Report Title: Change Request Details
Run Date and Time: 2024-04-25 11:16:02 Eastern Daylight Time
Run by: Matthew Economou
Table name: change_request

Change Request

Number:	CHG0032037	Approval:	Approved
Requested by:	Matthew Economou	Change Type:	Normal
Are you putting a new Service in Production:	No	State:	Review
		On hold:	false
Service:	Server	Impact:	3 - Low
Category:	Configuration Management	Urgency:	3 - Low
Configuration item:		Priority:	4 - Low
Number of Users Affected:	10-50	Assignment group:	IBRSP - Global
Assigned to:	Matthew Economou	Milestone:	false
		Scientific approval:	false
		Security Impact Analysis:	No

Short description:

Give IBRSP Operations control over production deployments from GitHub Actions workflows

Description:

The IBRSP Engineering and Infrastructure team is adopting continuous integration/continuous delivery (CI/CD) as part of its enterprise performance life cycle implementation. We will use CI/CD pipelines implemented using GitHub Actions workflows to automate deployments. However, we still want people in control of production deployments following principle of dual authorization (a/k/a the two-person rule); cf. NIST SP 800-53 Rev. 5 AC-03(02). The Manual Approval workflow for GitHub Actions (https://github.com/trstringer/manual-approval) lets us implement a simple, multi-person consent protocol using GitHub Issues and GitHub organization teams similar to IBRSP's change approval process in ServiceNow.

To implement this consent protocol using role-based access controls, where IBRSP Operations would be represented as a team in the IBRSP organization on GitHub, we need to give the Manual Approval workflow permission to look up organization team memberships. The default GitHub Actions automatic token does not permit this, so we must create and install a custom GitHub app with read access to the IBRSP organization's members and associated metadata. In production deployment jobs, we would use the GitHub App Token workflow (https://github.com/tibdex/github-app-token) to switch from the default GitHub Actions automatic token to this custom GitHub app.

Note that because the GitHub App Token workflow completely replaces the default GitHub Actions automatic token, the custom GitHub app must also be given permission to read/write repositories' issues. If necessary, this may be limited to select repositories when installing the custom GitHub app in the organization.

On hold reason:

Planning

Implementation plan:

In the IBRSP organization on GitHub (https://github.com/ibrsp):

1. Create a GitHub app named "IBRSP Org Team Approvers" with read-only access to organization members.

2. Set the app's description to the following

```
From the trstringer/manual-approval action documentation:

> If you want to have approvers set to an org team, then you need to take a different approach. The default [GitHub Actions automatic token](https://docs.github.com/en/actions/security-guides/automatic-token-authentication#permissions-for-the-github_token) does not have the necessary permissions to list out team members. If you would like to use this then you need to generate a token from a GitHub App with the correct set of permissions.
>
> Create a GitHub App with read-only access to organization members. Once the app is created, add a repo secret with the app ID. In the GitHub App settings, generate a private key and add that as a secret in the repo as well. You can get the app token by using the [tibdex/github-app-token](https://github.com/tibdex/github-app-token) GitHub Action...
```

3. Set the app's homepage URL to https://github.com/trstringer/manual-approval#org-team-approver.

4. Generate a private key for the app and save it in the Global vault of the IBRSP 1Password account.

5. Give the app access to the following:

Repository permissions: Issues = read and write
Repository permissions: Metadata = read-only
Organization permissions: Members = read-only

6. Install the app in the IBRSP organization and give it access to all repositories.

7. Create a team named ibrsp-operations with members David Ireland (aadireland), Brian Moyer (bkmoyay), and Matthew Economou (niheconomoum).

8. Add an organization variable named APPROVALS_APP_ID containing the app ID. Give all repositories access to the variable.

9. Add an organization secret named APPROVALS_APP_PRIVATE_KEY containing the app's private key. Give all repositories access to the secret.

10. Add an organization variable named APPROVERS set to "ibrsp-operations". Give all repositories access to the variable.

11. Add an organization variable named MINIMUM_APPROVALS set to 2. Give all repositories access to the variable.

Test plan:

Create a simple GitHub Actions workflow:

```yaml
---
name: Test Approvals
on:
workflow_dispatch:

concurrency:
group: ${{ github.workflow }}-${{ github.ref }}
cancel-in-progress: true

jobs:
myjob:
runs-on: ubuntu-latest
steps:
- name: Generate token
id: generate_token
uses: tibdex/github-app-token@v1
with:
app_id: ${{ vars.APPROVALS_APP_ID }}
private_key: ${{ secrets.APPROVALS_APP_PRIVATE_KEY }}
- name: Wait for approval
uses: trstringer/manual-approval@v1
with:
secret: ${{ steps.generate_token.outputs.token }}
approvers: ibrsp-operations
minimum-approvals: ${{ vars.MINIMUM_APPROVALS || 1 }}
```

Upon invocation, the workflow should create an issue in the repository asking to proceed with the workflow. It should be assigned to Matthew and Brian, who should receive email notifications accordingly. Once both people approve the workflow, it should finish successfully.

Monitoring Plan:
n/a
Communication Plan:
n/a

Backout plan:	Delete the GitHub app and secrets from the organization. Delete the corresponding 1Password entry.	Maximum Hours for Backing Out:	5 Minutes

Documentation:
This will be documented in a forthcoming IBRSP Instruction.
Target Outcome:
Automated continuous delivery actions will require the consent of two people to run.
Resources:
Matthew Economou

Schedule

Planned start date:	2024-04-24 12:00:00	Planned start date in UTC:	2024-04-24 16:00:00
Planned end date:	2024-04-24 12:15:00	Planned end date in UTC:	2024-04-24 16:15:00
		Unauthorized:	false

Conflicts

Notes

Watch list:	Work notes list:

Additional comments:

Work notes:

2024-04-25 10:55:48 - Matthew Economou (Work notes)
Addendum:

- Uncheck (disable) "Expire user authorization tokens".

- Disable the webhook.

- Limit app installation to only this account.

Closure Information

Close code:

Close notes:

New Service

Service Name:	Access:
Abbreviation:	Customer Instructions:
Business Continuity:	Developer Support:
Disaster Recovery:	Hosts:
Licensing:	Monitoring Procedure:
Software:	SOE:
Best Practice Guidelines:	Knowledge Base Documents:
Validation Procedures:	Service Desk Queues:
Support Tiers:	Support Escalation Plan:
Power and Heat Calculations:	Training Plan Attached:
User Acceptance Attached:	

New Service Description:

Related List Title: Conflict List
Table name: conflict
Query Condition: Change = CHG0032037
Sort Order: None

None

Related List Title: Impacted CIs List
Table name: task_cmdb_ci_service
Query Condition: Task = CHG0032037
Sort Order: None

1 Impacted CIs

Configuration Item	Managed by	Owned by	Approval group	Location	Operational status	Manually added	TD Discovery State	TD Discovery Last Updated
Server	David Ireland				Operational	true	[code]Not applicable	2024-04-25 11:15:54

Related List Title: Approval List
Table name: sysapproval_approver
Query Condition: Approval for = CHG0032037
Sort Order: Created in descending order

4 Approvals

State	Approver	Assignment group	Comments	▼ Created
Approved	Brian Moyer	Change advisory board approval		2024-04-11 18:48:45
No Longer Required	David Ireland	Change advisory board approval		2024-04-11 18:48:44
Approved	Matthew Economou	Change advisory board approval		2024-04-11 18:48:44
No Longer Required	Christopher Whalen	Change advisory board approval		2024-04-11 18:48:44

Related List Title: Change Task List

Table name: change_task

Query Condition: Change request = CHG0032037

Sort Order: Number in ascending order

2 Change Tasks

▲ Number	Short description	Type	State	Planned start date	Planned end date	Assignment group	Assigned to
CTASK0012381	Implement	Implementation	Canceled				
CTASK0012382	Post implementation testing	Testing	Canceled				