The Why, How and Lessons Learned of Using SSO with Oracle BI

Case study for lessons learned
Thursday, June 20, 2024

Emily Fuller – HDR
Mike Miller –Syntax

June 17 – 20, 2024 • Caesars Palace • Las Vegas, NV

ASCEND 2024

Agenda

- Introductions

- SSO and OCI Identity and Access Management (IAM)

- How HDR implemented SSO

  - Business problem
  - Architecture
  - Lessons learned

Emily Fuller

BI Technical Manager, HDR

- Over 20 years of working in the IT industry

- Experience with on-prem and cloud enterprise solutions, databases, data warehouses, data platforms, and Business Intelligence systems

- Veteran Oracle and OCI customer

HDR

- HDR has been pushing boundaries in Engineering, Architecture, Environmental and Construction services for 107 years.

- We create an unshakable foundation for progress because our multidisciplinary teams also include scientists, economists, builders, analysts and artists.

- We have over 12,000 employees working in more than 200 locations around the world, operating in 15 countries.

- Employee Owned since 1996.

- The largest 100% employee-owned A/E company, and the 5th largest overall 100% employee-owned company
  - Source: National Center for Employee Ownership 2023 U.S. Rankings

Mike Miller

Senior Solution Architect, Syntax

- Over 25 years of working with enterprise software and information security technologies

- Experience with enterprise software implementation and support, cloud operations, and executing compliance and risk management programs.

- A CISSP, Certified Information Systems Security Professional
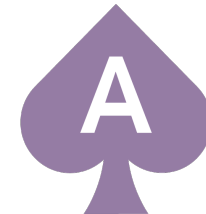
Syntax

- Syntax was founded in 1972 in Montreal, Canada, and is celebrating 50 years in the ERP space

- Syntax provides full-stack, full-lifecycle Cloud Managed Services and Application Managed Services focused on leading ERP solutions such as JD Edwards, Oracle E-Business Suite, and SAP

- Syntax is cloud agnostic and supports both public and private solutions, including AWS, Azure, OCI, and Syntax Enterprise Cloud®

- Our ERP solutions include an array of value-add services, including our monitoring and automation platform, CxHub customer experience portal, security management, and enhanced security

- Syntax is a global company with offices and data centers in the Americas, Europe, and Asia

ORACLE | Partner

ORACLE | Sell Partner
Expertise in
JD Edwards EnterpriseOne
in North America

ORACLE | Sell Partner
Expertise in
Oracle E-Business Suite
in North America

ORACLE | Service Partner
Expertise in
JD Edwards Applications to Oracle Cloud
in North America

ORACLE | Service Partner
Expertise in
Oracle E-Business Suite Applications to Oracle Cloud
in North America

ORACLE | Service Partner
Expertise in
CSPE: Oracle Cloud Platform - Oracle E-Business Suite Applications to Oracle Cloud
in North America

ASCEND 2024

Identity Access Management

Oracle Cloud Infrastructure

Authentication And Authorization

Authentication

- Example: username and password to log in
- The larger the organization, the more applications, which means many passwords
- Single Sign On (SSO) is as much an end-user convenience as it is a security/compliance solution. SSO frees you from typing passwords. You login once to your laptop and your identity is then passed to each application you want to access
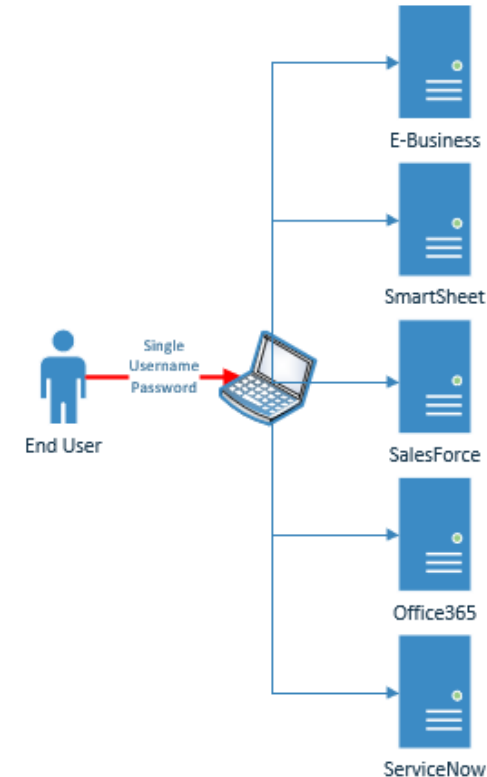
Authorization

- What do you have access to?
- Even small organizations have complex rules and compliance requirements for who is authorized for what.
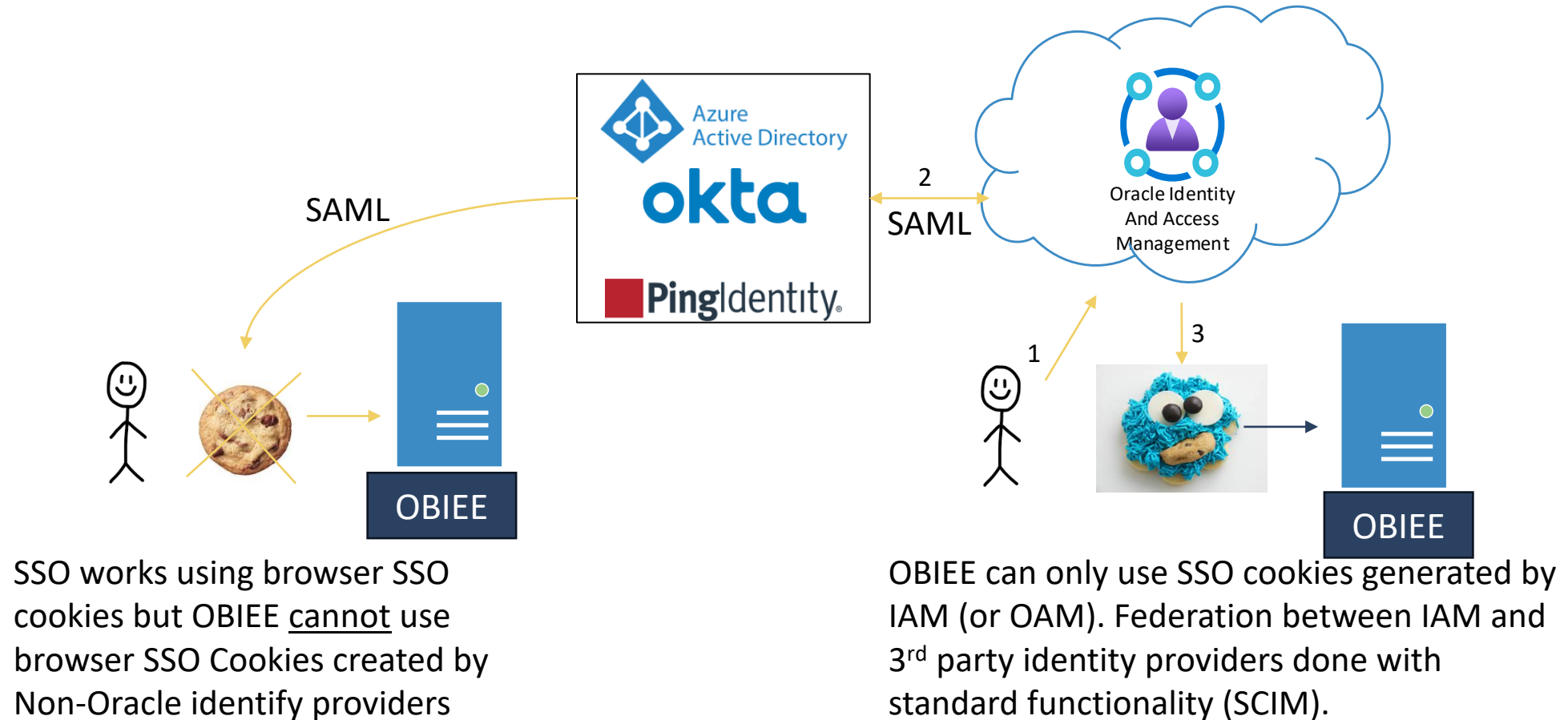
Oracle Identity and Access Management (IAM)

Is a solution for enterprise Authentication and Authorization

- Previously named Oracle Identity Cloud Service (IDCS)
- Automates and solves complex security and compliance processes
- Makes end-users happy
- Makes security and compliance teams happy

End User — Single Username Password → E-Business, SmartSheet, SalesForce, Office365, ServiceNow

Why do you need OCI IAM?

SAML

Azure Active Directory

okta

PingIdentity

2 SAML

Oracle Identity And Access Management

1

3

OBIEE

OBIEE

SSO works using browser SSO cookies but OBIEE cannot use browser SSO Cookies created by Non-Oracle identify providers

OBIEE can only use SSO cookies generated by IAM (or OAM). Federation between IAM and 3rd party identity providers done with standard functionality (SCIM).

Oracle IDCS Merged with OCI IAM

Oracle recently merged the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. IDCS is no longer offered as a separate service.

Single Sign On (SSO) for any Oracle product: JD Edwards, E-Business Suite, Fusion, OBIEE, APEX, RDBMS, OEL, and more
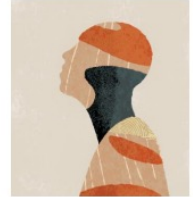
Economics: 25 cents user/month, and each $1 spent on OCI services reduces Oracle technology (e.g. database) support by 25 cents

An active user is a user account that is not end-dated

ORACLE

OCI IAM Identity Domains: What Oracle IDCS customers need to know

Oracle recently merged the capabilities of Oracle Identity Cloud Service (IDCS) into the native Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) service. IDCS is no longer offered as a separate service, but all features and functionality continue to exist as part of OCI IAM. As a native OCI service, customers will see improved performance and scale, immediate availability in more global regions, and a new cross-region disaster recovery feature.

Additional Resources
To learn more about OCI IAM, please visit:
- Oracle Cloud Infrastructure Identity and Access Management documentation
- OCI Identity and Access Management Solution Page
- Identity Cloud Service Documentation
- Oracle Cloud Security Blog

What is OCI IAM?

OCI IAM is the access control plane for Oracle Cloud. It's the OCI-native authentication service and policy engine for OCI and Oracle Cloud Applications that has been used to manage access to OCI resources such as networking, compute, storage, and analytics.

What changed for IDCS and OCI IAM?

Oracle recently made available new capabilities for the OCI IAM service offering broader IAM features and capabilities. As part of this upgraded service release, all features and functionality of the existing Oracle Identity Cloud Service (IDCS) have been merged into OCI IAM. IDCS is no longer offered as a separate service, but all its features and capabilities will continue to function as part of the updated OCI IAM service.

OCI IAM will support the following core functions:

- OCI IAM will continue to serve as the critical access control plane for Oracle Cloud.
- Oracle Cloud applications are expected to standardize over time on OCI IAM as the native IAM service for the application.
- OCI IAM will support a wide range of enterprise Identity and Access Management (IAM) use cases for complex, hybrid IT environments.
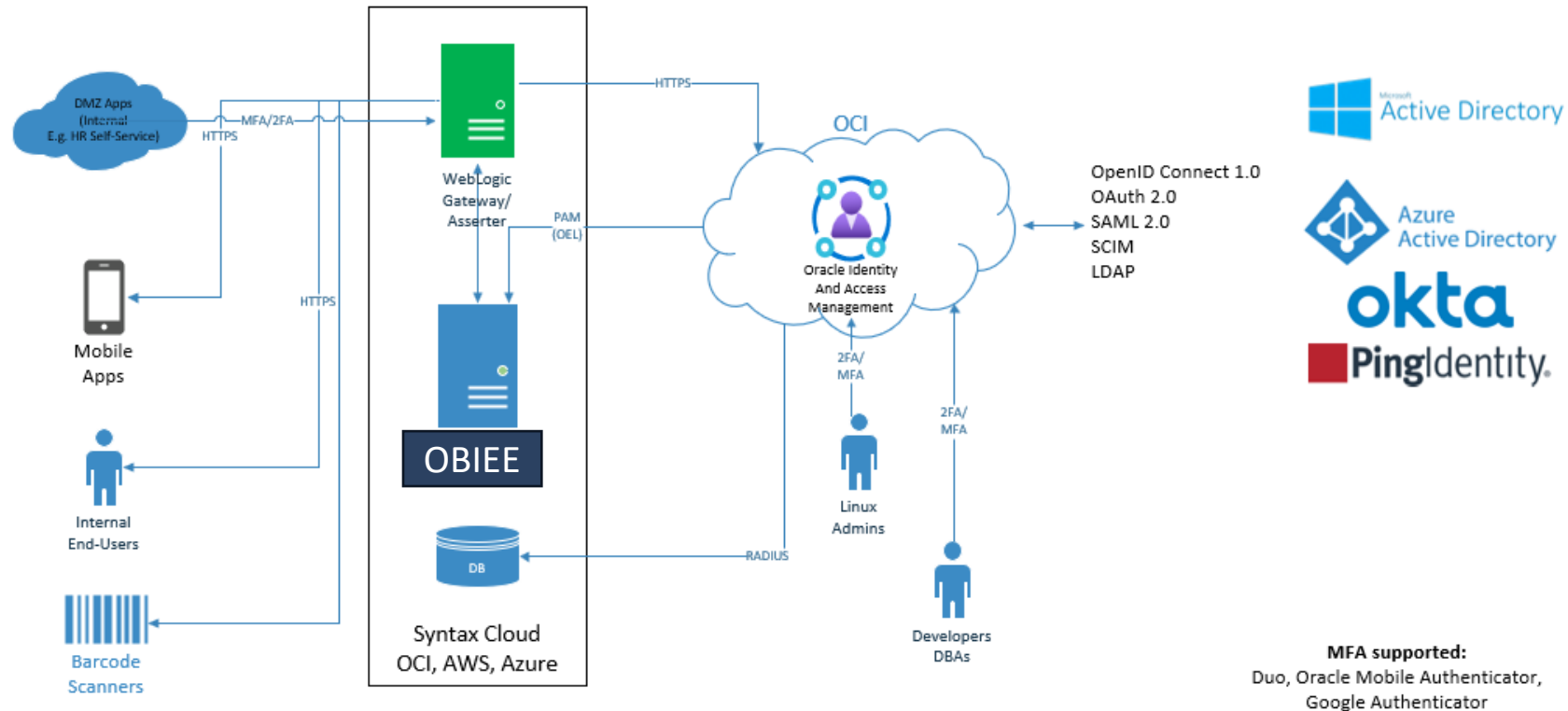- OCI IAM will provide a developer friendly IAM engine for custom and consumer applications.

By unifying administration and user experiences across these key IAM functions, the new service helps simplify administration, reduce cost of ownership, and improve time to value. The service spans cloud and on-premises, providing the flexibility to handle a wide variety of IAM use cases across employee, partner,

https://www.oracle.com/a/ocom/docs/security/what-idcs-customers-should-expect-post-migration.pdf

ASCEND 2024

Full Stack Single Sign On (SSO)
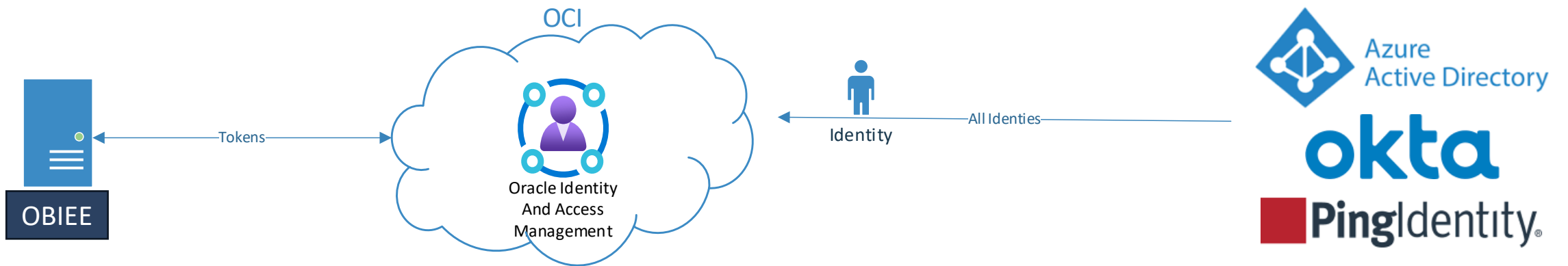
Oracle Applications

Oracle Applications

- Oracle E-Business Suite (12.1+)
  - Mobile Applications
- Fusion/ERP Cloud
- PeopleSoft
- JD Edwards
- NetSuite
- OBIEE
- APEX

Supporting Applications and Technologies

- Identity
  - Internet Directory
  - Unified Directory
- Oracle database
  - RADIUS Proxy authentication, Oracle 12c+
  - Use for support personnel (e.g., not EBS APPS schema)
  - Multi-Factor Authentication (MFA) possible
- Oracle Enterprise Linux (OEL)
  - Linux Pluggable Authentication Module (PAM), OEL 6.8+
  - Use for support personnel (e.g., not EBS APPLMGR account)
 - Multi-Factor Authentication (MFA) possible

IAM Billing

OBIEE —Tokens→ **OCI**

Oracle Identity And Access Management

Identity ←All Identies— Azure Active Directory / okta / PingIdentity

Each Identity added to IAM costs 25 cents/month
Metered Hourly/Billed Monthly

Each login Generates 2+ Tokens
First 10,000 Tokens are Free
Then .004 cents a Token

Oracle EBS SSO with Azure AD Federation
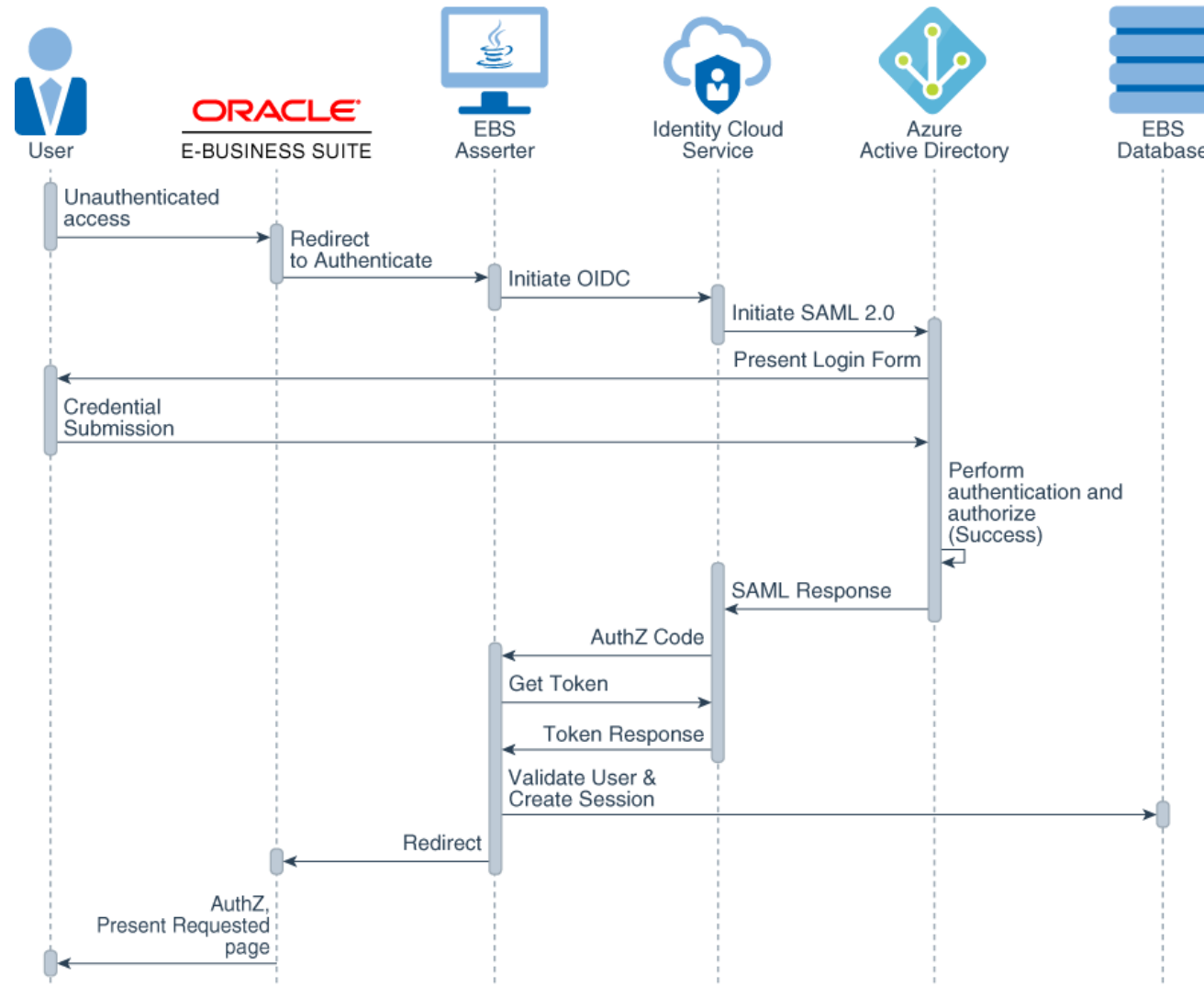
The Business Need

- BI Application Footprint
  - OAS is 5.5 and OBIEE 12.2.1.4
  - Hosted at OCI
  - Heavily integrated with Oracle E-Business Suite 12.2
  - BI database is 40TB
  - 10,000 users within the last Twelve (12) months
    - 80% of employees use BI
- The company decided to move away from Oracle Access Manager (OAM)
  - Where using OAM for pass-through-SSO with BI Applications
  - Given early 2022 to replace
- Reached out to our managed service provider for solutions
  - Said they would charge significantly more for non-Oracle solutions
  - IAM was largely selected by price
  - IAM is also now used by Oracle E-Business Suite for SSO

The Gateway Appliance
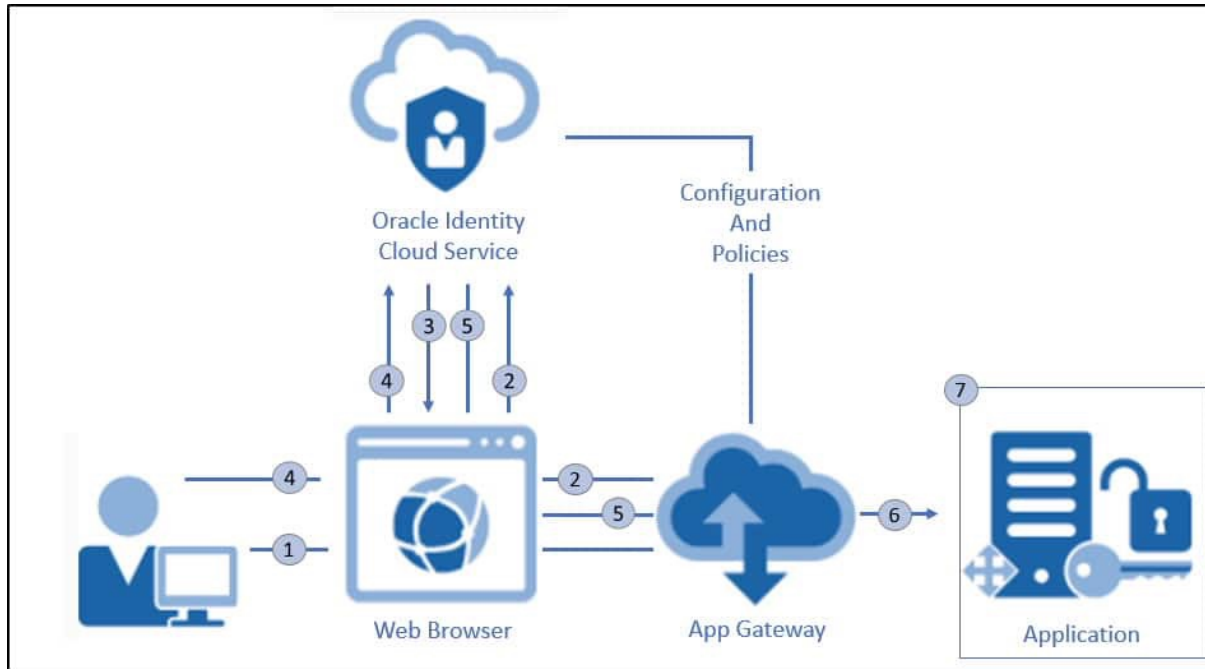
Understanding App Gateway

App Gateway is a software appliance that lets you integrate applications hosted either on a compute instance, in a cloud infrastructure, or in an on-premises server with IAM for authentication purposes.

App Gateway acts as a reverse proxy protecting web applications by restricting unauthorized network access to them. App Gateway intercepts any HTTP request to these applications and ensures that the users are authenticated with IAM before forwarding the request to these applications. App Gateway propagates the authenticated user's identity to the applications.

If the user isn't authenticated with IAM, then App Gateway redirects the user to the sign-in page for credential validation.

The IAM App Gateway
- Is a software appliance ~ software application with just enough o/s to run on industry std virtual machine
- Acts as a reverse proxy protecting resources by restricting unauthorized network access
- Intercepts HTTP requests and ensures that the users are authenticated with IDCS or IAM Identity Domain
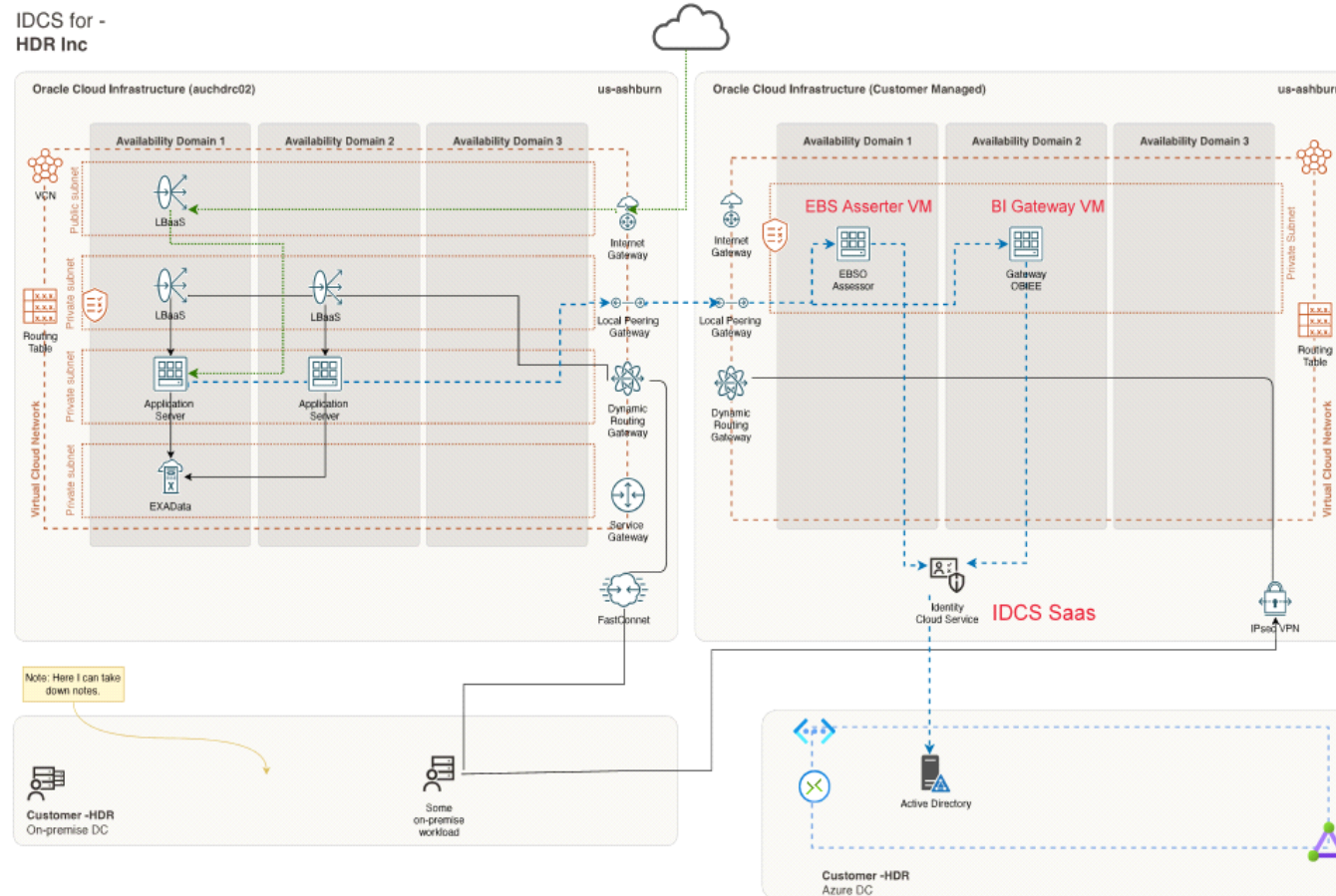- Propagates the authenticated user's identity to the Application

https://blogs.oracle.com/analytics/post/oas-sso-idcs-iam-app-gateway

https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/Identity/appgateways/understand-app-gateway.htm

HDR SSO Architecture Overview

Timeline
- 4 months of planning
- 2 months of execution

Go-Live Motion
- While old SSO solution in place, swapped in new DNS entry
- Old solution sunsetted after a few weeks

Lessons Learned

What Did Not Go Well

- BI team's first with https certs
  - https certs need to be correctly ordered with the internal security team
- Installed the gateway appliance a number of times ~ more than anticipated
  - The prebuilt machine image is complex
  - Bounce if in doubt
  - Don't debug, re-install
    - Security configs are tedious

What went well

- Finding documentation – oracle's excellent, 3rd party blogs
- OCI was very helpful

Q&A

Emily.Fuller@hdrinc.com

Michael.Miller@syntax.com

ASCEND
2024

Thank You For Attending!

Please complete the session survey in the conference app.

ASCEND
2024