



OPITZ CONSULTING

JAVA: COMPLIANCE UND SECURITY

03/2022

Webinarreihe 2022

Michael Paege
Klaus Kramer

Online, 29.03.2022



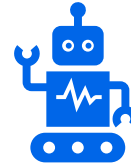
BITTE BEACHTEN SIE...



Alle Teilnehmer sind stummgeschaltet. Nur so können wir ein störungsfreies Webinar bei großer Personenzahl gewährleisten.



Wir werden Ihnen die Aufzeichnung dieses Webinars sowie die Vortragsfolien in den nächsten Tagen zusenden.



Bitte melden Sie sich bei technischen Störungen während des Webinars über die Frage-Funktion an die Organisatoren.



Ihre inhaltlichen Fragen stellen Sie bitte auch über die Frage-Funktion. Wir beantworten diese gerne zum Ende des Webinars.

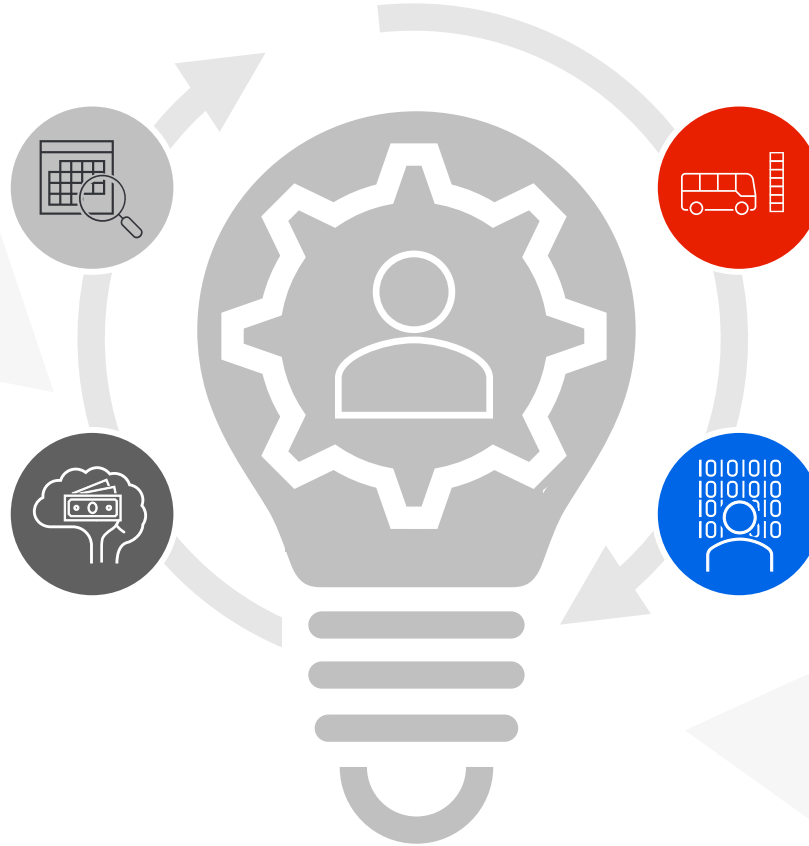
IT-MODERNISIERUNG

Strukturelle Zukunftsfähigkeit sichern

- Skalierbarkeit
- Flexibilität

Investitionsschutz

- Geistiges Eigentum
- Kosten
- Stabilität
- Akzeptanz



Vermeiden der Wartungsfall

- Legacy Technologien
- Sicherheit
- Fachkräftemangel

Grundlage der Digitalisierung

- Wettbewerbsfähigkeit
- Dynamikrobustheit
- Kundenerwartung

1

ALLGEMEINES ZU
(ORACLE) JAVA

2

COMPLIANCE UND
SECURITY

3

AKTUELLE SITUATION IM
MARKT

4

SECURITY-ASPEKTE

5

WAS TUN?

6

UNSER ANGEBOT

7

IHRE FRAGEN

8

LIVE-DEMO

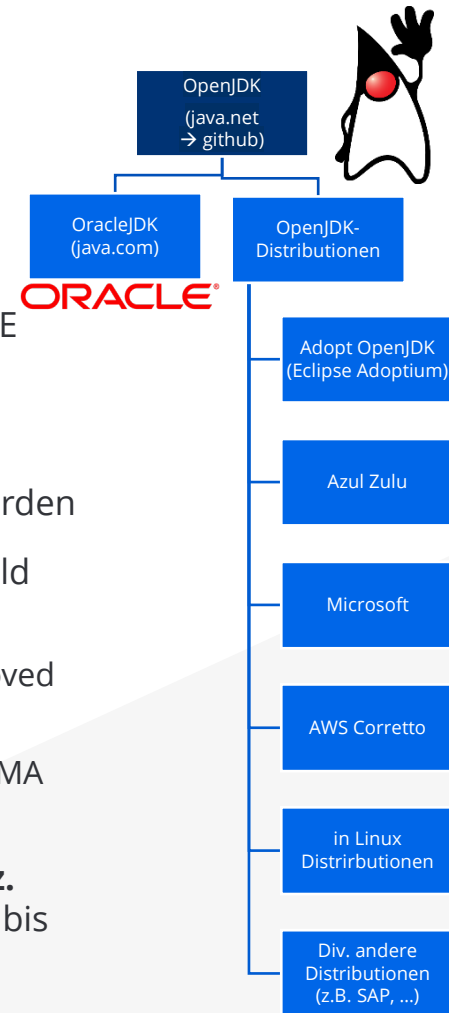
1

ALLGEMEINES ZU (ORACLE) JAVA

HISTORIE, GEGENWART UND ZUKUNFT



- 2006: Sun stellt Java unter Open Source: **GNU GPL**
- 2009: Oracle kauft Sun
- ab 2010: das OracleJDK wird mittels Oracle Binary Code License Agreement for Java SE (**BCL**) lizenziert
- ab 09.2018: Der JCP verkürzt die Release-Kadenz von 3 Jahren auf 6 Monate
- ab 09.2018: für Download des OracleJDK 11 muss **OTN-Lizenz für Java** akzeptiert werden
- ab 04.2019: **OTN-Lizenz für Java** wurde geändert und gilt nun für OracleJDK 8 ab Build 211 sowie für OracleJDK 11, 12, 13, ff
 - kostenfreie Nutzung des OracleJDK nur für Personal Use, Development Use, Oracle Approved Product Use und Oracle Cloud Infrastructure Use
 - Andere Nutzung des OracleJDK muss durch Subscription und Oracle Standardverträge (OMA oder TOMA plus LDR) lizenziert werden
- **NEU:** ab 09.2021: Ab OracleJDK**17** gilt für die LTS-Versionen die **Oracle No-Fee Lizenz**. Dies bedeutet kostenfreie Nutzung auch für kommerziellen Einsatz für den Zeitraum bis 1 Jahr nach Erscheinen der nächsten LTS-Version.
Release-Kadenz für LTS-Versionen wurde auf 2 Jahre verkürzt.



ORACLE JDK UND OTN-LIZENZ WAS IST DAMIT MÖGLICH ?

■ Personal Use

- “Personal Use” refers to an Individual's use of the Programs solely on a desktop or laptop computer under such Individual's control only to run Personal Applications.
- “Personal Applications” refers to Applications designed for individual personal use only, such as games or personal productivity tools

■ Development Use

- “Development Use” refers to Your internal use of the Programs to develop, test, prototype and demonstrate Your Applications. For purposes of clarity, the “to develop” grant includes using the Programs to run profilers, debuggers and Integrated Development Environments (IDE Tools) where the primary purpose of the IDE Tools is profiling, debugging and source code editing Applications

■ Oracle Approved Product Use

■ Oracle Cloud Infrastructure Use

ORACLE JDK UND OTN-LIZENZ WAS IST DAMIT MÖGLICH ?

■ Oracle Approved Product Use

- “Oracle Approved Product Use” refers to Your internal use of the Programs only to run: (a) the product(s) identified as Schedule A Products at <https://java.com/oaa>; and/or (b) software Applications developed using the products identified as Schedule B Products at java.com/oaa by an Oracle authorized licensee of such Schedule B Products. If You are unsure whether the Application You intend to run using the Programs is developed using a Schedule B Product, please contact your Application provider

■ Oracle Cloud Infrastructure Use

- “Oracle Cloud Infrastructure Use (“OCI Use”)” refers to Your use of the Programs on Oracle's Cloud Infrastructure with the Oracle Cloud Infrastruktur products identified in the Oracle PaaS and IaaS Universal Credits Service Descriptions available at <http://oracle.com/contracts> during the period in which You maintain a subscription for such Oracle Cloud Infrastructure products

WELCHE ORACLE-JAVA-VERSIONEN SIND KOSTENFREI ?

- OracleJDK 6 bis einschließlich Patchlevel 45 (April 2013)*
- OracleJDK 7 bis einschließlich Patchlevel 80 (April 2015)*
- OracleJDK 8 bis einschließlich Patchlevel 202 (Januar 2019)*
- Ab Oracle JDK11, 12, ... bis einschließlich Patchlevel 2*
(analog zum OpenJDK)
- Für OracleJDK >8.202 und 11-16 gilt:
 - Kostenfrei für personal Use, Development, Cloud Infrastructure Use und wenn ausschließlich in Verbindung mit einem supporteten Oracle-Produkt verwendet (bis auf wenige Ausnahmen wie bspw. SQL Developer)
- OracleJDK 17 bis einschließlich Patchlevel 6 (Oktober 2024)*

* kostenfrei, sofern keine kommerziellen Features verwendet werden (früher: z.B. MSI Installer, heute: z.B. GraalVM)

NO-FEE LIZENZ FÜR ORACLE JDK 17

- Gültig bis 1 Jahr nach Erscheinen der nächsten LTS Version, also Oktober 2024
- Kostenfreie Nutzung auch für produktive/kommerzielle Nutzung
- Updates und Patches

License Rights and Restrictions

Oracle grants to You, as a recipient of this Program, subject to the conditions stated herein, a nonexclusive, nontransferable, limited license to:

- (a) internally use the unmodified Programs for the purposes of developing, testing, prototyping and demonstrating your applications, and running the Program for Your own personal use or internal business operations; and
- (b) redistribute the unmodified Program and Program Documentation, under the terms of this License, provided that You do not charge Your licensees any fees associated with such distribution or use of the Program, including, without limitation, fees for products that include or are bundled with a copy of the Program or for services that involve the use of the distributed Program.

2

COMPLIANCE UND SECURITY

2 ASPEKTE: COMPLIANCE/KOSTEN UND SECURITY

Compliance

kostenpfl. Versionen ermitteln

Was tun?

Inventur

- Systeme sammeln
- höchste Java Versionen sammeln
 - kostenpfl. identif.
- Compliance Risiko bewerten

Optimierung

- Entscheidung für OpenJDK(s) treffen
- OpenJDK möglich?
 - Ja → migrieren
- nein → Cluster konsolidieren mögl?
 - Konsolidierung planen/umsetzen
- Anzahl Server- und Desktop-Subscriptions beschaffen

Security

„alte“ Versionen ermitteln

Was tun?

Inventur

- alle Java Versionen sammeln
 - Security-Risiko bewerten

Optimierung

- Entscheidung für OpenJDK(s) treffen
- OpenJDK möglich?
 - Ja → migrieren
- nein → Cluster konsolidieren mögl?
 - Konsolidierung planen/umsetzen
- Anzahl Server- und Desktop-Subscriptions beschaffen

3

AKTUELLE SITUATION IM MARKT

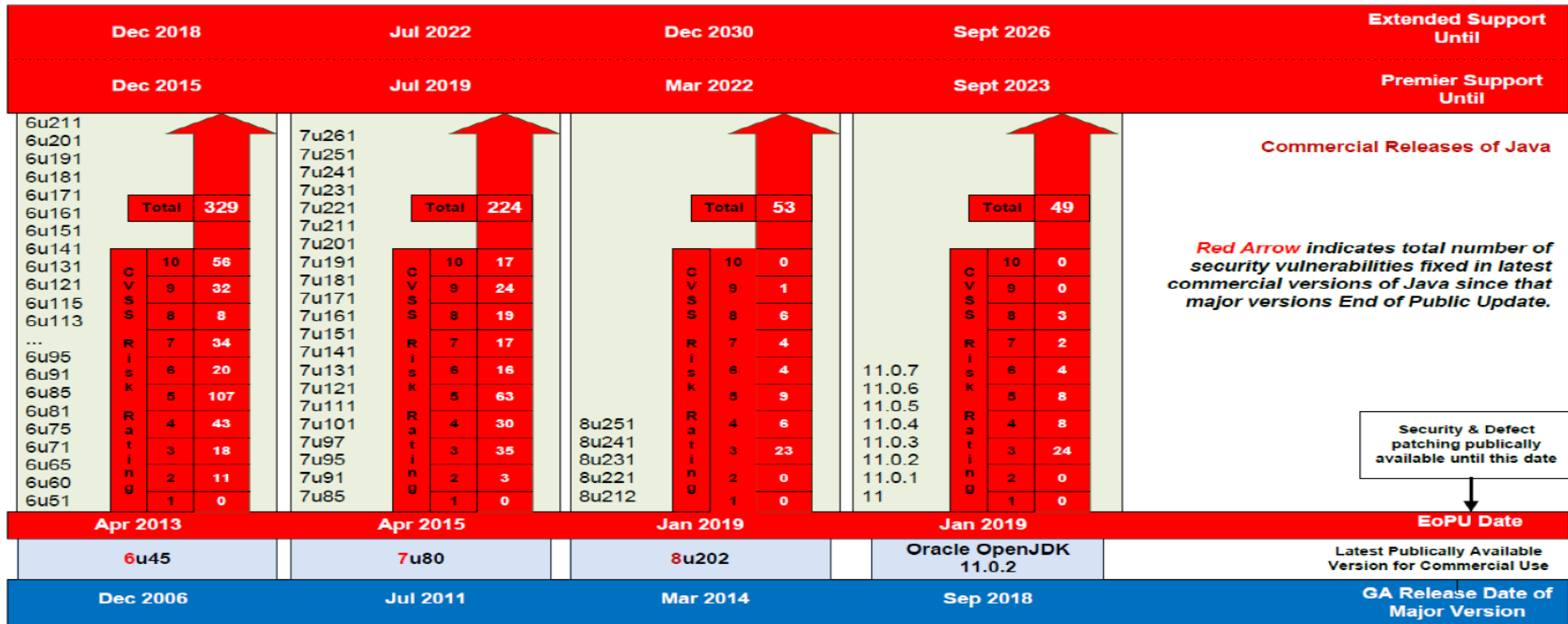
AKTUELLE SITUATION IM MARKT

- Viele Kunden haben vor 3 Jahren die Oracle-Java-Updates gestoppt um nicht bzgl. der kostenpflichtigen OracleJDK-Versionen incompliant zu werden bzw. um Kosten zu sparen
- Die dann eigentlich geplanten Migrationsvorhaben auf OpenJDK mussten anderen Prioritäten und Notwendigkeiten (Corona-Auswirkungen) weichen
- Viele Kundenworkshops haben gezeigt, dass auch noch viele noch ältere Versionen (Java4, Java5 etc.) im produktiven Einsatz sind
- Bei einigen Kunden sind noch Java-Applets im Einsatz ...
... und der Microsoft Internet Explorer geht am 15.06.2022 aus dem Support
(<https://blogs.windows.com/windowsexperience/2021/05/19/the-future-of-internet-explorer-on-windows-10-is-in-microsoft-edge/>)
- Wenige Kunden sind schon komplett auf OpenJDK
- Wenige Kunden zahlen Java-Subskription, weil sie – zumindest teilweise – nicht vom OracleJDK weg können oder wollen
- Neu ist nun die Option, weiter kostenfrei OracleJDK zu nutzen, wenn man auf OracleJDK17 upgradet

4

SECURITY-ASPEKTE

JAVA 8 OHNE UPDATES WEITER BETREIBEN JAVA OHNE SECURITYPATCHES ?



Quelle: Oracle

JAVA 8 OHNE UPDATES WEITER BETREIBEN JAVA OHNE SECURITY PATCHES ?

Oracle JDK 8 CVE's & Resolved Issues* Since End of Public Updates

Update	Date	CVSS Score 1-3	CVSS Score 4-6	CVSS Score 7-10	Total Security Patches	Resolved Issues
JDK 8u211	Apr 2019	0	1	4	5	142
JDK 8u221	Jul 2019	3	5	0	8	136
JDK 8u231	Oct 2019	11	7	0	18	121
JDK 8u241	Jan 2020	4	3	4	11	114
JDK 8u251	Apr 2020	5	3	3	11	161
JDK 8u261	Jul 2020	4	2	3	9	246
JDK 8u271	Oct 2020	6	1	0	7	199
JDK 8u281	Jan 2021	0	1	0	1	115
JDK 8u291	Apr 2021	0	2	0	2	108
Total		33	25	14	72	

* Resolved issues include bug fixes, enhancements and backports. Search results derived from the JDK Bug System at <https://bugs.openjdk.java.net>

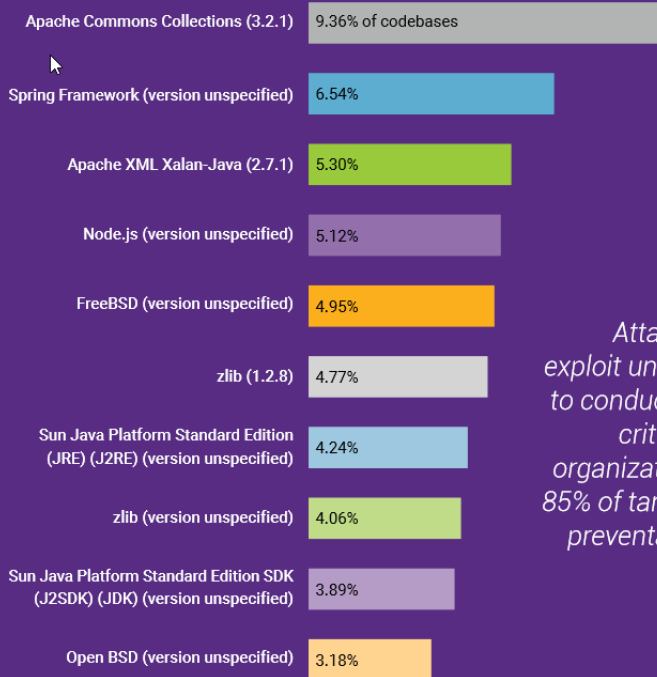
2 Copyright © 2021, Oracle and/or its affiliates. All rights reserved.



Quelle: Oracle

SICHERHEITSRISIKEN FÜR EIGENENTWICKLUNGEN

Top 10 high-risk components found



Attackers continue to exploit unpatched software to conduct attacks against critical infrastructure organizations. As many as 85% of targeted attacks are preventable, according to US-CERT.

- Mit Vorsicht zu genießen
- Aber:
 - Sicherheitsrisiken lauern überall
 - Java Abhängigkeiten (Apache Commons, Spring, XML, ...) sind ebenfalls prominent vertreten
 - ... wie adressieren Sie diese Abhängigkeiten?

JAVA SECURITY STORIES AUS DEM LEBEN

- Uralte BI Applikation verwendet heute noch Java Applets,
Java-Applets werden nur noch vom IE unterstützt,
Java-Applets gehören nicht mehr zum Feature-Umfang Java9 ff.
Der IE wird nach dem 15.06.2022 nicht mehr supportet
- Equifax hack
 - Apache Struts 2 vulnerability (CVE-2017-9805)
 - Großer Datenabfluss von Kundendaten
- Aus der Ferne Java-Code mit JSON ausführen
 - Exploiting the Jackson RCE: (CVE-2017-7525)
 - Bibliothek "Jackson Databinding" in vielen RESTful Service Stacks im Einsatz
- Log4j Risiko (Dez. 2021)

SICHERHEITSRISIKEN FÜR EIGENENTWICKLUNGEN MINIMIEREN

- Beachtung aus dem Standarddokument OWASP Top 10 Risiken für Webanwendungen
- <https://owasp.org/www-project-top-ten>
- OWASP Dokument sollten Sie sich zu eigen machen, um dafür zu sorgen, dass ihre Webanwendungen diese Risiken minimieren
 - Auszug TOP 10
 - Injection (SQL usw.)
 - Broken Authentication (Session Token)
 - Insecure Deserialization (Daten in XML- Dokumenten oder in JSON Dokumenten)

5

WAS TUN?

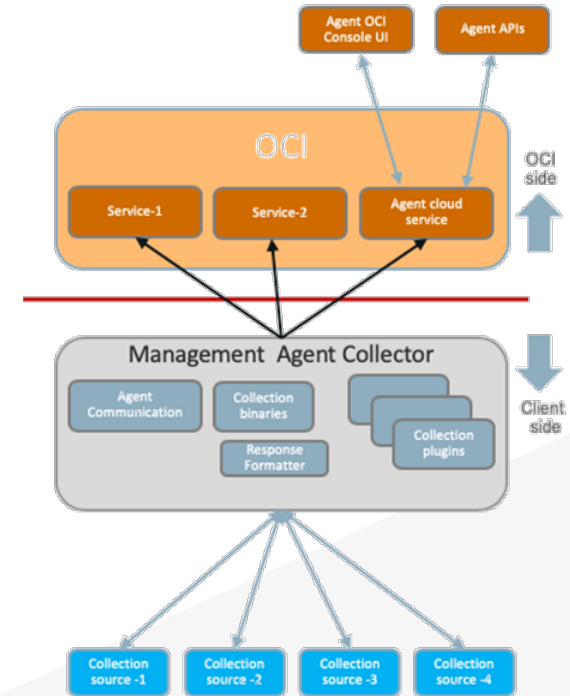
5.1 DETECTION

DETECTION – WO IST DENN ÜBERALL JAVA INSTALLIERT ?

- Professionelle Scanner (USU, Snow, Flexera, VisualVM, ...)
- Oracle Java Monitoring Services (Oracle JMS)
 - siehe nächste Folien
- Selbst entwickelte Scanner, die Registry, Prozesse, Umgebungsvariablen und ggf. Filesystem durchsuchen

GRUNDLAGEN / FUNKTIONALITÄT

- Teil von OCI (Oracle Cloud Infrastructure – Account notwendig)
 - Agent für jede Instance (Host)
 - Übertragung der Reports nach OCI
- Übersicht von Java-Anwendungen
 - Installation: Anbieter, Version – separat installiert oder Bestandteil von Drittanbieter-Software
 - Laufende Applikationen – Performance Monitoring
 - Bisher nur Linux-Unterstützung, nur Oracle JVMs (kein OpenJDK etc.*)
 - Basiert auf Java Usage Tracker, der weiterhin commercial Feature des OracleJDK bleibt
→ Java Subscription notwendig
- Vorteile von Cloud
 - Aufbereitung der Ergebnisse von Java Usage Tracker (Bestandteil seit Java 7, aber kostenpflichtig)
 - Kontinuierliche Überwachung/Rückmeldung



ANWENDUNGSSZENARIEN

■ Einmaliger Überblick über Java

- Sind alle Java-Installationen aktuell? Welche Applikationen laufen derzeit?
- Korrekte Lizenzierung wird nicht überprüft, Übersicht kann aber als Startpunkt helfen
- Laufen ggf. nicht autorisierte Anwendungen?

■ Kontinuierliche Überwachung

- Haben einzelne Anwendungen zeitweise Performance-Probleme z.B. zu wenig Rechnerkapazitäten?

LIZENZBESTIMMUNGEN VON JMS

- JMS Agent ist kostenlos
 - Voraussetzung für die Erhebung ist eine gültige Oracle Java Lizenz, z.B. Java SE Desktop
 - JMS basiert auf Java Usage Tracker
 - Java Usage Tracker ist enthalten in Oracle Java „SE Products“
- OCI Monitoring
 - Free tier – kostenlos zum Ausprobieren
 - bis 500 Mio. Datenpunkte zur Erhebung
 - bis 1 Milliarde Datenpunkte für Abfragen
 - OCI Preise
 - 0,0025\$ pro 1Mio Datenpunkte zur Erhebung
 - 0,0015\$ pro 1Mio Datenpunkte für Abfragen

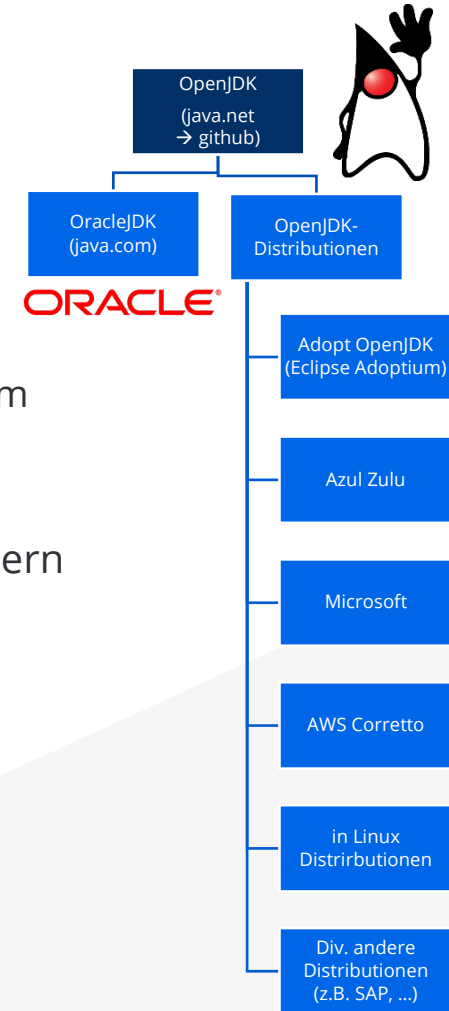
5.2 LÖSUNGEN ERARBEITEN

- Migration auf passende Open JDK Distribution
- Migration auf OracleJDK 17
- Oracle Java SE Subscription beziehen

OPEN JDK



- Open JDK ist die Grundlage von diversen Java Distributionen
- Kostenfreie OpenSource Angebote
 - AdoptOpenJDK (unterstützt durch IBM & Microsoft Azure) → Eclipse Adoptium
 - Amazon Corretto
 - Microsoft Java
- Kommerzielle Angebote in Linux Distributionen und von anderen Herstellern
 - RedHat (auch Java for Windows)
 - SUSE
 - SAP
- Kommerzielle Angebote
 - Oracle Java SE
 - Azul Zulu

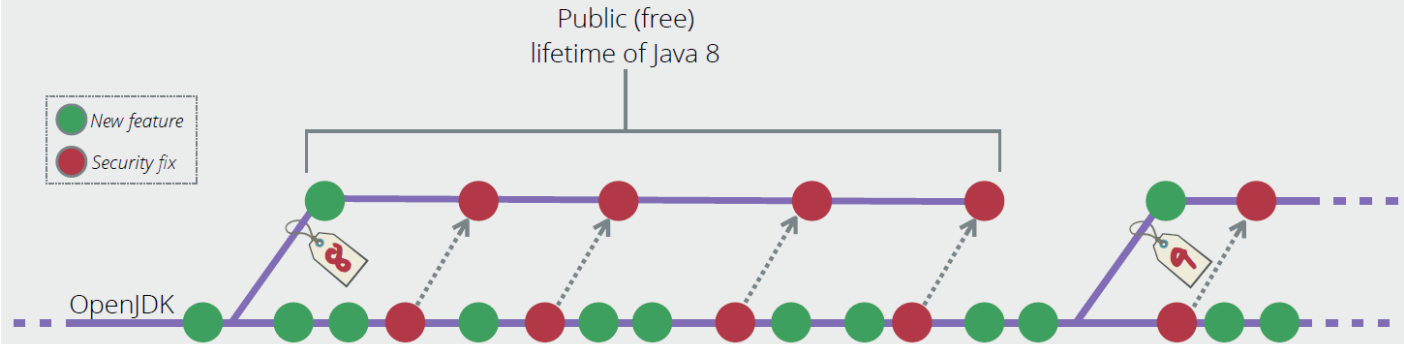


UNTERSCHIEDE ZW. OPENJDK AND ORACLE JDK

- Viele Projekte haben mit früheren Java-Versionen die Erfahrung gemacht,
 - dass OracleJDK stabiler war
 - und eine bessere Performance bot
 - oder ein größeres Feature Set hatte
- Oracle ist dabei, die technischen Unterschiede zwischen OpenJDK und OracleJDK auszugleichen
- Und Oracle hat die kommerziellen Features wie den Java Flight Recorder oder Mission Control ab Java 11 open source gestellt
- Anbieter stellen Kompatibilität über das TCK (Technical Compatibility Kit) sicher

OPENJDK: WORKFLOW DER DISTRIBUTOREN

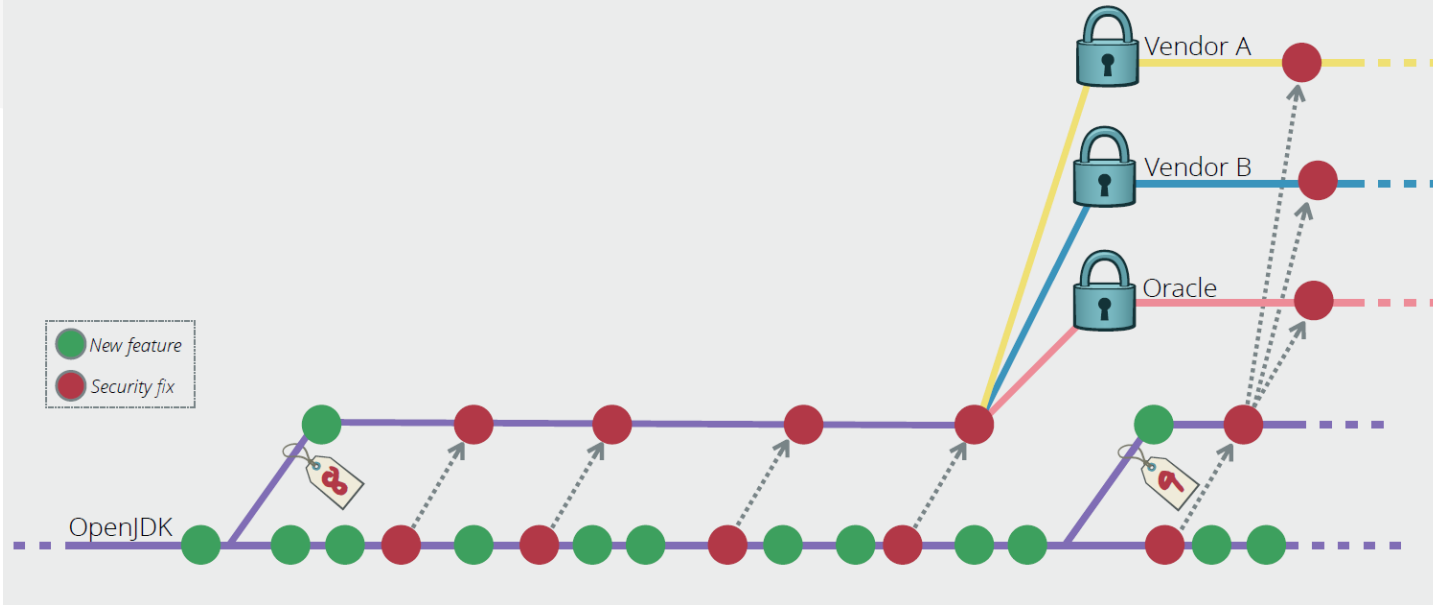
OpenJDK workflow



Quelle: Hendrik Ebbers: Java11 Keynote  @HendrikEbbers)

OPENJDK: WORKFLOW DER DISTRIBUTOREN

OpenJDK workflow



Quelle: Hendrik Ebbers: Java11 Keynote  @HendrikEbbers)

OPENJDK: AT THE END: SAME SAME BUT DIFFERENT

OpenJDK workflow

- All companies have the same workflow but the concrete versions will differ more and more
- Maybe security fixes can be handled in an open branch in future

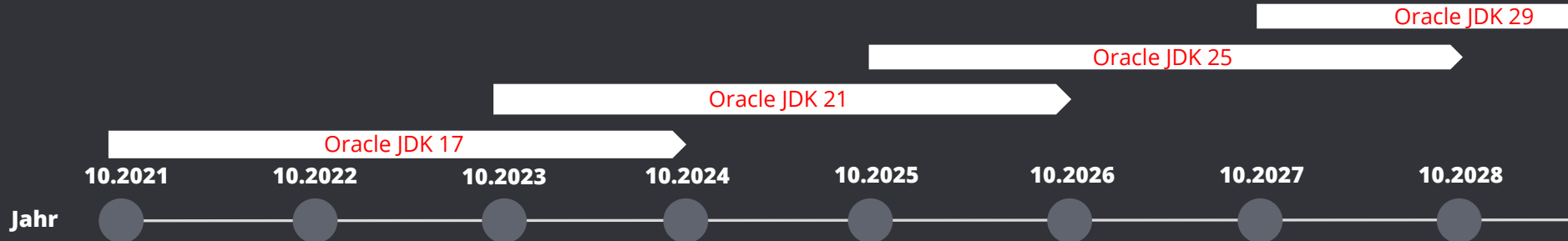


@HendrikEbbers

Quelle: Hendrik Ebbers: Java11 Keynote  @HendrikEbbers)

MIGRATION AUF ORACLE JDK 17

- No Fee Lizenz und Updates/Patches - auch für kommerziellen, produktiven Einsatz – bis Oktober 2024
- Danach dann Migration auf nächste LTS-Version (voraussichtlich Oracle JDK 21), die bis Oktober 2026 kostenfrei ist und unterstützt wird
- Abstrakt:
 - die jeweilige Oracle LTS Version ist kostenfrei und mit Updates/Patches versorgt für 3 Jahre
 - die aktuell geplante Release-Kadenz für OracleJDK mit LTS beträgt 2 Jahre



JAVA SE SUBSCRIPTION

- Beinhaltet Lizenz & Support
 - Lizenz auf OracleJDK & kommerzielle Tools (z.B. Flight Recorder, Mission Control, MSI Installer)
 - Sicherstellung des Supports (Patches, Updates, 24x7, MyOracleSupport) durch:
 - bisher: Lizenz & Support (bis 15.7.18) , läuft aus
 - Neu: (seit 15.7.18) Subskription, günstiger , einfacher zu lizenzieren
Kommerzieller Support für Java 8 gewährleistet die Verfügbarkeit von Patches für insgesamt 8 Jahre (5 Jahre Premier Support plus 3 Jahre Extended Support)
 - Bedeutet für Oracle JDK 8:
 - Premier Support bis Ende März 2022
 - Extended Support bis Ende März 2030

JAVA SE SUBSCRIPTION - PREISLISTE

Prices in Germany (Euro)

Java SE Platform Products

Java SE Desktop Subscription

Monthly
Subscription
Price

2,1330
1,7064
1,4931
1,2798
1,0665
0,8532

Java SE Subscription

21,3300
20,2635
19,1970
17,0640
14,9310
12,7980
10,6650
8,5320

Subscription
Metric

Volume

Pricing
Notes

Named User Plus	1-999	1,2
Named User Plus	1,000-2,999	1,2
Named User Plus	3,000-9,999	1,2
Named User Plus	10,000-19,999	1,2
Named User Plus	20,000-49,999	1,2
Named User Plus	50,000+	1,2

Processor	1-99	1,2
Processor	100-249	1,2
Processor	250-499	1,2
Processor	500-999	1,2
Processor	1,000-2,999	1,2
Processor	3,000-9,999	1,2
Processor	10,000-19,999	1,2
Processor	20,000+	1,2

6

UNSER ANGEBOT

JAVA – ZUKUNFTSPLANUNG UND –GESTALTUNG

Compliance

kostenpfl. Versionen ermitteln

Inventur

- Systeme sammeln
- höchste Java Versionen sammeln
 - kostenpfl. identif.
- Compliance Risiko bewerten

Was tun?

Optimierung

- Entscheidung für OpenJDK(s) treffen
- OpenJDK möglich?
- Ja → migrieren
- nein → Cluster konsolidieren mögl?
 - Konsolidierung planen/umsetzen
 - Anzahl Server- und Desktop-Subscriptions beschaffen

Security

„alte“ Versionen ermitteln

Inventur

- alle Java Versionen sammeln
 - Security-Risiko bewerten

Was tun?

Optimierung

- Entscheidung für OpenJDK treffen
- OpenJDK möglich?
- Ja → migrieren
- nein → Cluster konsolidieren mögl?
 - Konsolidierung planen/umsetzen
 - Anzahl Server- und Desktop-Subscriptions beschaffen

UNSER ANGEBOT FÜR SIE

Unser Angebot für Sie besteht aus drei Säulen.
Wir arbeiten eng mit Ihnen zusammen damit das beste Ergebnis erzielt werden kann!

Datenerfassung

- Sie sammeln die Daten mit dem Scanner-Tool ihrer Wahl
- Wir beraten Sie bei der zielgerichteten Erhebung der Daten
- Wir prüfen laufend die Qualität der entstehenden Daten

Kunde + 

Datenauswertung

- Wir werten die von Ihnen gesammelten Daten aus
 - Wir ermitteln die benötigten Lizenzen um die Oracle JDKs zu lizensieren
 - Wir berechnen die daraus resultierenden Kosten
 - Wir zeigen Security-Schwachstellen auf



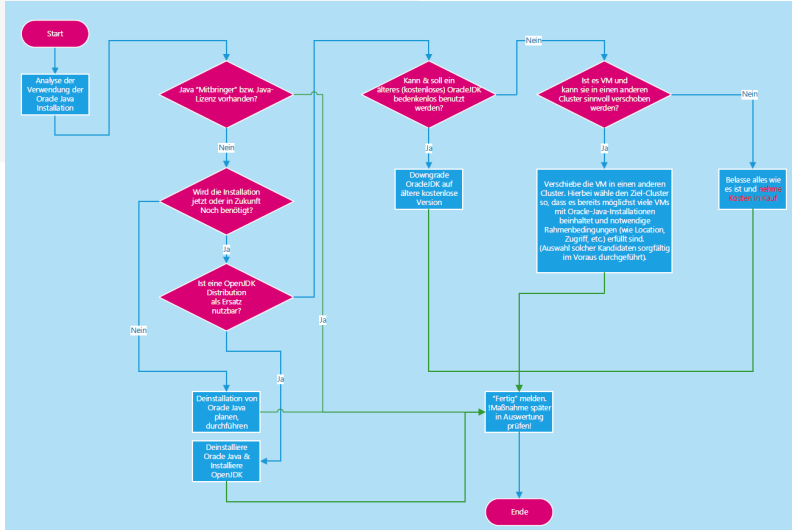
Handlungsstrategien entwickeln

- Gemeinsam prüfen wir, wie identifizierte Security-Schwachstellen geschlossen werden können
- Gemeinsam erarbeiten wir ein Konzept wie die Kosten bei einer Compliance gerechten Lizenzierung minimiert werden können

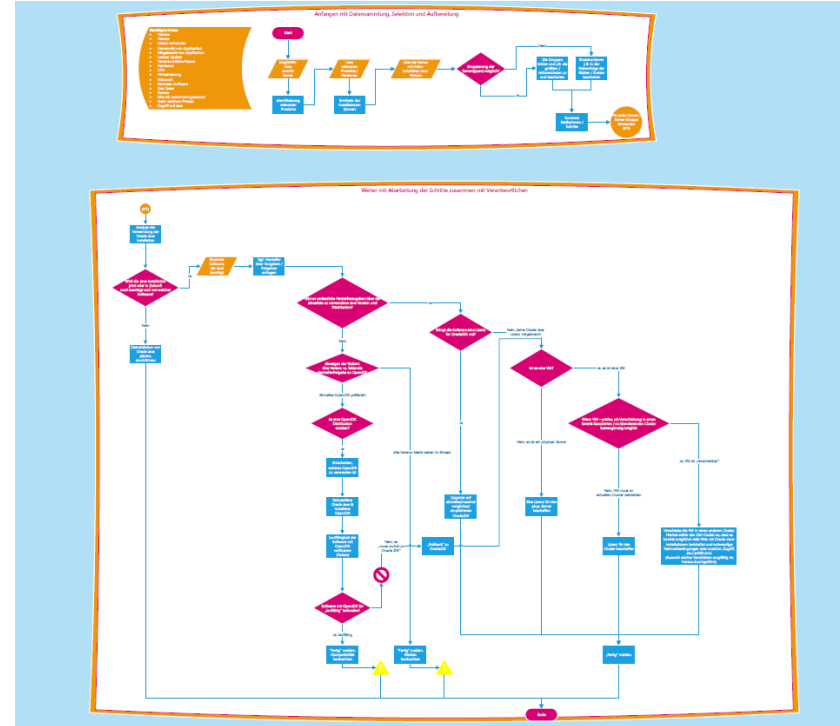
Kunde + 

VORGEFERTIGTE „DREHBÜCHER“/ABLAUFPLÄNE FÜR COMPLIANCE- UND SECURITY-BEARBEITUNG

■ Compliance / Kostenoptimierung



■ Security / Versionsupgrades



UNSER ANGEBOT FÜR SIE

Unser Angebot für Sie besteht aus drei Säulen
Wir arbeiten eng mit Ihnen zusammen damit das beste Ergebnis erzielt wird

Datenerfassung

- Sie sammeln die Daten mit dem Scanner-Tool Ihres Betriebes

Und natürlich unterstützen wir Sie auch gerne bei der **Umsetzung** der gewählten Strategie

- Migration der Anwendungen auf Open JDK
- Auch langfristige Wartung und Weiterentwicklung der Systeme (Managed Service)
- Ermittlung/Sizing der ggf. noch benötigter Subscription-Mengen

Identifizierung von security-schwachstellen auf

Wir arbeiten mit Ihnen zusammen wie wir ein Konzept wie die Kosten bei einer Compliance gerechten Lizenzierung minimiert werden können



Kunde +



7

IHRE FRAGEN

- vorab gestellte Fragen aus den Anmeldungen
- Im Webcast gestellte Fragen

DIE FRAGEN AUS DEN ANMELDUNGEN

- Oracle Java SE Desktop, Metriken
- Kostenlose Subscription bei Entwicklern? Wenn ja, wie ist das nachzuweisen bzw. anzuzeigen?
- Auditrecht durch Download? Rechtswirksamkeit dieser AGBs in der EU?
- Was hat sich ggf in den letzten 2 Jahren verändert?
- Ist eine User-Lizenzierung ausreichend oder muss zwingend der Server und der User lizenziert werden?

DIE FRAGEN AUS DEM CHAT

■ ...

KONTAKTDATEN



Michael Paege

Senior Manager Cloud & Compliance

OPITZ CONSULTING Deutschland GmbH
Standort Hamburg
Landwehr 2
22087 Hamburg
Tel.: +49 40 741122 1322
Mobil: +49 172 9461961
michael.paege@opitz-consulting.com

Klaus Kramer

Solution Architect

OPITZ CONSULTING Deutschland GmbH
Standort Essen
Lazarettstraße 15
22087 Hamburg
Tel.: +49 201 892994 1724
Mobil: +49 172 2048790
klaus.kramer@opitz-consulting.com