INTEGRIGY

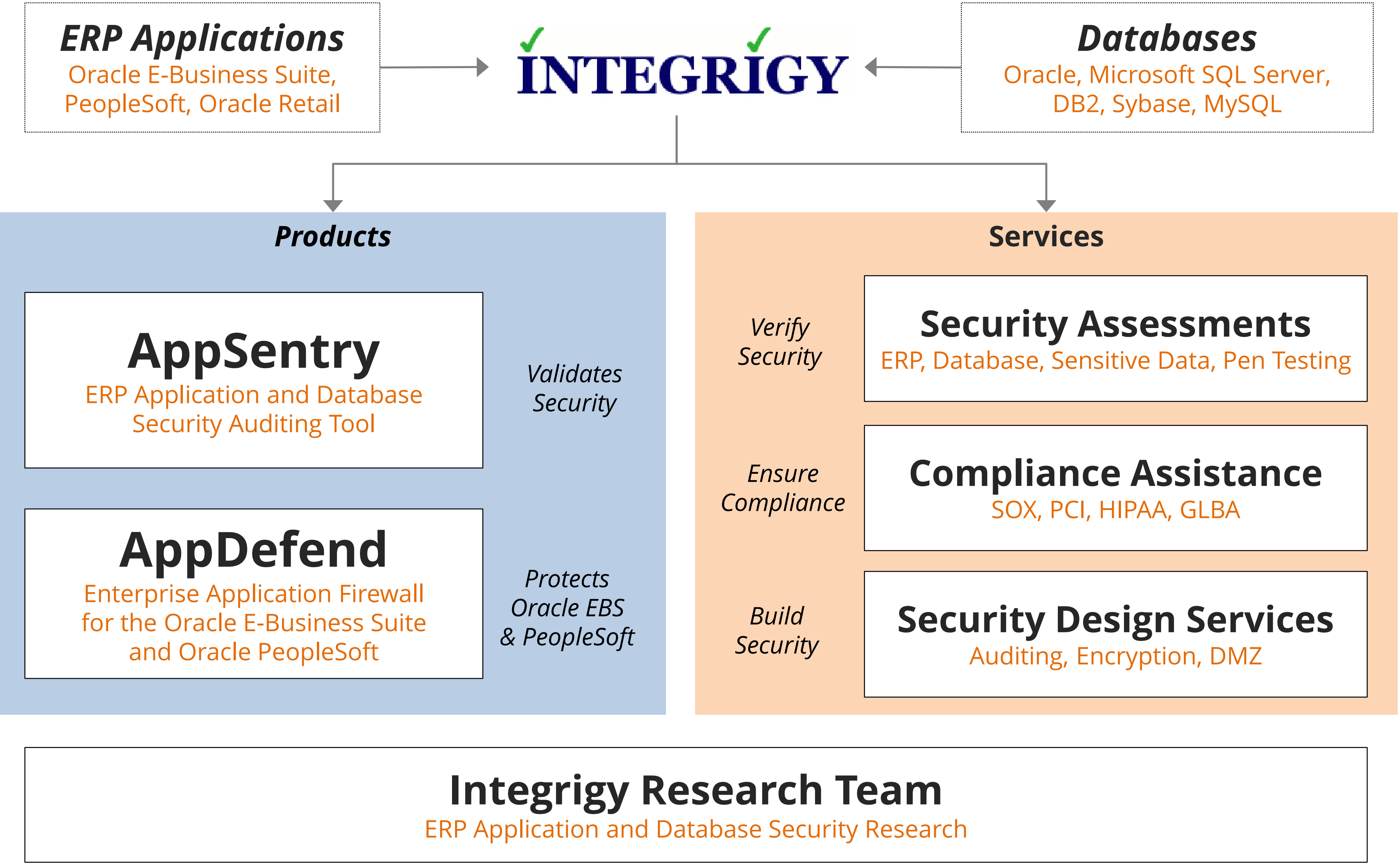
Oracle E-Business Suite and Java Security – What You Need to Know

March 26, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications
Oracle E-Business Suite,
PeopleSoft, Oracle Retail

INTEGRIGY

Databases
Oracle, Microsoft SQL Server,
DB2, Sybase, MySQL

Products

AppSentry
ERP Application and Database Security Auditing Tool

Validates Security

AppDefend
Enterprise Application Firewall for the Oracle E-Business Suite and Oracle PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments
ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance
SOX, PCI, HIPAA, GLBA

Build Security

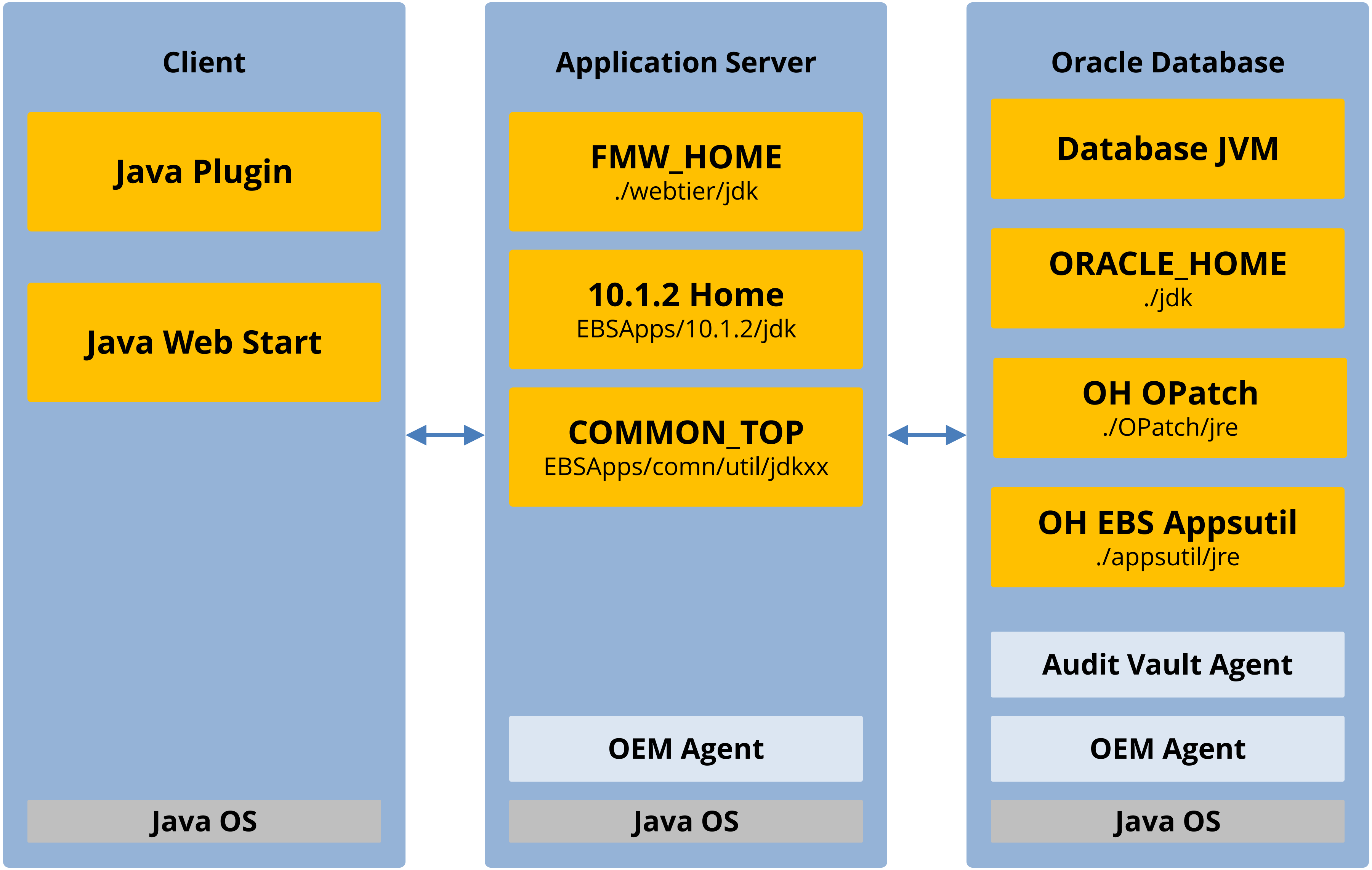
Security Design Services
Auditing, Encryption, DMZ

Integrigy Research Team
ERP Application and Database Security Research

Terminology

Term	Definition
JVM	**Java Virtual Machine** is virtual machine that runs Java programs. Multiple JVMs may run on a single machine. A JVM is also run within the Oracle Database.
JDK	**Java Development Kit** is a full install of a JVM along with development resources and potentially Java source code. The JDK is typically installed on a server.
JRE	**Java Runtime Environment** is a limited install of a JVM in order to run a Java application. A client-side install of Java is typically a JRE rather than a JDK.
Java Versions	Java versions may be specified by a major version number such as 6, 7, 8, or 9; a point version 1.6, 1.7, 1.8, or 1.9, or a full version such as JRE 1.8.0_201.
Java Editions	Java is available as **Standard Edition** (SE), Enterprise Edition (EE), and Mobile Edition (ME). For Oracle E-Business Suite, **Standard Edition** (SE) is the only edition used.

Oracle EBS 12.2 Java Installations



Client

Java Plugin

Java Web Start

Java OS

Application Server

FMW_HOME
./webtier/jdk

10.1.2 Home
EBSApps/10.1.2/jdk

COMMON_TOP
EBSApps/comn/util/jdkxx

OEM Agent

Java OS

Oracle Database

Database JVM

ORACLE_HOME
./jdk

OH OPatch
./OPatch/jre

OH EBS Appsutil
./appsutil/jre

Audit Vault Agent

OEM Agent

Java OS

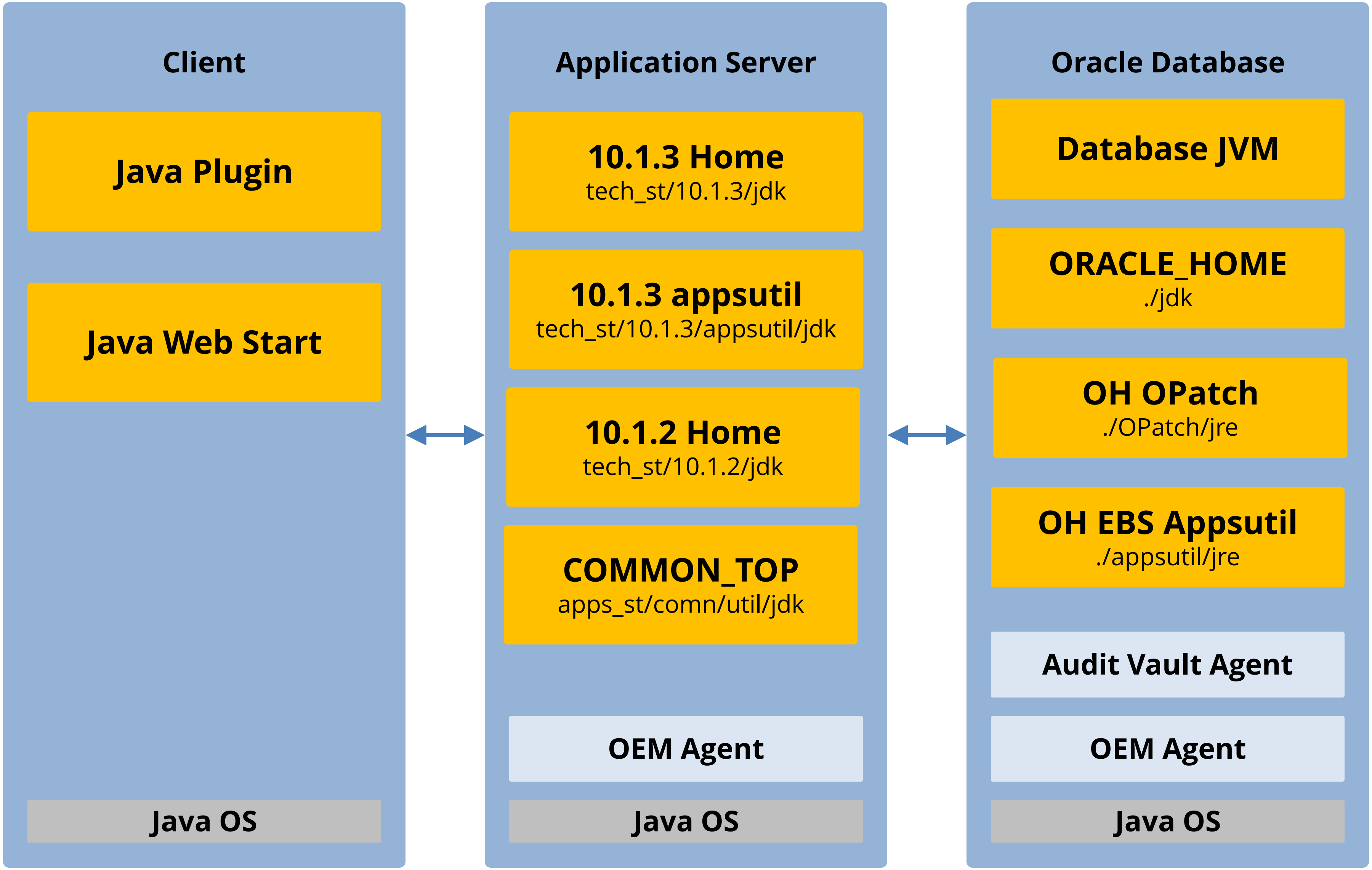
Oracle EBS 12.2 Java Install Locations (Example)

EBS 12.2.7
Single Node
Vision Database

find . -executable -type f -name java

```
./u01/install/APPS/fs2/FMW_Home/webtier/jdk/jre/bin/java
./u01/install/APPS/fs2/FMW_Home/webtier/jdk/bin/java
./u01/install/APPS/fs2/EBSapps/10.1.2/jdk/jre/bin/java
./u01/install/APPS/fs2/EBSapps/10.1.2/jdk/bin/java
./u01/install/APPS/fs2/EBSapps/10.1.2/jdk-old/jre/bin/java
./u01/install/APPS/fs2/EBSapps/10.1.2/jdk-old/bin/java
./u01/install/APPS/fs2/EBSapps/comn/util/jdk64/jre/bin/java
./u01/install/APPS/fs2/EBSapps/comn/util/jdk64/bin/java
./u01/install/APPS/fs2/EBSapps/comn/util/jdk32/jre/bin/java
./u01/install/APPS/fs2/EBSapps/comn/util/jdk32/bin/java
./u01/install/APPS/fs2/EBSapps/appl/msc/12.0.0/bin/SNO/scp/12.2/sno/installer_jre/bin/java
./u01/install/APPS/fs2/EBSapps/appl/msc/12.0.0/bin/PS/scp/12.2/ps/jre/bin/java
./u01/install/APPS/fs1/FMW_Home/webtier/jdk/jre/bin/java
./u01/install/APPS/fs1/FMW_Home/webtier/jdk/bin/java
./u01/install/APPS/fs1/EBSapps/10.1.2/jdk/jre/bin/java
./u01/install/APPS/fs1/EBSapps/10.1.2/jdk/bin/java
./u01/install/APPS/fs1/EBSapps/10.1.2/jdk-old/jre/bin/java
./u01/install/APPS/fs1/EBSapps/10.1.2/jdk-old/bin/java
./u01/install/APPS/fs1/EBSapps/comn/util/jdk64/jre/bin/java
./u01/install/APPS/fs1/EBSapps/comn/util/jdk64/bin/java
./u01/install/APPS/fs1/EBSapps/comn/util/jdk32/jre/bin/java
./u01/install/APPS/fs1/EBSapps/comn/util/jdk32/bin/java
./u01/install/APPS/fs1/EBSapps/appl/msc/12.0.0/bin/SNO/scp/12.2/sno/installer_jre/bin/java
./u01/install/APPS/fs1/EBSapps/appl/msc/12.0.0/bin/PS/scp/12.2/ps/jre/bin/java
./u01/install/APPS/12.1.0/jdk/jre/bin/java
./u01/install/APPS/12.1.0/jdk/bin/java
./u01/install/APPS/12.1.0/OPatch/jre/bin/java
./u01/install/APPS/12.1.0/appsutil/clone/jre/bin/java
./u01/install/APPS/12.1.0/appsutil/jre/bin/java
```

Oracle EBS 12.1/12.0 Java Installations



Client

Java Plugin

Java Web Start

Java OS

Application Server

10.1.3 Home
tech_st/10.1.3/jdk

10.1.3 appsutil
tech_st/10.1.3/appsutil/jdk

10.1.2 Home
tech_st/10.1.2/jdk

COMMON_TOP
apps_st/comn/util/jdk

OEM Agent

Java OS

Oracle Database

Database JVM

ORACLE_HOME
./jdk

OH OPatch
./OPatch/jre

OH EBS Appsutil
./appsutil/jre

Audit Vault Agent

OEM Agent

Java OS

Java Security Patching

- **Java security updates released Quarterly as part of the Oracle Critical Patch Updates (CPU)**
- **Security vulnerabilities are fixed by a version upgrade rather than a patch**
  - Different than other Oracle EBS patching
- **January 2019 CPU**
  - JDK/JRE 11.0.1
  - JDK/JRE 1.8_192
  - JDK/JRE 1.7_201 (commercial license see MOS Note 1439822.1)

Java Versions and Support

Version	Public Support End	Premier Support End (requires support)	Extended Support End (additional fee)
Java 6 (1.6)	April 2013	December 2015	December 2018
Java 7 (1.7)	April 2015	July 2019	July 2022
Java 8 (1.8)	January 2019	March 2022	March 2025
Java 9-12	*No EBS support*	*No EBS support*	*No EBS Support*

Support Entitlement for Java SE When Used As Part of Another Oracle Product (Doc ID 1557737.1)

Java Versions and Support – EBS Impact

Version	Client	Server
Java 6	▪ Client support ended Jun 2017 ▪ Upgrade to JRE 8 for support	▪ Support and updates ended December 2018 ▪ Must upgrade to JDK 7 for updates
Java 7	▪ Client support under extended support ▪ Java Plugin only	▪ Support and updates through July 2022 ▪ Latest versions automatically certified
Java 8	▪ Client support and updates through March 2025 ▪ Java Web Start and Java Plugin	▪ Currently no server support
Java 9-12	▪ No Oracle EBS support	▪ No Oracle EBS support

Overview of Using Java with Oracle E-Business Suite Release 12.x (Doc ID 418664.1)

Java Vulnerability Attack Vectors

- Client-side Plugin/Web Start
- Untrusted Code
- Untrusted Data
- Java Deserialization
- Cryptographic Issues
- Local

Client-side Attack Vector

- Triggered through a redirect or phishing attack
- End-user must client on a link in browser to start malicious applet or JNLP file
- Attacker can access different and older Java plugins by specifying version numbers
- Compromise machine through Java vulnerabilities

Client	Application Server	Database Server
▪ All Java Plugins installed on client ▪ All Java Web Start installed on client	Not Applicable	Not Applicable

Untrusted Code Attack Vector

- **Execute malicious Java code to bypass or escape the Java SecurityManager**
- **Must have the ability to execute Java code**
  - For client, same as client-side attack vector
- **Depending on the type of Java vulnerability, exploit may access limited information, network functions, and/or execute code at the operating system**

Client	Application Server	Database Server
▪ All Java Plugins installed on client ▪ All Java Web Start installed on client	Not applicable	▪ Database JavaVM

Untrusted Data Attack Vector

- Exploit vulnerabilities in Java APIs based on application vulnerabilities that allow access to these Java APIs
- Malicious payload through web server to exploit vulnerabilities in image processing, web services, …
- Access to sensitive data, execute OS commands, etc.

Client	Application Server	Database Server
▪ All Java Plugins installed on client ▪ All Java Web Start installed on client	▪ WebTier/10.1.3 JVM ▪ Limited 10.1.2 JVM	▪ Database JavaVM

Java Deserialization Attack Vector

- Specific type of untrusted data attack that exploits the Java object serialization process
- Requires vulnerable helper classes (such as Apache Struts) to be exploited
- Application accepts serialized objects and deserializes objects – while deserializing calls the helper class

Client	Application Server	Database Server
▪ All Java Plugins installed on client ▪ All Java Web Start installed on client	▪ WebTier/10.1.3 JVM	▪ Database JavaVM

Java Vulnerabilities – January 2019 CPU

Vulnerability	Component
CVE-2018-11212	ImageIO (libjpeg)
CVE-2019-2426	Networking
CVE-2019-2449	Deployment
CVE-2019-2422	Libraries

This vulnerability applies to Java deployments, typically in clients running sandboxed **Java Web Start** applications or sandboxed Java applets (in Java SE 8), that load and **run untrusted code** (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.

Cryptographic Issues Attack Vector

- Java install provides the support for encryption using TLS and strong cryptographic ciphers
- In order to upgrade to TLS 1.2 and strongest ciphers, Java must be upgraded for the web server
- Limited but may lead to access of sensitive data
- For 12.2, see MOS Note ID 1367293.1
- For 12.1, see MOS Note ID 376700.1

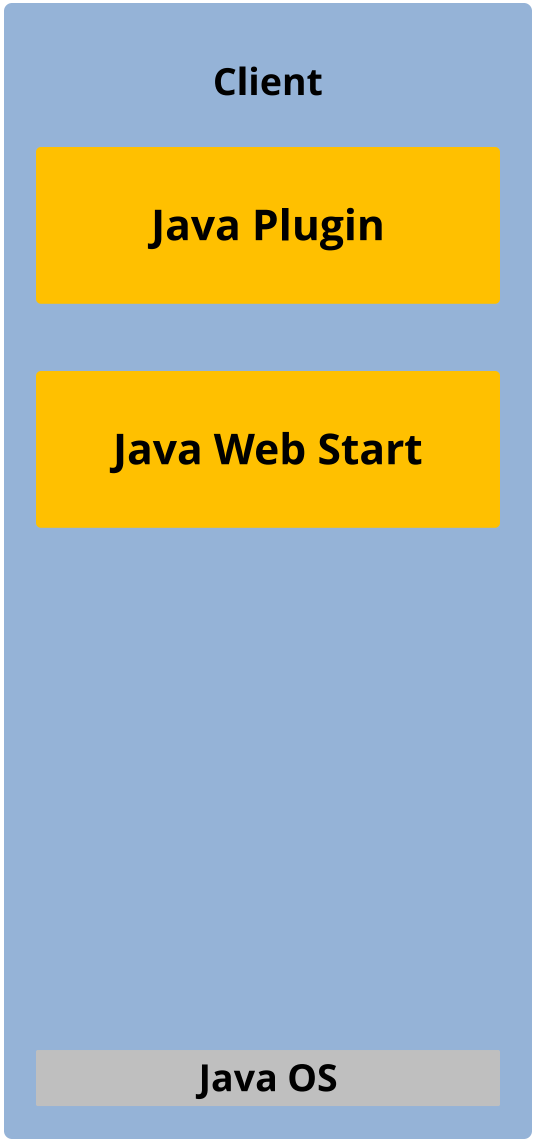
Client	Application Server	Database Server
▪ All Java Plugins installed on client ▪ All Java Web Start installed on client	▪ WebTier/10.1.3 JVM	Not applicable

Local Issues Attack Vector

- Java installation exploited by local operating system user
- Requires operating system access to application or database servers
- Access sensitive data, Java security configuration
  - Such as temporary files, etc.

Client	Application Server	Database Server
Not applicable	▪ All installed JVMs	▪ All installed JVMs ▪ Not database

EBS Java Client-side



Client

Java Plugin

Java Web Start

Java OS

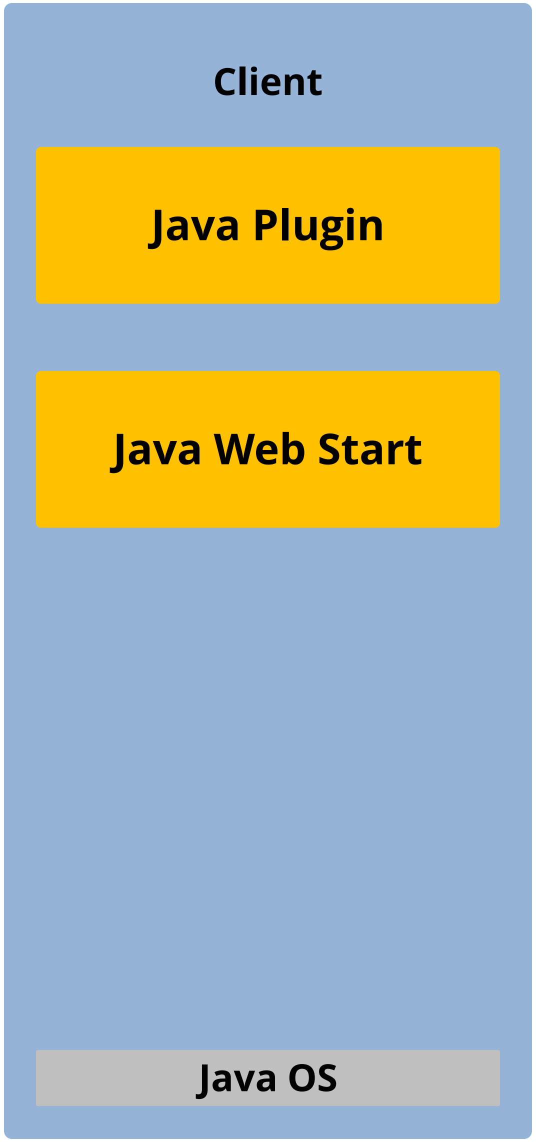
Background

- **Java Web Start** supported by EBS 12.1 and 12.2 as of April 2017
- **Java Plugin** desupported by Firefox, Chrome, and MS Edge
- Java Web Start only supports JRE 8

Security

- Only limited security improvements in Java Web Start vs Plugin

EBS Java Client-side



Client

Java Plugin

Java Web Start

Java OS

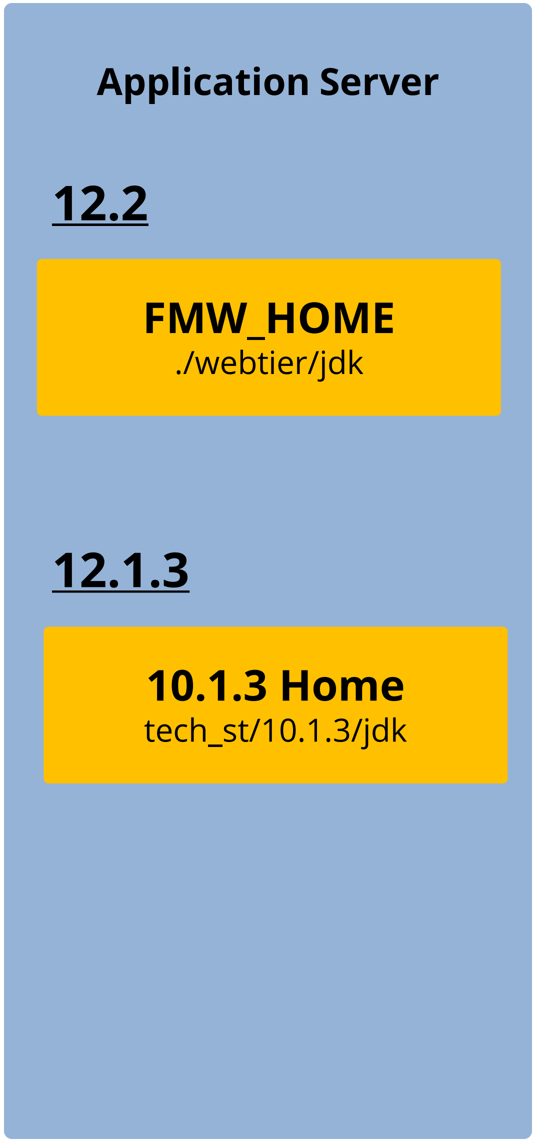
Recommendations

- Use Web Start rather than Plugin
- Update Quarterly for CPUs
- See MOS Note 2188898.1 to upgrade from Plugin to Web Start
- Java Web Start JRE 8 Update 181 required for multiple Forms sessions
- Auto-Update is supported by Oracle

CRITICAL

- Verify all Jinitiator installations are removed from ALL desktops.

EBS Java 12.2 WebTier/12.1 10.1.3



Application Server

12.2

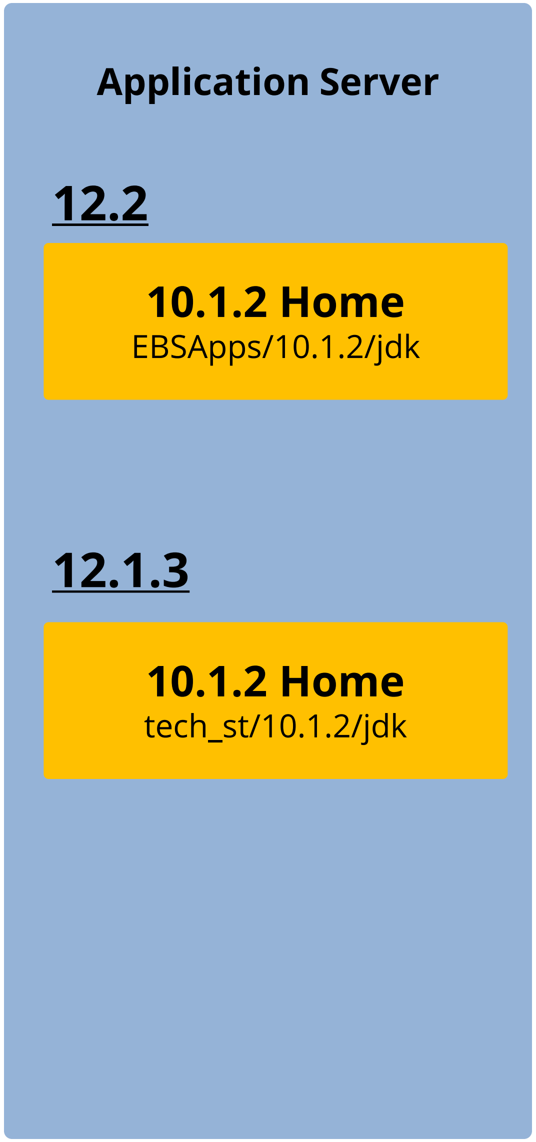
FMW_HOME
./webtier/jdk

12.1.3

10.1.3 Home
tech_st/10.1.3/jdk

- Upgrade the application server web tier JDK quarterly for CPUs
- Always use the latest version of the JDK
- Only minimal testing of basic self-service functionality is required
- 12.2 = MOS Note 1530033.1
- 12.1 = MOS Note 1467892.1

EBS Java 12.2/12.1 10.1.2 Home



Application Server

12.2

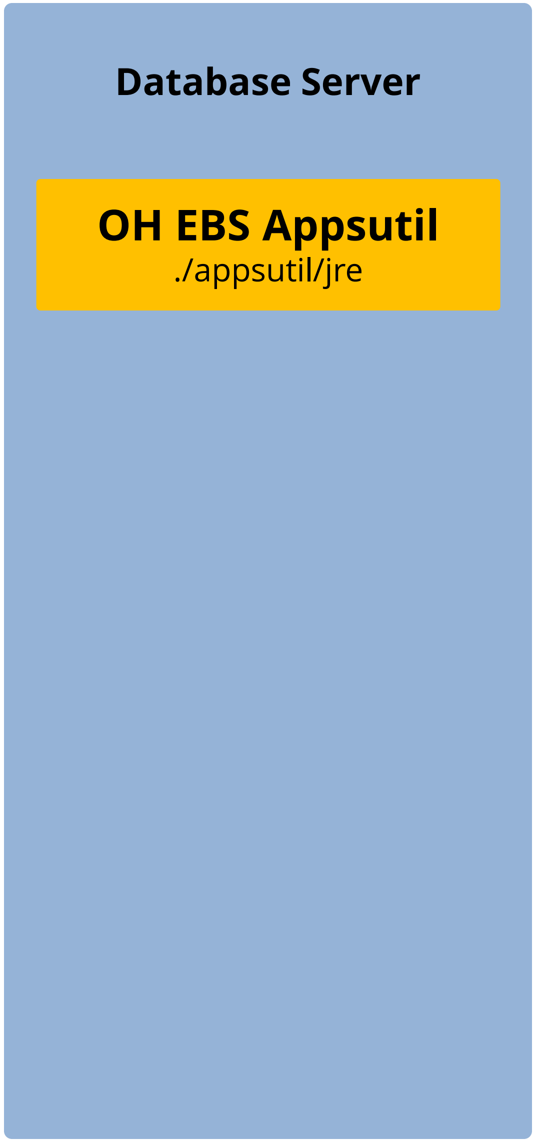
10.1.2 Home
EBSApps/10.1.2/jdk

12.1.3

10.1.2 Home
tech_st/10.1.2/jdk

- Less risk and more difficult to exploit Java vulnerabilities
- Upgrade whenever upgrading 10.1.2 Oracle Forms
- Always use the latest version of the JDK
- Same testing as required when upgrading Oracle Forms
- 12.2 = MOS Note 1530033.1
- 12.1 = MOS Note 1467892.1

EBS Oracle Database Appsutil JDK

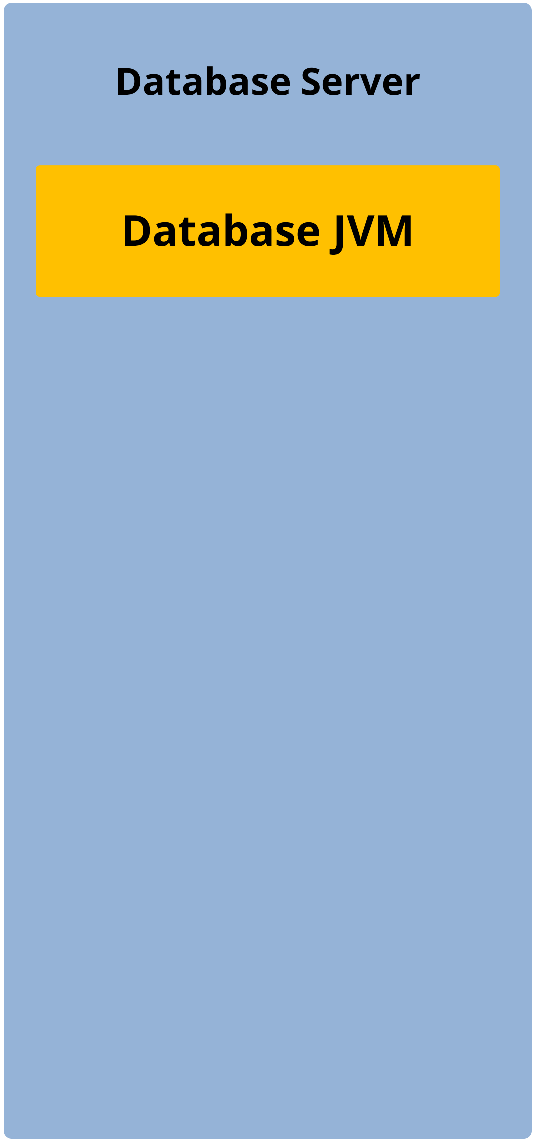


Database Server

OH EBS Appsutil
./appsutil/jre

- Only used for administrative and patching activities
- Update whenever upgrading database
- Always use the latest version of the JDK
- No testing required
- 12.2 = MOS Note 1530033.1
- 12.1 = MOS Note 1467892.1

EBS Oracle Database JVM



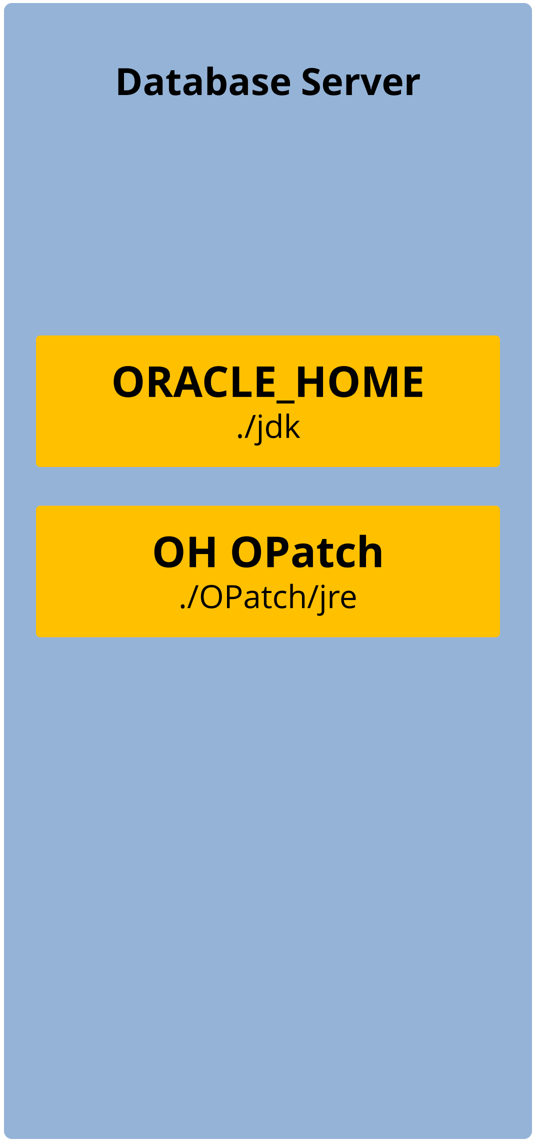
Database Server

Database JVM

Database JVM

- Any database account can potentially execute Java classes
- Multiple exploits allow for deserialization attacks, bypass of security manager, or operating system/network access
- Some vulnerabilities require only CREATE SESSION and others require CREATE PROCEDURE
- Updates as part of database CPU patches
- Mandatory additional steps are required as part of the CPU patch (SPU/PSU)

EBS Oracle Database JVM



Database Server

ORACLE_HOME
./jdk

OH OPatch
./OPatch/jre

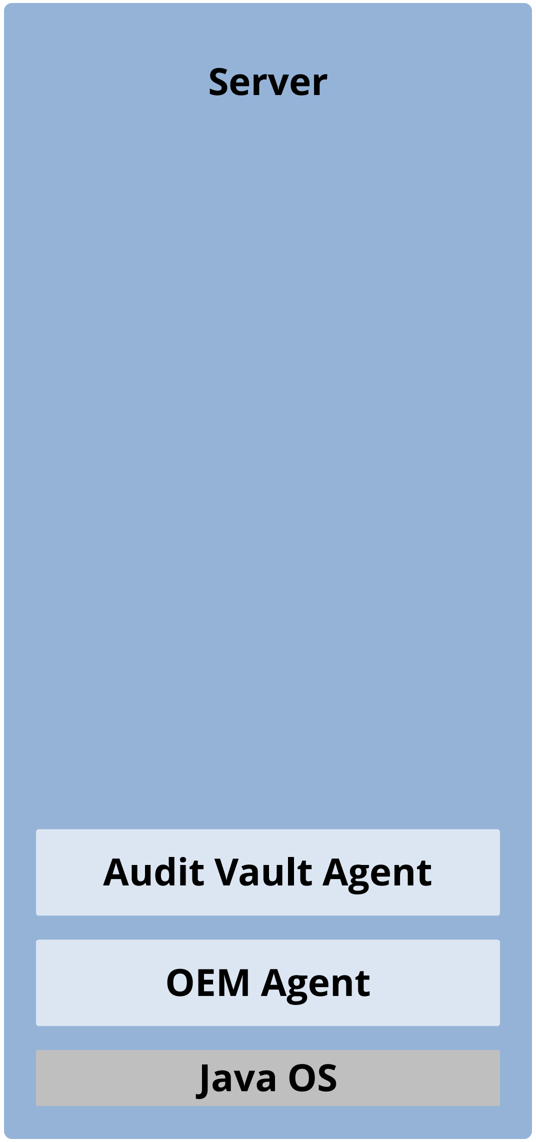
Oracle Home JDK

- Used only for administrative functions
- Oracle does not support upgrading this JDK – see MOS Note 1449674.1

OPatch JDK

- Used only by OPatch for patching
- OPatch JDK can be updated by updating OPatch to the latest version – always multiple version behind

Other JVMs



Server

Audit Vault Agent

OEM Agent

Java OS

Java OS JDK

- Installed by OS and not used by EBS
- Risk determined by how non-EBS applications or services use it

OEM Agent

- Used only for OEM Agent
- Must upgrade OEM then agents – JDK always multiple versions behind

Oracle Audit Vault Agent

- Used only by Audit Vault Agent
- Requires Oracle Audit Vault to upgraded and then agent upgraded – JDK always multiple versions behind

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**