Tenancy Uplift

Executive Summary

Te Whatu Ora, with support from AWS, and Koan, delivered an uplift to the existing AWS tenancy, that was originally the National Digital Services, Ministry of Health, and had over 100 current AWS Accounts.

Te Whatu Ora faced the challenges of uplifting the existing tenancy, and the use of future product teams in the goal to bring new projects into the tenancy in a streamlined, secure, consistent manner.

Customer Challenges

For such a large organization recently formed with so many vendors, internal product teams, and departments, the key challenge was to create a “self serve” tenancy that enables product teams.

Why AWS

Te Whatu Ora have existing services and DHBs using AWS Cloud.

Why Koan

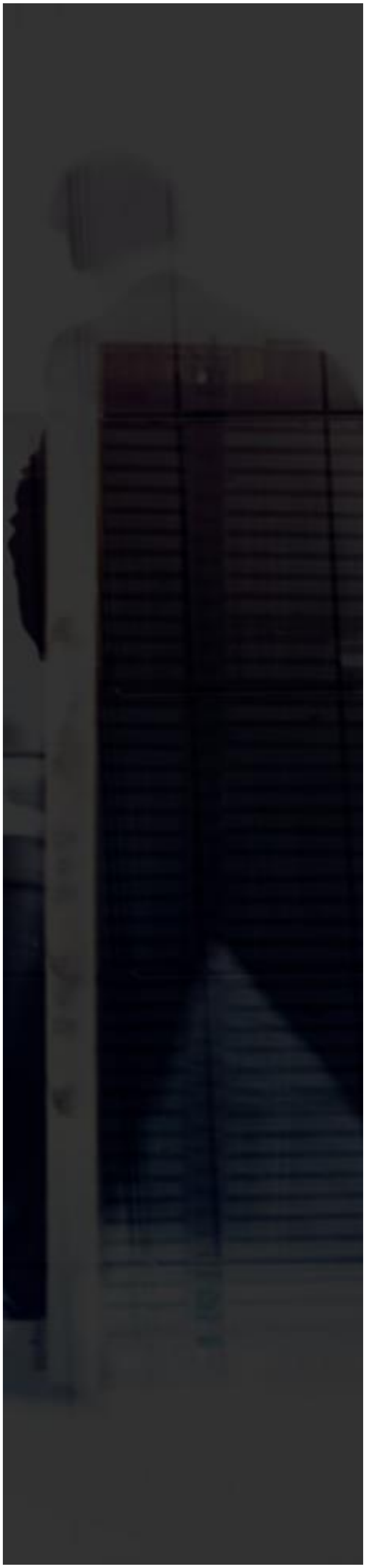
Koan personnel had worked with Te Whatu people in previous projects, and were able to join with Te Whatu to both back fill in certain cases, and streamline the delivery of the tenancy.

Te Whatu Ora

Te Whatu Ora
Health New Zealand

Te Whatu Ora Health New Zealand is a public health agency established by the New Zealand Government to replace the country's 20 district health boards (DHBs) on 1 July 2022.

Te Whatu Ora manages all health services, including hospital and specialist services, and primary and community care. Hospital and specialist services are planned nationally and delivered more consistently across the country.



Solution

Koan worked in partnership with Te Whatu and AWS, supporting the delivery of Landing Zone Accelerator (LZA) and Terraform Enterprise across 100 AWS accounts, used by product teams.

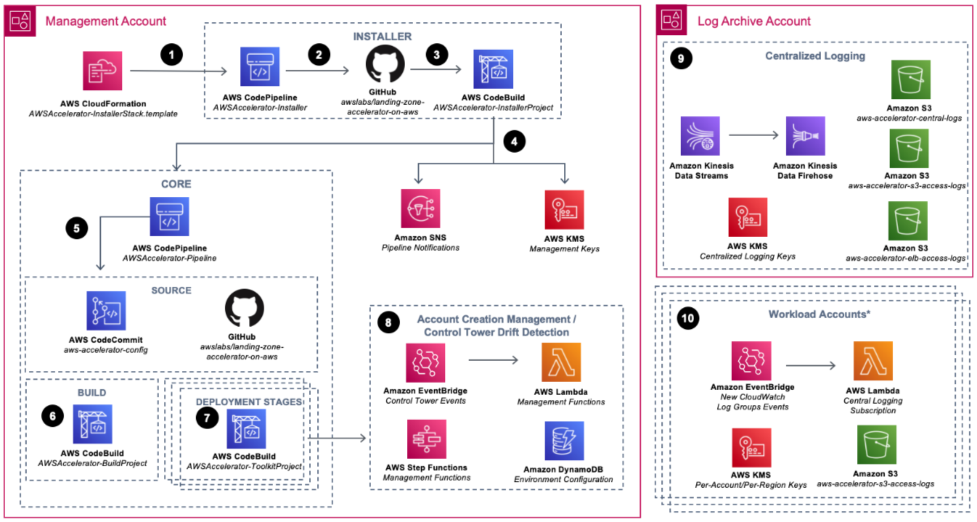
Koan enabled automatic provisioning of Terraform Enterprise (TFE) workspaces & authentication with AWS accounts including:

1. LZA customization to provision core bootstrap roles to accounts
2. TFE workspaces provisioned with Terraform
3. Python to read Terraform output of workspaces and use bootstrap role to provision roles into AWS

The migration of existing SSO accounts into the new tenancy, primarily on Azure AD, to copy user groups across.

Architecture

The foundation of the new Tenancy used Landing Zone Accelerator, along with Terraform Enterprise.



This required the provisioning or user accounts using TFE:

CI/CD Tooling

EKS Gitlib Runner - A specific EKS GitLab repo is trusted to assume the bootstrap role and can then assume the provisioning role in every account and create the required roles for each workspace to be able to access the AWS accounts it needs.

This also supports granting workspaces access to other accounts so teams can create resources in shared accounts (i.e. public ingress, public hosted zone entries).

Results and Benefits

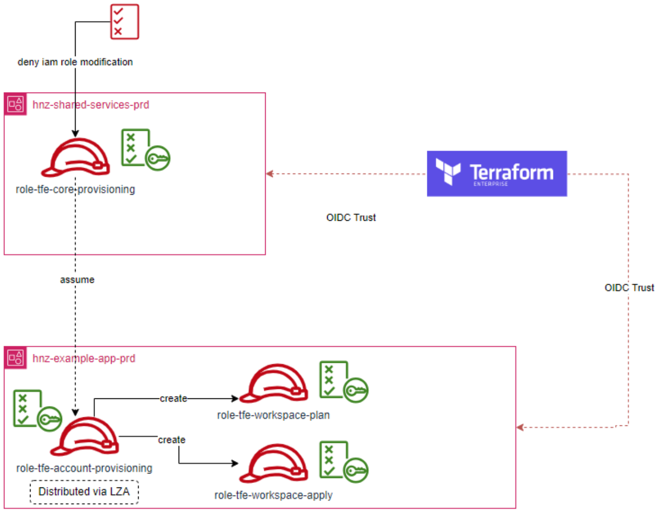
New products wanting to build on AWS have the process streamlined. They require AWS Accounts, and User access to those accounts including:

1. Groups in Azure assigned to AWS SSO enterprise application
2. Permission sets assigned to their AWS accounts

Teams using Terraform require

1. Project & workspaces created in terraform enterprise
2. Access to Terraform Enterprise
    a. Groups in Azure assigned to AWS SSO enterprise application
    b. Teams and permissions setup within TFE
3. Terraform Enterprise access to deploy to their AWS accounts.
    a. AWS OIDC trust with TFE
    b. Each TFE workspace has its own roles in AWS
    c. TFE workspace TFC variables set with correct role arns

This solution works with 100+ accounts. Including setting up Azure groups and assigning them to the correct enterprise application.



Next Steps

Koan are working with product teams onboarding new applications into the AWS tenancy, namely the National Data Platform and the Hira project .

About Koan

Koan is an AWS and software development consultancy based in Wellington, New Zealand. Koan has been building and deploying secure, compliant, enterprise applications for Global and New Zealand customers for 20 years. Koan is an AWS Advanced Tier Partner providing AWS Certified resources for DevSecOps AWS Migrations, Modernizations, Data Analytics.