ORACLE

Who Are You?

APEX + Oracle Identity and Access Management

Scott Spendolini

Senior Director

GBU APEX Central Engineering

The Educational Conference For Oracle Technology Users

ODTUG Kscope23

aurora, co june 25-29

Welcome

About Me

A History of KScopes…

- 2004 - Scottsdale, AZ
- 2005 - New Orleans, LA
- 2006 - Washington, DC
- 2007 - Daytona Beach, FL
- 2008 - New Orleans, LA
- 2009 - Monterey, CA
- 2010 - Washington, DC
- 2011 - Long Beach, CA
- 2012 - San Antonio, TX
- 2013 - New Orleans, LA
- 2014 - Seattle, WA
- 2015 - Hollywood, FL
- 2016 - Chicago, IL
- 2017 - San Antonio, TX
- 2018 - Orlando, FL
- 2019 - Seattle, WA
- ~~2020 - Corona~~
- 2021 - Virtual
- 2022 - Dallas, TX
- 2023 - Denver, CO

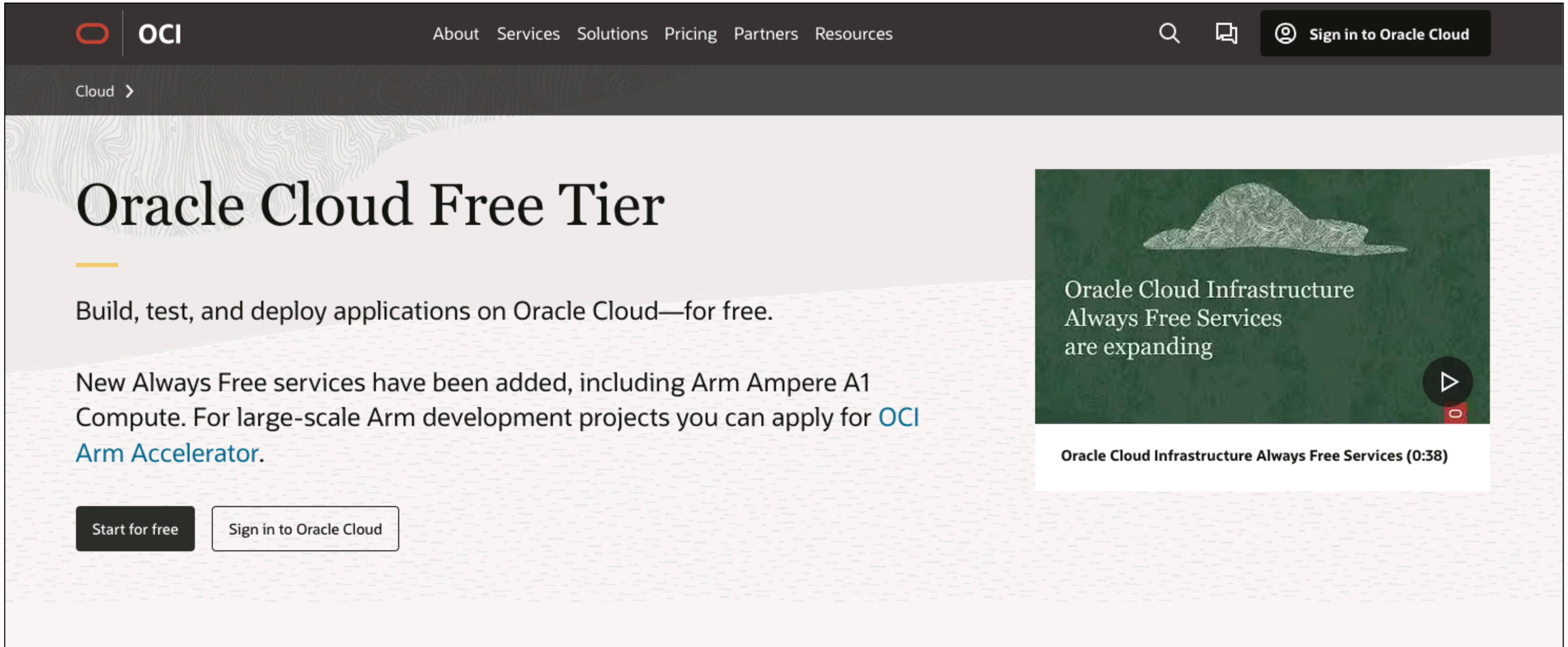
Agenda

- Overview
- APEX & Oracle IAM
  - Domains
  - Applications
  - Users & Groups
  - MFA
  - Reports
- Summary

Overview

Oracle Cloud Free Tier

- Everything that I am going to demonstrate is being done on the Oracle Cloud Free Tier
  - Sign up today to get started
  - https://www.oracle.com/cloud/free/



Oracle Cloud Free Tier

Build, test, and deploy applications on Oracle Cloud—for free.

New Always Free services have been added, including Arm Ampere A1 Compute. For large-scale Arm development projects you can apply for OCI Arm Accelerator.

Start for free
Sign in to Oracle Cloud
Oracle Cloud Infrastructure Always Free Services are expanding

Oracle Cloud Infrastructure Always Free Services (0:38)

Overview

- **Identity Management** is a **key part** of any corporate IT strategy
- Ideally, each person has a **single set of credentials** that they can use to access corporate resources
  - This way, it's easy to onboard & off-board them
  - Can also manage discrete access in a central place
- The obvious downside is a single point of failure
  - Which we can mitigate with multi-factor authentication

Overview

- APEX has **no business being the source of truth** for users & roles / groups
- These functions should be:
  - Managed Externally to APEX
  - Federated
  - Audited
  - Secured
- Sure, you can build out all of this manually - but why?
  - Much better approach is to embrace something like **Oracle IAM**

Oracle Identity & Access Management (IAM)

- **Oracle IAM** - Identity & Access Management - is a **cloud-based Identity Management Platform** that is provided as part of **OCI**
  - You can use this as part of the free tier at no cost with some limitations:
    - Limit of 2000 users, 2 non-Oracle apps & 3 external Identity Providers
- Almost any type of application - **cloud or on-prem** - can be managed via Oracle IAM
- Includes **pre-configured integrations** to most popular **SaaS applications**
  - All you need to bring are your credentials
- In most cases, customers will **federate their existing IdP** with Oracle IAM
  - Enabling users to login with their current SSO credentials and not have to create yet another username & password

APEX & Oracle IAM

APEX & Oracle IAM

- Oracle IAM can be used to “take over” some of the security management of an APEX application
  - **Authentication**
    - Rather than using APEX users or a custom scheme, user management can be done by Oracle IAM
  - **Authorization**
    - Managing groups and group membership can also be done by Oracle IAM
    - Either manually via the console or via API calls that can be made from APEX
  - **Multi-Factor Authentication**
    - This is possible to implement in APEX with some code & integrations, but why?
    - Oracle IAM has a robust set of MFA options that are all turn-key and require no code
  - **Monitoring**
    - Since we’re going to delegate these tasks to Oracle IAM, we can use its reports to monitor access attempts, user to role assignments, etc.

Domains

- An **identity domain** is a container for managing users and roles, federating and provisioning of users, secure application integration through Oracle Single Sign-On (SSO) configuration, and SAML/OAuth based Identity Provider administration
- It represents a **user population** in Oracle Cloud Infrastructure and its associated configurations and security settings
- Oftentimes, domains are **federated with corporate identity management repositories**
  - Microsoft 365, Google G-Suite, etc.
- This allows for **true single-sign on** and eliminates the proliferation of redundant credentials across multiple places

Domains

- **Domains** contain the following components / options:
    - Users
    - Groups
    - Dynamic Groups
    - Applications
    - Oracle Cloud Services
    - Jobs
    - Reports
    - Security
    - Settings
- Well cover most - but not all - of these options today

Demonstration

Create a new Identity Domain in OCI

Applications

- An **Application** in IAM can be one of several types
  - Application Catalog, SAML, Mobile, Confidential or Enterprise
- An **APEX application** would be considered a **Confidential** application in IAM
  - Secured by OAuth 2.0
- Applications can have **Groups** & **Users** associated with them

Demonstration

Create a new Application in OCI

Web Credentials

- Since our Application requires authentication via OAuth2, we need to store those credentials securely in APEX
- The best - and really only way to do this - is to use **Web Credentials**
- **Web Credentials** are shared across a workspace, not application
  - Can be created, set & updated via API calls
  - Ideal for when they need to be rotated

Demonstration

Create a new Web Credential in APEX

Authentication Schemes

- Now that we have an IAM application configured, we need to point APEX that that
- This is done via an **APEX Authentication Scheme**
- Since we need to present the OAuth2 credentials to IAM, we need to use **Social Sign In**
  - Social Sign In is a bit of a misnomer
  - While this is how you integrate with Facebook, LinkedIn, etc., Social Sign In also supports generic **OpenID Connect** and **OAuth2**
- Since that's how we talk to IAM, we can use that type of scheme here

Authentication Schemes

- Remember the callback URL (**apex_authentication.callback**) we set up?
  - That's what IAM is going to call and POST data to once your user authenticates
- This includes:
  - User Name
  - Group Memberships
- We can inspect the JSON passed back and parse it out to capture IAM groups
- Using that data, we can use APEX's dynamic groups feature to map a user to the corresponding groups in a view - **APEX_WORKSPACE_SESSION_GROUPS**
- We can even go one step further and **map AuthZ schemes** to these **groups** declaratively

Capturing Groups from IAM

```
procedure group_setup
as
  l_this_group_name       varchar2(255);
  l_group_count           number;
  l_group_membership_list apex_t_varchar2;
begin
  l_group_count := apex_json.get_count('groups');

  if l_group_count is not null then

    for i in 1..l_group_count
    loop
      l_this_group_name := apex_json.get_varchar2(p_path => 'groups[%d].name', p0 => i);
      apex_string.push(p_table => l_group_membership_list, p_value => l_this_group_name);
    end loop;

    apex_authorization.enable_dynamic_groups(p_group_names => l_group_membership_list);

  end if;
end group_setup;
```

Demonstration

Create a new AuthN Scheme in APEX

Groups

- IAM uses **Groups** to allow **users to access resources**
  - Typically done via OCI policies for OCI resources
  - Can easily be used for application-specific groups
- Since IAM will pass back the group membership of a user, it’s an **ideal choice for access management** for all APEX applications
  - Centralized & federated
  - Single point of management for an enterprise
  - APEX can simply point to an IAM Group with a simple AuthZ scheme
- When using multiple applications, you may want to prefix the Group name with the application ID or alias to keep things organized
  - This allows you to re-use similar names across more than one application

Demonstration

Create a Group in IAM and integrate it with APEX

Multi-Factor Authentication

- To add an additional layer of security, we can enable **Multi-Factor Authentication** - or MFA
  - In some industries, such as healthcare & government, MFA is a requirement
- This is a **built-in feature of IAM** and takes minutes to configure
- Several options are available
  - Mobile App
  - Security Questions
  - FIDO
  - Duo
  - Email
  - SMS
  - Phone Call

Demonstration

Enable MFA in IAM

Restrict Access

- As it stands, any user we add to our Domain can access our APEX application
    - Even if they don’t have a role
- We should prevent that from happening, and it’s literally a single checkbox to do so

Demonstration

Restrict Access to an Application

Domain Reports

- There are a number of very useful reports available for your domain
  - All of them automatically run; no configuration or setup steps
- These reports include:
  - Audit Log
  - Notification Delivery
  - Successful & Failed Logins
  - Dormant Users
  - Application Access
  - Application Roles
  - Diagnostics & Logging

Demonstration

Domain Reports

Summary

Summary

- Implementing a **central security policy** has never been more important than it is today
- Products like **Oracle IAM** provide **enterprise-grade identity management** for all of your applications - regardless where they live
- **Oracle APEX** can easily **integrate with Oracle IAM**, making it much more of a “first class” cloud citizen
  - User & Group management can be easily move to Oracle IAM
  - MFA can be turned on and required for all or some users
  - All with almost no code and in just ~30 minutes

ORACLE

The Educational Conference For Oracle Technology Users

ODTUG Kscope23

aurora, co june 25-29

Interested in volunteering?
Scan the code to sign up

Don't Forget To
Fill Out Your Evals

References

- Integrating SSO between APEX Cloud and Identity Cloud Service the Easy Way
  - https://www.ateam-oracle.com/post/integrating-sso-between-apex-cloud-and-identity-cloud-service-the-easy-way
- APEX Auth-N and Auth-Z using Oracle Identity Cloud Service (IDCS)
  - https://wphilltech.com/apex-auth-n-using-idcs/