source Code
- Read Environment Variables
- Read Service Connections
- Read Secrets
- Exploit Vulnerability in Agent

Agents

Cloud Village



Add agent pool

Agent pools are shared across an organization.

Pool type: Self-hosted

A pool of agents that you set up and manage on your own to run jobs. Learn more.

Name: SelfHostedAgents

Description (optional):

Markdown supported.

Pipeline permissions:

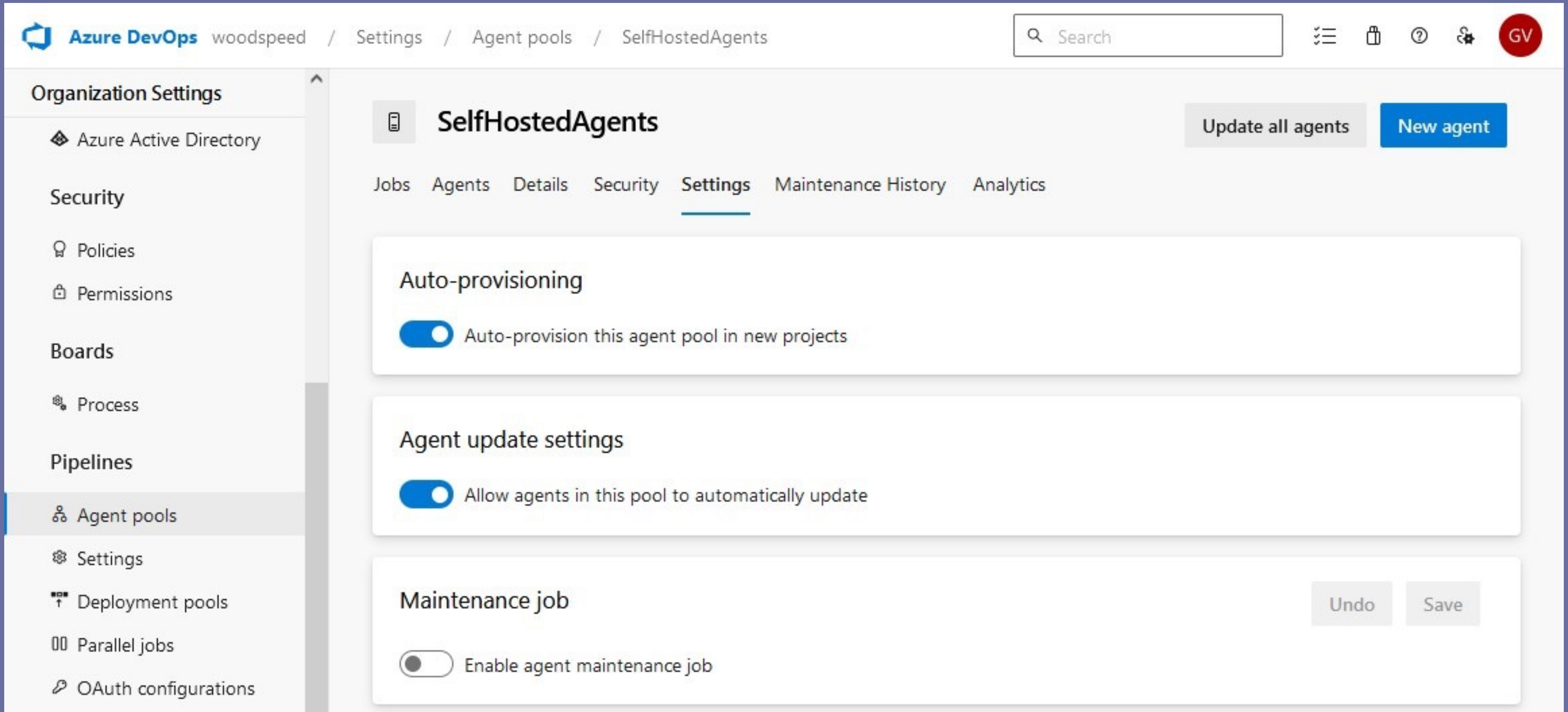
☐ Grant access permission to all pipelines

☑ Auto-provision this agent pool in all projects

Create

Agents

Cloud Village



SelfHostedAgents

Auto-provisioning

☑ Auto-provision this agent pool in new projects

Agent update settings

☑ Allow agents in this pool to automatically update

Maintenance job

□ Enable agent maintenance job

Artifact

- Feed
- Upstream Sources
- Permission

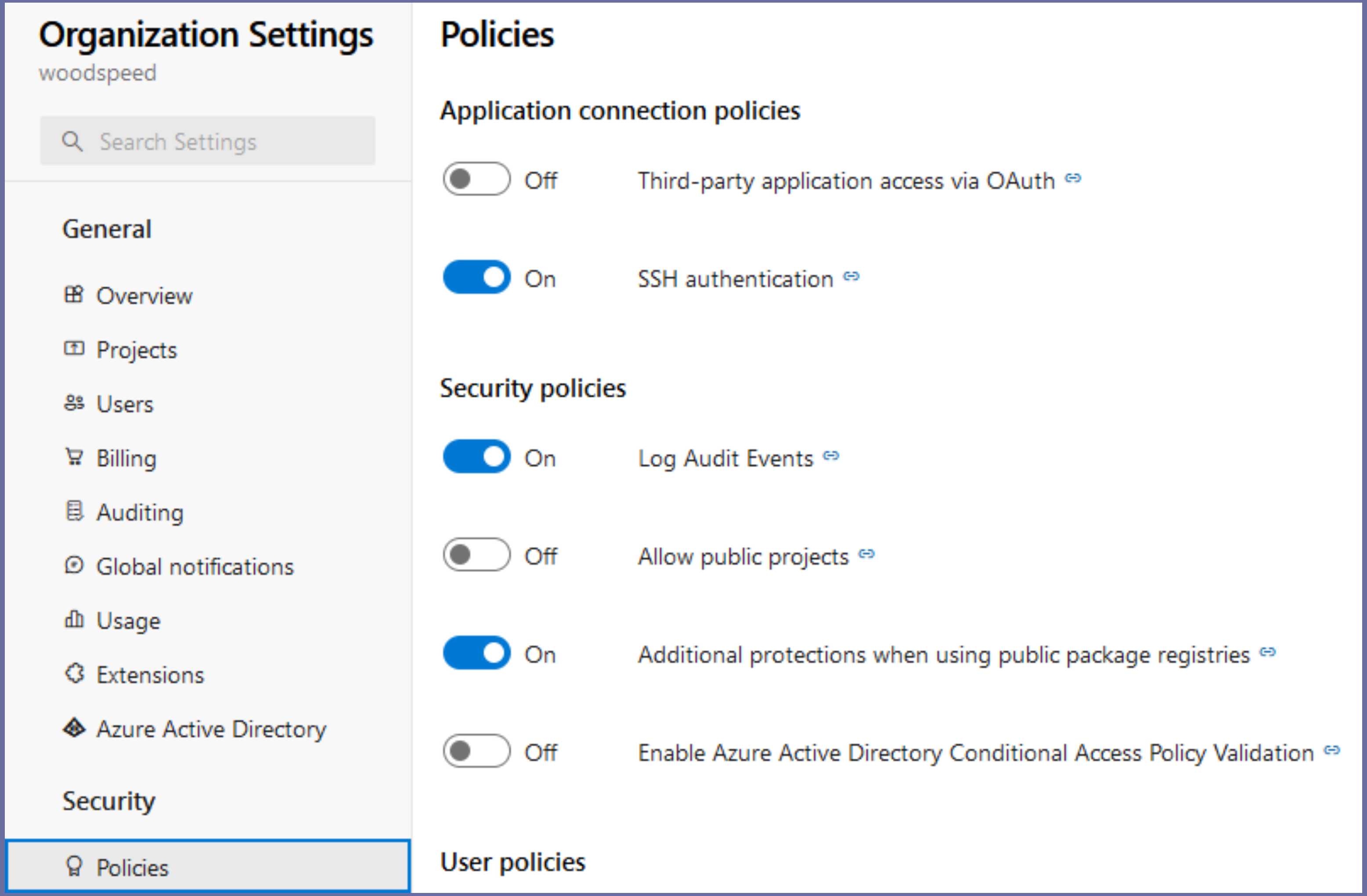
Artifact

Cloud Village

- Dependency Confusion Attack (Higher public version)
- Dependency Poisoning Attack (Internal version)
- Dependency Hijacking Attack (Account takeover)
- Typo Squatting Attack (axios vs axioss)

Artifact

Cloud Village



Organization Settings

woodspeed

Search Settings

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory

Security

- Policies

Policies

Application connection policies

Off — Third-party application access via OAuth

On — SSH authentication

Security policies

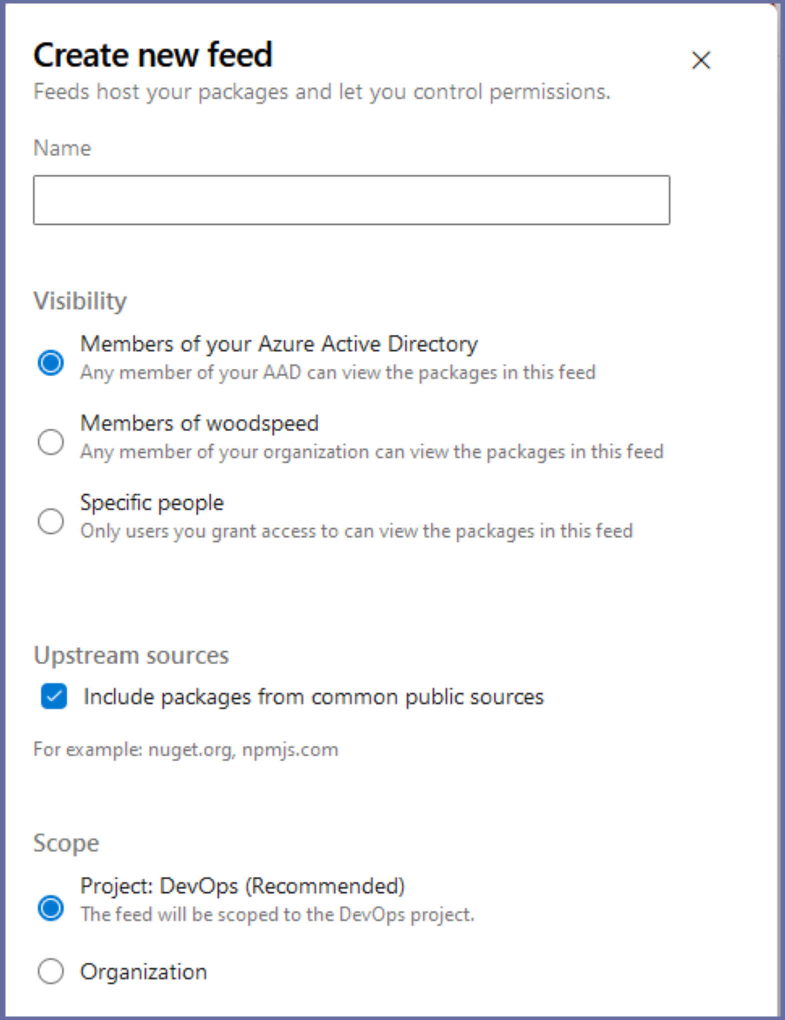
On — Log Audit Events

Off — Allow public projects

On — Additional protections when using public package registries

Off — Enable Azure Active Directory Conditional Access Policy Validation

User policies



Create new feed

×

Feeds host your packages and let you control permissions.

Name

Visibility

● Members of your Azure Active Directory
Any member of your AAD can view the packages in this feed

○ Members of woodspeed
Any member of your organization can view the packages in this feed

○ Specific people
Only users you grant access to can view the packages in this feed

Upstream sources

☑ Include packages from common public sources

For example: nuget.org, npmjs.com

Scope

● Project: DevOps (Recommended)
The feed will be scoped to the DevOps project.

○ Organization

Audit & Logging

Cloud Village

- By default turned off
- Require Azure AD
- Organization Owners, Project Collection Admin
- Audit Log vs Audit Stream

- Audit, Checks, Extension, Git, Library, Policy, Pipelines, Permissions, Projects, Tokens etc

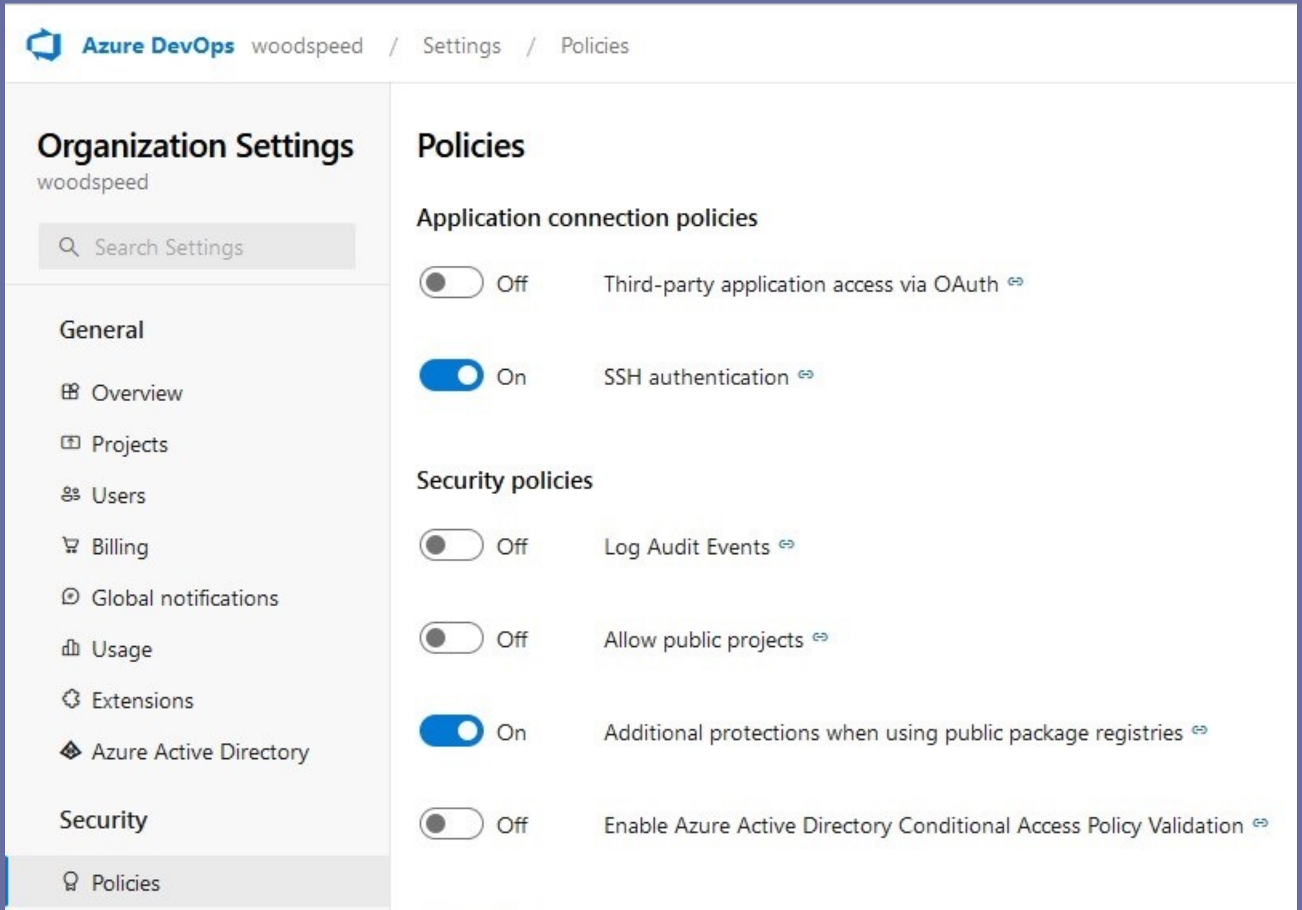
Audit & Logging

Cloud Village

- Compliance
- Incident Response
- Track Changes

Audit & Logging

Cloud Village



Policies

Application connection policies

Off Third-party application access via OAuth

On SSH authentication

Security policies

Off Log Audit Events

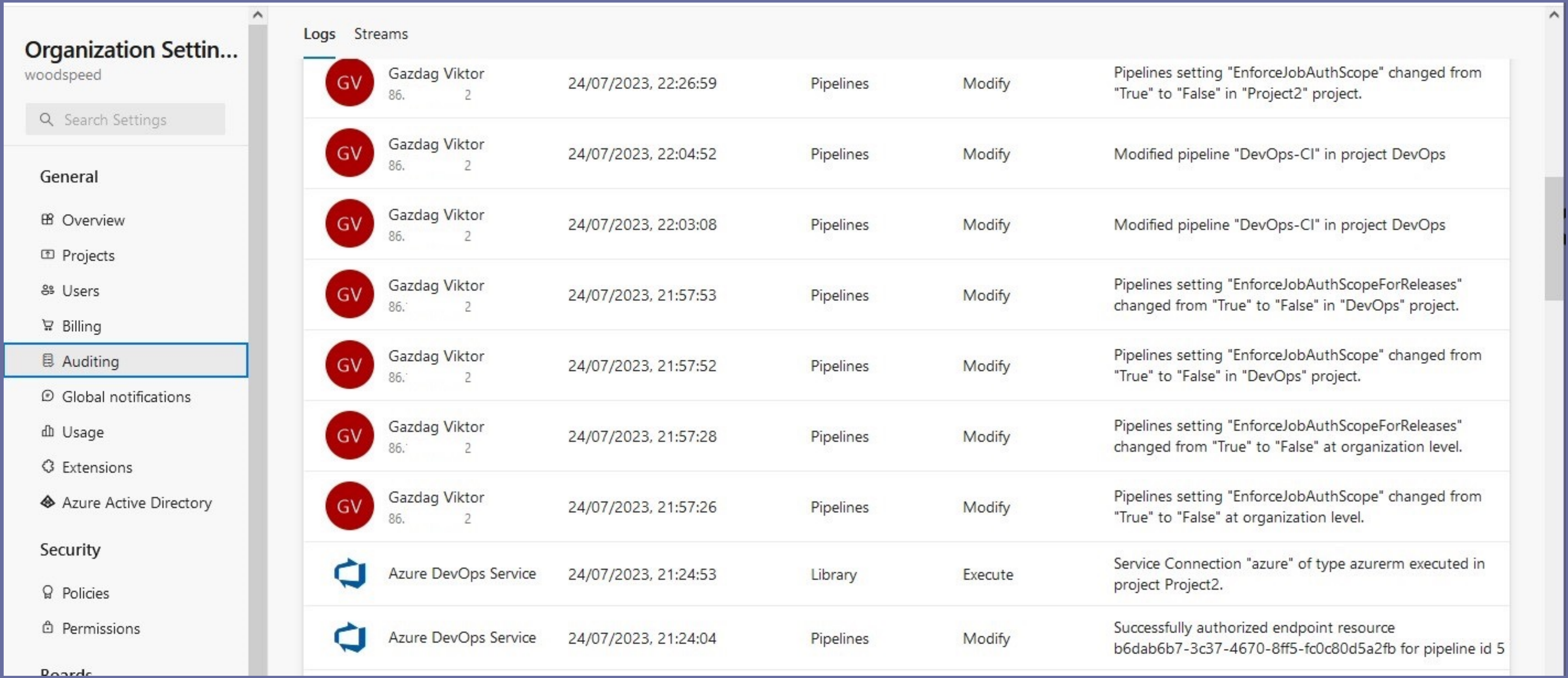
Off Allow public projects

On Additional protections when using public package registries

Off Enable Azure Active Directory Conditional Access Policy Validation

Audit & Logging

Cloud Village



Organization Settin...
woodspeed

Search Settings

General

- Overview
- Projects
- Users
- Billing
- Auditing
- Global notifications
- Usage
- Extensions
- Azure Active Directory

Security

- Policies
- Permissions

Boards

Logs Streams

GV	Gazdag Viktor 86. 2	24/07/2023, 22:26:59	Pipelines	Modify	Pipelines setting "EnforceJobAuthScope" changed from "True" to "False" in "Project2" project.
GV	Gazdag Viktor 86. 2	24/07/2023, 22:04:52	Pipelines	Modify	Modified pipeline "DevOps-CI" in project DevOps
GV	Gazdag Viktor 86. 2	24/07/2023, 22:03:08	Pipelines	Modify	Modified pipeline "DevOps-CI" in project DevOps
GV	Gazdag Viktor 86. 2	24/07/2023, 21:57:53	Pipelines	Modify	Pipelines setting "EnforceJobAuthScopeForReleases" changed from "True" to "False" in "DevOps" project.
GV	Gazdag Viktor 86. 2	24/07/2023, 21:57:52	Pipelines	Modify	Pipelines setting "EnforceJobAuthScope" changed from "True" to "False" in "DevOps" project.
GV	Gazdag Viktor 86. 2	24/07/2023, 21:57:28	Pipelines	Modify	Pipelines setting "EnforceJobAuthScopeForReleases" changed from "True" to "False" at organization level.
GV	Gazdag Viktor 86. 2	24/07/2023, 21:57:26	Pipelines	Modify	Pipelines setting "EnforceJobAuthScope" changed from "True" to "False" at organization level.
	Azure DevOps Service	24/07/2023, 21:24:53	Library	Execute	Service Connection "azure" of type azurerm executed in project Project2.
	Azure DevOps Service	24/07/2023, 21:24:04	Pipelines	Modify	Successfully authorized endpoint resource b6dab6b7-3c37-4670-8ff5-fc0c80d5a2fb for pipeline id 5

Marketplace

- Extensions
- Dashboard widgets, Build tasks, Extend Work Item
- Project Collection Administrators Group

Marketplace

Cloud Village

- Install Malicious Extension
- Install Vulnerable Extension

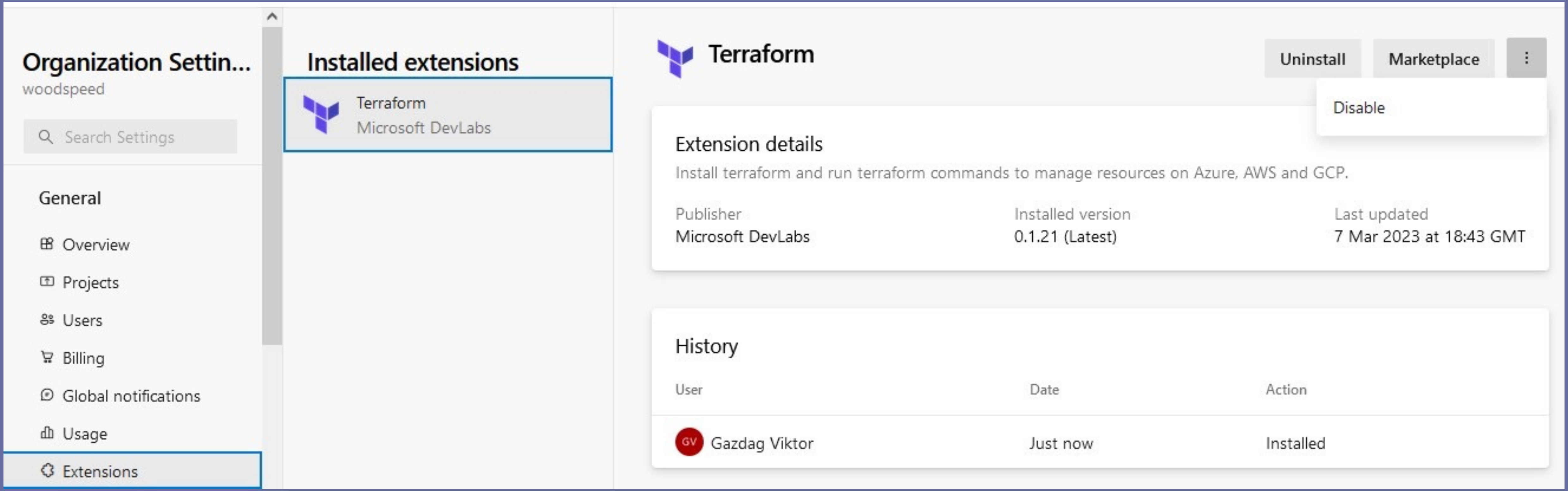
Marketplace

- “…there are 1460 extensions in the "Azure Pipelines" category. More than 500 have one or more vulnerabilities or vulnerable dependencies.” - Jesse Houwing

- https://jessehouwing.net/security-state-of-the-azure-devops-marketplace/

Marketplace

Cloud Village



Extension details

Install terraform and run terraform commands to manage resources on Azure, AWS and GCP.

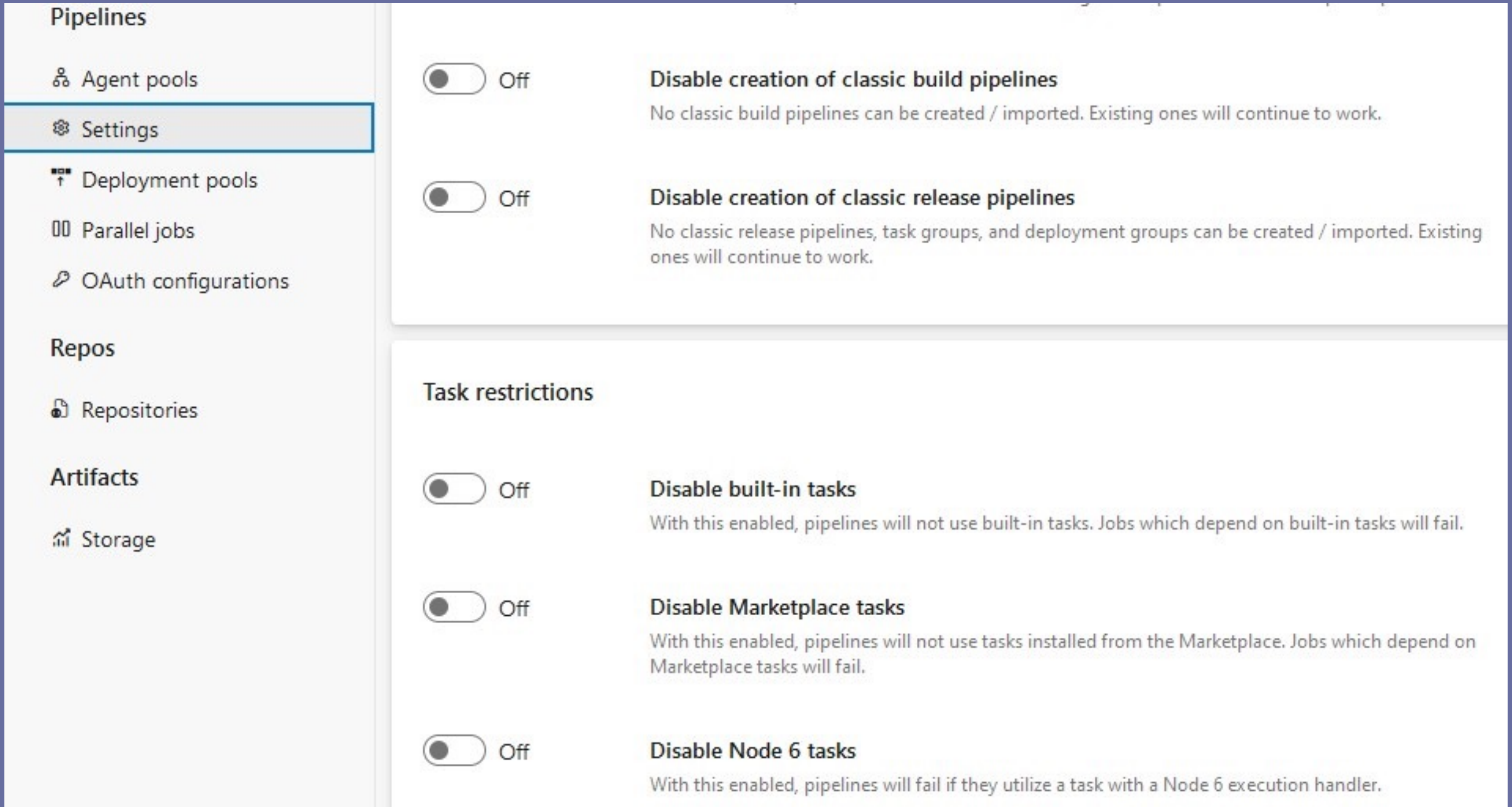
Publisher	Installed version	Last updated
Microsoft DevLabs	0.1.21 (Latest)	7 Mar 2023 at 18:43 GMT

History

User	Date	Action
GV Gazdag Viktor	Just now	Installed

Marketplace

Cloud Village



○ Off **Disable creation of classic build pipelines**

No classic build pipelines can be created / imported. Existing ones will continue to work.

○ Off **Disable creation of classic release pipelines**

No classic release pipelines, task groups, and deployment groups can be created / imported. Existing ones will continue to work.

Task restrictions

○ Off **Disable built-in tasks**

With this enabled, pipelines will not use built-in tasks. Jobs which depend on built-in tasks will fail.

○ Off **Disable Marketplace tasks**

With this enabled, pipelines will not use tasks installed from the Marketplace. Jobs which depend on Marketplace tasks will fail.

○ Off **Disable Node 6 tasks**

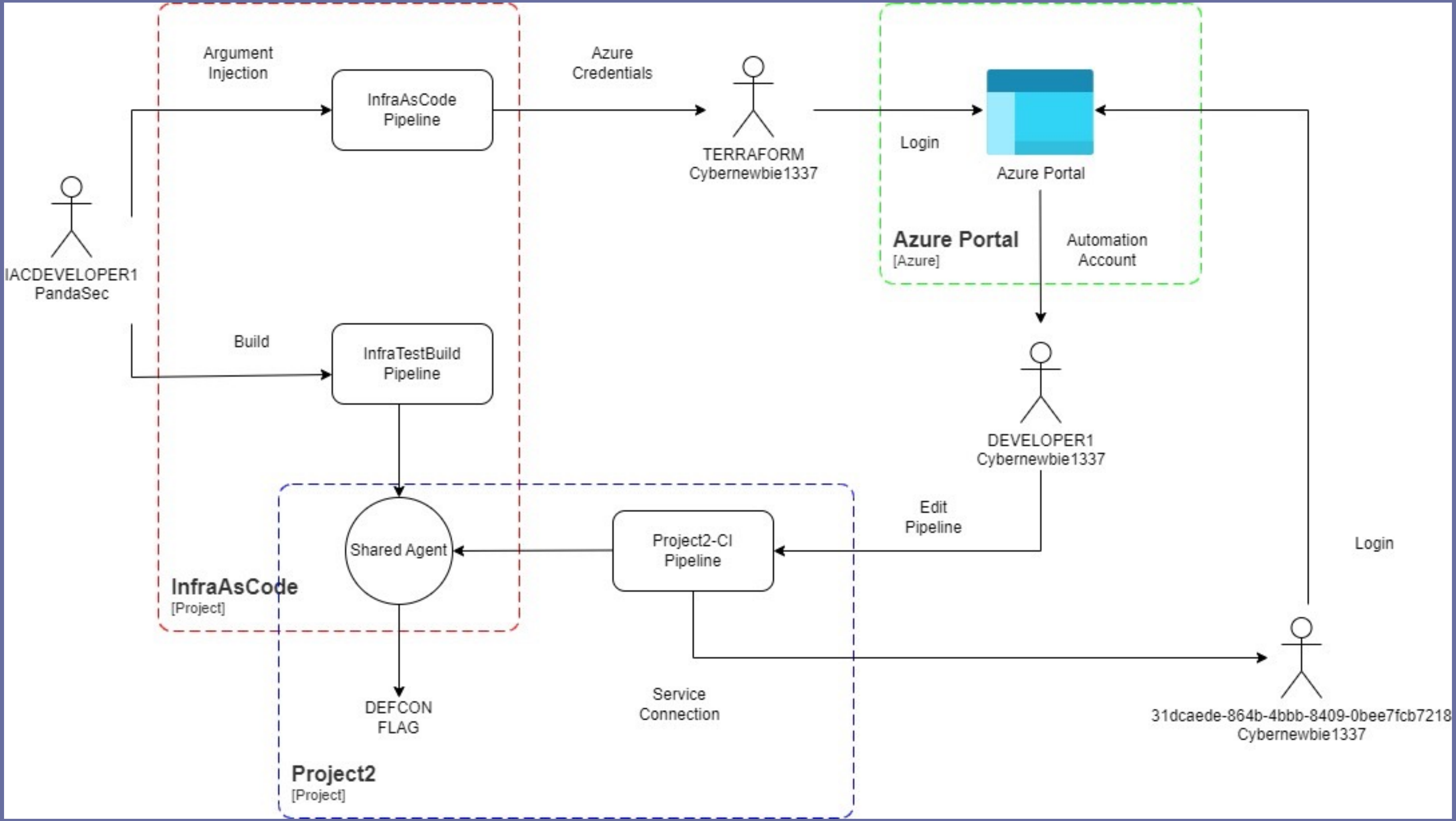
With this enabled, pipelines will fail if they utilize a task with a Node 6 execution handler.

Demo

Cloud Village

- VIDEO

Name	InfraAsCode	Project2	DevOps
IACDEVELOPER1	X	---	X
DEVELOPER1	---	X	X



Additional Resources 1

Cloud Village

- Black Hat USA 2022 - RCE-as-a-Service: Lessons Learned from 5 Years of Real-World CI/CD Pipeline Compromise - https://www.youtube.com/watch?v=Pe9nJLZvABM

- BSides LV 2022 - GF - Climbing the Production Mountain: Practical CI/CD Attacks Using CI/CD Goat - https://www.youtube.com/watch?v=w-R2PT2jfdU

- BSides LV 2022 - GF - CICD security: A new eldorado (talk) - https://www.youtube.com/watch?v=a3SeASgtINY

Additional Resources 2

- RSA Conference - CI/CD: Top 10 Security Risks - https://www.youtube.com/watch?v=IiFwwEf-Y8s

- Black Hat USA 2022 - Controlling the Source: Abusing Source Code Management Systems - https://www.youtube.com/watch?v=P44opLFcgpA

- Hacking CI/CD (Basic Pipeline Poisoning) - https://www.youtube.com/watch?v=fcibOy-zoN8

Additional Resources 3

Cloud Village

- Hacking CI/CD (Basic Pipeline Poisoning) - https://www.youtube.com/watch?v=fcibOy-zoN8

- USENIX Security 22 Characterizing the Security of Github CI Workflows - https://www.youtube.com/watch?v=JlaFfMmXpXg

- How hackers can breach your C.I / C.D systems - https://www.youtube.com/watch?v=EqLIJEqsPEg

Additional Resources 4

Cloud Village

- CIS Software Supply Chain Security Guide - https://github.com/aquasecurity/chain-bench/blob/main/docs/CIS-Software-Supply-Chain-Security-Guide-v1.0.pdf
- OWASP TOP 10 CI/CD Security Risk - https://owasp.org/www-project-top-10-ci-cd-security-risks/
- Microsoft DevOps Threat Matrix - https://www.microsoft.com/en-us/security/blog/2023/04/06/devops-threat-matrix/

Additional Resources 5

Cloud Village

- 10 real-world stories of how we’ve compromised CI/CD pipelines - https://research.nccgroup.com/2022/01/13/10-real-world-stories-of-how-weve-compromised-ci-cd-pipelines/
- Let’s Hack a Pipeline: Argument Injection - https://devblogs.microsoft.com/devops/pipeline-argument-injection/
- Supply-Chain Security: Evaluation of Threats and Mitigations - https://engineering.mercari.com/en/blog/entry/20221215-supplychain-security-reevaluation/

Additional Resources 6

- CI/CD secrets extraction, tips and tricks - https://www.synacktiv.com/publications/cicd-secrets-extraction-tips-and-tricks.html

- Defending CI/CD Environments - https://media.defense.gov/2023/Jun/28/2003249466/-1/-1/0/CSI_DEFENDING_CI_CD_ENVIRONMENTS.PDF

- Microsoft Learn AZ-400 Training - https://learn.microsoft.com/en-gb/certifications/exams/az-400/

Cloud Village

Questions

- @wucpi
- viktor.gazdag@nccgroup.com