trivadis

O-DB-DOCKER

Lab and Exercise Guide

2019 October 07, Version 0.1

Trivadis AG
Sägereistrasse 29
8152 Glattbrugg

info@trivadis.com
+41 58 459 55 55

Table of Contents

1 Preface

1.1 Über TVD-CriticalPatchReport

Das Oracle Critical Patch Advisory wird alle drei Monate veröffentlicht und behebt Sicherheitsprobleme in Oracle-Datenbanken, Applikationsserver und anderen Oracle Produkten. In vielen Fällen ist es schwierig zu entscheiden, ob ein kritischer Patch sofort in einer Produktionsumgebung angewendet werden muss oder nicht. Hier kommt der Trivadis Critical Patch Report ins Spiel. Trivadis testet mehrere kritische Patches auf verschiedenen Oracle-Produkten und -Versionen. Insbesondere die kritischen Patch-Updates für die Oracle Datenbanken auf den Plattformen SUN, AIX, Linux und Windows sowie den Oracle Applikation Server, der unter Linux und Windows getestet wird. Die Testergebnisse werden im TVD-CriticalPatchReport zusammengefasst und im gleichen Zyklus freigegeben. Der Bericht hilft bei der Entscheidung, ob ein kritisches Patch-Update installiert werden muss oder nicht, ausserdem gibt er Ihnen wertvolle Tipps.

Ihre Vorteile

- Empfehlungen: Wann Sie den Patch installieren sollen - und wann nicht.
- Tipps, die Sie bei der Installation der CPU beachten sollten.
- Informationen darüber, ob sich die Datenbank nach der Installation der CPU anders verhält.

Der TVD-CriticalPatchReport wird im Rahmen des Managed Service Agreement an Trivadis Kunden verteilt oder kann alternativ als separater Service[1] erworben werden.

1.2 Copyright und Lizenz

Die Qualifikationen der Oracle Critical Patch Updates (CPU) basieren auf Oracle-Standardinstallationen. Die technischen Spezialisten von Trivadis führen die Tests und Bewertungen durch. Es kann jedoch nicht ausgeschlossen werden, dass Systeme in einer Kundenumgebung nach dem Anwenden bzw. Nichtanwenden der CPUs nicht wie erwartet funktionieren. Für Schäden, die durch die Verwendung bzw. Nichtverwendung von CPUs entstehen, übernimmt Trivadis keine Haftung.

Oracle und Java sind eingetragene Marken von Oracle und/oder seinen verbundenen Unternehmen. Andere Namen können Marken ihrer jeweiligen Eigentümer sein. Für die in diesem Bericht aufgeführten Oracle-Produkte gelten die Lizenzbedingungen von Oracle.

1.3 Dokumentinformation

- Document: Trivadis CPU-Report

[1] Trivadis Toolbox and TVD-CriticalPatchReport

- Classification: Restricted / Trivadis customer
- Status: Published
- Last changes: 2019.10.16
- Document name: Example_documentation.pdf

Hauptautoren	Mitwirkende & Reviewer
Stefan Oehrli	Patrick Joss

1.4 Revisionshistorie

Version	Datum	Visum	Bemerkung
0.1	2019.10.16	soe	Intial Release CPU Report July 2019
0.2	2019.07.20		Add Database check information
0.3 - 0.8			Complete revision of the CPU Report template
1.0			Finalize CPU Report July 2019

Bei Fragen stehen wir Ihnen gerne via cpureport@trivadis.com zur Verfügung.

2 Generelle Information

2.1 Datenbank Versionen

Mit dem neuen Release Zyklus hat Oracle eine neue Bezeichnung für die Critical Patch Updates eingeführt. Die Critical Patch Updates für Oracle 12.2.0.1 heissen Release-Updates, abgekürzt RU. Dementsprechend wurden unsere Tests angepasst. Bei Oracle 12c werden neu die Patch Set Updates respektive Release Updates, wo verfügbar, getestet. Aktuell gibt es nur Patch Set Updates für 12.1.0.2, respektive Release Updates für Oracle 12.2.0.1, 18.0.0.0 und 19.0.0.0. Für Oracle 11.2.0.4 gibt es seit Januar 2019 keinen regulären Critical Patch Update mehr. Der Premier Support endete per 1. Januar 2015. Per 31. Dezember 2018 ist auch der Extended Support Fee Waiver abgelaufen. Seit dem 1. Januar 2019 wird für diesen Release ein Extended Support Vertrag benötigt, um Patch sowie Critical Patch Update herunterladen zu können. Siehe auch My Oracle Support 742060.1 Note Release Schedule of Current Database Releases. Siehe auch in der My Oracle Support 742060.1 *Note Release Schedule of Current Database Releases*.

Neben einem PSU respektive RU für die Datenbank, gibt es für Oracle Java VM entsprechende Patches. Mehr dazu in der My Oracle Support Note 1929745.1 In der Note wird darauf hingewiesen, dass die Post Install Tasks im UPGRADE Mode ausgeführt werden sollten, wenn die JavaVM installiert ist.

Neben dem PSU, Oracle Java VM PSU gibt es zusätzlich quartalweise ein proaktiver Bundle Patch. Die

Bundle Patches sind ein Superset der PSU und enthalten neben den Security Fixes weiter Bugfixes. Mehr dazu in der My Oracle Support Note 1998563.1 und 1962125.1. Mit der Installation des Combo Patch, welcher den PSU, JVM PSU und BP enthält, ist das Datenbank System jeweils auf dem aktuellsten Patchlevel.

Seit November 2015 hat Oracle für die Versionsbezeichnung der neuen Bundle Patches, Patch Set Updates und Security Patches ein neues Format eingeführt. Neu wird statt der 5. Stelle das Release Datum in der Form YYMMDD angehängt:

- YY letzte zwei Ziffern vom Jahr
- MM Monat (2 Ziffern)
- DD Tag im Monat (2 Ziffern)

2.2 Weblogic Server

Bis zur Weblogic Version 12.1.1 wurden die Patches jeweils mit BEA Smart Update (BSU) eingespielt. Ab Version 12.1.2 wird Smart Update durch das im Datenbankumfeld bekannte OPatch abgelöst. Ein Patchen mit BSU ist ab dieser Version nicht mehr möglich.

3 Trivadis Empfehlung

3.1 Oracle Datenbank

Das höchste Base Ranking im Rahmen des Common Vulnerability Scoring System (CVSS) im Bereich der reinen Datenbank liegt beim vorliegenden CPU bei 9.8 von 10 und betrifft die Core RDBMS Komponente in 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c und 19c auf allen Betriebssystemen. Zudem kann diese Sicherheitslücke remote über das Netzwerk ausgenutzt werden.

Mit 9 Korrekturen für Sicherheitslücken beim Oracle Database Server ist dies ein etwas grösserer CPU. Die Sicherheitslücken können teilweise remote über das Netzwerk ausgenutzt werden.

Der CPU konnte auf allen unseren Testumgebungen mit kleineren Issues installiert werden. Aufgrund des sehr hohen CVSS Rating für Core RDBMS wird empfohlen das Critical Patch Update auf allen entsprechenden Systemen einzuspielen. Bei allen Systemen ist es ebenfalls sinnvoll, das Critical Patch Update einzuspielen, speziell wenn das letzte Critical Patch Update übersprungen wurde. Die My Oracle Support Note 1929745.1 enthält weitere Informationen zu den speziellen Oracle Java VM Patches.

Dieser Patch ist einzuspielen, wenn:

- Nur der Oracle Client installiert ist.

Sicherheitslücken sind ausnutzbar, wenn folgende Optionen installiert oder benutzt werden:

- Oracle 11.2 Core RDBMS, Java VM, Oracle Text
- Oracle 12.1 Core RDBMS, Java VM, Oracle Text
- Oracle 12.2 Core RDBMS, Java VM, Oracle Text, Spatial

- Oracle 18 Core RDBMS, Java VM, Oracle Text, Spatial
- Oracle 19 Core RDBMS, Java VM

3.2 Oracle Fusion Middleware

Das höchste Ranking im Rahmen des Common Vulnerability Scoring System (CVSS) liegt bei 9.8 von maximal 10.0 Punkten. Mit 9.8 Punkten sind Komponenten wie Oracle Security Service, Oracle SOA Suite, Oracle WebCenter Site und der Weblogic Server selbst betroffen. Alle Sicherheitslücken mit einem Score von 9 sind remote ohne Authentifizierung ausnutzbar. Weitere Details sind in der Support Note 2534806.1 Critical Patch Update (CPU) Program July 2019 Patch Availability Document (PAD) dokumentiert.

Da der Grossteil der Lücken ohne Authentifizierung und remote ausgenutzt werden können, wird das Einspielen des Juli 2019 Patches empfohlen.

Für den Oracle WebLogic Server werden in diesem Critical Patch Update diverse Sicherheitslücken mit einem Base Score von 9.8 und diverse mit tieferem Score behoben. Daher wird empfohlen, dieses Critical Patch Update einzuspielen.

Ab CPU Oktober 2017 empfiehlt Oracle in der Readme die Verwendung und/oder Upgrade des JDK, welches dem WebLogic Servers zugrunde liegt, je nach WebLogic Server Release auf folgende Versionen:

- Java SE Development Kit 8, Update 221 (JDK 8u221)
- Java SE Development Kit 7, Update 231 (JDK 7u231)
- Java SE Development Kit 6 ist End of Life

CVE #	Base Score	Affected WebLogic Server Release
CVE-2019-2856	9.8	12.2.1.3
CVE-2018-15756	7.5	10.3.6, 12.1.3.0,12.2.1.3
CVE-2016-7103	6.1	10.3.6, 12.1.3.0, 12.2.1.3
CVE-2019-2824	5.5	10.3.6, 12.1.3.0, 12.2.1.3
CVE-2019-2827	5.5	10.3.6, 12.1.3.0, 12.2.1.3

3.3 Oracle Enterprise Manager Base Platform

Für Oracle Enterprise Manager Cloud Control wird empfohlen auf die neuste Version von Oracle Enterprise Manager Cloud Control 13c Release 3 zu wechseln.

- Base Platform OMS home PSU 29433931
- Die von der Enterprise Manager Base Platform benutzte Datenbank und der Applikationsserver muss wie eine normale Datenbank respektive Applikationsserver betrachtet werden. Wir empfehlen deshalb das Einspielen des CPUs.

3.4 Oracle Audit Vault and Database Firewall

Die Patch Set Updates respektive Bundle Patches for Oracle Audit Vault and Database Firewall werden üblicherweise mit einer Verzögerung veröffentlicht. Der aktuell letzte Patch für AVDF ist 29030059. In der My Oracle Support Note 1328209.1 werden jeweils die aktuellsten Bundle Patch für AVDF 12 Release 1 und 12 Release 2 ausgewiesen.

- New Oracle Audit Vault and Database Firewall
- Oracle Technology Network Oracle Audit Vault and Database Firewall
- Oracle Audit Vault and Database Firewall 12.1 and Database Firewall 5.x bundled patch reference 1328209.1
- Oracle Technology Network What's New in Oracle Audit Vault and Database Firewall Release 12.2

4 Workshop

Im Rahmen des Workshop besteht die Gelegenheit verschiedene Themen am praktischen Beispiel zu vertiefen. Dazu gibt es zu jedem Kaptiel Aufgaben, welche nach Anleitung oder individuell auf einer Testumgebung umgesetzt werden können. Die Testumgebung besteht, wie man in der folgenden Abbildung sehen kann, jeweils aus drei virtuellen Systemen. Pro zweier Team steht jeweils eine entsprechende Testumgebung zur Verfügung.

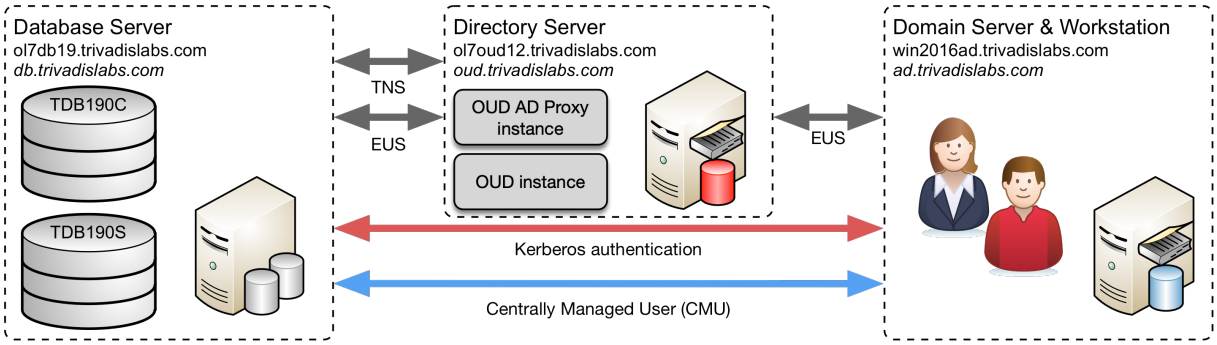

Abb. 2: Architektur Schulungsumgebung

4.1 Übung 01: Titel der Übung

4.1.1 Übungsziel

Etwas lernen...

4.1.2 Aufgabe

- Erstellen HTTP Servers für das Software Repository basierend auf dem Images `busybox`.
- Erstellen einer `docker-compose` Datei für das automatische starten des HTTP Servers.
- Einbinden der Software via Volume.

- Sicherstellen des Zugriffs auf das HTTP Server.

Zusatzaufgabe und weitere Überlegungen:

- Wieso wird gerade `busybox` als basis für diesen HTTP Server verwendet?
- Welche weiteren Basis-Images lassen sich ebenfalls verwenden?
- Wozu dient diese Software Repository?
- Was für Alternative zum Download der Software beim Build der Docker Images gibt es?

Vorsausetzungen: Für diese Übung müssen die folgenden Anforderungen erfüllt sein:

- Sicherstellen des Zugriffs auf die Docker Übungs- und Entwicklungsumgebung

4.2 Lösung 01: Titel der Übung

Für diese Übung werden folgende Punkte umgesetzt:

- Interaktives starten eines Docker Containers mit `docker run`
- Erstellen einer `docker-compose` Datei.

4.2.1 Detaillierte Lösungsschritte

Es muss folgendes gemacht werden

- Sicherstellen des Zugriffs auf die Docker Übungs- und Entwicklungsumgebung

4.3 Übung 02: Titel der Übung

4.3.1 Übungsziel

Etwas lernen...

4.3.2 Aufgabe

- Erstellen HTTP Servers für das Software Repository basierend auf dem Images `busybox`.
- Erstellen einer `docker-compose` Datei für das automatische starten des HTTP Servers.
- Einbinden der Software via Volume.
- Sicherstellen des Zugriffs auf das HTTP Server.

Zusatzaufgabe und weitere Überlegungen:

- Wieso wird gerade `busybox` als basis für diesen HTTP Server verwendet?
- Welche weiteren Basis-Images lassen sich ebenfalls verwenden?
- Wozu dient diese Software Repository?
- Was für Alternative zum Download der Software beim Build der Docker Images gibt es?

Vorsausetzungen: Für diese Übung müssen die folgenden Anforderungen erfüllt sein:

- Sicherstellen des Zugriffs auf die Docker Übungs- und Entwicklungsumgebung

4.4 Lösung 02: Titel der Übung

Für diese Übung werden folgende Punkte umgesetzt:

- Interaktives starten eines Docker Containers mit `docker run`
- Erstellen einer `docker-compose` Datei.

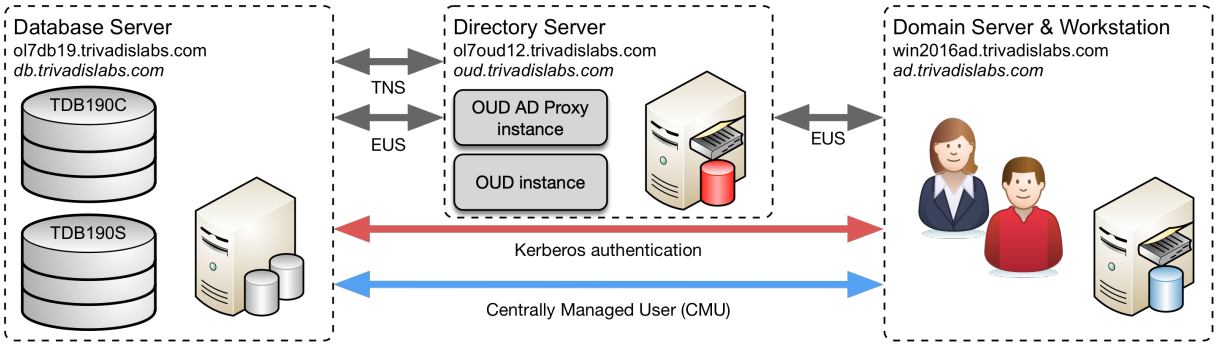

Figure 1: "LAB Environment"

4.4.1 Detaillierte Lösungsschritte

Es muss folgendes gemacht werden

- Sicherstellen des Zugriffs auf die Docker Übungs- und Entwicklungsumgebung

5 Anhang B: Quellen

Die folgenden Verweise sind im Zusammenhang mit dem Trivadis CPU Report nützlich und haben bei der Erstellung dieses Berichts geholfen.

Allgemeine Informationen zur Oracle Critical Patch Advisory:

- Oracle Recommended Patches Oracle JavaVM Component Database PSU (OJVM PSU) Patches (1929745.1)
- Patch Set Updates Known Issues Notes (1227443.1)
- Database Security Patching from 12.1.0.1 onwards (1581950.1)
- Quick Reference to Patch Numbers for Database PSU, SPU(CPU), Bundle Patches and Patchsets (1454618.1)
- Risk Matrix Glossary – terms and definitions for Critical Patch Update risk matrices (394486.1)
- Use of Common Vulnerability Scoring System (CVSS) by Oracle (394487.1)
- Release Schedule of Current Database Releases (742060.1)

Informationen über das aktuelle Critical Patch Update:

- Official Oracle web site for this patch Oracle Critical Patch Update Advisory - October 2019
- Text Form of Oracle Critical Patch Update - October 2019 Risk Matrices
- Oracle Critical Patch Update October 2019 Documentation Map - MOS Note 2566013.1
- Critical Patch Update (CPU) Program Oct 2019 Patch Availability Document (PAD) 2568292.1
- Oracle Database / Grid Infrastructure / OJVM Release Update & Release Update Revision 12.2.0.1 Jul 2018 Known Issues - MOS Note 2359048.1
- Known Issues for Oracle WebLogic Server (OWLS) 12.1.3.0.X Patch Set Updates - MOS Note 2137518.1
- Known Issues for Oracle WebLogic Server (OWLS) 12.2.1.3.X Patch Set Updates - MOS Note 2350415.1
- 12.1.0.2 Patch Set - Availability and Known Issues - MOS Note 1683799.1
- 12.2.0.1 Base Release - Availability and Known Issues - MOS Note 2239820.1
- 18.0.0.0 Base Release - Availability and Known Issues - MOS Note 2387295.1

Datenbanksicherheitsstandards und Best Practice:

- CIS Oracle Database Benchmarks - https://www.cisecurity.org/benchmark/oracle_database/
- STIGs Document Library - Database STIG
- Common Vulnerability Scoring System CVSS

6 Appendix A: Glossary

- API – Application programming interface
- BSU - BEA Smart Update ist ein Dienstprogramm, um Patches auf WebLogic Server einzuspielen
- CA – Certificate Authority
- CLI – Command Line Interface
- CPU - Critical Patch Update
- CVSS - Common Vulnerability Scoring System CVSS
- EUS - Oracle Enterprise User Security
- IAM - Identity and Access Management
- LDAP – Lightweight Directory Access Protocol
- OUD - Oracle Unified Directory
- PSU - Patch Set Update
- RBAC – Role-Based Access Control
- RDP – Remote Desktop Protocol
- RU - Release Update
- SPU - Security Patch Update
- SSH – Secure Shell
- SSL – Secure Sockets Layer
- SSO – Single Sign-On
- TLS – Transport Layer Security, the successor to Secure Sockets Layer (SSL)