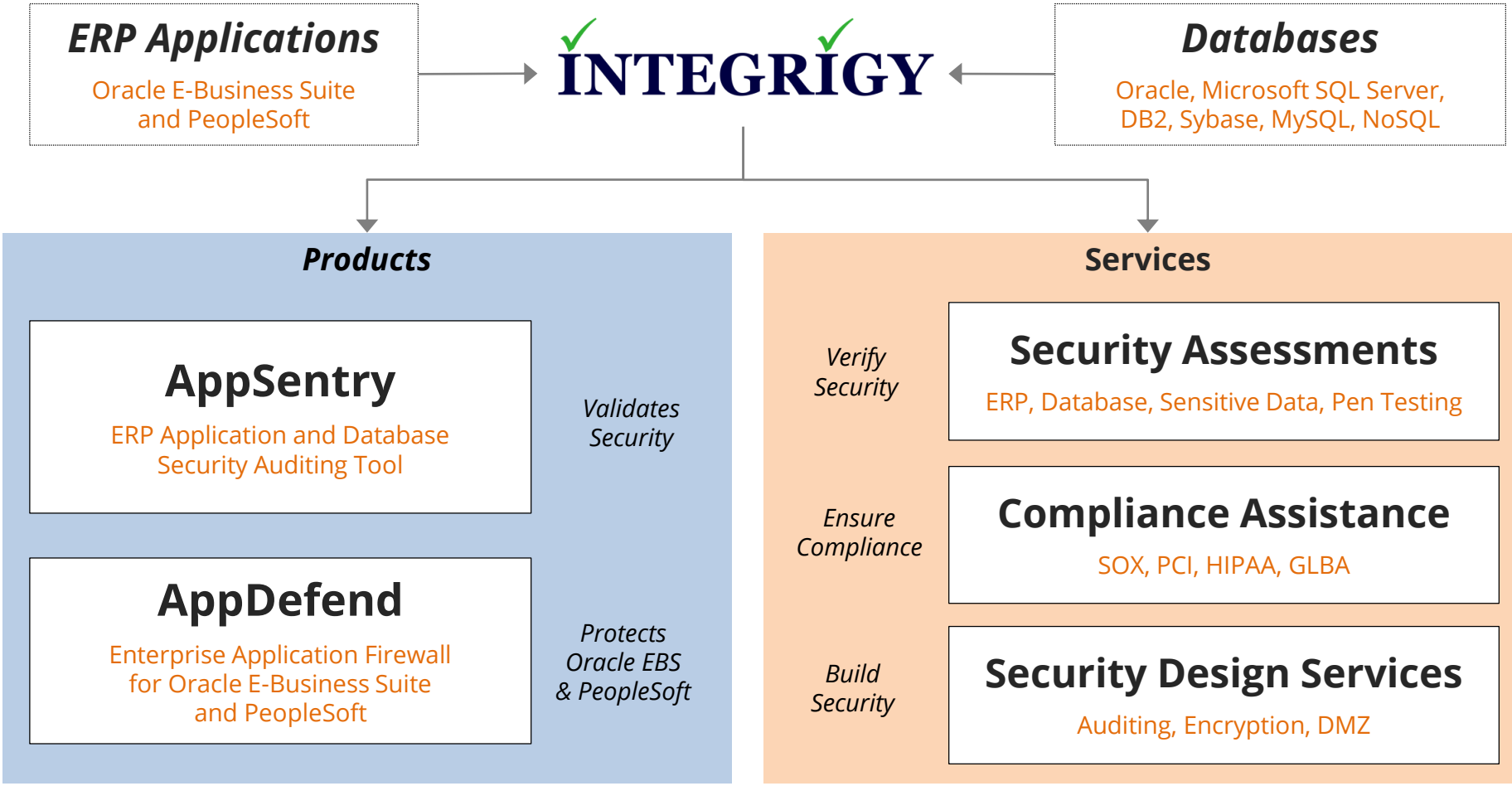
Leveraging New Oracle Database 19c Security Features with the Oracle E-Business Suite

November 14, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



Agenda

1. Oracle EBS and 19c
2. Oracle 19c Security Features Overview
3. Upgrading to 19c
4. 19c New Security Features
5. Q & A

Agenda

1. **Oracle EBS and 19c**
2. Oracle 19c Security Features Overview
3. Upgrading to 19c
4. 19c New Security Features
5. Q & A

Oracle 12c – 19c Certifications For Oracle EBS

DB Version	EBS	DB Release Date	EBS Cert Date (Linux)
12.1.0.1	11.5.10.2 12.0.6 12.1.3 12.2.1 – 12.2.4	June 2013	Sept 2013 (11.5.10.2, 12.0.6, 12.1.3) Sept 2014 (12.2)
12.1.0.2	11.5.10.2 12.0.6 12.1.3 12.2.1 – 12.2.5	July 2014	Sept 2014 (12.1) Jan 2015 (12.2) Feb 2015 (11.5.10.2)
19.3	12.1.3 12.2.1 – 12.2.9	April 2019	Sept 2019 (12.1) Sept 2019 (12.2)
19.5 (19.3 → 19.5)	12.1.3 12.2.1 – 12.2.9	October 2019	Nov 2019 (12.1) Nov 2019 (12.2)

Notes

- No certification for Oracle Database 12.2, 18.x, or 19.4.
- Oracle Database certifications are platform and version dependent, so certifications may be staggered for some platforms. (https://blogs.oracle.com/ebstech)

Oracle Product Support

Premier	▪ Five years from release ▪ Security patches and Critical Patch Updates
Extended	▪ Three years additional ▪ Security patches and Critical Patch Updates ▪ Additional annual fee – often waived
Sustaining	▪ Indefinite as long as you pay annual maintenance and have a minimum patch level – usually terminal patchset for database ▪ **NO security patches or Critical Patch Updates**

Source – http://www.oracle.com/us/support/lifetime-support/index.html

Why Upgrade from 11.2 or 12.1?

- **11.2 enters sustaining support December 2020**
  - No security patches after October 2020
  - Extended support fees have been waived for entire time
  - Market Driven Support an option for additional fee starting 2021
- **12.1 enters sustaining support July 2021**
  - No security patches after July 2021
  - No extended support fees through December 2020 for EBS
- **19c terminal release of 12c/18c/19c**
  - Premier support through March 2023
  - Extended support through March 2026

References

- EBS Database Extended Support Fees = MOS Note ID 2522948.1
- Database 12.1 Extended Support Fees = MOS Note ID 2569754.1

Oracle Database Version Support

Major Releases	Extended Support End Date	Patchsets	CPU Support End Date
Oracle 19c	March 2026	**19.x**	**January 2026**
Oracle 12c R1	July 2021	**12.1.0.2**	**July 2021**
		12.1.0.1	**July 2016**
Oracle 11g R2	December 2020	**11.2.0.4**	**October 2020**
		~~11.2.0.3~~	~~July 2015~~
		~~11.2.0.2~~	~~January 2013~~
		~~11.2.0.1~~	~~July 2011~~
~~**Oracle 11g R1**~~	~~August 2015~~	~~11.1.0.7~~	~~July 2015~~
~~**Oracle 10g R2**~~	~~July 2013~~	~~10.2.0.5~~	~~July 2013~~
~~**Oracle 10g R1**~~	~~January 2012~~	~~10.1.0.5~~	~~January 2012~~

What Version is 19c Really?

- **With 18c, Oracle changed versioning and release schedule**
  - Versions named after years, 18c = 2018, 19c = 2019, 20c = 2020, …
  - 19c is the terminal/long term support release of 12.2
  - Release Updates (RUs) and Release Update Revisions (RURs)
  - PSU → RUR and BP → RU

Version	Old Versioning	Release Type
12.2.0.1	**12.2.0.1**	Annual release
18c	**12.2.0.2**	Annual release
19c	**12.2.0.3**	Long term support release
20c	**13.1.0.1**	Annual release

Agenda

1. Oracle EBS and 19c
2. **Oracle 19c Security Features Overview**
3. Upgrading to 19c
4. 19c New Security Features
5. Q & A

Oracle 12c/19c Security Feature Certifications

Certified/ Supported	▪ Transparent Data Encryption (TDE) - Column and Tablespace ▪ Advanced Security Option - SQL*Net Encryption/SSL ▪ Virtual Private Database (VPD) ▪ Label Security (OLS) ▪ SecureFiles ▪ Connection Manager (12.1.0.1 only) ▪ Multitenant – single tenant only (19c only) ▪ Database Vault (12c)
Pending Certified	▪ **Database Vault (19c)** ▪ **Data Masking (19c)**
Not Certified	▪ Data Redaction

Reference – https://blogs.oracle.com/ebstech

Oracle Database 12.1 New Security Features

- **Major new security features for EBS**
  - Unified Auditing – lots of auditing changes
- **Incremental security improvements for EBS**
  - Mandatory Auditing
  - SHA-512 for password hash (12.1.0.2)
  - FIPS-140 for TDE (12.1.0.2)
  - SELECT ANY DICTIONARY no access to USER$, other tables
  - extproc run as specific OS user rather than oracle
  - READ privilege which is SELECT without locking (12.1.0.2)

Oracle Database 12.1 New Security Features

- **Unsupported by Oracle EBS**
  - Transparent Sensitive Data Protection (TSDP)
  - Real Application Security (RAS) – next-generation VPD
  - Multitenant (pluggable databases)
  - Data Redaction

- **Not directly relevant to Oracle EBS**
  - Audit trail cleanup in read-only databases (12.1.0.2)
  - Predefined Unified Audit policies for CIS and DV (12.1.0.2)

Oracle 12.2 – 19.5 Major New Security Features for EBS

12.2	▪ Automatically lock inactive database accounts ▪ Transparent Sensitive Data Protection (TSDP) works with Unified Auditing, FGA, and TDE ▪ SELECT ANY TABLE access to Unified Auditing removed
18.x	▪ **Direct integration of Active Directory** ▪ **UTL_FILE_DIR desupported** ▪ Schema only accounts ▪ Encrypt credentials in LINK$ and SCHEDULER$_CREDENTIAL tables ▪ Write Unified Audit to SYSLOG
19.x	▪ **Privilege Analysis now included in Enterprise Edition** ▪ Most default database accounts now schema only accounts ▪ Audit top-level SQL Statements

Agenda

1. Oracle EBS and 19c
2. Oracle 19c Security Features Overview
3. **Upgrading to 19c**
4. 19c New Security Features
5. Q & A

Oracle 19c and EBS References

EBS Version	19c References
All	Database Initialization Parameters for Oracle E-Business Suite Release 12 (Doc ID 396009.1) FAQ: Oracle E-Business Suite and the Oracle Multitenant Architecture (Doc ID 2567105.1) Using UTL_FILE_DIR or Database Directories for PL/SQL File I/O in Oracle E-Business Suite Releases 12.1 and 12.2 (Doc ID 2525754.1)
12.1	Interoperability Notes: Oracle E-Business Suite Release 12.1 with Oracle Database 19c (Doc ID 2580629.1) Using Oracle 19c RAC Multitenant (Single PDB) with Oracle E-Business Suite Release 12.1 (Doc ID 2530680.1) Cloning Oracle E-Business Suite Release 12.1 with Multitenant Database using Rapid Clone (Doc ID 2560690.1)
12.2	Interoperability Notes: Oracle E-Business Suite Release 12.2 with Oracle Database 19c (Doc ID 2552181.1) Using Oracle 19c RAC Multitenant (Single PDB) with Oracle E-Business Suite Release 12.2 (Doc ID 2530665.1) Export/Import Process for Oracle E-Business Suite Release 12.2 Database Instances Using Oracle Database 19c (Doc ID 2554156.1) Cloning Oracle E-Business Suite Release 12.2 with Multitenant Database using Rapid Clone (Doc ID 2552208.1)

Upgrading Oracle EBS to Oracle 12c

- **Follow Oracle Support Note ID 2580629.1 (12.1) or 2552181.1 (12.2)**
- **19c upgrade only supported going to 19.3 then to 19.5**

12.1 Step	12.2 Step	Security Notes Regarding Step
3	**3**	▪ Allow case sensitive passwords (optional) = This step should be mandatory.
16	**18**	▪ Store the UTL_FILE_DIR parameter values = As part of update, only the EBS temp directory should be allowed. All other directories should be specifically migrated to Oracle Directory objects.
21	**21**	▪ Remove the MGDSYS schema (conditional) = Verify if MGDSYS exists and remove it.
46	**44**	▪ Apply latest Release Update (Recommended) = This step should be mandatory and the latest RU should be applied in order to have the latest security patches. ▪ As of November 2019, upgrade from 19.3 to 19.5. See latest Database Patch Availability Document (PAD)

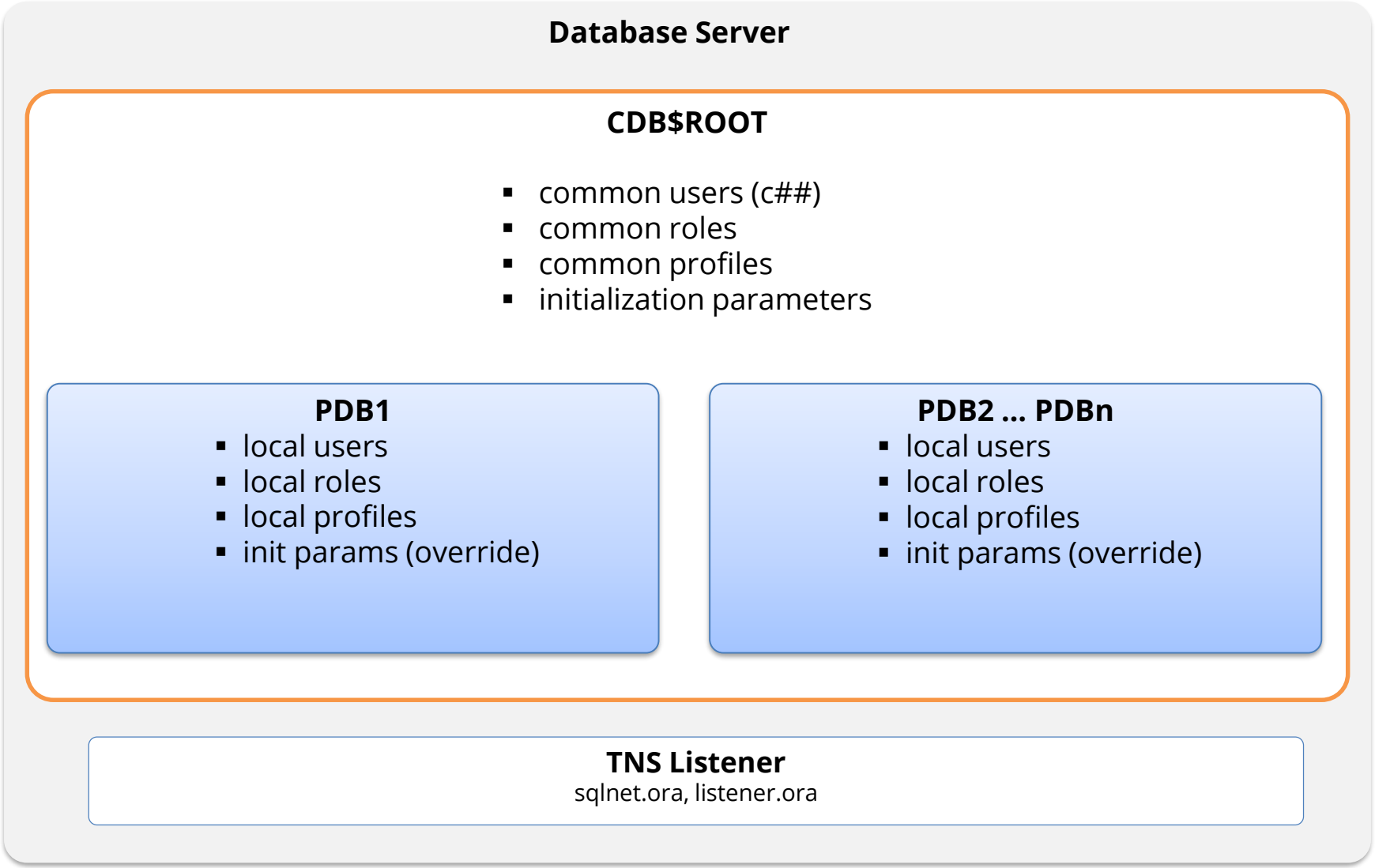
Steps and notes based on November 2019 versions of the Support Notes

Oracle Multitenant Quick Introduction

- **Oracle multitenant architecture was introduced in Oracle 12c**
  - 12c supports both multitenant and non-CDB
  - 19c deprecates non-CDB
  - 20c desupports/removes non-CDB

Container Database CDB	▪ Super database or root database ▪ Contains one or more pluggable databases (PDB) ▪ Up to 252 PBDs supported in a CDB
Pluggable Database PDB	▪ Sub database which in plugged into a container database ▪ Easy to move PDB from one CDB to another CDB

Oracle Multitenant Architecture



19c Multitenant Mandatory for EBS

- **EBS with 19c must run using Multitenant using a single tenant**
  - Multiple tenants (more than one PDBs) are not supported
  - EBS will be only PDB in the CDB
  - No additional licenses – 3 user-created PDBs allowed in Enterprise Edition
- **Database patches only applied to CDB**
- **Relocating or cloning EBS PDB is not supported**
- **See MOS Note ID 2567105.1 *FAQ: Oracle E-Business Suite and the Oracle Multitenant Architecture* for more information**

UTL_FILE_DIR

- **UTL_FILE_DIR desupported in 18c and removed in 19c**
  - 19.3 added feature to allow UTL_FILE to specify either a directory object or a physical directory which has a corresponding directory object
  - All directories in UTL_FILE_DIR accessible for reading and writing by all database accounts – a security risk
- **Custom code using UTL_FILE_DIR must be reviewed and if possible, convert custom code to use Directory objects**
- **See MOS Note ID 2525754.1 *Using UTL_FILE_DIR or Database Directories for PL/SQL File I/O in Oracle E-Business Suite Releases 12.1 and 12.2* for more information**

Agenda

1. Oracle EBS and 19c
2. Oracle 19c Security Features Overview
3. Upgrading to 19c
4. **19c New Security Features**
5. Q & A

Active Directory Integration for Database Accounts

- **18c adds Centrally Managed Users (CMU) for simple integration with Active Directory users and roles**
  - Requires Windows Server 2008R2 or higher
  - Replaces Enterprise User Security (EUS) and Oracle Internet Directory (OID)
  - Not intended for application or service accounts
  - Eliminates some decentralized Oracle database accounts
  - Configuration shared between CDB and EBS PDB
- **Use CMU for all named accounts including DBAs and ad-hoc users**
  - Does not replace DBA use of APPS, SYS, or SYSTEM
  - Users may be mapped to a specific account (recommended) or a shared schema account

Privilege Analysis

- **12c added Privilege Analysis to report on actual privileges used by database accounts**
  - Used to determine Least Privileges required for an account
  - Captures privilege tracking similar to auditing
  - Prior to 19c, included with Database Vault Option
- **For 19c, Privilege Analysis included with Enterprise Edition**
- **Use to analyze the privileges for custom database accounts of ad-hoc users, interfaces, 3rd applications, and other customizations**
  - Helpful for 3rd party applications that grant DBA or excessive privileges
  - Precisely define privileges for interfaces and ad-hoc accounts

Real Application Security (RAS)

- **New with Oracle 12c**
  - Next generation Virtual Private Database (VPD)
  - Ideal for APEX applications
- **Define users separately from DBA_USERS**
  - DBA_XS_USERS
  - Can directly connect to the database
  - Flag in 12.1.0.2
- **RAS role and event auditing with Unified Audit**
- **Not used by Oracle E-Business Suite**

READ Privilege (12.1.0.2)

- **READ Object**
  - READ object privilege enables users to query, but not modify database tables, views, materialized views and synonyms
  - SELECT object privilege can still be used
  - SELECT object privilege also allows users to lock rows when reading

- **READ ANY TABLE**
  - Allows user to query any table in the database
  - GRANT ALL PRIVILEGES TO user SQL also now includes the READ ANY TABLE system privilege as well as the READ object privilege

TSDP 19c Improvements

- **Transparent Sensitive Data Protection (TSDP)**
  - New functionality, views, and Cloud Control integration
- **Use TSDP to identify, create and manage policies to protect sensitive data. Use with –**
  - Oracle Data Redaction
  - Oracle Virtual Private Database (VPD)
  - Unified Auditing
  - Fine-grained Auditing (FGA)
  - Transparent Data Encryption (TDE) column encryption

Last Login Date

- Knowing when users last logged-in is required for effective user account management and auditing
- `last_login` date added to `SYS.DBA_USERS`

```
select username, account_status, common, last_login
from sys.dba_users
order by last_login asc;
```

Username	Account Status	Common	Last Login
C##INTEGRIGY	OPEN	YES	05-AUG-14 12.46.52.000000000 PM AMERICA/NEW_YORK
C##INTEGRIGY_TEST_2	OPEN	YES	02-SEP-14 12.29.04.000000000 PM AMERICA/NEW_YORK
XS$NULL	EXPIRED & LOCKED	YES	02-SEP-14 12.35.56.000000000 PM AMERICA/NEW_YORK
SYSTEM	OPEN	YES	04-SEP-14 05.03.53.000000000 PM AMERICA/NEW_YORK

Unified Auditing Super View

SYS.UNIFIED_AUDIT_TRAIL Content	# of Columns
Standard auditing including SYS audit records	44
Real Application Security (RAS) and RAS auditing	17
Oracle Label Security	14
Oracle Data Pump	2
Fine-grained Auditing (FGA)	1
Database Vault (DV)	10
Oracle RMAN	5
SQL*Loader Direct Load	1
Total	**94**

Audit Any Role

- **Any database role can be audited, including user-created roles**
  - Audits all system privileges granted to a role
  - Eliminates need to update audit policies when roles are updated

```
CREATE AUDIT POLICY role_dba_audit_pol
ROLES DBA
CONTAINER = ALL;
AUDIT POLICY role_dba_audit_pol;
```

Oracle 19c Mandatory Auditing

- **Oracle 19c always-on-auditing for SYS operations**
  - Always audited roles and users = SYS, SYSDBA, SYSOPER, SYSASM, SYSBACKUP, SYSDG, SYSKM
- **Mandatory Auditing Events –**
  - CREATE AUDIT POLICY
  - ALTER AUDIT POLICY
  - DROP AUDIT POLICY
  - AUDIT
  - NOAUDIT
  - Database Vault configurations
  - DBMS_FGA PL/SQL package
  - DBMS_AUDIT_MGMT PL/SQL package
  - ALTER TABLE attempts on the AUDSYS audit trail

Agenda

1. Oracle EBS and 19c
2. Oracle 19c Security Features Overview
3. Upgrading to 19c
4. 19c New Security Features
5. Q & A

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

web – **www.integrigy.com**

e-mail – **info@integrigy.com**

blog – **integrigy.com/oracle-security-blog**

youtube – **youtube.com/integrigy**