Oracle Database Automation

Design Draft

Document History:

Date	*Author*	*Role*	*Version*	*Comments*
30/11/2022	**Andrew Williams**	**Solutions Architect**	**0.1**	**Draft version for review**

Document Approval:

Date	*Name*	*Role*	*Version*	*Comments*

Document Contribution:

Date	*Name*	*Role*	*Contribution*

Document Distribution:

Date	*Reason for Issue*	*Name*	*Role*	*Version*	*Comments*

Introduction

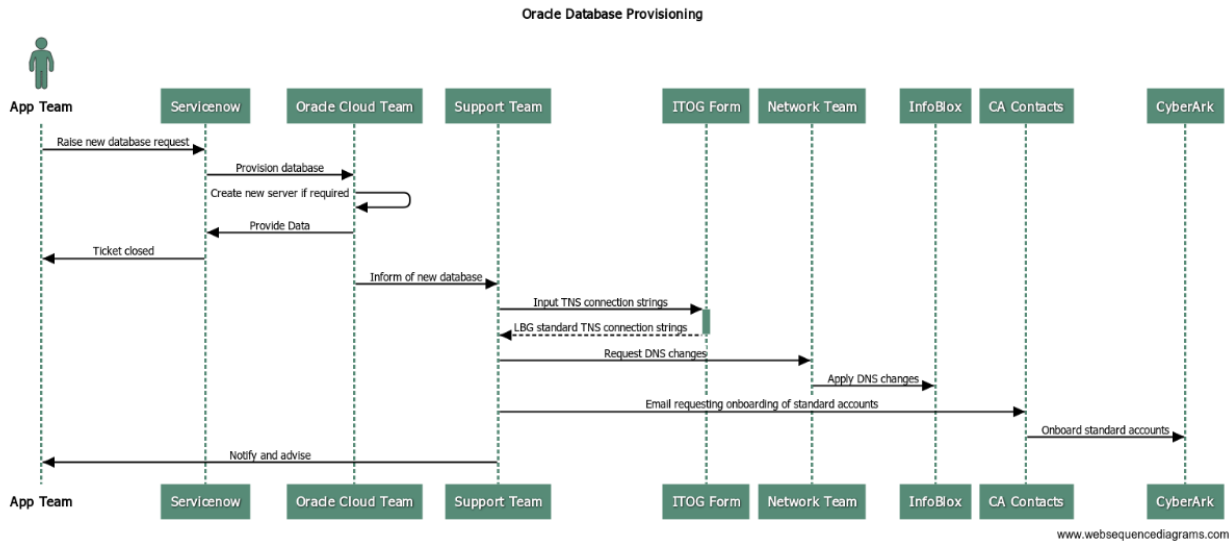
This document is intended to provide an improved solution for the automated provisioning and configuration of Oracle databases

Problem Statement
For application teams, requesting a new Oracle database is a disjointed process. There are numerous manual processes and handoffs which are prone to human error and take up a considerable amount of time. This leads to uncertainty in project and BAU delivery times and confusion for users.

Current state

The current process is initiated when an application team raises a ServiceNow request for a new Oracle database.

- The Oracle Cloud Team is assigned the request. According to SLA's they then create the database; provisioning new servers where necessary. Once complete they inform the application team that the database has been created, close the Servicenow ticket and inform the support team that a new database has been provisioned.
- The support team then take the information provided by the Oracle Cloud Team:
    - TNS connection strings
    - Environment
    - Database name
    - Service name
    - Database type
    - ADG service name
- and conduct the following steps
    - Manually enter each of the TNS connection strings into an ITOG Form (Excel spreadsheet) along with the corresponding environment type to generate the LBG standard equivalent.
    - Request DNS changes with the network team for the TNS connection strings generated by the ITOG form.
    - Request that the standard DB accounts are onboarded into CyberArk.



Target State

The application team raises a Servicenow request for a new Oracle Database.

The Oracle Cloud Team are assigned the request and creates the database; creating new servers when required. Once complete they provide a standardized data payload to the ServiceNow ticket. This triggers the invocation of a webhook within ServiceNow to an external endpoint that executes a pipeline which includes the following:

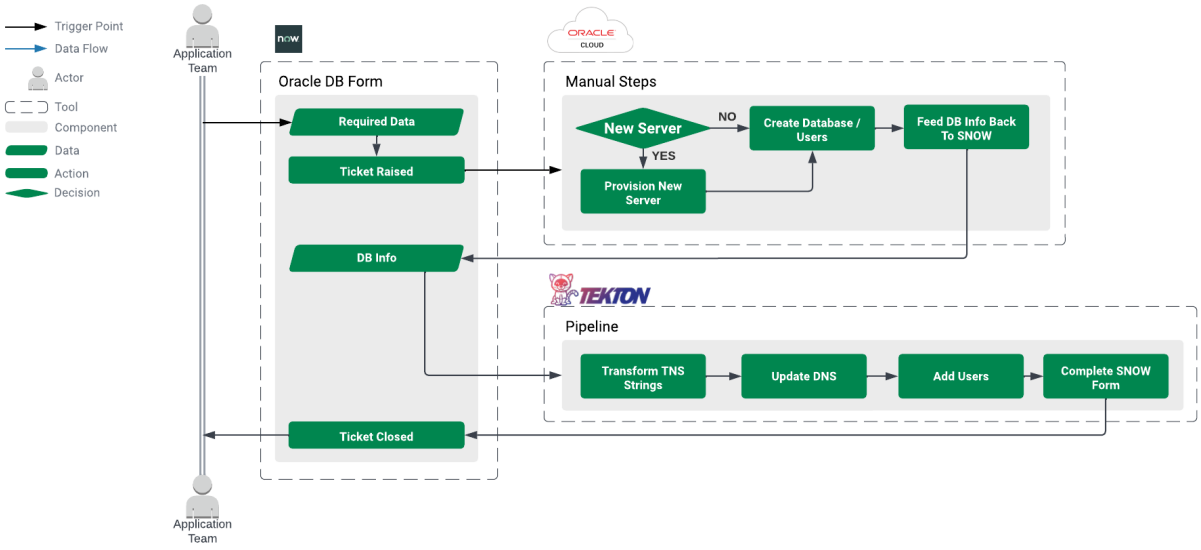
- Payload validation
- TNS connection string transformation
- InfoBlox DNS record creation
- Onboarding CyberArk standard database accounts
- Closing/fulfilling the Servicenow ticket

Due to the nature of the pipeline trigger it can be invoked from any system that has HTTP POST capability ensuring that this capability can be consumed by other processes as necessary.

Design Decisions

Issue / Problem / Requirement	Manual ITOG form for TNS translation
Assumptions	Moving to something more centrally managed
Options	1. ITOG Form 2. Pipeline step 3. Database backed web application
Decision	2. Pipeline step
Justification	The pipeline step will be automated and easily configured in the event that LBG standards change. Furthermore it will be executed ephemerally which reduces the necessity for infrastructure and operational processes, SI etc
Implications	Reduced effort and risk Possible upskill required to maintain rules/access data

Issue / Problem / Requirement	Automation orchestrator
Assumptions	DevOps COE CICD Blocks framework will be used
Options	1. Jenkins 2. Tekton 3. Github Actions
Decision	2. Tekton
Justification	Tekton is a powerful yet flexible Kubernetes-native open source framework that will provide OOTB resiliency
Implications	The development and maintenance of the automation will be simple and flexible. The Tekton pipelines will run on the OCP clusters which are inherently highly available and resilient further reducing the support requirements on the owners of this process.



Once the required standardized data has been captured in ServiceNow from the Oracle Cloud Team following the creation of the database. ServiceNow will trigger a Tekton Event Listener over https using a RESTful POST request with a JSON payload in the body. This mechanism of triggering a Tekton event listener from ServiceNow has already been demonstrated in the bank and webhooks in general are used widely for fulfilling the majority of automated IT@LBG requests from ServiceNow.

A Tekton trigger binding will extract fields from the event payload provided by the Event Listener and bind them to named parameters of the Tekton pipeline.

The Tekton Pipeline will orchestrate the following tasks:

- Validation of the payload to assert that all required fields have been provided in the correct format using the standard JSON Schema Validation

```
{
    "application_name": "",
    "source_database_name": "",
    "environment": "",
    "database_owner": "",
    "database_type": "",
    "primary_oracle_scan_name": "",
    "service_name": "",
    "adg_service_name": "",
    "dr_oracle_scan_name": "",
    "port_number": ""
}
```

- Translation of TNS connection strings that then get stored as YAML in a github repository which will have limited visibility and a standard set of controls. If this data source is consumed outside of this process then a provision will need to be made for

access. This repository will act as a centralized state in lieu of the ITOG form (Excel spreadsheet).
GitHub App Auth will be used to authenticate with GitHub Enterprise

- Creation of DNS records in LBG on-premise InfoBlox using a dedicated active directory service account in the GLOBAL domain. An Active Directory security group will be required to grant the service account the required permissions within InfoBlox.
- Onboarding standard database accounts in CyberArk using https endpoints authenticated using an AIM Certificate identity.
- Closing the Servicenow ticket via a https endpoint.

A Vault namespace is required to store a CyberArk AIM Certificate for consumption within the pipeline via the kubernetes authentication method. This binds a Vault policy to a Kubernetes identity.

Scope

In scope
The scope of this design covers automating the manual steps undertaken by the <TEAM> team.

1. The transformation of the TNS connection strings
2. Updating InfoBlox DNS
3. Adding DB user credentials into CyberArk

Out of scope
migration

There is a process that is out of scope but should still be understood around the creation of new servers when the current capacity is reached. The servers provisioned by Oracle Cloud to host the DBs are shared (not always). When capacity is reached; Oracle Cloud provides a new server. The details of this server are sent *monthly to the <TEAM> team via an email. This team will manually configure the DNS records for the newly provisioned servers.