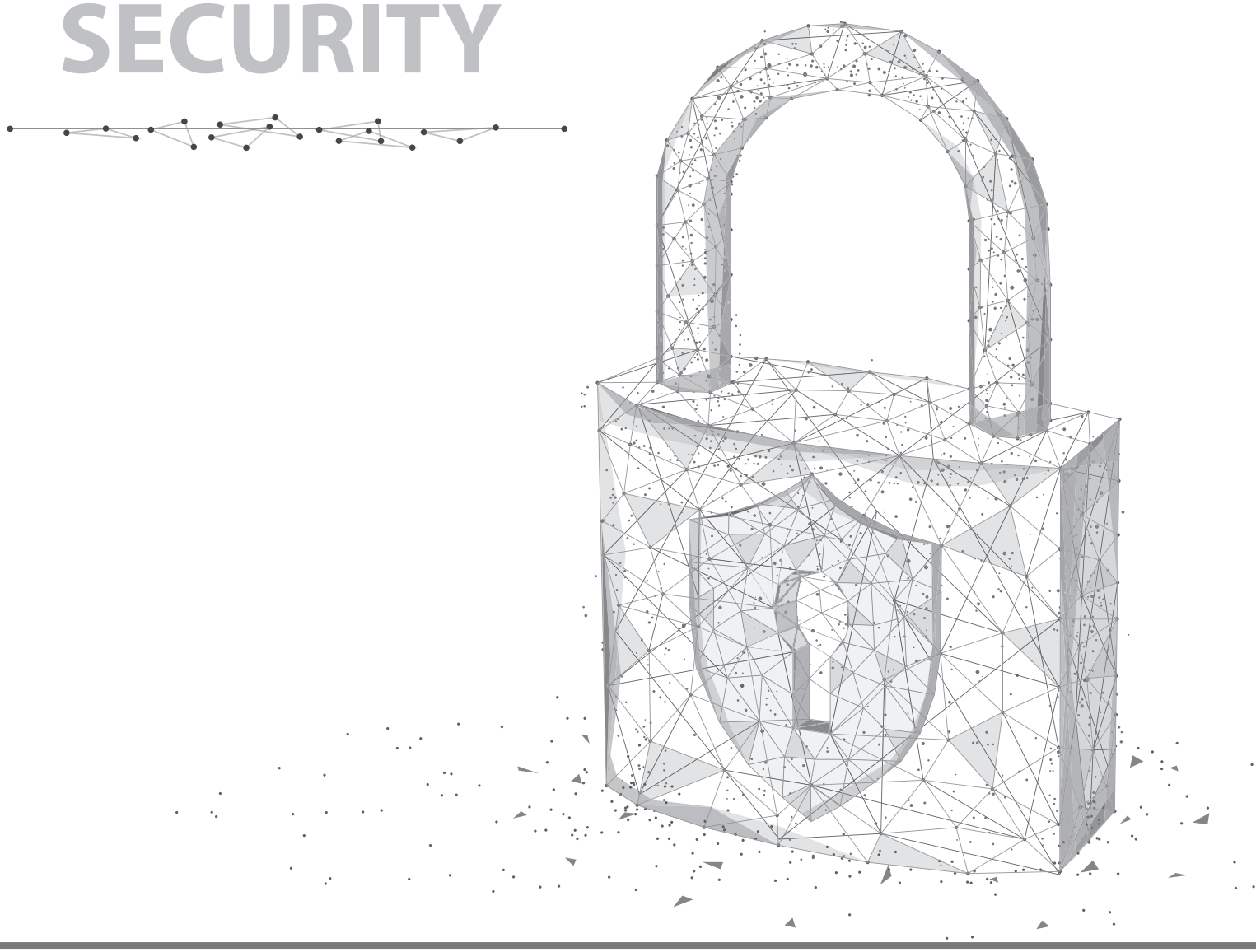
Nr. 4 | September 2021 | ISSN 2366-7915 | www.doag.org

Red Stack Magazin

DOAG SOUG swiss oracle user group AOUG AUSTRIAN ORACLE USER GROUP

inklusive BUSINESS NEWS

SECURITY



Aus der Praxis

Datenbankhärtung mit DBSAT

Im Interview

Sebastian Schreiber, Geschäftsführer SySS GmbH

Business News

Digital Twins: Von der Digitalisierung der realen in die virtuelle Welt

Bruno Cirone
Themenverantwortlicher Security

Ausgabe Nr. 4/2021
auf Abruf!

Liebe Mitglieder, liebe Leserinnen und Leser,

eine der Fragen, die mir am häufigsten im Zusammenhang mit Security-Themen gestellt wird, lautet: „Wie teuer ist Security?". Diese Frage kann nicht pauschal mit einem Betrag beantwortet werden. Natürlich kostet „Security" mehr Personal, Zeit, Geld und vieles mehr.

Bei der Beantwortung dieser Frage versuche ich herauszuarbeiten, welchen Wert diese Daten für das Unternehmen haben. Der Schaden, der durch mangelhafte „Security" entsteht, ist bestimmt nur ein Bruchteil dessen, was „Security" kostet.

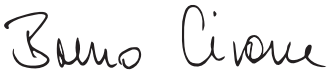
Aus meiner Sicht ist die wichtigste Security-Maßnahme, die auch Zeit und damit Geld kostet, eine ständige Weiterbildung und ein stetiger Wissensaustausch.

Neuere Themen wie etwa „Digital Twins" sind für uns bald selbstverständlich. Hierbei werden reale mit digitalen Produkten verbunden. Es ist eine gewaltige Herausforderung für Mitarbeiter, Datenbanken und Ihre „Security".

Die DOAG und die vielen Artikel in dieser Ausgabe sollen Ihnen helfen, diese Ziele zu erreichen.

Ich wünsche Ihnen viel Spaß beim Lesen.

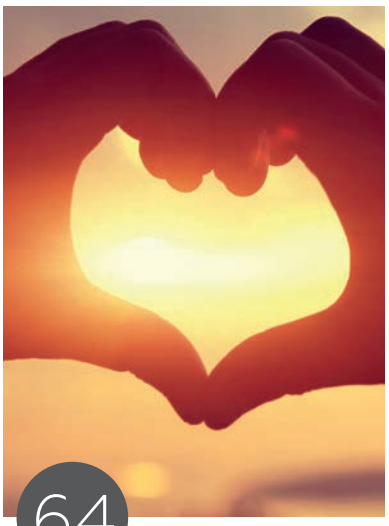
Bruno Cirone



Einleitung

Security

Enterprise Grade High Availability mit Patroni

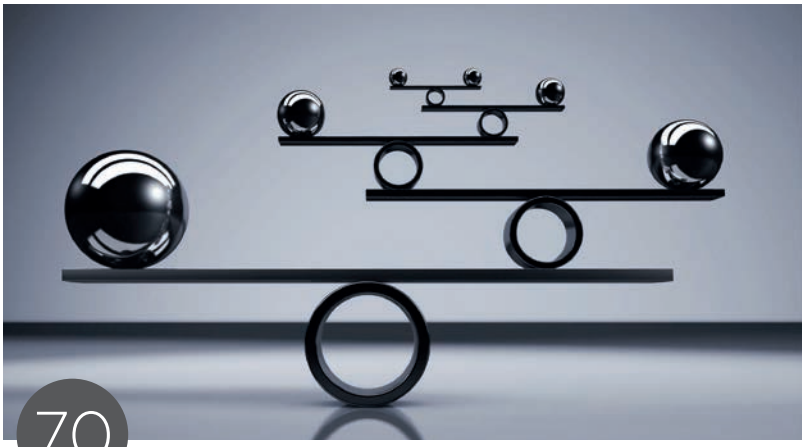


Lockdown oder: Wie ich lernte die Cloud zu lieben – Teil 2

Datenbank

Cloud

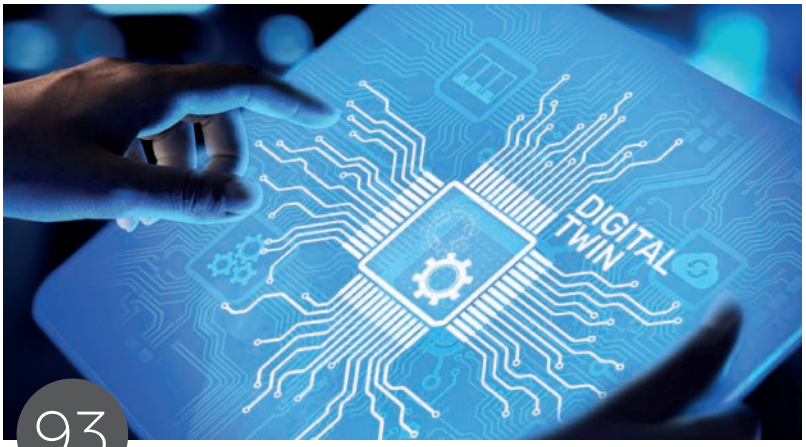
SQL



70

Mythen über SQL-Performance

Digital Twins: Von der Digitalisierung der realen in die virtuelle Welt



93

Vom Organizational Twin zur Single Source of Truth

News

Intern

TIMELINE

29. JUNI 2021

In der DOAG BSC WebSession zu NetSuite mit dem Referenten Peter von Zimmermann geht es um die Umsatzsteuerreform zum 1.7.2021 und das OSS-Verfahren und deren Abbildung in NetSuite. In einem Open Panel wird mit neuen Mitgliedern und anderen Interessierten anschließend offen über Fragen im Zusammenhang mit NetSuite in Deutschland diskutiert.

01. JULI 2021

In einer weiteren Ausgabe der „DOAG Dev Talk"-Reihe heißt das Thema diesmal „Codegeneratoren: Sinnvoll oder Unsinn?" Kai Donato und Moritz Klein referieren unter der Moderation von Niels de Bruijn.

09. JULI 2021

In der DOAG DB WebSession referiert Marco Mischke über das Thema „Datenbankhärtung mit der Standard Edition 2" und stellt die Verschlüsselung auf verschiedenen Ebenen und mehrere Härtungs-Möglichkeiten vor.

13. JULI 2021

Im Berliner Expertenseminar „Erfolgreiche Entwicklung von Oracle Data Warehouses" zeigt Dani Schnider, wie man mit den aktuellen Oracle-Versionen moderne DWH-Systeme entwickeln und betreiben kann.

15. JULI 2021

In einem weiteren DOAG Dev Talk mit den Referenten Christian Schwitalla, Ulrike Schwinn und Jürgen Sieben steht die Frage „Braucht man heutzutage noch SQL?" auf der Agenda.

21. JULI 2021

In der DOAG DAC WebSession widmen sich Germans Hirsch und Oliver Fuhrmann in einer ersten Session dem Thema „Intelligente Prozessanalyse mit KI".

29. JULI 2021

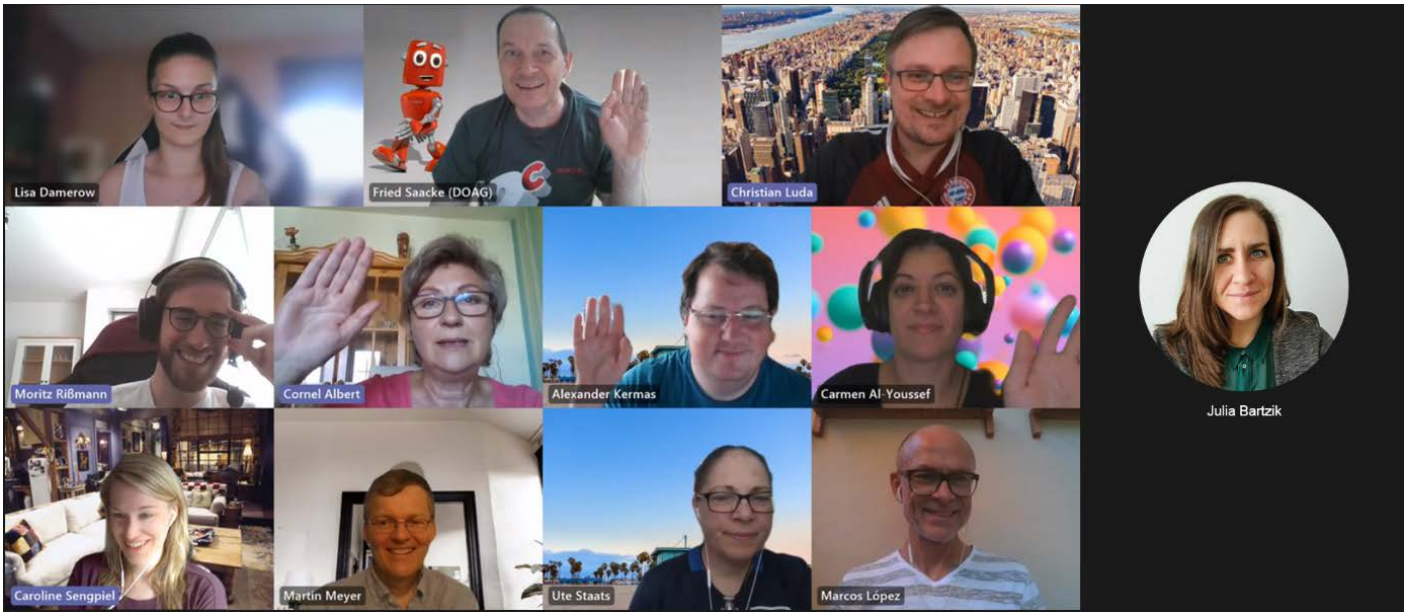
Im heutigen DOAG Dev Talk der Development Community (DEVC) wird das Thema „Barrierefreiheit" diskutiert. Es referieren diesmal Maximilian Liesegang und Anja Hildebrandt.

12. AUGUST 2021

Das spannende Thema „1 Jahr Home-Office" wird in einem DOAG Dev Talk mit den Referenten Carolin Hagemann & Sven Bernhardt unter der Moderation von Christian Schwitalla besprochen.

18. AUGUST 2021

Die Fortsetzung der DOAG DAC WebSession „Intelligente Prozessanalyse mit KI II" mit Referent Jens Horstmann von Trevisto steht auf dem Programm.



Die DOAG-Geschäfsstelle im Home-Office

26. AUGUST 2021

Der DOAG Dev Talk mit den Referenten Christian Schwitalla & Arne Hattendorf widmet sich diesmal dem Thema „Wieviel Datenschutz geht?“ Es moderiert Tobias Schweiker.

01. UND 02. SEPTEMBER 2021

Im Berliner Expertenseminar mit Moritz Klein und Markus Dötsch wird den Teilnehmern verdeutlicht, welche Schritte einzuleiten sind, um die Qualität, Wartbarkeit und Erweiterungsfähigkeiten in APEX-Projekten zu gewährleisten. Als Gast berichtet Carsten Czarski aus dem Oracle APEX Development Team über Neues aus dem Entwickler-Labor und Neuheiten zu APEX 21.1.

07. UND 08. SEPTEMBER 2021

Im Berliner Expertenseminar führt Christian Pfundtner die Teilnehmer in das Thema Oracle Data Guard ein und behandelt dabei dessen Architektur, Konfiguration und praktischen Einsatz.

09. SEPTEMBER 2021

Im DOAG Dev Talk mit Tobias Schweiker und Niels de Bruijn geht es diesmal um das Thema Requirements Engineering für SW-Entwicklung.

10. SEPTEMBER 2021

Die DOAG DB WebSession mit Ernst Leber behandelt das Thema "Autoupgrade kann nix dafür".

15. SEPTEMBER 2021

Die DOAG DAC WebSession zum Thema Data Catalog steht auf dem Programm.

16. BIS 18. SEPTEMBER 2021

Alle Delegierten und Gäste sind eingeladen zur Ordentlichen Delegiertenversammlung der DOAG einschließlich des Leitungskräfteforums vom 16. bis 17. September 2021 in Bonn.

Ein wichtiges Thema ist die Festlegung der Strategie, wie, wann und mit welchen Themen Präsenzveranstaltungen ab Herbst oder ab 2022 wieder geplant werden können. Des Weiteren wird der Vorstand neu gewählt.

16. UND 17. SEPTEMBER 2021

Im Berliner Expertenseminar behandeln Sven Bernhardt und Guido Schmutz das Thema Cloud-native als einer verteilten, leichtgewichtigen Applikationsarchitektur und vermitteln den Teilnehmern Kernprinzipien der Microserviceentwicklung.

23. SEPTEMBER 2021

Im DOAG Dev Talk der Development Community diskutieren die Teilnehmer mit Jan-Peter Timmermann und Carolin Hagemann unter der Moderation von Tobias Schweiker über Forms & APEX.

„Perfekte Sicherheit bekommen wir nicht hin, das ist viel zu aufwendig und nicht realistisch."

Martin Meyer, Redaktionsleiter des Red Stack Magazin, sprach mit Sebastian Schreiber, Gründer und Geschäftsführer der SySS GmbH in Tübingen, zum Thema IT-Security.

Womit beschäftigen Sie sich in Ihrem Unternehmen?

Die SySS GmbH führt simulierte Cyber-Attacken durch. Das bedeutet, dass wir Penetrationstests machen und die Systeme unserer Kunden unter Beschuss nehmen, wir finden Schwachstellen, schreiben einen Bericht und setzen den Kunden so in die Lage, die Schwachstellen zu beheben und ein sicheres Netz zu bekommen.

Welche Security-Themen sind besonders wichtig und bei Unternehmen und Verwaltung besonders gefragt?

Gerade im Jahr 2021 haben wir sehr viele Krypto-Ransomware-Attacken. Das bedeutet, dass Täter Systeme oder Datenbanken unserer Kunden erobern, die Daten verschlüsseln und ein Lösegeld erpressen, das man bezahlen muss, um wieder an die Daten heranzukommen. Das ist ein heißes Thema und wir unterstützen Unternehmen sowohl im Falle eines Falles, wenn also ein Schaden vorgefallen ist, den Schaden sinnvoll zu behandeln, als auch eben in der Prävention, was bedeutet, Sicherheitslücken zu finden und zu stopfen.

Welche Tipps können Sie Entwicklern im Zeitalter der allgegenwärtigen Vernetzung (Internet der Dinge) zur Durchsetzung von IT-Security-Prinzipien geben?

Böse Zungen sagen, dass der Buchstabe S im Begriff Internet of Things (IoT) für Security steht. In aller Regel werden in diesem Bereich Produkte sehr schnell entwickelt und die Security wird vergessen, was dazu führt, dass die Systeme leicht hackbar sind. Schlimm im Bereich IoT ist, dass die Schwachstellen dann oft nicht ohne Weiteres zu beheben sind und dass es Rückrufaktionen oder Ähnliches gibt, daher sollte man gerade im Bereich IoT sicherstellen, dass die Systeme updatebar und wartbar sind und man optimalerweise die IT-Grundprinzipien direkt mit reinprogrammieren sollte, ähnlich wie beim Bau eines Gebäudes. Wenn man beim Fundament pfuscht und Fehler macht, dann lässt sich das hinterher nur mit immensem Mehraufwand beheben. Das heißt also, man sollte das „S" in IoT einbauen.

Wir kennen in vielen Bereichen den 80:20-Ansatz. Welche 20% einfacher Security-Prinzipien erscheinen geeignet, 80% der Angriffsfläche verteilter Anwendungen zu schließen?

Perfekte Sicherheit bekommen wir nicht hin, das ist viel zu aufwendig und nicht realistisch. Eine angemessene Sicherheit zu schaffen ist hingegen sinnvoll. Teilweise ist es nämlich nahezu unmöglich, wenn man etwa an alte Geräte denkt wie zum Beispiel in einem Kraftwerk, bei einem Staudamm oder bei medizinischen Geräten. Da haben wir oftmals ganz alte Windows-Versionen und da ist es eben wichtig, diese entsprechend zu separieren, denn ordentlich pflegen, härten und absichern kann man sie eben nicht. Das Wichtigste ist hier, jene Schwachstellen zu erkennen und zu beheben, die andere auch finden können. Man kann nicht alle Schwachstellen beheben, manche Sachen müssen wir dulden. Man sollte die low hanging fruits, die für den Täter einfach zu erreichenden Güter, entsprechend identifizieren und dazu eignet sich eben ein Penetrationstest. Auch bei einem knappen Penetrationstest werden die Dinge gefunden, die für andere auffindbar sind, also die Risiken, aus denen wirklich ein konkretes Problem resultiert, und nicht jene Risiken, aus denen sich eher ein akademisches Problem ergibt. Einen 80:20-Ansatz kann man leider nicht daraus herleiten, man kann das nur grob betrachten.

Wie sollten Unternehmen das Thema IT-Security angehen, die ihre IT-Systeme in einer oder mehreren Clouds betreiben (lassen)?

Man muss sich darüber im Klaren sein, dass die Hoheit über die Daten dann jemand anderes hat. Die Cloud-Betreiber befinden sich typischerweise nicht in Europa und nicht in Deutschland, und wenn doch, dann werden sie von den amerikanischen Playern beherrscht. Die großen Clouds sind die Microsoft Cloud Azure, Office 365, AWS, Sales Force oder Ähnliche; bei deren Nutzung macht man sich komplett abhängig von Anbietern mit einem Sitz außerhalb Europas. Wenn die amerikanische Regierung beispielsweise möchte, dass wir nicht mehr in der Azure-Cloud arbeiten können oder dass wir nicht mehr Amazon Web Services oder Sales Force nutzen, dann ist das problematisch. Man muss sich bewusst darüber sein, dass wir eine erhebliche Abhängigkeit schaffen. Wenn man die Risiken klug abgewogen hat, kann es in der Tat Sinn ergeben, Cloud-Anwendungen zu nutzen. In diesem Fall ist es aber sinnvoll, wenn man noch irgendeine Form von Sicherheitskopie hat, sodass man im Falle eines Falles an die Daten auch herankommt. Außerdem sollte man unbedingt eine Zwei-Faktor-Authentifizierung benutzen und die Cloud regelmäßig einem Cloud-Penetrationstest oder einem Cloud-Review unterziehen.

Ein Team bei uns im Hause beschäftigt sich mit nichts anderem als dieser Art von Projekten und freut sich über eine riesige Nach-

frage. Das heißt also, dass die Unternehmen sich durchaus bewusst darüber sind, dass wir bei der Cloud neue Sicherheitsrisiken haben.

Das wirtschaftliche, politische und tägliche Leben wird immer „digitaler". Wo besteht, Ihrer Meinung nach, der größte Nachholbedarf hinsichtlich IT-Security?

Es wird tatsächlich alles digitaler und wir verlassen uns immer mehr auf die digitalen Welten und erzeugen dabei eine erhebliche Abhängigkeit. Das bedeutet, dass, wenn die IT-Systeme nicht mehr funktionieren, dann eben zum Beispiel auch ein Lebensmittelunternehmen keinen Käse mehr herstellen oder keinen Kuchen backen kann. Diese Abhängigkeit muss uns bewusst sein und deswegen müssen wir noch genauer hinschauen, wenn es um IT-Security geht, sonst steht da eben mal hinterher eine Fertigung, eine Pipeline, eine Behörde oder eine Kommune komplett still und nichts geht mehr.

Welche Bereiche sind gut aufgestellt? Welche Problematiken hindern Sie daran, in Betrieben erfolgreich zu arbeiten?

Ich habe gerade heute mit einem Kunden gesprochen, der eine Roboter-Fertigung hat und dessen Roboter relativ sicher aufgestellt sind, da sie nicht vernetzt sind. Unser Kunde ist hier so ein bisschen „gestrig" und denkt nicht an Industrie 4.0 und IoT, aber dafür sind seine Systeme nahezu unhackbar, da sie eben nicht konnektiert sind. Grundsätzlich möchte der Kunde aber auch rein in die Vernetzung und aus den modernen Technologien Nutzen ziehen, aber dann wird er sich auch mit den gleichen Problemen konfrontiert sehen.

Ich sehe grundsätzlich keine Problematiken bei den Kunden, die uns behindern. Wir arbeiten gewöhnlich erfolgreich bei unseren Kunden und erzielen einen erheblichen Nutzen.

Können Sie einen typischen Angriffsfall mit den entsprechenden Gegenmaßnahmen, soweit es Ihnen möglich ist, beschreiben?

Stichwort Cloud. Wir haben da zum Beispiel ein Unternehmen mit 180 Mitarbeitern als Kunden, das alle Systeme in der Microsoft Cloud mit einer Zwei-Faktor-Authentifizierung hat, also gar nicht so einfach zu hacken. Bis auf den Vorstandsvorsitzenden, der aus Komfortgründen darauf bestanden hat, dass seine Zwei-Faktor-Authentifizierung deaktiviert wird, damit er schnell von überall, auch aus seinem Ferienhäuschen, komfortabel arbeiten kann. Dann ist passiert, was passieren musste: Der Vorstandsvorsitzende wurde „gephisht" und der Täter hatte Zugriff auf die gesamten Daten des Unternehmens. Gegenmaßnahme: zu spät! Gestohlene Daten kann man nicht zurückholen, die sind einfach weg.

Wie bewerten Sie die Themen „Blockchain" und „Big Data" hinsichtlich des IT-Security-Aspektes?

Beides sind große Themen für die Zukunft und es ist ganz klar, dass diese Technologien scheitern werden, wenn die IT-Sicherheitsprobleme nicht gelöst sind. Wenn ich etwa in der Blockchain zum Beispiel Bitcoins manage und mein Account gehackt wird, dann ist eben mein ganzes Geld weg und dies kann sonst nicht so ohne Weiteres so schnell passieren. Bei Big Data ist es genau das Gleiche. Big Data ist ja wirklich ein riesiges Asset eines Unternehmens und dies kann gestohlen, gefälscht und gelöscht werden; gerade deswegen muss man hier wirklich Datensicherheit als wichtiges Kriterium festlegen.

Können Sie einen Ausblick auf zukünftig zu erwartende Entwicklungen geben?

Ganz eindeutig, die Digitalisierung, die Vernetzung geht weiter, die Anzahl der digitalen Endgeräte in der täglichen Nutzung nimmt zu. Wir werden noch mehr IT, noch mehr Smartphones, noch mehr Videokonferenzen und noch mehr digitale Assistenten haben, die uns weiterhelfen, für uns kommunizieren, unsere Kalender führen, unsere Routen planen, wir werden mobile Fahrzeuge haben und auch im Bereich der Geräte-Medizin wird viel geschehen. Ich bin mir nicht sicher, wie lange es den Beruf des Anästhesisten noch geben wird, vielleicht wird in Zukunft eine KI dessen Arbeit machen und die Big-Data-Auswertung dann viel besser die entsprechenden Maßnahmen treffen. Das heißt, wir befinden uns in einer sich sehr schnell wandelnden Zeit und ich freue mich darauf, nicht nur weil diese Entwicklungen meinem Unternehmen stetig neue Herausforderungen bietet, sondern auch weil ich davon ausgehe, dass wir noch sehr viel mehr spannende Veränderungen in den nächsten Jahren erleben werden, und da bin ich super gespannt.

SEBASTIAN SCHREIBER

Diplom-Informatiker Sebastian Schreiber, geboren 1972, studierte Informatik, Physik, Mathematik und BWL an der Universität Tübingen. Von 1996 bis 1998 war er Mitarbeiter bei Hewlett-Packard. Noch während seines Studiums gründete er 1998 das IT-Sicherheitsunternehmen SySS GmbH in Tübingen, das Sicherheitsprüfungen bei einer Vielzahl von Unternehmen durchführt. Seit 2000 tritt Schreiber regelmäßig bei Messen und Kongressen im In- und Ausland als Live Hacker auf und zeigt anschaulich, wie IT-Netze übernommen, Passwörter geknackt und Daten abgezogen werden können. Er ist gern gesehener IT-Sicherheitsexperte in Printmedien, Rundfunk und Fernsehen, so beispielsweise in der Tagesschau, ZDF heute, Plusminus oder bei Günther Jauch. Als langjähriges Mitglied engagiert er sich darüber hinaus im Verband für Sicherheit in der Wirtschaft Baden-Württemberg e.V. oder auch im Beirat der Zeitschrift „Datenschutz und Datensicherheit".

AUS DER FERNE BETRACHTET:

FAREWELL JOEL!

APEX ohne Joel Kallman?
Völlig unvorstellbar, bis zum 25. Mai 2021.
Joel hat APEX repräsentiert, Joel war das Gesicht, die Stimme und die Seele von APEX.

Joel war APEX und APEX ist das coolste Produkt, das Oracle – nach der Datenbank selbst – je auf den Markt gebracht hat.

Oracle Forms hat dereinst den Datenbankwettlauf zwischen Sybase, Ingres, Informix und DB2 maßgeblich zugunsten der Oracle-Datenbank entschieden.

Heute hilft APEX, die Datenbankdominanz von Oracle zu festigen, und dies trotz der unsäglichen Lizenzdiskussionen und der Arroganz, mit der Oracle manchmal seinen Kunden gegenübertritt.

Joel war ein genialer Programmierer, aber zugleich ein unglaublich guter Menschenfänger. Kundenorientierung war für ihn eine Selbstverständlichkeit, ein absolutes Muss. Respekt gegenüber seinen Gesprächspartnern tief in ihm verwurzelt. Arrogantes Auftreten waren ihm ein Gräuel.

In einem sehr lesenswerten Blogeintrag vom Dezember 2018 (https://joelkallman.blogspot.com/2018/12/) beschreibt er unter anderem fünf einfache Prinzipien, die er als Schüler und Student von einem McDonalds-Manager gelernt hat und nach denen er zu leben und zu arbeiten versuchte:

1. Greet the customer with a smile, always.
2. When talking to a customer, look at them directly in the eye.
3. Talk clearly and repeat back to the customer what they told you.
4. Treat the customer (and really everyone) with respect and dignity.
5. Genuinely thank the customer and wish them farewell.
   Klingt nicht so schwierig und wird doch zu selten praktiziert.

Wer Joel kennt, weiß, dass das nicht eine bloße Aufzählung von Punkten ist, sondern dass er dies tatsächlich so praktiziert hat. Immer. Zu jeder Zeit.

Joel war das Gesicht von APEX, aber er war nicht allein. Er hat ein unglaublich gutes Entwickler-Team über die Jahre zusammengestellt. Ein Team aus aller Herren Länder. Unterschiedliche Typen zwar, aber alle mit der gleichen Grundüberzeugung. Exzellente Entwickler, die aber auch die Fähigkeiten besitzen, mit Kunden auf Augenhöhe zu sprechen, auch dann, wenn es um banale Fragen ging und geht. Ich weiß, von was ich rede, meine Fragen an Joel, Carsten und andere waren oft sehr banaler Art – im Nachhinein betrachtet. Sie haben es mich nie merken lassen.

Joel hat für sein Produkt gekämpft und seine große Sorge war stets, dass Oracle die Weiterentwicklung einstellen könnte. APEX stand und steht auf keiner Preisliste. APEX wurde nie aktiv vom Vertrieb angepriesen und vermarktet. Der Erfolg von APEX (und damit der Erfolg der Oracle-Datenbank) wurde durch das Entwicklungsteam, die technischen Oracle Teams, die Oracle-Anwendergruppen dieser Welt (!) und vor allem durch die stetig wachsende Partnergemeinde sowie unzählige sehr kreative Fans getragen.

Ein Erfolg, der für viele „EXCEL-Manager“ innerhalb von Oracle völlig unsichtbar war. Manche dieser „Strategen" sahen nur Kosten ohne Nutzen. Was für eine Fehleinschätzung!

APEX hat heute eine unglaublich gute Reputation im Markt und eine riesige Entwickler-Community. Joel und sein Team haben hervorragende Arbeit geleistet. Riesige Marketing-Budgets haben nicht annähernd die gleiche positive Wirkung erzielt.

APEX ist der Sympathieträger par excellence, das beste Marketing, das man sich vorstellen kann.

Die Corona-APEX-Applikation, die im Frühjahr 2020 innerhalb von wenigen Tagen entwickelt und US-weit ausgerollt wurde, hat das Renommee von APEX – vor allem innerhalb von Oracle – massiv verbessert. Joel hat voller Zuversicht in die Zukunft geblickt. APEX ist endlich auch innerhalb von Oracle angekommen.

„Things are really starting to turn for APEX and Oracle – I fully believe in #MOCA (Make Oracle Cool Again)”, schrieb er mir noch im März 2021.
Ein Herzenswunsch von ihm hat sich erfüllt!

Thank you, Joel!

GÜNTHER STÜRNER

E-Mail: *guenther.stuerner@dbms-publishing.de*

Datenbankhärtung mit DBSAT

Marco Mischke, Robotron Datenbank-Software

Sicherheit in der IT ist schon seit Jahrzehnten ein Thema. Dies gilt für alle Systeme, egal ob On-Prem oder Cloud. Oracle hat ein Tool entwickelt, um vorhandene Datenbanksysteme auf mögliche Schwachstellen hin zu untersuchen, das DBSAT. Wie man es einsetzt und wie man seine Datenbanken mithilfe dieses Tools besser absichert, erläutert dieser Artikel.

Um die Funktionalität des Tools und die sich daraus ergebenden Maßnahmen anschaulich zu machen, wird eine mit dem Database Creation Assistant erstellte Datenbank geprüft und gehärtet. Die Datenbank ist eine Container Database mit einer Pluggable Database, die das Beispielschema HR enthält. Für das DBSAT wurde darin ein separater Nutzer DBSAT_USER angelegt, dem die nötigen Berechtigungen zugewiesen wurden.

DBSAT einrichten

Die aktuelle Version des Database Security Assessment Tool, kurz DBSAT, kann über die My Oracle Support Note 2138254.1 *[1]* bezogen werden. Die Dokumentation des Tools wiederum findet sich unter docs.oracle.com *[2]*.

Das Tool wird als ZIP-Datei bereitgestellt, die Installation besteht aus dem einfachen Entpacken dieser Datei in das gewünschte Verzeichnis auf dem Datenbankserver, der die zu härtende Datenbank beherbergt. Zur Ausführung von DBSAT wird zum einen Java 1.8 oder höher für den Discoverer sowie Python mindestens in der Version 2.6 für den Reporter benötigt. Der Collector benutzt nur SQL*Plus und Shell- beziehungsweise CMD-Funktionalitäten.

Funktionsweise

DBSAT besteht aus drei Komponenten, dem Collector, dem Reporter und dem Discoverer. Der Collector dient zum Sammeln aller nötigen Informationen. Die Informationen stammen zum Großteil aus der Datenbank selbst, es werden aber auch Informationen auf Betriebssystemebene gesammelt. Daher muss der Collector lokal auf dem Datenbankserver mit einem Benutzer, der zumindest lesenden Zugriff auf das ORACLE_HOME hat, ausgeführt werden. Weiterhin benötigt er das CREATE SESSION Privilege und zumindest SELECT_CATALOG_ROLE zur Analyse der Datenbank.

Die Report-Komponente wertet die durch den Collector gesammelten Daten aus und erstellt daraus Auswertungen im HTML, Text, JSON und als Excel-Tabelle. Der Reporter bildet zusammen mit dem Collector den Workflow, um eine Datenbank zu analysieren und letztendlich auch zu härten.

```
./dbsat collect dbsat_user/dbsat_user@localhost:1521/pddbsat pdbdbsat
```

Listing 1: DBSAT Daten sammeln

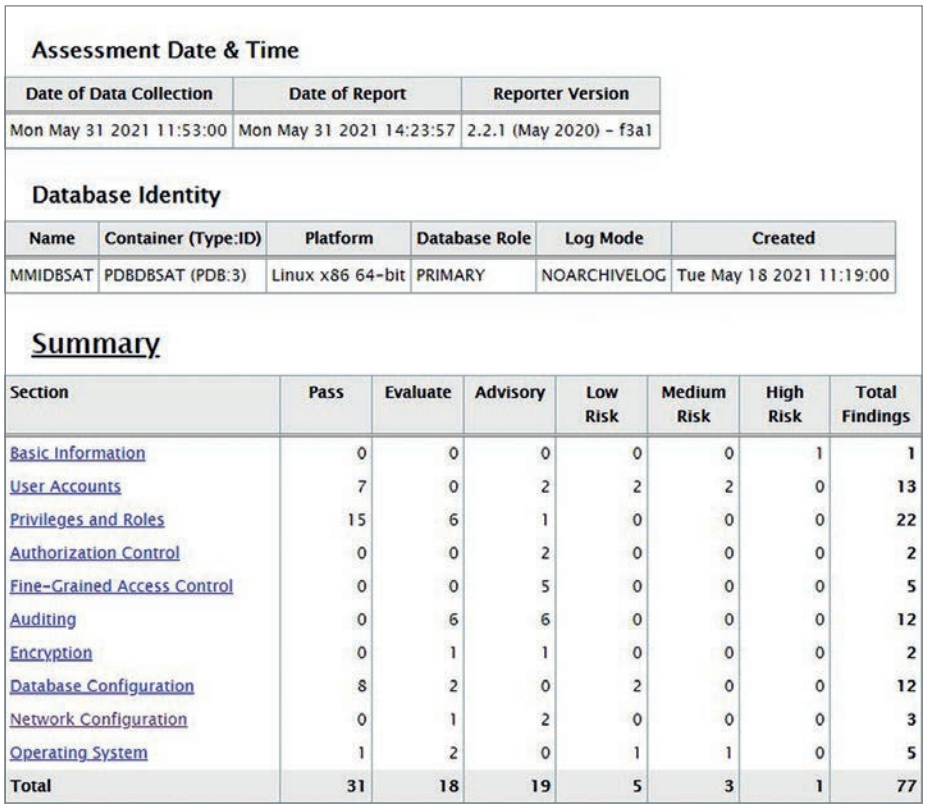
```
./dbsat report pdbsat
```

Listing 2: DBSAT Reports erstellen

Davon losgelöst kann die dritte Komponente, der Discoverer, verwendet werden, um sensitive Daten innerhalb der Datenbank ausfindig zu machen. Auf diese Komponente wird im Artikel jedoch nicht näher eingegangen.

Eine Datenbank analysieren

Wie bereits beschrieben, ist der erste Schritt zur Härtung das Einsammeln der aktuellen Konfiguration. Dazu wird der DBSAT Collector aufgerufen *(siehe Listing 1)*.



Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Mon May 31 2021 11:53:00	Mon May 31 2021 14:23:57	2.2.1 (May 2020) - f3a1

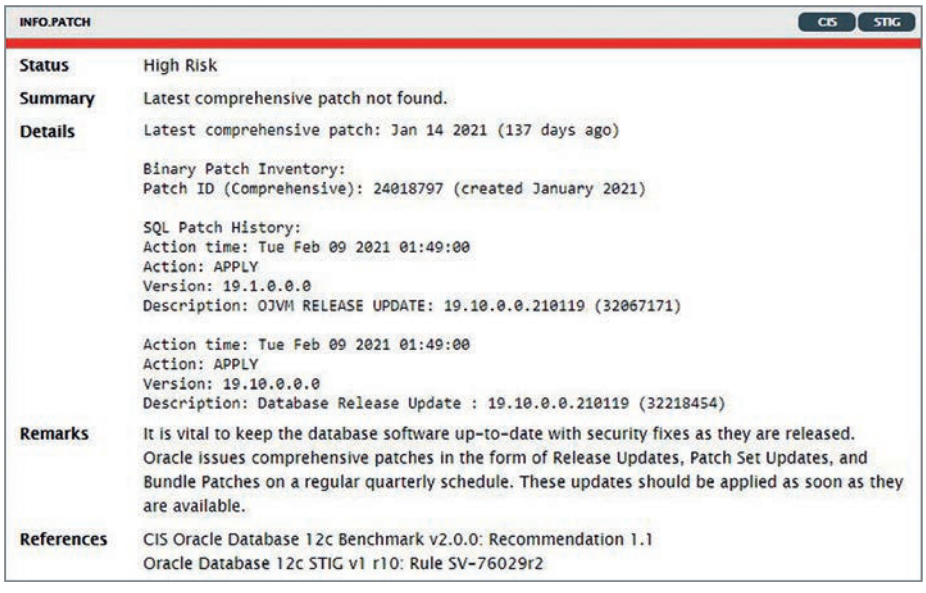
Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
MMIDBSAT	PDBDBSAT (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Tue May 18 2021 11:19:00

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	7	0	2	2	2	0	13
Privileges and Roles	15	6	1	0	0	0	22
Authorization Control	0	0	2	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	0	6	6	0	0	0	12
Encryption	0	1	1	0	0	0	2
Database Configuration	8	2	0	2	0	0	12
Network Configuration	0	1	2	0	0	0	3
Operating System	1	2	0	1	1	0	5
Total	**31**	**18**	**19**	**5**	**3**	**1**	**77**

Abbildung 1: Initialer Report (© M.Mischke, DBSAT Report)



INFO.PATCH CIS STIG

Status	High Risk
Summary	Latest comprehensive patch not found.
Details	Latest comprehensive patch: Jan 14 2021 (137 days ago) Binary Patch Inventory: Patch ID (Comprehensive): 24018797 (created January 2021) SQL Patch History: Action time: Tue Feb 09 2021 01:49:00 Action: APPLY Version: 19.1.0.0.0 Description: OJVM RELEASE UPDATE: 19.10.0.0.210119 (32067171) Action time: Tue Feb 09 2021 01:49:00 Action: APPLY Version: 19.10.0.0.0 Description: Database Release Update : 19.10.0.0.210119 (32218454)
Remarks	It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates, Patch Set Updates, and Bundle Patches on a regular quarterly schedule. These updates should be applied as soon as they are available.
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.1 Oracle Database 12c STIG v1 r10: Rule SV-76029r2

Abbildung 2: Patch Check (© M.Mischke, DBSAT Report)

Wie man sieht, muss ein DB-Connect angegeben werden. Für die Multitenant-Architektur bedeutet das, dass die Analysen auf Ebene der Pluggable Databases durchgeführt werden müssen. Verbindet man sich zur Container Database, erhält man zwar ebenfalls Ergebnisse, jedoch nur für die CDB als solches und nicht für deren PDBs. Weiterhin ist die Angabe einer Ausgabedatei erforderlich. In diesem Fall trägt diese den Namen „pdbdbsat". Das Ergebnis der Sammlung wird in ein passwortgeschütztes ZIP gespeichert, dessen Name ist im Beispiel dann „pdbdbsat.zip". Wer das ZIP lieber ungeschützt erstellen möchte, kann an dieser Stelle die Option „-n" verwenden. Zu beachten ist hierbei, dass unter Windows die Prüfungen auf Betriebssystemebene nicht durchgeführt werden.

Die gesammelten Daten werden nun im zweiten Schritt analysiert. Das geschieht mit dem Reporter und kann auf einem beliebigen Host durchgeführt werden, der über ein installiertes Python verfügt *(siehe Listing 2)*.

Als Parameter ist mindestens wieder der Dateiname erforderlich, jedoch ohne Endung. Wichtig ist, dass Dateien nicht nachträglich umbenannt werden können, denn dann findet DBSAT sie nicht mehr. Das Ergebnis ist wiederum eine passwortgeschützte ZIP-Datei, die nunmehr aber „pdbdbst_report.zip" heißt und die Auswertungen in verschiedenen Formaten enthält. Auch hier kann der Passwortschutz mit der Option „-n" ausgelassen werden.

Der initiale Report

Um sich einen ersten Überblick zu verschaffen, wirft man am besten einen Blick auf den HTML-Report. Bei einer Datenbank der Version 19.10 bietet sich das in *Abbildung 1* dargestellte Bild.

In jedem einzelnen Abschnitt finden sich dann die einzelnen Checks, die Angabe, auf welchen Empfehlungen sie basieren, deren Status sowie detaillierte Erläuterungen, was geprüft wurde und welche Einstellungen beziehungsweise Änderungen vorzunehmen sind. *Abbildung 2 und 3* sind zwei exemplarische Beispiele für diese Checks.

Wie man sieht, werden die Checks in sechs Kategorien unterteilt:

- Pass: Der Check wurde bestanden
- Evaluate: Eine Auffälligkeit, die eine manuelle Prüfung erfordert
- Advisory: Empfehlungen zur Verbesserung der Sicherheit
- Low/Medium/High Risk: Sicherheitsrisiken in verschiedenen Stufen

Das Ziel muss also sein, möglichst alle Checks mit Status „Pass" abzuschließen. Außerdem können noch Checks mit den Status „Evaluate" oder „Advisory" übrigbleiben, wenn die empfohlenen Maßnahmen aufgrund von Voraussetzungen der Applikation oder durch Einschränkungen in der Lizenzierung nicht umgesetzt werden können.

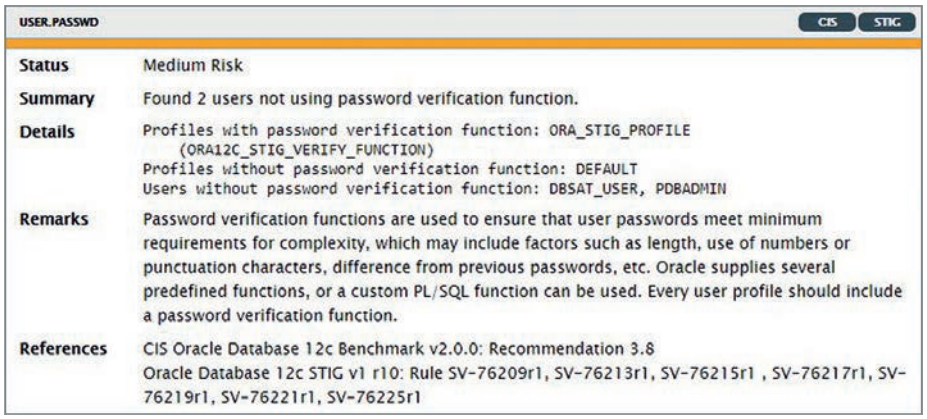


Abbildung 3: Check: Password Verify Function (© M.Mischke, DBSAT Report)

Die Empfehlungen umsetzen

Die erste Empfehlung ist zugleich auch die naheliegendste, das Einspielen des neuesten Release-Updates. Ist der momentan installierte Patch älter als 90 Tage, dann ist er vermutlich nicht der neueste Patch. Dieser Check wird also bestanden, wenn regelmäßig gepatcht wird.

Weitere Checks betreffen das User Management. Hier geht es um Dinge wie die Verwendung einer Password Verify Function und Password Policies. Um diese Checks zu bestehen, kann man entweder eigene Profiles anlegen, die die geforderten Einstellungen umsetzen oder das DEFAULT Profile anpassen. Letztere Variante sollte man auf alle Fälle in Betracht ziehen, denn so gelten die Einstellungen auch tatsächlich für alle Datenbankbenutzer, auch wenn nicht explizit ein Profile zugewiesen wurde. Oracle liefert zur Überprüfung der Passwortkomplexität eine Funktion mit. Diese kann mit dem Skript $ORACLE_HOME/rdbms/admin/catpvf.sql eingespielt werden und trägt den Namen „ora12c_verify_function". Im Grunde prüft diese Funktion das Passwort auf Folgendes:

- Mindestens 8 Zeichen
- Mindestens 1 Buchstabe, 1 Zahl, 1 Sonderzeichen
- Nutzer ist nicht gleich Passwort
- Passwort enthält nicht: Nutzername, Nutzername rückwärts, Servername oder „oracle"
- Unterscheidet sich vom alten Passwort in mindestens 3 Stellen

Außerdem gehört die Art und Weise der Passwortverschlüsselung in diesen Bereich. Der Algorithmus wurde in der Vergangenheit mehrfach geändert. Seit der Datenbankversion 12.1.0.2 existiert die Version 12a zur Generierung der Passwort-Hashes, der Standard ist hingegen 12. Man sollte also den Wert für SQLNET.ALLOWED_LOGON_VERSION_SERVER in der SQLNET.ORA entsprechend auf 12a setzen, so es die eingesetzten Programme zulassen. Dieser Parameter bestimmt im Übrigen auch, welche Passwort-Hashes beim CREATE / ALTER USER überhaupt in der Datenbank generiert werden. Die nötigen Einstellungen werden durch *Listing 3* vorgenommen.

Weitere Vorgaben, die relativ einfach umzusetzen sind, betreffen die SQL*Net-Konfiguration. Hierüber wird die Netzwerkverschlüsselung aktiviert, die seit geraumer Zeit in allen Editionen kostenfrei einsetzbar ist. Dazu genügt es, dass der Server die Netz-

```
@?/rdbms/admin/catpvf.sql
column _sessions new_value sessions noprint
select round(value *2/3) "_sessions" from v$parameter where name='sessions';
alter profile default limit INACTIVE_ACCOUNT_TIME 35;
alter profile default limit PASSWORD_REUSE_MAX 10;
alter profile default limit PASSWORD_REUSE_TIME 365;
alter profile default limit PASSWORD_VERIFY_FUNCTION ora12c_verify_function;
alter profile default limit SESSIONS_PER_USER &sessions;
alter profile ORA_STIG_PROFILE limit SESSIONS_PER_USER &sessions;

host echo SQLNET.ALLOWED_LOGON_VERSION_SERVER=12a >> $ORACLE_HOME/network/admin/sqlnet.ora
```

*Listing 3: SQL*Plus-Skript-Passwortrichtlinie umsetzen*

```
host echo SQLNET.ENCRYPTION_SERVER=REQUIRED >> $ORACLE_HOME/network/admin/sqlnet.ora
host echo SQLNET.CRYPTO_CHECKSUM_SERVER=REQUIRED >> $ORACLE_HOME/network/admin/sqlnet.ora
```

*Listing 4: SQL*Plus-Skript SQL*Net-Verschlüsselung aktivieren*

```
TCP.VALIDNODE_CHECKING=YES
TCP.INVITED_NODES=(192.168.*.*, 10.16.36.*)
```

*Listing 5: SQL*Plus-Skript SQL*Net-Verschlüsselung aktivieren*

```
C:\>sqlplus user/pass@dbconnect

SQL*Plus: Release 19.0.0.0.0 - Production on Di Jun 1 14:41:17 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

********************************************************************************
*
* Warning: Unauthorized access is prohibited!
*
********************************************************************************


********************************************************************************
*
* Warning: This is a mission-critical system. Suspicious activities
*          will be audited and evaluated.
*
********************************************************************************

Letzte erfolgreiche Anmeldezeit: Di Jun 01 2021 14:41:12 +02:00

Verbunden mit:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.11.0.0.0
```

*Listing 6: SQL*Plus-Connect mit Security-Bannern*

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Tue Jun 01 2021 14:04:00	Tue Jun 01 2021 14:04:25	2.2.1 (May 2020) - f3a1

Database Identity

Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
MMIDBSAT	PDBDBSAT (PDB:3)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Tue May 18 2021 11:19:00

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	1	0	0	0	0	0	1
User Accounts	13	0	0	0	0	0	13
Privileges and Roles	15	6	1	0	0	0	22
Authorization Control	0	0	2	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	0	6	6	0	0	0	12
Encryption	0	1	1	0	0	0	2
Database Configuration	8	3	0	1	0	0	12
Network Configuration	1	1	1	0	0	0	3
Operating System	1	2	0	1	1	0	5
Total	39	19	16	2	1	0	77

Abbildung 4: Report nach Optimierung (© M.Mischke, DBSAT Report)

werkverschlüsselung zwingend verlangt. Damit kommen ausschließlich verschlüsselte Verbindungen zustande. Verweigert ein Client aufgrund seiner Einstellungen die Verschlüsselung, dann kommt keine Verbindung zustande und der Verbindungsversuch wird mit einem ORA-1250 abgebrochen. Auch die Integrität der Netzwerkpakete kann geprüft werden. Dazu bildet Oracle eine Prüfsumme über jedes Paket und übermittelt diese mit. Die Gegenseite kann dann das Paket gegen diese Prüfsumme verifizieren und so Änderungen am Paket, die auf dem Übertragungsweg passiert sind, entdecken. *Listing 4* dient zum Aktivieren dieser beiden Mechanismen.

Ein weiteres interessantes Sicherheitsfeature von SQL*Net ist das Valid Node Checking. Auch das wird von DBSAT empfohlen. Im Prinzip handelt es sich hierbei um eine Art Black- oder White-Listing. Ist das Feature aktiviert, so können Verbindungen von bestimmten Hosts, IP-Adressen oder IP-Bereichen entweder explizit ausgeschlossen (Black-List, excluded nodes) oder erlaubt (White-List, invited nodes) werden. Dabei hat die White-List Vorrang vor der Black-List. Die Einstellungen dafür werden dieses Mal in der SQLNET.ORA des Listener vorgenommen und gelten dementsprechend für alle Datenbanken, die diesen Listener verwenden. *Listing 5* zeigt eine beispielhafte Konfiguration, die nur Verbindungen aus dem lokalen Netzwerk zulässt. Dabei ist zu beachten, dass auch der oder die Serveradressen zur Registrierung am Listener gelistet sein sollten.

Somit kann man mit dem Valid Node Checking ungewünschte Clients explizit aussperren oder eben nur die gewünschten Clients zulassen. Gerade in mehrschichtigen Architekturen mit Applikations- oder Webservern kann man diese explizit zulassen und verhindert damit ungewollte Verbindungen oder Verbindungsversuche von anderer Stelle.

Das letzte einfach zu konfigurierende Feature sind die Banner, um Benutzer vor unerlaubten Zugriffen zu warnen. Die Banner werden in Textdateien hinterlegt und dann in der SQLNET.ORA des Oracle Home mit den beiden Parametern SEC_USER_AUDIT_ACTION_BANNER beziehungsweise SEC_USER_UNAUTHORIZED_ACCESS_BANNER referenziert. Um die Banner zu aktivieren, muss die Datenbank neu gestartet werden. Die Wirkung bei einem Verbindungsaufbau mit SQL*Plus zeigt *Listing 6*.

Jedoch muss man hier auch eventuell vorhandene Skripte beachten, die die Ausgaben von SQL*Plus auswerten. Dies kann zu Problemen führen.

Extra Cost Options

Durch das DBSAT werden auch weitere Empfehlungen ausgesprochen wie etwa die Aktivierung von Database Vault, um die Trennung der administrativen Zuständigkeiten zu forcieren, oder das verschlüsselte Erstellen von Tablespaces per Transparent Data Encryption. Da dies aber kostenpflichtige Optionen der Enterprise Edition sind, deren Einrichtung vermutlich eines eigenen Artikels würdig ist, soll an dieser Stelle nicht näher darauf eingegangen werden.

Vorher / Nachher

Durch die erläuterten Änderungen an der Datenbank hat man nun eine Verbesserung in mehreren Punkten erzielt. *Abbildung 4* zeigt eine Zusammenfassung.

Es sind keine kritischen Punkte mehr offen und auch die Anzahl der weniger kritischen offenen Punkten konnte reduziert werden.

```
def diff_section(left, right):
   li = 0
   ri = 0
   while li < len(left) and ri < len(right):
       if left[li].get('title') == right[ri].get('title'):
           if left[li].get('severity') < right[ri].get('severity'):
               print_title(left[li])
               print('degraded from ' + sev_labels[left[li].get('severity')] + ' to ' + sev_labels[right[ri].
get('severity')])
               print('')
           if left[li].get('severity') > right[ri].get('severity'):
               print_title(left[li])
               print('improved from ' + sev_labels[left[li].get('severity')] + ' to ' + sev_labels[right[ri].
get('severity')])
               print('')
```

Listing 7: Angepasste Funktion diff_section für dbsat_diff

```
$ ./dbsat_diff2 1/pdbdbsat_report.json 2/pdbdbsat2_report.json
< 1/pdbdbsat_report.json: MMIDBSAT PDBDBSAT (PDB:3) Mon May 31 2021 11:53:00
---
> 2/pdbdbsat2_report.json: MMIDBSAT PDBDBSAT (PDB:3) Tue Jun 01 2021 14:04:00

INFO.PATCH: Patch Check
improved from High Risk to Pass

USER.SAMPLE: Sample Schemas
improved from Medium Risk to Pass

USER.INACTIVE: Inactive Users
improved from Low Risk to Pass

USER.AUTHVERS: Minimum Client Authentication Version
improved from Advisory to Pass

USER.NOEXPIRE: Users with Unlimited Password Lifetime
improved from Advisory to Pass

USER.PASSWD: Password Verification Functions
improved from Medium Risk to Pass

USER.SESSIONS: Users with Unlimited Concurrent Sessions
improved from Low Risk to Pass

CONF.TRIG: Triggers
improved from Low Risk to Pass

NET.CRYPT: Network Encryption
improved from Advisory to Pass
```

Listing 8: Erzielte Verbesserungen

```
$ ./dbsat_extract -i info.patch pdbdbsat2_report.json
=== pdbdbsat2_report.json: MMIDBSAT PDBDBSAT (PDB:3) Tue Jun 01 2021 14:04:00

INFO.PATCH: Patch Check
| Status: Pass
| Summary:
|     Latest comprehensive patch has been applied.
```

Listing 9: Status des Patch-Standes mit dbstat_extract

Companion Utilities

Über die eingangs erwähnte My Oracle Support Note *[1]* können auch die Companion Utilities bezogen werden. Die Utilities bestehen aus einem Skript zum Extrahieren einzelner Checks (dbsat_extract) und einem weiteren Skript zum Finden von Unterschieden in zwei JSON-Reports (dbsat_diff). Leider entspricht die Ausgabe des Diff-Skripts in etwa der eines gängigen Diff, man überblickt also nicht auf Anhieb die Stellen, an denen eine Verbesserung oder Verschlechterung eingetreten ist. Um eine kurze Übersicht zu erhalten, ändert man einfach in dbsat_diff die Funktion diff_section und ersetzt diese durch *Listing 7*.

Die Ausgabe dieses angepassten Skriptes ist nun wesentlich kürzer und übersichtlicher. *Listing 8* zeigt noch einmal die erzielten Verbesserungen.

Will man den Status eines bestimmten Checks prüfen, dann bietet sich die Verwendung von dbsat_extract an. Damit lässt sich jeder einzelne Check aus einem JSON-Report extrahieren, im *Listing 9* beispielsweise für den aktuellen Patch-Stand der Datenbank.

Automatisierung

Da das beschriebene Vorgehen zur Analyse und Härtung von Oracle-Datenbanken ein manueller Prozess ist, bietet es sich an, diesen zu automatisieren. Je nach Anforderung kann ein JSON-Report regelmäßig für jede kritische Datenbank erzeugt werden. Diese Reporte können dann beispielsweise wie oben beschrieben auf einzelne Checks hin untersucht oder auf Änderungen überprüft werden. So ließe sich eine Benachrichtigung für die als kritisch bewerteten Themen realisieren, ohne dass man regelmäßig wiederkehrende Arbeiten durchführen muss.

Quellen

[1] Oracle: Oracle Database Security Assessment Tool (DBSAT): *https://support.oracle.com/epmos/faces/DocContentDisplay?id=2138254.1*

[2] Oracle: DBSAT Online Documentation: *https://docs.oracle.com/cd/E93129_01/SAT-UG/toc.htm*

Über den Autor

Marco Mischke ist seit mehr als zwanzig Jahren im Umfeld der Oracle-Datenbank tätig und beschäftigt sich dabei vor allem mit den Themen Standard Edition, Sicherheit und Hochverfügbarkeit.

Marco Mischke
Marco.Mischke@robotron.de

25. Ausgabe der Oraworld erschienen

DOAG Online

Seit gestern ist die neueste Ausgabe des englischsprachigen EOUC-eMagazines online verfügbar – wie immer kostenfrei.

Die Titelstory "Fast and Furious: Capturing Edge Computing Data With Oracle 19c Fast Ingest" widmet sich der Datenanalyse in Zeiten des Internet of Things (IoT): Der US-amerikanische Oracle ACE Director Jim Czuprynski zeigt, wie perfekt sich die Fast-Ingest-Funktionen von Oracle Database 19c eignen, um Streaming-Daten in Echtzeit zu erfassen und analysieren. Darüber hinaus erwarten Sie auf 52 Seiten viele weitere spannende Artikel und Geschichten aus dem Oracle-Kosmos.

Die 25. ORAWORLD-Edition ist die letzte von Dr. Dietmar Neugebauer als Chefredakteur betreute Ausgabe. Der ehemalige und langjährige DOAG-Vorstandsvorsitzende geht nun in den wohlverdienten Ruhestand und übergibt den Redaktionsvorsitz, den er seit der ersten Ausgabe vor fünf Jahren innehatte, an Mirela Ardelean von der rumänischen User Group: "Ich bin sehr froh, dass Mirela diese Verantwortung übernimmt. Mirela verfügt nicht nur über ein langjähriges und tiefes Wissen über Oracle. Als Mitglied des EOUC Boards ist sie auch eine anerkannte Persönlichkeit mit einem weltweiten Netzwerk. Ich wünsche ihr und ihrem Team alles Gute für die Zukunft und bedanke mich bei allen, die mich bei der Erstellung der Magazine unterstützt haben." Sämtliche Ausgaben: *http://www.oraworld.org/home/*

Datenbanksicherheit: Masking. Warum? Wo? Wie?

Ekaterina (Katharina) Koschkarova

Neue Rekorde bei der Entdeckung von Datenlecks werden schon nicht mehr nur wöchentlich, sondern täglich aktualisiert. Nachrichten im Internet sind voller Berichte über Fälle von Lecks in Banken, Unternehmen, Reisebüros, Fluggesellschaften...

Was bedeuteten die Datenlecks früher für uns? Eine Situation mit 100.000 verlorenen Passwörtern oder E-Mails war eine Katastrophe! Und jetzt sprechen wir schon über Millionen Datensätze. Wie können die Betrüger solche Datenmengen kompromittieren, wenn die Entwicklung der Informationssicherheit nicht stillsteht? Eine neueste Statistik besagt, dass im Jahr 2020 91% der russischen Unternehmen bereits mit dem Problem eines Datenlecks konfrontiert waren; 60% dieser Vorfälle – gelten als Arbeit von Insidern. Es ist ganz wichtig, an diese Statistik zu denken: Manchmal müssen Hacker

nicht nur neue Viren, Ransomware und Verschlüsselungsverfahren erfinden, sondern nur die richtigen Leute finden.

Es gab immer Mitarbeiter in Unternehmen und Banken, die nichts dagegen hatten, etwas mehr Geld zu verdienen, wodurch es durch unehrliches, illegales Verhalten und Vorgehen sogar auch zum Weiterverkauf vertraulicher und kommerzieller Daten des Unternehmens kam. Die Krise, die durch die Corona-Pandemie entstanden ist, hat nur den Wunsch vieler Büroangestellter angeheizt, sich zusätzliches Geld zu verdienen. Manche entlassenen Mitarbeiter tun das zum Beispiel, um sich an ihren Arbeitgebern zu rächen. In solchen Momenten erinnern sich nur wenige an die drohende Strafbarkeit.

Der kürzeste Weg für die Betrüger, Daten illegal zu erhalten, ist das Finden und Werben eines Insiders. Die Berichte von Sicherheitsdienst-Leitern bei Unternehmen und Banken besagen, dass es heute eine Vielzahl von Möglichkeiten solcher „Rekrutierung" gibt, etwa die, in sozialen Netzwerken verschiedene Angebote "zusammenzuarbeiten". In einigen Fällen rekrutiert man die Mitarbeiter einfach auf der Straße neben dem Eingang zum Büro oder im „Raucherraum" und bietet ihnen die Möglichkeit, Geld damit zu verdienen, gewünschte Daten aus den Unternehmens-Datenbanken zu liefern. Die durchschnittlichen Kosten für diese Dienstleistung beträgt dann etwa 1000 bis 1500 Euro für ein paar Hundert oder Tausend Datensätze; das hängt von ihrem Wert ab. Sicherheitsexperten betrachten heute als beliebteste Methoden, um Daten aus dem Büro herauszutragen, die folgenden Vorgehensweisen:

- die Daten auf einem USB-Stick zu speichern; dies ist ganz leicht und schnell möglich. Deshalb sind in einigen Banken USB-Ports geblockt oder entfernt.
- eine E-Mail zu senden, wenn es nicht viele Daten gibt. Das ist riskant, da es Technologie-Methoden gibt, einen Insider schnell zu ermitteln.
- „Share Document": Diese Methode wird häufig in Unternehmen praktiziert, die Cloud-basierte Dokumentationslösungen aktiv nutzen, insbesondere offene.
- ein Foto von Datensätzen mit der Handy-Kamera aufzunehmen: eine ungewöhnliche, aber superschnelle und sehr populäre Möglichkeit, um heute Daten zu stehlen. Ein Betrüger kann jedoch nicht viele Datensätze bekommen, aber für E-Mails oder Konten von VIP-Bankkunden etwa reicht es.

Ein weitere Möglichkeit besteht darin, durch die Bereitstellung des Zugriffs auf Datenbanken für externe Entwicklerteams Daten zu stehlen, etwa beim Testen von Informationssystemen oder Softwareprodukten in der Entwicklungsphase.

Der Zugriff auf Datenbanken für Entwickler und Analysten, die an einem Projekt arbeiten, birgt immer Risiken. Der menschliche Faktor spielt generell eine Rolle in der Informationssicherheit, auch in allem, was Datenbanken betrifft. Einfache Unaufmerksamkeit bei der Bereitstellung von Zugriffen; Fahrlässigkeit; das Vertrauen darauf, dass die Daten dieses Unternehmens „niemand braucht"; die Unwissenheit und Hoffnung auf Informationssicherheit im Unternehmen („Wir haben Antivirenprogramme!") – alles schafft Möglichkeiten für Betrüger. Es erscheint logisch, dass eine Datenbank so sicher wie möglich sein sollte, aber... Statistiken zufolge zahlen Unternehmen und Firmen im Durchschnitt nur 15% der Gesamtkosten für die Datenbanksicherheitssoftware.

Zum Vergleich: Für die Netzwerksicherheit liegt der Wert bei 67 %. Nein, nein, wir müssen nicht die Rolle von Hackerangriffen, Viren und Spyware unterschätzen. Während der Pandemie nahm das Ausmaß des Datendiebstahls in großem Maßstab zu. Die Fernarbeit – also wenn Mitarbeiter von zuhause arbeiten und manchmal zu persönlichen Zwecken mit dem Arbeitslaptop im Internet surfen – das muss zu einer Zunahme der Opferzahl führen. Dazu kommt, dass öfter keine Informationssicherheitsexperten und Systemadministratoren in der Nähe sind, die helfen und gegebenenfalls geeignete Maßnahmen veranlassen könnten, und die Rechner sich außerhalb des sicheren Unternehmens-Umfeldes befinden.

Welche Daten finden die Betrüger am interessantesten?

Vor allem stehen in dieser Liste alle persönlichen Daten: Telefonnummern, E-Mail-Adressen, Kontonummern, Passdaten... Heute sind Konten, das „Mobile Banking" und andere Anwendungen durch eine Nummer verbunden; diese Daten werden zum Leckerbissen für Betrüger. Mit einer kompromittierten Telefonnummer und einer E-Mail-Adresse kann man versuchen, den Zugriff auf das persönliche Konto mit der App zu bekommen. Und manche Betrüger beginnen regelmäßig, diese Nummern anzurufen, indem sie sich als ein Mitarbeiter eines Sicherheitsdienstes der Bank vorstellen, um die Nummer einer Bankkarte herauszubekommen.

Zu allen Zeiten werden Daten, die ein Geschäftsgeheimnis darstellen, sehr geschätzt: Kundenlisten, Kontaktpersonen, Informationen über Konten. Alle diese Daten werden oft mit dem Begriff „sensible" Daten markiert. In der Tat ist der Datenverlust nicht nur gefährlich, weil die Betrüger die gestohlenen Daten nutzen können. Die Tatsache eines Daten-Lecks kann zu einem Reputationsverlust führen und die Zukunft des Unternehmens gefährden.

Wo befinden sich die Daten nach dem Auftreten eines Lecks?

In vielen Fällen können kompromittierte Daten sich im Darknet befinden. „Darknet" ist der allgemeine Name für Netzwerke mit anonymer Übertragung von Informationen: Websites, die dem Handel gewidmet sind, soziale Netzwerke, Portale für den Austausch von Informationen ... meistens mit illegalem Kontext. Oft wird das Darknet „der versteckte Teil des Internets" oder „die dunkle Seite des Internets" genannt. Die Anonymität des Datenaustausches wird durch verschiedene Technologien gewährleistet, zum Beispiel „Zwiebelroute": wenn Nachrichten mehrmals verschlüsselt und über mehrere Knoten (Nodes) übertragen werden, von denen jeder die Nachricht entschlüsselt. Das sieht wie eine Zwiebel aus. Diese Architektur macht die Kontrolle über die Übertragung von Informationen sehr schwierig und das ist eine Möglichkeit, viele Dienste zu starten, um beispielsweise den Verkauf gestohlener Daten zu organisieren. Normalerweise werden die kompromittierten Datenbanken mehrere Male verkauft; der Preis der „frischen Datenbank" ist höher als der Preis der „alten", nicht aktuellen Datenbank. Die Käufer können eine bestimmte Anzahl von

Datensätzen oder die ganze Datenbank bekommen. Heute sind illegale Auktionen für den Verkauf gestohlener Daten immer populärer geworden! Wenn die Daten eines großen Unternehmens im Darknet erscheinen, kontaktieren Mitglieder von Hacker-Gruppen sowie „weiße" Hacker (ethische Hacker, die bei Unternehmen mögliche Schwachstellen aufspüren, diesen bei der Behebung helfen und zudem auch alle Instrumente der Hacker benutzen) die Vertreter der betroffenen Unternehmen, um festzustellen, ob diese Daten tatsächlich kompromittiert sind. Üblicherweise bekommen zu diesem Zweck die Vertreter der betroffenen Unternehmen ein paar Datensätze der gestohlenen Datenbank als Beweis.

Im Darknet kann man nicht mit dem üblichen Browser surfen. Die Verwendung von versteckten Netzwerken ist in vielen Ländern offiziell verboten.

Welche Lösungen gibt es?

Wahrscheinlich ist der beliebteste und populärste Weg, Daten vor Kompromittierung zu schützen, die Verschlüsselung. Eine gute Idee – aber wird einen ein solcher Ansatz vor Insidern beschützen? Viele Mitarbeiter müssen auf Daten zugreifen, um mit ihnen zu arbeiten!

Eine geeignete Option besteht darin, die Daten zu maskieren, ihre Darstellung und ihr Aussehen zu verändern. Wahrscheinlich haben viele von uns die Nummer einer Bankkarte gesehen, bei der drei Oktette mit Sternchen geschlossen sind: Dies ist nur ein Beispiel, nur eine Möglichkeit, die Darstellung der Daten zu ändern oder eine Maskierung zu verwenden. Es gibt tatsächlich viele Ansätze zur Maskierung. Dazu gehört die bereits erwähnte Maskierung mit Sonderzeichen, Shuffle oder eine Mischung mit Symbolen, Ersatz mit Konstanten…

Natürlich existieren Maskierungs-Regeln, die auf unternehmensinternen Standards basieren und mit bestimmten Algorithmen und Funktionen implementiert werden. Alle diese Methoden beruhen auf der Grundidee, die Daten nicht attraktiv für Betrüger zu machen, aber gleichzeitig Entwicklern und Analysten die Möglichkeit zu geben, mit diesen Daten arbeiten zu können.

Falls diese Daten doch ins Darknet gelangen sollten, bringen sie den Betrügern doch keinen praktischen Nutzen. Mit E-Mail-Adressen, in denen zum Beispiel alles bis auf das @-Symbol durch Sternchen versteckt ist, können die Hacker nichts anfangen. Telefonnummern, in den alle Zahlen miteinander vermischt und sogar nach einem bestimmten Algorithmus verändert sind, werden auch nutzlos für Betrüger sein.

Die Maskierung kann mit verschiedenen Mitteln realisiert werden: mit den vorinstallierten Tools etwa von DBMS oder mit den Drittanbieter-Dienstprogrammen (die von den großen Anbietern wie Oracle oder von eigenen Teams entwickelt werden). Das Hauptmerkmal solcher Tools ist, dass die Verbindungen zwischen DB-Objekten auch nach der Datenkonvertierung gespeichert werden, denn Maskierung soll nicht nur die Datensicherheit garantieren, sondern auch die Konsistenz von Daten sichern. Hauptsächlich geschehen Datendiebstähle nicht ohne die „Hilfe" von DBA-Benutzern oder Datenbankadministratoren, da diese Rolle die notwendigen technischen Möglichkeiten bietet. Laut einer Statistik sind etwa 90% der Daten im Darknet von Unternehmens-Mitarbeitern zur Verfügung gestellt worden, die durch ihre Rolle Daten kompromittieren können. Und was ist zu tun, um die Daten vor unbefugtem Administratorzugriff zu schützen? Hier helfen uns Produkte wie Oracle Data Vault … und auch natürlich Data Masking! Wenn sogar Ihr DBA, Ihre Entwickler oder Analytiker die maskierten Daten sehen, aber nicht verkaufen oder verwenden können, hat Ihre Firma fast keine Risiken.

Ekaterina Koshkarova
ekaterina.koshkarova@gmail.com

Java 16 im Detail

DOAG Online

Die im März veröffentlichte aktuelle Version des OpenJDK 16 ist die letzte Major-Version vor dem nächsten Long-Term-Support-Release OpenJDK 17, das im September erscheint.

Falk Sippach gibt in der Java aktuell 3/21 *(https://www.doag.org/de/home/news/java-aktuell-032021-jvm-sprachen/detail/)* ab Seite 11 einen Überblick über die Inhalte des Updates und die neuen Features. Dabei geht er näher auf alle neuen Java Enhancement Proposals (JEPs) ein. Zum Abschluss wagt er auch einen Blick in die Zukunft und auf das kommende Update 17.

Exadata – sicher ist sicher!

Frank Schneede, Oracle Deutschland

Die Notwendigkeit der Absicherung von IT-Systemen gewinnt mehr und mehr an Bedeutung. Dieser Umstand wird unterstrichen durch den Risk Based Security Bericht Q3/2020 *(https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf)*, in dem von 2935 Schadensereignissen mit insgesamt rund 36 Milliarden gestohlenen Datensätzen die Rede ist – allein für die Zeit vom Jahresbeginn bis September letzten Jahres! Es liegt also im Interesse eines jeden IT-Verantwortlichen, seine gesamte Landschaft entsprechend abzusichern. Die Oracle Exadata Database Machine ist integraler Bestandteil der Oracle Cloud Infrastructure und vieler Kunden-IT-Landschaften, an die besonders hohe Sicherheitsanforderungen gestellt werden. In diesem Artikel wird aufgezeigt, mit welchen Mitteln eine Maximum Security Architecture auf der Exadata aufgebaut werden kann, angefangen mit der Herstellung des Systems, über dessen Implementierung bis hin zum Systembetrieb.

Die **Exadata Database Machine** können Kunden bekanntermaßen in drei Deployment-Alternativen nutzen: als **Exadata Cloud Service**, als Exadata Cloud at Customer oder als klassisches On-Premises-System im eigenen Rechenzentrum. Der Exadata Cloud Service verfügt über die wichtigsten Zertifizierungen, wie PCI DSS, HIPAA, ISO27001, SOC I/SOC II und andere mehr. Eine Zertifizierung ist nur erreichbar, indem einerseits die Systemarchitektur entsprechend gehärtet ist, andererseits aber auch eine Absicherung des Systembetriebes auf allen Ebenen sichergestellt ist. Die Verfahren, die dazu führen, dass die genannten Standards erreicht werden, kann jeder, der ein Exadata-System betreibt, für sich umsetzen. Daher beschränke ich mich in diesem Artikel auf die Maßnahmen, die für On-Premises-Exadata-Systeme umgesetzt werden müssen.

Database Security

Die Sicherheit der Oracle-Datenbank selbst wird durch ein umfangreiches Port-

folio an Datenbank-Funktionen und -Optionen erreicht. Welche Anwender oder Anwendungen auf sensitive Daten Zugriff haben, wo diese Daten liegen und wie die Daten abgesichert sind, kann man über das Cloud-Tool **Data Safe** für Cloud- und On-Premises-Datenbanken ermitteln. Nach diesem umfangreichen Security Assessment geht es darum, Daten vor unberechtigtem Zugriff zu schützen. Auch hierfür gibt es eine Reihe von Werkzeugen:

- **Data Redaction** – zur Maskierung der Anzeige sensitiver Daten
- **Transparent Data Encryption** – zur Verschlüsselung sensitiver Daten in der Datenbank beziehungsweise beim Transport dieser Daten
- **Key Vault** – zum sicheren Abspeichern von Verschlüsselungsinformationen
- **Data Masking and Subsetting** – zur Veränderung sensitiver Daten bei der Erstellung von Test- und Entwicklungsdatenbanken
- **Database Vault** – zum Schutz sensibler Daten vor dem Zugriff durch privilegierte Benutzer
- **Database Firewall** – zum Schutz sensibler Daten vor unberechtigtem Zugriff und zur Protokollierung von Zugriffen

Wenn die Daten vor unberechtigtem Zugriff geschützt sind, besteht der nächste Schritt darin, Datenzugriffe und mögliche Sicherheitsverletzungen zu entdecken und zu protokollieren. Neben **Audit Vault**, das Datenzugriffe aus unterschiedlichen Datenbanken protokollieren und auswerten kann, dient auch **Data Safe** der Entdeckung und Dokumentation von Sicherheitsverletzungen.

Der Zugriff auf Inhalte sensibler Daten wird umgesetzt durch:

- **Virtual Private Database** – zur transparenten Umsetzung eines „Need-To-Know"-Prinzips für sensitive Daten
- **Label Security** – zur granularen Steuerung des Zugriffs auf sensitive Daten
- **Real Application Security** – zur Authentifizierung von Benutzern nicht nur auf Datenbank-, sondern auch auf Anwendungsebene

Abbildung 1 zeigt eine schematische Darstellung des Oracle-Database-Security-Produktportfolios.

Auf der Exadata Database Machine können natürlich alle oben genannten Optionen und Funktionen eingesetzt werden, doch allein durch den Einsatz intelligenter Softwarelösungen zur Absicherung im Umfeld der Anwendung und des Netzwerkes ist noch kein vollständiger Schutz des Systems erreicht. Die Angriffe setzen nämlich bereits wesentlich früher ein! Schon die Lieferketten sind gefährdet, jedoch hat Oracle mit seinen Lieferanten umfangreiche Sicherheitsvorkehrungen getroffen, um den Schutz bereits auf dieser Ebene sicherzustellen.

Die gesamte Lieferkette ist integriert und wird streng überwacht. Oracle ist Eigentümer der zentralen Hardware und Firmware. Bereits im Entwicklungsprozess eines neuen Exadata-Modells erfolgen Sicherheitsaudits für alle Design Releases. Die Zulieferer sind verpflichtet, die hohen Oracle-Sicherheitsrichtlinien einzuhalten. Der Austausch von Designdaten erfolgt verschlüsselt. Alle Systemqualifizierungstests und Systemvalidierungen werden durch Oracle kontrolliert. Digitale Signaturen und Zertifikate schützen alle Firmware- und Softwarekomponenten. Die Fertigung für die Systemintegration erfolgt nach dem Regelwerk des Trade Agreements Act (TAA). Durch diese umfangreichen Maßnahmen wird dafür Sorge getragen, dass während des Entwicklungsprozesses keine Schadsoftware in das System eingeschleust werden kann.

Die Entwicklung der Exadata Database Machine verfolgt drei Schwerpunkte:

- Eine **intelligente Systemsoftware**, die für den Einsatz der Oracle-Datenbank optimiert ist und hohe Performance in OLTP, Analytics oder für konsolidierte Transaktionslasten ermöglicht
- Eine **hochverfügbare Architektur**, die den störungsfreien Betrieb kritischer Unternehmensanwendungen ermöglicht
- **End-to-End Security**, die Umsetzung von Sicherheitsprinzipien (z. B. Least-Privilege-Prinzip) über den gesamten Exadata Stack

Optimiert für höchste Sicherheit

Durch die Entfernung des Zugriffs auf alle Funktionen, die nicht zur Kernfunktionalität der Exadata gehören, und durch Ein-

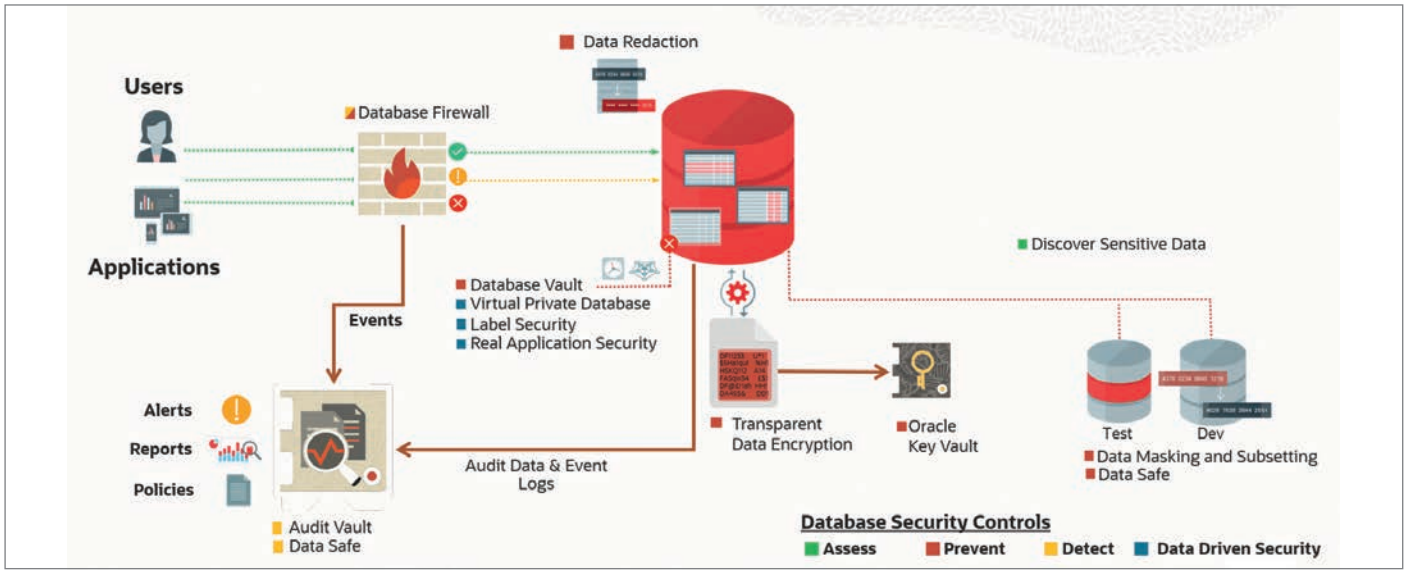


Abbildung 1: Database Security (Quelle: Frank Schneede)

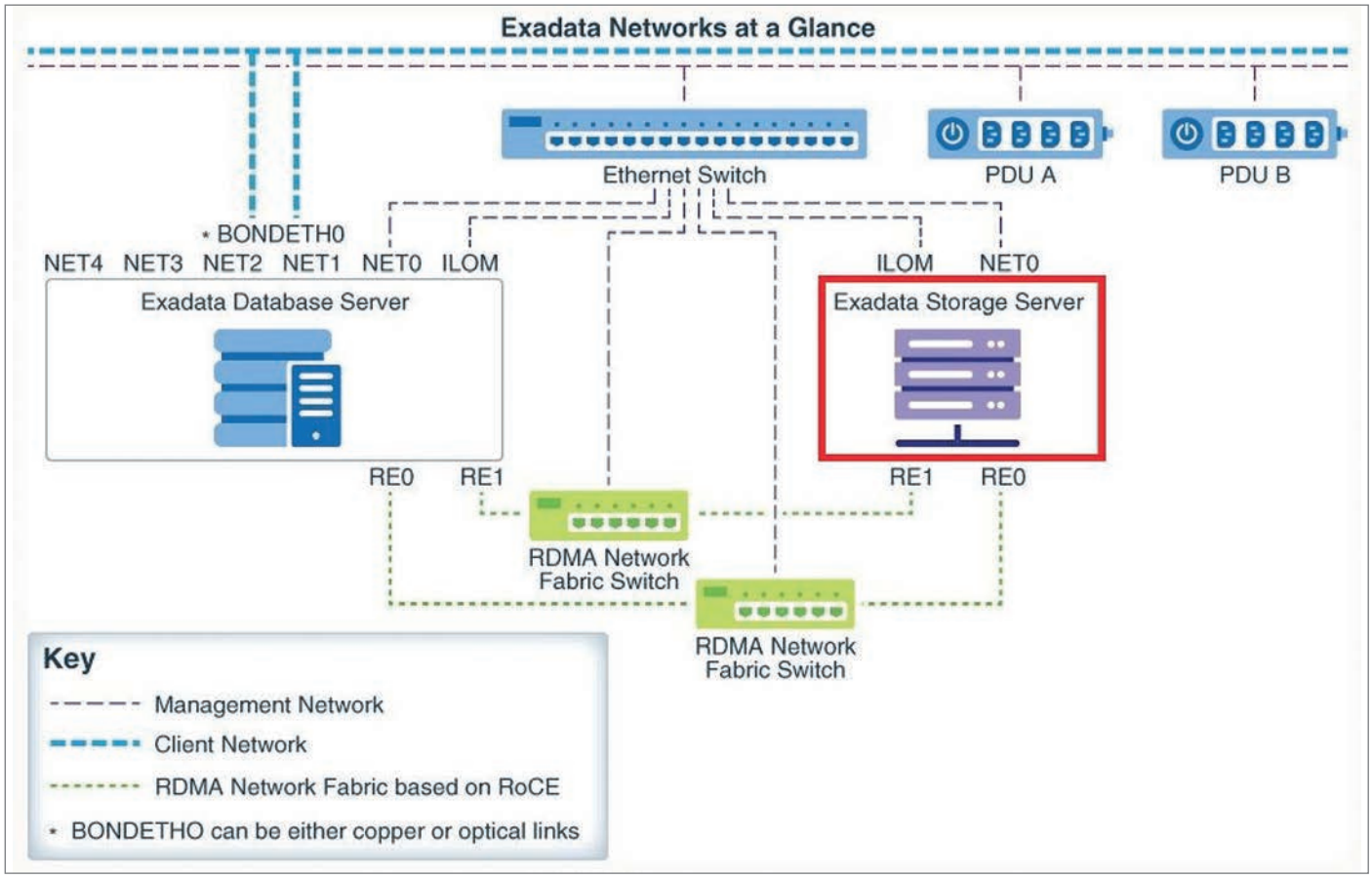


Abbildung 2: Exadata-Netzwerk (Quelle: Frank Schneede)

schränkung des Zugriffs, wenn die entsprechende Funktion nicht benötigt wird, wird die Exadata-Implementierung auf Sicherheit hin optimiert. Mit der Komplexität einer Software steigen im Allgemeinen auch die Möglichkeiten für Angriffe. Daher ist das Betriebssystem der Exadata minimiert, das heißt, es enthält nur Komponenten, die für den Betrieb der Oracle-Datenbank notwendig sind. Eine herkömmliche Oracle-Linux-7-Installation enthält circa 5400 Packages; das DB-Server-Installationspaket in der Version 20.1 enthält hingegen nur 701 Packages! Sichtbar wird das auch am Linux Kernel, der in der DomU auf Exadata eingesetzt wird und der Funktionen, die in einer Enterprise-IT nicht benötigt werden, nicht enthält. Der mit Exadata 20.1 ausgelieferte Nano-Kernel hat lediglich eine Größe von 38MB, während der Standard-Kernel für Oracle Linux 7 167MB umfasst. Damit werden gleich mehrere Ziele erreicht:

- Weniger Abhängigkeiten
- Weniger Treiber für Komponenten
- Weniger Platzbedarf
- Weniger Zeitbedarf für Upgrades

Die in der Exadata verbauten Storage Server *(siehe Abbildung 2)* verfügen über keine direkte Anbindung ans Client-Netzwerk, der Zugriff erfolgt nur mittelbar über die Datenbankserver.

Auf jedem Storage Server läuft ein `cellwall`-Service, der auf dem Storage Server als Firewall dient und nicht autorisierte Zugriffe unterbindet. Der ssh-Server antwortet lediglich auf Verbindungsanfragen, die über das Management-Netzwerk (net0) und das ausschließlich intern genutzte RDMA-Netzwerk Fabric kommen.

Fokussiert auf höchste Sicherheit

Das **Least-Privilege-Prinzip** ist eine der grundlegenden Regeln einer erfolgreichen Sicherheitsstrategie. Der Zugriff auf bestimmte Daten sollte durch die unbedingt notwendigen Zugriffsrechte ermöglicht werden – nicht weniger, aber erst recht nicht mehr. Viele Rechte werden nach wie vor nach dem Motto *„Ach was, gib mir DBA-Privilegien, dann klappt es auf jeden Fall!"* vergeben, einfach weil es einfacher ist, als die notwendigen Rechte in möglicherweise mehreren Iterationen zu ermitteln. Ein großes Sicherheitsrisiko! Wenn dieses Vorgehen bereits in der Programmierung so erfolgt, dann ist eine nachträgliche Behebung oftmals kaum mehr möglich, und wenn, dann nur sehr aufwendig. Gleiches gilt für Aufgaben, die bislang mit `root`-Zugriff erfolgen mussten. Dem ist in Bezug auf die in der Exadata laufenden Prozesse Rechnung getragen worden:

- **Smart-Scan-Prozesse** zur Ausführung der Smart-Scan-Funktionalität (Scannen und Filtern von Daten auf dem Storage Server) laufen unter User `cellofl`, Group `celltrace`
- **`ExaWatcher`-Prozesse** zum Sammeln von Informationen durch Kommandos wie `iostat`, `netstat`, `ps`, `top` laufen unter User `exawatch`, Group `exawatch`

Darüber hinaus werden standardmäßig unnötige und tendenziell unsichere Dienste wie `telnet` oder ftp auf Exadata-Systemen deaktiviert.

Seit der Exadata-Software-Version 19.1.0 gibt es eine neue Funktion, mit der Benutzer Access-Control-Listen für den `https`-Zugriff auf den RESTful-Service konfigurieren können. Eine Liste von IP-Adressen oder Subnetzmasken kontrolliert den Zugriff auf den RESTful-Service über `https`, natürlich kann der RESTful-Service auch komplett deaktiviert werden, wenn er nicht benutzt wird. Das gilt für Datenbank und Storage Server gleichermaßen. Das Syntaxbeispiel in *Listing 1* zeigt das Vorgehen.

Ein weiterer Schritt zur Absicherung der Exadata besteht darin, Aktivitäten auf der Betriebssystemebene zu überwachen. Hierzu wird das Linux Tool `auditd` verwendet. Exadata-spezifische Audit-Regeln sind in der Datei `/etc/audit/rules.d/01-exadata_audit.rules` definiert. Audits können über den Befehl `auditctl` verwaltet und ausgewertet werden. Ein kleines Beispiel findet sich in *Listing 2*.

Der **Management-Server-Prozess (MS)** läuft auf Datenbank- und Storage Servern zur Überwachung und unterstützt das Attribut `syslogconf`. Seit Exadata Version 19.3 kann nun die Übertragung der System-Log-Dateien verschlüsselt werden. Das `syslogconf`-Attribut ergänzt die `syslog`-Regeln für einen Datenbankserver. Das Attribut kann verwendet werden, um festzulegen, dass syslog-Meldungen an einen bestimmten entfernten `syslogd`-Dienst weitergeleitet werden sollen. Auf dem MS werden die weitergeleiteten Nachrichten an eine Datei, eine Konsole oder eine Managementanwendung weitergeleitet, je nach `syslog`-Konfiguration auf dem MS. Auf diese Weise können Systemprotokolle von verschiedenen Servern zusammengefasst und in einem zentralen Protokollierungsserver für Sicherheitsüberprüfungen, Data Mining usw. ausgewertet werden.

Die Verschlüsselung geschieht über Zertifikate und das Attribut `syslogconf` in mehreren Schritten:

1. Richten Sie eine Zertifizierungsstelle (CA) ein. Dies kann ein beliebiger Knoten sein, der über den Befehl `certtool` verfügt. Es wird empfohlen, einen Nicht-Exadata-Server zu verwenden. Die CA erstellt ein selbstsigniertes Zertifikat. Der Schlüssel für die Zertifikatsverschlüsselung muss an einem sicheren Ort gespeichert werden. Dieses Zertifikat wird zum Signieren anderer Zertifikate verwendet.
2. Erzeugen Sie Zertifikate auf jedem teilnehmenden Knoten. Wenn Sie keine zentrale CA haben, kann der Exadata-Administrator sowohl den privaten als auch den öffentlichen Schlüssel auf der CA generieren und Kopien an jeden vertrauenswürdigen Server verteilen. Wenn Sie eine zentrale CA haben, dann generiert der Exadata-Administrator den privaten Schlüssel für jeden Server.
3. Wenn Sie eine zentrale CA verwenden, erstellt der Exadata-Administrator eine Zertifikatsanforderung. Diese Anforderung wird dann an den CA-Administrator gesendet, der wiederum das Zertifikat (mit dem öffentlichen Schlüssel) generiert. Der CA-Admin sendet dann das signierte Zertifikat an den Exadata-Administrator zurück.
4. Installieren Sie die signierten Zertifikate auf jedem teilnehmenden Knoten. Wenn Sie eine zentrale CA verwenden, installiert der Exadata-Administrator das von der CA signierte Zertifikat. Wenn Sie keine zentrale CA verwenden, installiert der Exadata-Administrator eine Kopie der privaten und öffentlichen Schlüssel, die von der CA erzeugt wurden.
5. Richten Sie einen zentralen `syslog`-Server ein. Für den zentralen Server muss die Datei `syslog.conf` eingerichtet werden. Er benötigt außerdem signierte Zertifikate.
6. Aktivieren oder deaktivieren Sie die Verschlüsselung von `syslog` auf jedem Client mithilfe von `cellcli` oder `dbmcli`.

Nach Ausführung dieser Schritte wird jedes `syslog`, das transportiert wird, verschlüsselt.

Härtung des Systems

Zu den wichtigsten Maßnahmen zur Absicherung des Systems gegen unbefugten Zugriff ist die Härtung. Im Datenbank-

```
# lsof -i -P -n | grep LISTEN | grep java
java      <pid> dbmsvc   55u  IPv4   40193   0t0 TCP *:7879 (LISTEN)
# dbmcli -e alter dbserver httpsAccess=none
This command requires restarting MS. Continue? (y/n): y
Stopping MS services...
The SHUTDOWN of MS services was successful.
Updating HTTPs access control list.
Starting MS services...
The STARTUP of MS services was successful.
DBServer successfully altered
# lsof -i -P -n | grep LISTEN | grep java
```

Listing 1: Deaktivieren des https-Zugriffs

```
[root@vm01 ~]# auditctl -l
-a always,exit -F arch=b32 -S chmod,lchown,fchmod,fchown,chown,setxattr,lsetxattr,fsetxattr,removexattr,lre-
movexattr,fremovexattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S chmod,fchmod,chown,fchown,lchown,setxattr,lsetxattr,fsetxattr,removexattr,lre-
movexattr,fremovexattr,fchownat,fchmodat -F auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-EPERM -F
auid>=1000 -F auid!=-1 -F key=access
...
```

Listing 2: Auflisten von Audit-Regeln

umfeld ist es – hoffentlich – mittlerweile Standard, starke Regeln für Passwords festzulegen, nicht genutzte DB-Schemata zu sperren und vor allem die Passwords, die noch auf Standardwerten stehen, unmittelbar nach erfolgter Installation zu ändern. Für die Exadata gilt im Grunde das Gleiche, hier übernimmt der **Oracle Exadata Deployment Assistant (OEDA)** diese Aufgabe und

- fügt Regeln für die Password-Komplexität hinzu,
- setzt Passwords auf „abgelaufen“,
- aktiviert die Alterung von Passwords,
- verschärft Berechtigungen.

Weitere Einstellungen können mit dem Skript `host_access_control` vorgenommen werden, das bereits seit Exadata Version 11.2.3.3.0 auf den Datenbank- und Storage-Servern zur Verfügung steht – wenn auch an verdeckter Stelle und nicht sonderlich gut dokumentiert. So wird man auf der Suche nach Informationen eher in der Dokumentation des Sun-Miniclusters fündig oder in der **MOS Note Exadata OL7 System Hardening for STIG Security Compliance (Doc ID 2614471.1)** *(https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=2614471.1)*. Mit dem Kommando `/opt/oracle.cellos/host_access_control apply-defaults --strict_compliance_only` werden strengste Regeln implementiert, so zum Beispiel eine temporäre Account-Sperre nach erfolglosem Anmeldeversuch, eine dauerhafte Sperre nach fünf erfolglosen Anmeldeversuchen, Speichern der Password-Historie über zehn Generationen, Unterbinden eines root-Login, Verschlüsselungsstandards für Server und Client und vieles mehr. *Listing 3* zeigt die Einsatzmöglichkeiten.

Mit den bislang vorgestellten Maßnahmen ist die Sicherheit des Systems bereits auf einem sehr guten Niveau. Jedoch kann es vorkommen, dass auch bei einem optimal konfigurierten Exadata-System Schwachstellen entdeckt werden, für die es noch keine Lösung gibt, sogenannte **Zero-Day-Vulnerabilities**. Um die Verwundbarkeit möglichst gering zu halten, werden mögliche Schwachstellen gescannt. Die MOS Note **How to research Common Vulnerabilities and Exposures (CVE) for Exadata packages (Doc ID 2256887.1)** *(https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=22568871.1)* enthält eine Anleitung zum Auffinden möglicher Schwachstellen. Festgestellte Schwachstellen und deren Behebung sind dann in MOS Note **Responses to common Exadata security scan findings (Doc ID 1405320.1)** *(https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1405320.1)* aufgelistet. Diese Erkenntnisse fließen in die für die aktuellen Versionen monatlich veröffentlichten Exadata Security Updates ein. Kunden sei daher an dieser Stelle dringend empfohlen, stets einen aktuellen Softwarestand einzusetzen.

```
/opt/oracle.cellos/host_access_control -h

Usage: [-q|--quiet] command [argument]
   command is one of:
   access            - User access from hosts, networks, etc.
   access-ilomweb    - Control overall access from the ILOM Web Remote Console device (tty1)
   access-export     - Export access rules to a file
   access-import     - Import access rules via a supplied file
   audit-rules       - Import audit rules via a supplied file
   banner            - Login banner management
   fips-mode         - FIPS mode for openSSH
   grub-password     - GRUB password control
   idle-timeout      - Shell and SSH client idle timeout control
   ilom-configure    - ILOM settings control
   ilom-password     - ILOM root user password control
   kernel-dump       - kdump (kernel dump file creation) control
   maint-password    - Diagnostic ISO shell and Rescue password control
   pam-auth          - PAM authentication settings: pam_tally2 deny and lock_time, passwdqc, and password his-
tory values
   password-aging    - Adjust current users' password aging
   password-policy   - Adjust the system's password age policies
   rootssh           - Root user SSH access control
   sshciphers        - SSH cipher support control
   ssh-listen        - Control the SSHD service optional ListenAddress entries
   ssh-service       - Control the SSHD service and active connections
   sudo              - User privilege control through sudo
   sudodeny          - Manage the Exadata sudo users deny list
   get-runtime       - Maintenance command: import system configuration settings, storing them in host_access_
control parameter settings files.
   restore           - Maintenance command: reapply settings previously set by this utility, as in after an
upgrade
```

Listing 3: Utility host_access_control

Das **National Institute of Standards and Technology (NIST)** hat in der Auflistung **Common Vulnerabilities and Exposures (CVE) IDs** *(https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&pub_start_date=01%2F01%2F2020&pub_end_date=12%2F31%2F2020)* für 2020 eine unglaubliche Zahl von 18352 CVEs offengelegt! Das sind 50 pro Tag, deren Gefahrenpotenzial Exadata-Betreiber durch den Einsatz geprüfter SW_Images und monatlicher Releases abfedern können. Die Auswirkung der ständigen Korrektur aufgedeckter CVEs zeigt *Abbildung 3* für den Lebenszyklus von Exadata 20.1.x: In jedem neuen Update sind mehr Korrekturen bereits enthalten und so nimmt die Notwendigkeit weiterer

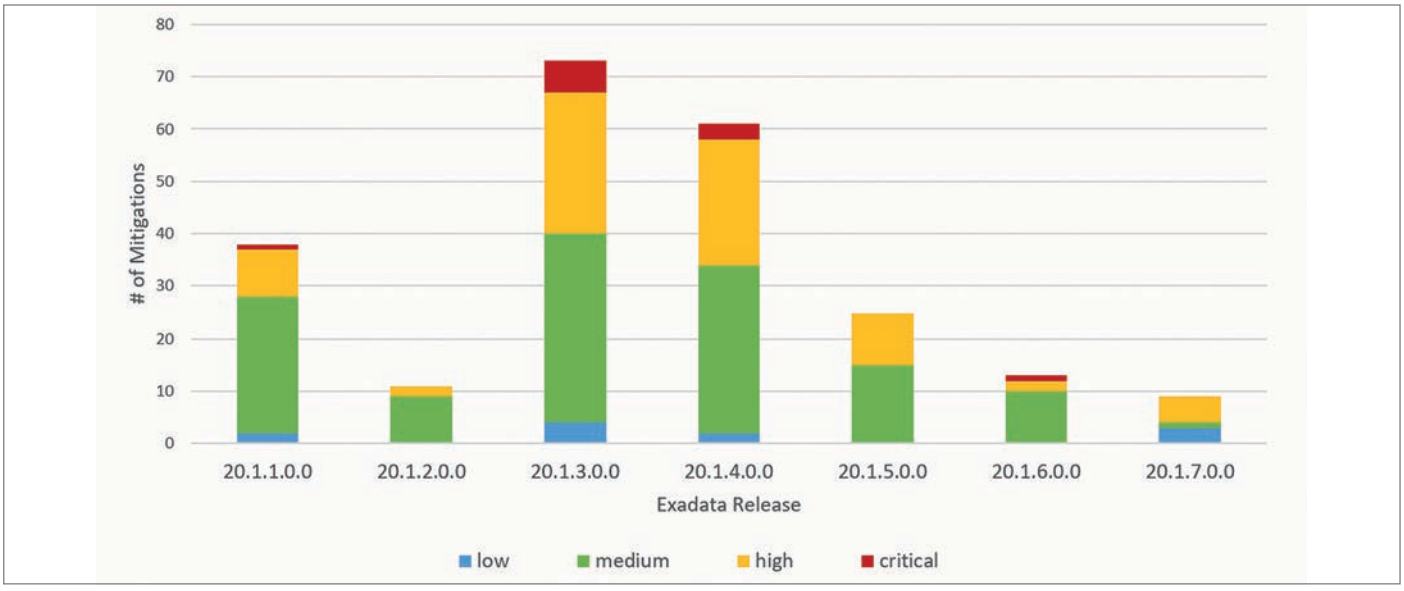


Abbildung 3: Oracle Linux CVE Mitigations für Exadata 20.1.x (Quelle: Frank Schneede)

Korrekturmaßnahmen nach einem anfänglichen Peak deutlich ab.

Durch die vielfältigen Härtungsmaßnahmen liefert der Oracle Linux 7 STIG SCAP Benchmark DomU auf 20.1.0.0.0 einer Exadata X8M einen Score von 90,16%, ausgeliefert quasi direkt ab Werk! Eine normale, standardmäßige Linux-Installation kommt hingegen lediglich auf einen Wert von 31,69%, ein Wert, der für Produktionssysteme so mit Sicherheit nicht akzeptabel ist!

Security Features in der Exadata Software

Mit Exadata Version 20.1 ist eine **Secure RDMA Fabric Isolation for RoCE** verfügbar *(siehe Abbildung 4)*. In einer virtualisiert aufgesetzten Maschine, deren internes Netzwerk über **RoCE (RDMA over Converged Ethernet)** läuft, besteht die Möglichkeit, jedem Exadata VM Cluster ein eigenes privates Netzwerk zuzuordnen. Die unterschiedlichen VMs können nicht mehr untereinander kommunizieren, der Zugriff auf den gemeinsam genutzten Storage bleibt davon natürlich unberührt. Diese Sicherheit kann nicht umgangen werden, da die Isolation durch die Netzwerkkarte für jedes Paket erzwungen und das Regelwerk automatisch im Hypervisor erstellt wird.

Ab Exadata Software 20.1 wird der **FIPS (Federal Information Processing Standard) 140-2** zur Verschlüsselung unterstützt, eine Einrichtung erfolgt über das bereits oben beschriebene Utility host_access_control. Das hat insbesondere Auswirkungen auf die Kommunikation über ssh, die entsprechende kryptographische Algorithmen verwenden muss.

Alle auf der Exadata laufenden Softwarekomponenten sollen möglichst wenig Angriffsfläche bieten, konsequenterweise kommt seit Exadata Version 20.1 mit der Management Server Application Engine **Eclipse Jetty** eine sehr schlanke Software zum Einsatz. Mit weniger Verbrauch an Systemressourcen, einer Unterstützung nur von Basisfunktionen, die durch weitere Module erweiterbar sind, bietet sie weniger CVE-Schwachstellen und benötigt vor allem keinen dedizierten http-Port für die Konfiguration.

Bereits mit Exadata 19.3 wurden für Exadata Hardware X7 oder neuer sogenannte **Memory Protection Keys** eingeführt. Durch die Aufteilung des Storage Server Software Memory in 16 durch 4 bit gekennzeichnete Farben wird sichergestellt, dass jeder Thread nur auf den Speicher zugreifen kann, der ihm zugeordnet ist, das heißt seine Farbe besitzt. Ein Zugriff auf einen Bereich einer anderen Farbe führt zum Abbruch des Prozesses. Diese Funktion ist standardmäßig aktiviert, ein Tuning ist nicht erforderlich. Ein zusätzlicher **Secure-Computing-Prozess (`seccomp`)** auf dem Storage Server sorgt dafür, dass die durch den Linux Kernel möglichen Systemaufrufe eingeschränkt werden. Die Einschränkung wird durch `seccomp`-Filter (White-List von Systemaufrufen) definiert, die im Rahmen des Upgrades für Cell Server und Offload-Prozesse automatisch installiert werden.

Auch beim Upgrade der Systemsoftware wird durch wechselnd genutzte Partitionen der internen M.2 SSD Volumes sichergestellt, dass bei jedem Upgrade eine vollständige Aktualisierung des Betriebssystems erfolgt. Das Upgrade wird auf der inaktiven Partition ausgeführt, nach vollständiger Installation wird auf dieser Partition gebootet. Durch dieses Vorgehen wird die mögliche Verbreitung infizierter Dateien minimiert, zudem sind die Betriebssystemdaten von den Datenbankdaten schon physikalisch strikt getrennt.

Advanced Intrusion Detection Environment (AIDE) sorgt dafür, dass über

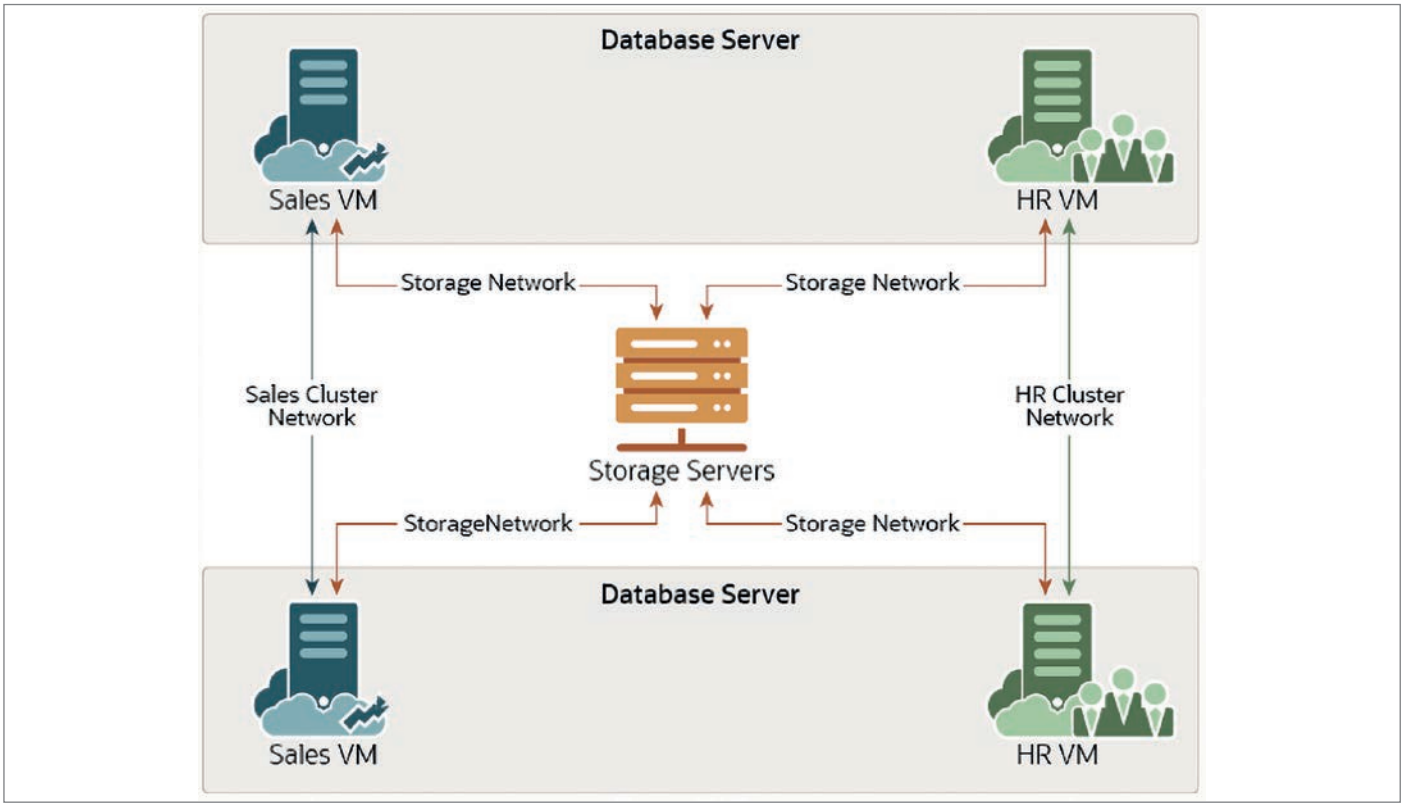


Abbildung 4: Secure RDMA Fabric Isolation mit Exadata 20.1 (Quelle: Frank Schneede)

eine kleine, interne Datenbank aller Dateien auf einem Exadata-System deren Stand und so auch mögliche Veränderungen durch schädlichen Code entdeckt werden können. Die Methode des **Secure Boot** sorgt zusätzlich dafür, dass nur bestimmte Binärdateien beim Bootvorgang des Systems ausgeführt werden können. Mit Secure Boot erlaubt die UEFI-Firmware des Systems nur die Ausführung von Bootloadern, die die kryptografische Signatur von vertrauenswürdigen Entitäten tragen. Bei jedem Neustart des Servers wird jede ausgeführte Komponente verifiziert, was verhindert, dass Malware eingebetteten Code im Boot-Vorgang versteckt.

Als letzten Sicherheitsmechanismus möchte ich die Beschränkung des Zugriffs auf ASM- und Datenbankebene anführen. Auf ASM-Ebene wird sichergestellt, dass der Zugriff nur auf die Grid-Disks möglich ist, die zu den Disk Groups des ASM-Clusters gehören. Analog kann eine Datenbank-Instanz nur auf die Disk Groups zugreifen, die ihr zugeordnet sind.

Fazit

Merksatz: **Die Sicherheit eines Gesamtsystems ist nur so gut wie die Sicherheit des schwächsten Glieds!** Dieser Satz mag wie eine Binsenweisheit klingen, hat aber nach wie vor seine Berechtigung. Angefangen von der Absicherung der Lieferketten bis hin zur Sicherheit auf Datenbankebene haben wir mit der **Exadata Database Machine** eine Plattform für die Oracle-Datenbank, die höchsten Sicherheitsanforderungen genügen **kann**. Das ist natürlich kein Automatismus, sondern muss durch **Sie** als Exadata-Betreiber durch geeignete Betriebsprozesse und organisatorische Maßnahmen wie physikalischen Zugriffsschutz sichergestellt werden:

- Führen Sie daher **regelmäßige Scans** des Systems durch, um Abweichungen vom Auslieferungsstandard zu erkennen.
- Spielen Sie regelmäßig die **neuesten Software Updates** ein, um die letzten Sicherheitslücken zu schließen.
- **Tools und Prozesse** sind dazu da, die Schaffung einer sicheren Umgebung zu unterstützen, aber sie müssen auch genutzt werden, um die sichere Umgebung tatsächlich zu schaffen

Wenn all diese Verfahren und Best Practices eingehalten werden, dann kann man mit Fug und Recht von einer **Maximum Security Architecture** auf Basis der Exadata sprechen.

Weiterführende Informationen

- *https://www.oracle.com/corporate/security-practices/*
- *https://www.oracle.com/technetwork/topics/security/alerts-086861.html*
- *https://blogs.oracle.com/security/*
- *https://docs.oracle.com/en/engineered-systems/exadata-database-machine/books.html*

Frank Schneede
Frank.Schneede@oracle.com

Oracle Datenbanken Monthly News

DOAG Online

Auf dem deutschsprachigen Oracle-Blog ist die Juli-Ausgabe der News-Serie erschienen.

Das Redaktionsteam von Oracle Deutschland hat wieder Neuigkeiten rund um die Datenbank zusammengetragen und in einem rund 15-minütigen Video sowie einem dazugehörigen PDF aufbereitet. Die aktuelle Ausgabe *(https://blogs.oracle.com/coretec/oracle-datenbanken-monthly-news%3a-juli-ausgabe)* wird von Wolfgang Thiem präsentiert und beinhaltet Produkt-Ankündigungen, Release-Stände und Patches sowie Veranstaltungstermine und eine Link-Sammlung zu interessanten Beiträgen aus dem Web.

Oracle IDM einmal anders: Self-Service-Autorisierung für die Datenbank

Thomas Petrik und Wolfgang Klinger, Sphinx IT Consulting

Freiheit für die DBAs! Self-Service-Provisionierung mit Genehmigung durch die Fachabteilung oder auch vollständig automatisierte Provisionierung ersparen den DBAs zeitraubende Provisionierungstätigkeiten. Ermöglicht wird das durch vorkonfiguriertes Oracle Identity Management im Zusammenspiel mit einem Security API in der Datenbank. Der Aufwand für Installation und Inbetriebnahme von Oracle Identity Management wird dabei auf ca. 90 Minuten reduziert. Wie das geht? Durch Lieferung der fertigen Installation in Docker-Containern.

End-User fordern im Self Service Zugangsberechtigungen an, die über sichere Genehmigungsworkflows automatisch implementiert werden. Die Genehmigung kann innerhalb der Fachabteilung erfolgen, die den Bedarf am besten beurteilen kann. Bei sensitiven Anforderungen können Sicherheitsbeauftragte in den Workflow eingebunden werden. In jedem Fall entlastet das die DBAs und beschleunigt die Berechtigungsvergabe enorm. Out of the box ist das mit SCURTY Plus für die Oracle Database Enterprise Edition realisiert.

SCURTY Plus ist eine Komplettlösung, um Zugriffsrechte für Oracle-basierte Anwendungen zu gewähren, zu verwalten und zu entziehen. Der Aufwand für die Berechtigungsvergabe wird dabei enorm reduziert, aber trotzdem kommen deutlich mehr sicherheitsrelevante Funktionen der Datenbank zur Anwendung als sonst üblich. Berechtigungen werden per Mausklick oder vollständig automatisiert bis auf Zeilen- und Spaltenebene vergeben. Die technische Implementierung der Berechtigungsvergabe erfolgt über ein API im Hintergrund. Genutzt werden dabei so ziemlich alle Sicherheits-Features der Oracle Database Enterprise Edition, allerdings absolut ohne den üblicherwei-

se damit verbundenen Aufwand: Virtual Private Database (VPD), Secure Application Roles, Proxy Authentication, Secure Application Context und Database Triggers. Es ist jedoch nicht nötig, sich mit diesen Features zu befassen, um SCURTY Plus anwenden zu können. Die Features erfüllen vollständig gekapselt im Hintergrund ihren Job.

Weniger Administration bei mehr Sicherheit

Endanwender kennen ihre Anforderungen, die Abteilung genehmigt sie und möglicherweise möchte ein Sicherheitsbeauftragter noch einen Blick auf die Anforderungen werfen, bevor der Zugriff tatsächlich gewährt wird. Sonst sollte keine weitere Person involviert sein. Es sind auch keine zusätzlichen Maßnahmen oder die Unterstützung der IT-Abteilung erforderlich. Das reduziert Zeit und Aufwand auf ein absolutes Minimum und befreit das technische Personal von sich wiederholenden Aufgaben.

Abbildung 1 zeigt den Self Service Home Screen nach dem Login.

Es geht allerdings nicht nur um Reduktion der Administration, sondern auch um ein Anheben der Sicherheit. Die Einschränkung des Zugriffs auf jene Daten, die auch wirklich benötigt werden, ist mit wenig Aufwand realisierbar. Der größere Aufwand ist dabei, zu überlegen, welche Daten das sind und wie diese identifiziert werden können. Die Implementierung der Zugriffsbeschränkungen ist dann relativ rasch erledigt.

Zugriffssteuerung im Hintergrund

Ermöglicht wird das durch SCURTY (ohne „Plus"), das in der Datenbank installiert wird. SCURTY realisiert die vollständige Automatisierung der Sicherheits-Features in der Oracle Database Enterprise Edition. Dadurch wird die Komplexität der Funktionen komplett verborgen und der Einsatz höherer Sicherheits-Levels in Bezug auf Authentifizierung und Datenzugriff ermöglicht. Die Reduktion des administrativen Aufwands macht die Sicherheits-Features oftmals erst verwendbar. Die nötigen Policies, Rollen und anderen Datenbank-Objekte werden von SCURTY im Hintergrund automatisch generiert und verwaltet. Eine manuelle Wartung dieser Objekte entfällt komplett, weshalb kein Detailwissen über die dahinterliegenden Funktionen wie VPD, Proxy Authentication etc. existieren muss.

SCURTY enthält ein komfortables PL/SQL-API, über das alle Definitionen vorgenommen werden können. Und genau hier setzt SCURTY Plus an: In der grafischen Oberfläche werden Zugriffsrechte definiert, die über einfache API-Aufrufe an SCURTY weitergeleitet und damit in der Datenbank implementiert werden.

Eine detailliertere Beschreibung von SCURTY finden Sie im Red Stack Magazin vom April 2020 (Ausgabe Nr. 3, Seite 62) unter dem Titel „Spielerisch leichte Security für Oracle-Datenbanken – komplexe Oracle Features genial einfach nutzen".

SCURTY Plus fügt der radikalen Reduktion des administrativen Aufwands für Berechtigungsvergabe durch SCURTY eine komfortable Benutzeroberfläche, Self-Service-Funktionalität mit Genehmigungs-Workflow, automatische Synchronisation mit Benutzerverzeichnissen und viele andere Funktionen hinzu.

Alle diese Vorteile sind sowohl in 2- und 3-Tier-Architekturen als auch lokal oder in der Cloud verfügbar.

Personalisierte Zugriffe

SCURTY Plus und SCURTY ermöglichen durchgängig personalisierte User-Zugriffe. Erst durch Zuordnung von Accounts zu

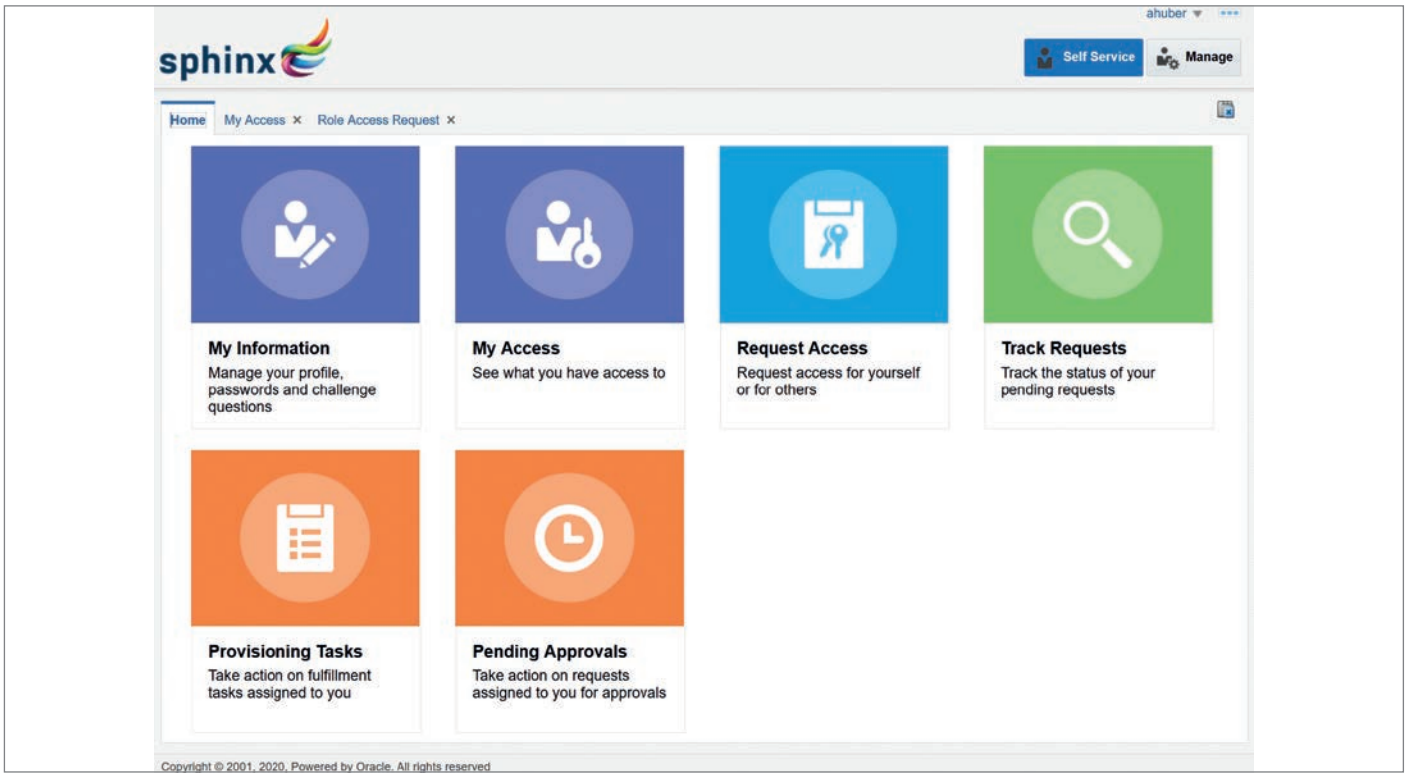


Abbildung 1: SCURTY Plus Home Screen (Quelle: Wolfgang Klinger)

Personen können Berechtigungen gezielt vergeben werden und der Audit Trail enthält sinnvolle Informationen.

Technische Applikations-User können weiterverwendet werden, aber mittels Application Context und Proxy Authentication wird die Information über die Person an die Datenbank geliefert. Dafür muss die Applikation die Identität der Person hinter einem möglicherweise generischen Account an die Datenbank weiterreichen. Fast alle Applikationen haben dafür Mechanismen wie Prozeduraufrufe beim Start einer Session vorgesehen. Erfreulicherweise reichen immer mehr Applikationen die Identität der User von sich aus, also ohne zusätzlichen Call, weiter.

Nur in ganz speziellen Fällen sollen generische User verwendet werden, beispielsweise bei Batch-Prozessen oder Zugriffen durch externe Systeme.

Die Welt außerhalb der Datenbank

Die Vergabe von Zugriffsberechtigungen für andere Systeme als die Oracle-Datenbank, wie zum Beispiel analytische Tools und andere Applikationen, kann mit etwas Consulting-Aufwand ebenfalls leicht integriert werden. Für diesen Zweck gibt es eine Reihe vorgefertigter Connectoren für verschiedene Zielsysteme. Sind die Applikationen an SCURTY Plus angebunden, stehen sie für die Provisionierung auch sofort zur Verfügung.

Drei Wege für die Provisionierung

Es gibt drei unterschiedliche Möglichkeiten, die Berechtigungsvergabe in SCURTY Plus zu nutzen:

- End-User Self Service mit Genehmigungsworkflow über die grafische Oberfläche
- Zuteilen der Rechte durch Administrator*innen über die grafische Oberfläche
- Vollständige Automatisierung durch Anlieferung von User-Daten etwa aus einem HR-System oder einem Directory Service

End-User Self Service mit Genehmigungsworkflow

Zunächst werden Gruppen von Zugriffsrechten in sogenannten Anwendungen zusammengefasst. End-User loggen sich danach in die grafische Oberfläche ein und fordern Zugriff auf die Anwendung an, die sie benötigen *(siehe Abbildung 2)*. Durch das Absenden der Anforderung wird ein Genehmigungsworkflow gestartet, der bei positivem Abschluss die automatisierte Vergabe der Berechtigungen bewirkt. Out of the box wird ein einstufiger Workflow mitgeliefert, es können aber praktisch beliebig komplexe Workflows eingerichtet werden. Zum Beispiel können mehrere Schritte parallel und/oder nacheinander ablaufen.

Zuteilen der Rechte durch Administrator*innen über die grafische Oberfläche

Auch die altbekannte Methode existiert: Mit den entsprechenden Berechtigungen ausgestattet können Super-User über die

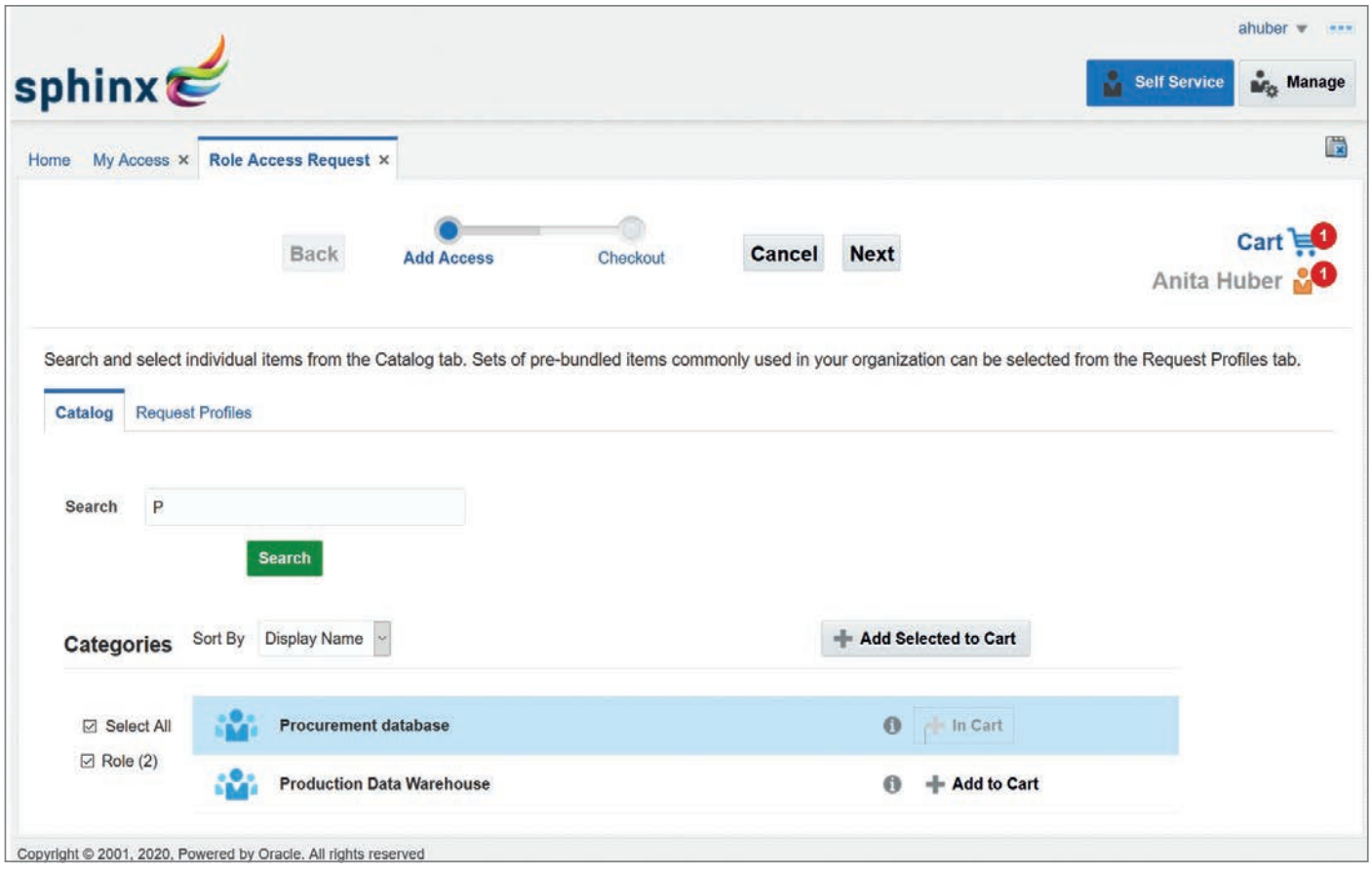


Abbildung 2: Anforderung von Zugriffsrechten im Self Service (Quelle: Wolfgang Klinger)

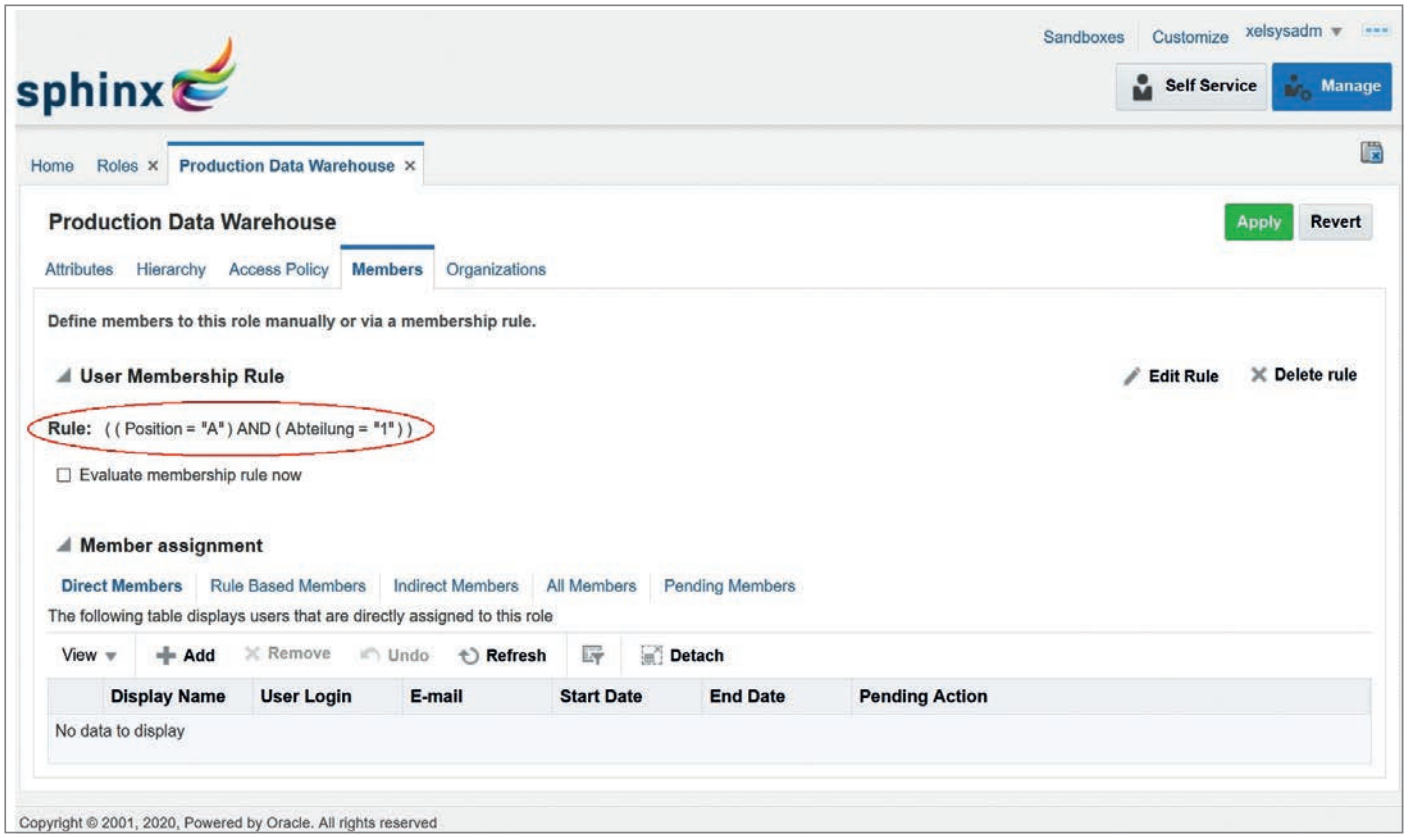


Abbildung 3: Automatische Zuweisung von Rollen über Regeln (Quelle: Wolfgang Klinger)

grafische Oberfläche direkt Zugriffrechte erteilen oder auch User anlegen. Und natürlich auch wieder entfernen.

Vollständige Automatisierung durch Anlieferung von User-Daten zum Beispiel aus einem HR-System

Nach der Installation von SCURTY Plus ist die Synchronisation von User-Daten über eine View vorkonfiguriert. Wenn hier Daten angeliefert werden, können daraus User-Accounts automatisiert in SCURTY Plus erstellt werden. User können sich danach in SCURTY Plus einloggen und Berechtigungen anfordern oder Super-User können den Accounts Berechtigungen zuteilen.

Die vollständige automatisierte Verwaltung von User-Berechtigungen ist mit etwas Zusatzaufwand ebenfalls möglich. Hier werden zunächst Informationen zur Organisation des Unternehmens in elektronischer Form benötigt. Dazu zählen unter anderem vorhandene Job-Positionen, Abteilungen, Niederlassungen und dergleichen. Die User-Daten müssen um Informationen zu Job-Position, eventuellen zusätzlichen Funktionen, Abteilungszugehörigkeit etc. ergänzt werden. Gibt es eine bestehende Benutzerverwaltung, ist es naheliegend, diese als Quelle zu verwenden. Beispiele für solche Quellen sind eine Personal-Datenbank oder das Microsoft Active Directory. Anschließend kann ein einfaches Regelwerk in SCURTY Plus erstellt werden, das aus den vorhandenen Informationen die zu provisionierenden Berechtigungen ableitet und implementiert.

Ein Beispiel für so eine Regel *(dargestellt auch in Abbildung 3)*: Position A in Abteilung 1 benötigt Zugriff auf Kundendaten der Region X, wobei sensitive Spalten ausgeblendet werden sollen. Gleichzeitig muss voller Zugriff auf System Y und Zugriff auf spezifische Inhalte aus System Z möglich sein. Klingt kompliziert, lässt sich aber leicht abbilden.

Regelmäßige, automatisierte Synchronisation sorgt für die Übernahme der Daten und die vollautomatische Implementierung der entsprechenden Zugriffsrechte in den Zielsystemen.

Die Anlieferung der Informationen kann in Form von Tabellen, Views oder Dateien (z.B. CSV als „external Table“) erfolgen.

Auch bei Verwendung der vollständig automatisierten Berechtigungsvergabe können zusätzlich manuell oder im Self Service Berechtigungen vergeben werden.

Die Software hinter SCURTY Plus

Die SCURTY Plus Workflow-Engine verwendet im Hintergrund eine vollständige Installation des Oracle Identity Manager (OIM) mit eingeschränkter Lizenz. Daher kann SCURTY Plus einfach per Lizenz-Upgrade als End-to-End-Lifecycle-Management-System für ALLE Benutzeridentitäten in ALLEN Unternehmensressourcen (Oracle und/oder andere Systeme) verwendet werden. Alle Vorteile eines Identity-Management-Systems (IDM) können genutzt werden – ohne die technischen Probleme, die normalerweise mit der Einführung von IDM in einem Unternehmen verbunden sind.

Erleichterung beim IT-Personal

Die Installation von SCURTY Plus ist einfach, da es sich um fertig vorbereitete Docker-Container handelt. Die komplet-

te, umfangreiche Installation des Oracle Identity Manager inklusive des Elastic Stack für die Auswertungen der Logs wurde vor der Lieferung von SCURTY Plus schon durchgeführt. Es fehlt nur noch die kundenspezifische Konfiguration, die im SCURTY Plus Installation Guide beschrieben ist. Die Installation und Konfiguration dauert ca. 90 Minuten.

Reporting

SCURTY ermöglicht jederzeit Einblick in vorhandene und historische Zugriffsberechtigungen. Das SCURTY Dictionary liefert die Information darüber, welche Objekte, Zeilen und Spalten für welche Personen zu welchem Zeitpunkt verfügbar waren oder es aktuell sind. Für die historischen Daten wird das Flashback Archive der Datenbank verwendet. Der zu bewahrende Zeitraum ist dabei natürlich einstellbar.

Auch die Änderungen in der Oberfläche SCURTY Plus sind über die Zeit nachvollziehbar. Eine optionale, zusätzliche Berichts-Engine steht dafür zur Verfügung.

Fazit

SCURTY Plus ist eine Komplettlösung, um Zugriffsrechte für Oracle-basierte Anwendungen bis auf Zeilen- und Spaltenebene zu gewähren, zu verwalten und zu entziehen. Die Hauptmerkmale der Lösung sind

- Berechtigungsvergabe im Self Service mit einem sicheren Workflow dahinter sowie
- die Möglichkeit zur vollständigen Automatisierung durch Anwenden von Regeln.

Daraus resultieren die beiden wesentlichsten Vorteile von SCURTY Plus: die drastische Reduktion des administrativen Aufwands für Berechtigungsvergabe und die gleichzeitige Erhöhung des erreichten Sicherheitsniveaus. SCURTY Plus und SCURTY sind Produkte der Sphinx IT Consulting GmbH.

Wolfgang Klinger
wolfgang.klinger@sphinx.at

Thomas Petrik
thomas.petrik@sphinx.at

Privilege Analysis in der Oracle-Datenbank

Du bekommst nur das, was du wirklich brauchst!

Markus Flechtner, Trivadis Germany

Welche Rechte braucht ein Datenbank-Benutzer wirklich? Eine einfache Frage, der allerdings in der Vergangenheit meist nur wenig Beachtung geschenkt wurde. Funktionalität hatte Priorität, Sicherheit war zweitrangig. Aber die Sicherheit von Datenbanken und Datenbank-Anwendungen wird immer wichtiger und auch sonst kommt diese Frage wieder auf die Tagesordnung. Bei der Beantwortung hilft das Oracle-Feature „Privilege Analysis".

Jede Anwendung, jeder Benutzer soll nur die Rechte bekommen, die für die Erfüllung der jeweiligen Aufgabe notwendig sind. Dieses Prinzip, „Least-Privilege-Prinzip" genannt, im Original „Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.", wurde erstmals von Jerome Saltzer in den 1970ern formuliert *[1]*. Leider wird dieses Prinzip im Alltag nicht immer beachtet. Installationsskripte von Software-Herstellern beginnen mit dem Befehl „GRANT DBA TO .." oder die internen Entwickler fordern erst mal ein ganzes Paket an Rechten. Die Analyse, welche davon wirklich benötigt werden, entfällt oder wird vergessen. Kurz gesagt: Dieser Aspekt der Datenbank-Sicherheit ist in der Vergangenheit oft zu kurz gekommen.

„Privilege Analysis" hilft nun, diese Versäumnisse der Vergangenheit zu korrigieren und dem „Least-Privilege-Prinzip" näher zu kommen, denn es hilft, die folgenden Fragen zu beantworten:

- Welche Rechte hat ein Benutzer (bzw. eine Applikation) bei der Verwendung einer Anwendung mindestens einmal benötigt und wie hat er dieses Recht bekommen?
- Welche Rechte hat ein Benutzer bekommen, die aber nicht benötigt werden?

Privilege Analysis hat Oracle mit der Datenbank-Version 12c Release 1 (12.1) eingeführt. Leider gab es damals einen lizenztechnischen Haken: Das Feature war mit Database Vault verknüpft, einer Option, die nur die wenigsten Kunden lizenziert haben. Erst im November 2018 hat Oracle die Lizenzierungsbedingungen geändert und Privilege Analysis für alle Kunden der Enterprise Edition verfügbar gemacht. Nutzer der Datenbank Standard Edition 2 können – wenn sie ihre Datenmenge auf 12 GB oder weniger reduzieren können – für die Tests auf die Express Edition der Datenbank (Oracle 18c XE) ausweichen, denn auch dort ist Privilege Analysis dabei.

Was stellt Oracle zur Verfügung?

Für die Analyse der benötigten Rechte stellt Oracle ein Framework bereit, das aus einem Package (DBMS_PRIVILEGE_CAPTURE) und einer Menge von Data Dictionary Views (DBA_USED%-Views und. DBA_UNUSED_%-Views) besteht. Damit man dieses Framework nutzen kann, muss dem entsprechenden Datenbank-Benutzer die Rolle CAPTURE_ADMIN zugewiesen werden.

Die Prozeduren des Packages DBMS_PRIVILEGE_CAPTURE beschreiben grob den Ablauf einer Analyse *(siehe Tabelle 1)*.

Die **Data-Dictionary-Tabellen und -Views** finden sie in *Tabelle 2* und die **Ergebnis-Views** in *Tabelle 3*.

Die Views mit dem „PATH" im Namen geben dabei auch den Grant-Pfad an, das heißt, es wird ersichtlich, über welche gegebenenfalls verschachtelten Rollen ein Benutzer ein Recht bekommen hat.

Im Rahmen einer derartigen Analyse wird zwar nicht protokolliert, wann genau eine gewisse Aktion erfolgt ist beziehungsweise wann ein bestimmtes Recht erforderlich war, aber insbesondere bei personalisierten Accounts können aus den Analysen Rückschlüsse auf das Be-

Prozedur	Verwendungszweck
CREATE_CAPTURE	Definieren einer Policy
ENABLE_CAPTURE	Aktivieren der Datensammlung
DISABLE_CAPTURE	Beenden der Datensammlung
GENERATE_RESULT	Übertragen der gesammelten Daten in das Data Dictionary
DROP_CAPTURE	Löschen einer Policy inkl. der gesammelten Daten
DELETE_RUN	Löschen eines einzelnen Durchlaufes inkl. der gesammelten Daten
CAPTURE_DEPENDENCY_PRIVS	Sammelt Rechte, die bei der Kompilierung von PL/SQL-Objekten (definer's and invoker's rights) erforderlich sind.

Tabelle 1: Prozeduren des Packages DBMS_PRIVILEGE_CAPTURE

Tabelle/View	Inhalt
DBA_PRIV_CAPTURES	Zeigt die vorhandenen Policies und die Testläufe
PRIV_CAPTURE$	(Grundlage für DBA_PRIV_CAPTURES)
CAPTURED_PRIV$	Genutzte Rechte, Grundlage für die Ergebnis-Views
CAPTURE_RUN_LOG$	Informationen über die durchgeführten Testläufe, inkl. Start- und Ende-Zeitpunkt

Tabelle 2: Data-Dictionary-Tabellen und -Views

nutzerverhalten gezogen werden. Daher kann es ratsam sein, vorher den Betriebsrat zu kontaktieren. Stichwort: Überwachung der Mitarbeiter.

Der Arbeitsablauf

Zuerst muss mittels CREATE_CAPTURE eine Policy definiert, also festgelegt werden, was protokolliert werden soll *(siehe Listing 1 und 2)*. Dafür gibt es vier Möglichkeiten:

1. Protokollierung aller Aktivitäten in der Datenbank (Type G_DATABASE)
2. Protokollierung aller Aktivitäten, für die eine bestimmte Rolle benötigt wird (G_ROLE)
3. Protokollierung auf Basis eines Kontextes (SYS_CONTEXT) (G_CONTEXT)
4. Kombination von Rolle und Kontext (G_ROLE_CONTEXT)

Für die Einschränkungen des Kontextes können alle Möglichkeiten der Funktion SYS_CONTEXT genutzt werden, wie zum Beispiel:

- SESSION_USER (angemeldeter Datenbank-Benutzer, siehe Beispiel)
- HOST (Rechner, von dem aus der Befehl aufgerufen wurde)
- OS_USER (Betriebssystembenutzer, der den Befehl aufgerufen hat)
- MODULE und ACTION (via DBMS_APPLICATION_INFO)

Eigene Kontexte können über DBMS_SESSION.SET_CONTEXT definiert werden.

Bevor die Tests gestartet werden, muss die jeweilige Policy aktiviert werden *(siehe Listing 3)*. Es gilt, dass pro Policy immer nur ein „Run" aktiv sein darf und dass immer nur eine auf Rolle oder Kontext basierende Rolle aktiv sein darf. Allerdings darf eine datenbankweite Sammlung zusätzlich gleichzeitig genutzt werden.

Der Parameter „run_name" ist optional, aber empfehlenswert, insbesondere wenn für eine Policy mehrere Testläufe durchgeführt werden sollen.

Sobald eine Policy aktiviert ist, können die Tests beziehungsweise Benutzeraktivitäten beginnen. Dabei ist wichtig, umfassend zu testen, damit nicht irgendeine Funktion vergessen wird, die besondere Rechte benötigt. Bei einer späteren Redu-

Views für genutzte Rechte	Views für vergebene, aber nicht genutzte Rechte
Überblick (alle Rechte)	
DBA_USED_PRIVS	DBA_UNUSED_PRIVS
Public-Rechte	
DBA_USED_PUBPRIVS	DBA_UNUSED_PUBPRIVS
System-Rechte	
DBA_USED_SYSPRIVS	DBA_UNUSED_SYSPRIVS
DBA_USED_SYSPRIVS_PATH	DBA_UNUSED_SYSPRIVS_PATH
Objekt-Rechte	
DBA_USED_OBJPRIVS	DBA_UNUSED_OBJPRIVS
DBA_USED_OBJPRIVS_PATH	DBA_UNUSED_OBJPRIVS_PATH
User-Rechte	
DBA_USED_USERPRIVS	DBA_UNUSED_USERPRIVS
DBA_USED_USERPRIVS_PATH	DBA_UNUSED_USERPRIVS_PATH

Tabelle 3: Ergebnis-Views

```
Procedure DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE
Argument Name    Type               In/Out  Default?
 ---------------- ------------------ ------ --------
 NAME             VARCHAR2           IN
 DESCRIPTION      VARCHAR2           IN     DEFAULT
 TYPE             NUMBER             IN     DEFAULT
 ROLES            ROLE_NAME_LIST     IN     DEFAULT
 CONDITION        VARCHAR2           IN     DEFAULT
```

Listing 1: Definition der Prozedur CREATE_CAPTURE

```
REM policy to capture all database activities
execute DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
   name => 'POLICY_ALL_DB_ACTIVITIES',
   description =>'captures all database privileges',
   type => DBMS_PRIVILEGE_CAPTURE.G_DATABASE
   );

REM which DBA privileges are used by a specific user
execute DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
   name => 'POLICY_CAPTURE_SCOTT_DBA',
   description =>'captures all required privileges granted to public',
   type => DBMS_PRIVILEGE_CAPTURE.G_ROLE_AND_CONTEXT,
   roles => 'DBA',
   condition=> q'[sys_context('USERENV','SESSION_USER') = 'SCOTT']'
   );
```

Listing 2: Beispiele für die Definition von Policies

```
Execute DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE(
 name => 'POLICY_CAPTURE_SCOTT',
 run_name => 'TEST_RUN_20191110');
```

Listing 3: Aktivieren einer Policy

zierung der Rechte auf Basis der „Privilege Analysis“ würde diese Funktion sonst nicht mehr fehlerfrei laufen. Wenn Sie ein komplettes Set von automatisierten Tests für Ihre Applikation haben, dann spielen Sie alle Tests einmal durch. Nach meinen Erfahrungen ist der Einfluss von Privilege Analysis auf die Datenbank-Performance sehr gering, sodass eine derartige Analyse auch in einem Produktionssystem durchgeführt werden kann.

Wenn die Tests abgeschlossen sind, dann kann die Policy, wie in *Listing 4* dargestellt, deaktiviert werden.

```
Execute DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE(
 name => 'POLICY_CAPTURE_SCOTT');
```

Listing 4: Deaktivieren einer Policy

```
 Execute DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT (
 name => 'POLICY_CAPTURE_SCOTT',
 run_name => 'TEST_RUN_20191110');
```

Listing 5: Schreiben der gesammelten Daten in die Datenbank

```
SQL> select USED_ROLE,SYS_PRIV,PATH
  2   from DBA_USED_SYSPRIVS_PATH
  3   where CAPTURE='POLICY_CAPTURE_SCOTT'
  4   and RUN_NAME= 'TEST_RUN_20191110';
USED_ROLE     SYS_PRIV            PATH
------------  -----------------  --------------------------------
SECRET        SELECT ANY TABLE   GRANT_PATH('SCOTT', 'SECRET')
SECRET        ANALYZE ANY        GRANT_PATH('SCOTT', 'SECRET')
CONNECT       CREATE SESSION     GRANT_PATH('SCOTT', 'CONNECT')
```

Listing 6: Beispielabfrage auf DBA_USED_SYSPRIVS_PATH

```
SQL> SELECT 'grant '||sys_priv||' to SCOTT_ROLE;' GRANT_PRIV
  2   FROM DBA_USED_PRIVS where SYS_PRIV not like '%ANY%'
  3   and CAPTURE='POLICY_CAPTURE_SCOTT'
  4   and RUN_NAME= 'TEST_RUN_20191110';
```

Listing 7: Generieren der gemäß Analyse erforderlichen System-Rechte

```
SQL> SELECT DISTINCT 'grant '||
  2   CASE SYS_PRIV
  3       WHEN 'SELECT ANY TABLE' THEN 'SELECT'
  4       WHEN 'EXECUTE ANY PROCEDURE'THEN 'EXECUTE'
  5           WHEN 'INSERT ANY TABLE' THEN 'INSERT'
  6       WHEN 'UPDATE ANY TABLE' THEN 'UPDATE'
  7           WHEN 'DELETE ANY TABLE' THEN 'DELETE'
  8           WHEN 'ANALYZE ANY' THEN 'ANALYZE'
  9           WHEN 'SELECT ANY SEQUENCE' THEN 'SELECT'
 10       ELSE
 11           OBJ_PRIV
 12           END
 13   ||' on '||OBJECT_OWNER||'.'|| OBJECT_NAME||
 14   ' to SCOTT_ROLE;' GRANT_PRIV
 15   FROM DBA_USED_PRIVS where capture='POLICY_CAPTURE_SCOTT'
 16   AND object_name is not null;
```

Listing 8: Generieren der erforderlichen Objekt-Rechte (basierend auf [2])

Wichtig: Zu diesem Zeitpunkt sind die Ergebnisse der Datensammlung noch nicht persistent, sondern nur im Hauptspeicher der Datenbank-Instanz vorhanden.

Das heißt insbesondere, dass beim Absturz der Instanz sämtliche gesammelten Daten verloren gehen.

Erst mit dem Befehl DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT werden die Daten in die Datenbank geschrieben und können dann ausgewertet werden *(siehe Listing 5)*.

Auswertung der Ergebnisse

Oracle stellt leider über die DBA_USED_%- und DBA_UNUSED_%-Views hinaus keine Hilfsmittel bereit, mit denen die Ergebnisse ausgewertet und die Korrekturen implementiert werden können. Hier ist man auf eigene Abfragen angewiesen *(siehe Listing 6)*.

Im Beispiel *(siehe Listing 6)* sieht man, dass der User SCOTT die Rechte „SELECT ANY TABLE“ und „ANALYZE ANY“ über die Rolle „SECRET“ bekommen hat.

Auf Basis der gesammelten Daten können dann GRANT-Befehle generiert werden, mit denen einem Benutzer die benötigten Rechte zugewiesen werden *(siehe Listing 7)*.

Listing 8 wandelt Objekt-Zugriffe, für die im Test „ANY“-Rechte genutzt wurden, in objektspezifische GRANT-Befehle um und macht so die kritischen „ANY-Rechte“ überflüssig.

Hat der Nutzer eigene Views oder PL/SQL-Objekte, die auf fremde Objekte verweisen, so sind direkte Grants erforderlich. In diesem Fall sollten die Abfragen gegebenenfalls mit DBA_DEPENDENCIES verknüpft werden, um solche Abhängigkeiten zu ermitteln.

Privilege Analysis im Oracle Enterprise Manager Cloud Control

Auch mit dem Enterprise Manager kann man Policies definieren, aktivieren und sich die Ergebnisse anzeigen lassen *(siehe Abbildung 2)*. Die in *Abbildung 1* aufgeführte Policy ORA$DEPENDENCY dient dazu, zusätzlich benötigte Rechte für den Zugriff auf Funktionen, Prozeduren etc. zu protokollieren, und sollte bei einer Auswertung nicht vergessen werden.

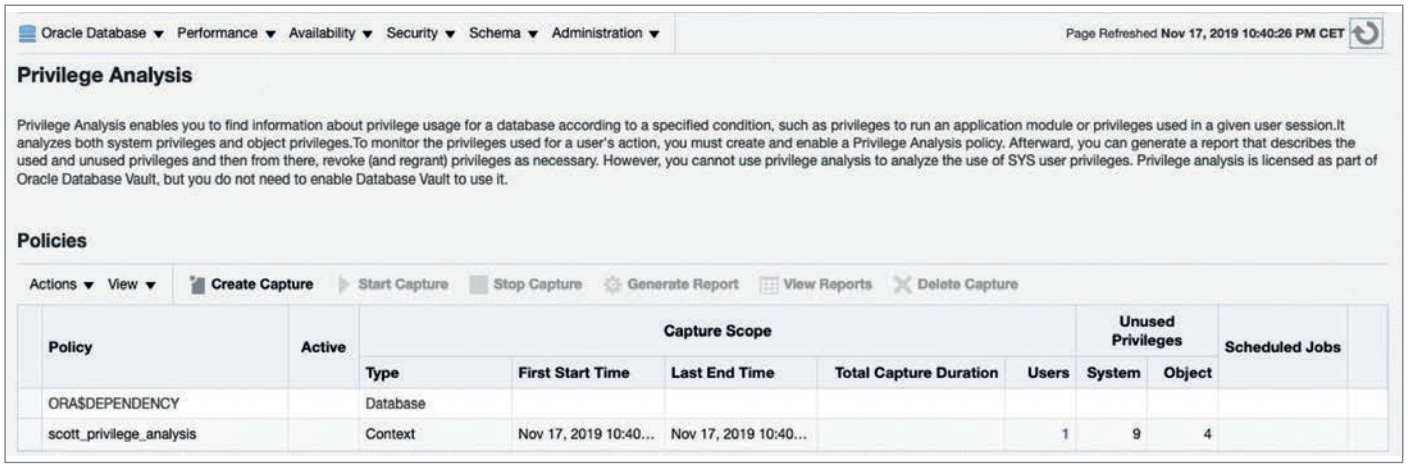


Abbildung 1: Anzeige der vorhandenen Policies im OEM (Quelle: Markus Flechtner)

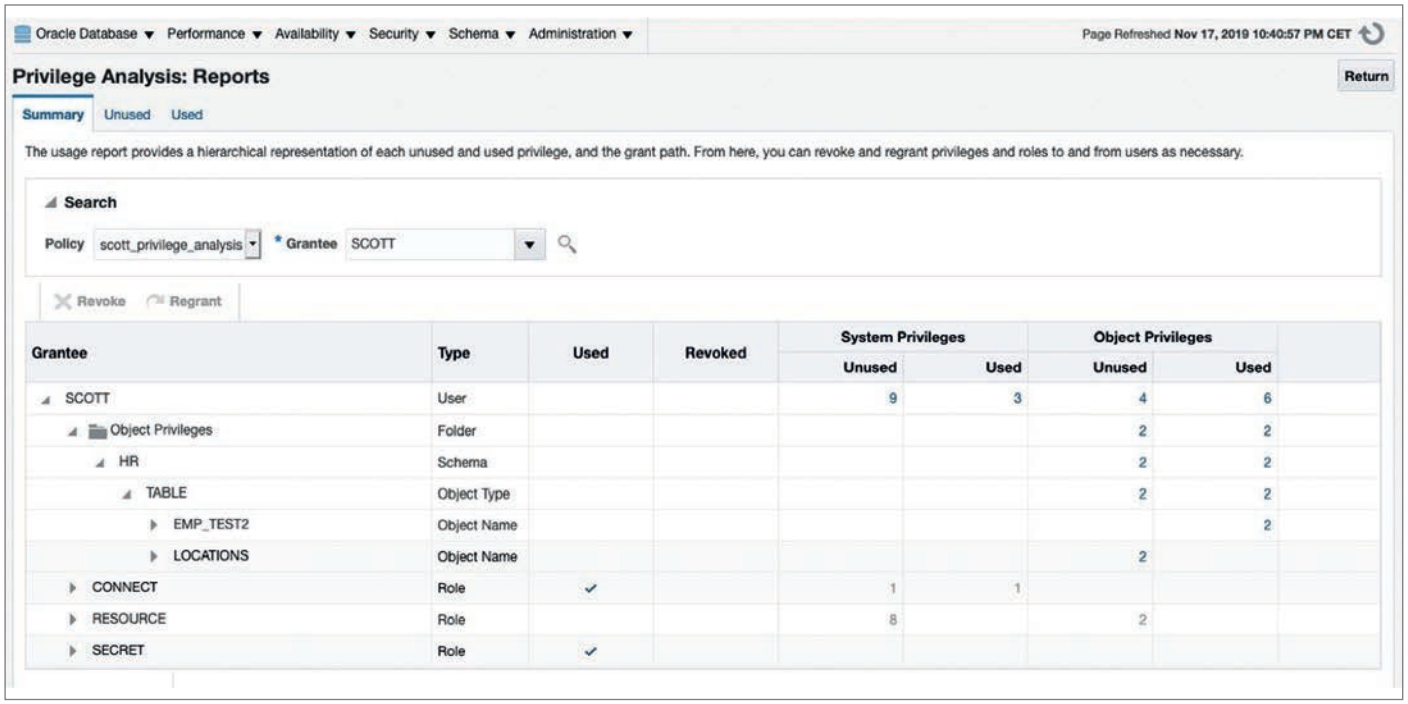


Abbildung 2: Anzeige der Ergebnisse im OEM (Quelle: Markus Flechtner)

Fazit

Privilege Analysis ist ein sehr hilfreiches Werkzeug, um das Least-Privilege-Prinzip für Datenbank-Applikationen zu erreichen. Durch die Änderung der Lizenzierung im November 2018 hat Oracle die Nutzung dieses Werkzeugs erfreulicherweise einem größeren Anwenderkreis ermöglicht.

Privilege Analysis sollte schon in Tests eingesetzt werden, um etwaige Sicherheitslücken frühzeitig zu erkennen. Wesentlich ist aber, dass diese Tests alle Funktionen der Anwendung beinhalten, um wirklich alle benötigten Rechte zu ermitteln.

Quellen und weitere Informationen

[1] Jerry H. Saltzer, Mike D. Schroeder (September 1975). "The protection of information in computer systems". *http://web.mit.edu/Saltzer/www/publications/protection/* Proceedings of the IEEE. 63

[2] Norman Sibbing: Least Privileges mit Privilege Analysis: *https://apex.oracle.com/pls/apex/germancommunities/dbacommunity/tipp/7141/index.html*

[3] Dokumentation zu DBMS_PRIVILEGE_CAPTURE: *https://docs.oracle.com/en/database/oracle/oracle-database/19/arpls/DBMS_PRIVILEGE_CAPTURE.html#GUID-6522AC3E-A457-4C7B-8996-B065957F73E4*

[4] Database Security Guide, Chapter 5 "Performing Privilege Analysis to Find Privilege Use": *https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/performing-privilege-analysis-find-privilege-use.html#GUID-44CB644B-7B59-4B3B-B375-9F9B96F60186*

Über den Autor

Markus Flechtner begann seine Tätigkeit im Oracle-Umfeld in den 1990ern als Software-Entwickler in den Bereichen PL/SQL, Oracle-Forms und Oracle-Reports. Später wechselte der Diplom-Mathematiker in den Oracle Support und spezialisierte sich auf die Tätigkeit als Datenbankadministrator. Seit 2008 ist er als Consultant bei Trivadis. Seine Schwerpunkte sind Oracle-

Hochverfügbarkeit sowie Upgrade- beziehungsweise Migrationsprojekte.

Als Hauptreferent ist er bei Trivadis verantwortlich für die Kurse „Oracle Database New Features für DBAs“, „Oracle Multitenant“ und „PostgreSQL für Oracle-DBAs“; weiterhin ist er Referent für den Kurs „Oracle Real Application Clusters“.

Bei der Deutschen Oracle-Anwendergruppe (DOAG) ist er seit 2015 Delegierter der jährlichen Delegiertenversammlung und seit 2019 verantwortlich für den Themenbereich „Open-Source-Datenbanken“. Er ist Mitautor des Buches „Der Oracle DBA: Handbuch für die Administration der Oracle Database 12c“ und wurde 2020 zum Oracle ACE ernannt.

Markus Flechtner
Markus.flechtner@trivadis.com

Enterprise Grade High Availability mit Patroni

Julia Gugel, dbi services

Mit Patroni steht im Bereich PostgreSQL eine hochverfügbare Open-Source-Lösung mit vielen Vorteilen zur Verfügung. Die kostenlose Lösung fodert allerdings ein gewisses Maß an Bastelfreude, denn sie liefert definitv keine „one-size-fits-all"- oder „plug-and-play"-Lösung. Eine Betrachtung des Setups und der wichtigsten Operationen gibt Aufschluss über die Vor- und Nachteile dieser Lösung, insbesondere für Produktivumgebungen, die nahezu keine Ausfallzeiten erlauben.

Wie oft im Open-Source-Bereich, gibt es für PostgreSQL viele Möglichkeiten für den Aufbau einer hochverfügbaren Lösung. Je nachdem, welche Anforderungen sich an das System ergeben, erweisen sich viele davon als schwer zu implementieren und zu administrieren.

Was ist Patroni?

Patroni ist ein Python-basiertes Open Source Tool, um hochverfügbare PostgreSQL-Cluster zu erstellen und zu administrieren. Entwickelt vom Zalando Tech Team, bewährt es sich auch für große Cluster-Umgebungen. Patroni lässt sich mit einigen Konfigurationsparametern als Backup, Replication und Restore Tool einsetzen und hält im Zusammenspiel mit etcd und HAProxy vielen Anforderungen einer Hochverfügbarkeitslösung stand.

Dabei ist Patroni keine Out-of-the-Box-Lösung, sondern ein Template, das sich an die Bedürfnisse der entsprechenden Umgebung und des Anwenders anpassen lässt.

Aufbau eines Patroni-Clusters

Patroni bietet für den Aufbau eines Clusters eine hohe Flexibilität. Vom einfachen Primary – Replica bis hin zu Primary – n Replicas ist patroniseitig alles möglich. Mein Favorit als optimaler Minimal-Cluster: eine Lösung mit drei Servern, eine Primary und zwei Replica-Datenbanken *(siehe Abbildung 1)*.

Für eine möglichst reibungslose Funktionsweise benötigt Patroni einige Tools:

- Distributed Key Value Store
  Um Patroni als hochverfügbares Cluster zu nutzen, benötigt es einen Distributed Key Value Store. Hierbei stehen etcd, zookeeper und consul zur Auswahl. Seit Version 2.0 kann Patroni auch mit pure Raft installiert werden. Da sich etcd als leicht zu initialisieren und administrieren erwiesen hat, ist es für mich die erste Wahl. Zu beachten: etcd benötigt immer eine ungerade Anzahl von Servern, damit im Falle eines Ausfalls die neue Primary durch ein Quorum gewählt werden kann. Drei Server sind Minimum, nach oben gibt es keine Grenzen, solange die Zahl der etcd-Server ungerade ist.

- Load Balancer
  Eine weitere Komponente für maximale Hochverfügbarkeit: ein Load Balancer. Patroni unterstützt jede Art von Load Balancer und bietet in der Dokumentation eine Konfiguration für HAProxy an, mit dem sich ein „Single Point of Entry" schaffen lässt.

- Watchdog
  Das Schlimmste für einen hochverfügbaren Patroni-Cluster wären Transaktionen, die aufgrund mehrerer Primary-Instanzen verloren gehen. Die Ursachen für dieses „Split-Brain"-Problem liegen unter anderem in einem Patroni Crash, einem zu langsamen Shutdown oder Memory-Problemen. Um dies zu verhindern, muss Patroni gewährleisten, dass PostgreSQL keine Transaktions-Commits annimmt, nachdem der DCS Leader Key abgelaufen ist. Um dies zu garantieren, unterstützt Patroni Watchdog Devices, die ermöglichen, dass beispielsweise das komplette System zurückgesetzt wird, falls in einem vordefinierten Zeitrahmen keine Rückmeldung vom System eingeht. Für die meisten Use Cases ist die im Linux Kernel implementierte Software ausreichend.

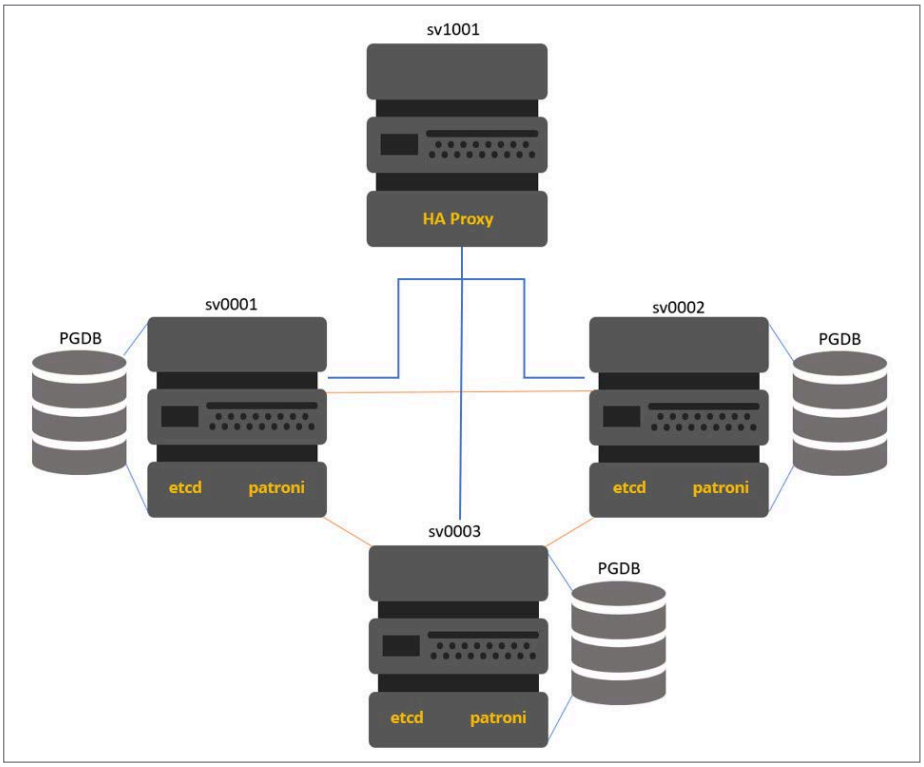


Abbildung 1: Aufbau eines Patroni-Clusters (© Julia Gugel, dbi services)

Setup eines Patroni-Clusters

Das Setup eines Patroni-Clusters ist in wenigen Schritten erledigt. Es kann sowohl aus Packeten im Community Repository als auch manuell installiert werden. Um maximale Flexibilität zu behalten, bevorzuge ich das manuelle Setup. Es benötigt mehrere manuelle Schritte und die Erstellung von Konfigurationsdateien.

In den folgenden Schritten gehe ich von einem Cluster mit drei Knoten aus, auf dem die PostgreSQL Binaries bereits installiert sind. All diese Knoten werden gleich aufgesetzt – mit entsprechender Vorbereitung lässt sich dies mit einem Automatisierungstool umsetzen.

Vorab werden einige Pakete für die Einrichtung von Patroni installiert, diese unterscheiden sich gegebenenfalls – je

```
yum install python3-pip python3-pyyaml bind-utils keepalived haproxy
chrony watchdog
```

Listing 1: Benötigte Packages für Patroni Setup

```
192.168.22.201 Patroni1
192.168.22.202 Patroni2
192.168.22.203 Patroni3
```

Listing 2: /etc/hosts-Datei

```
cd ~
wget https://github.com/etcd-io/etcd/releases/download/v{{etcd_version}}/etcd-v{{ etcd_version }}-linux-amd64.
tar.gz
tar axf etcd-v{{etcd_version}}--linux-amd64.tar.gz
mkdir /u02/pgdata/etcd
chmod 700 /u02/pgdata/etcd
```

Listing 3: Installation etcd

```
name: Patroni1
data-dir: /u02/pgdata/etcd
enable-v2: true

initial-advertise-peer-urls: http://192.168.22.201:2380
listen-peer-urls: http://192.168.22.201:2380
listen-client-urls: http://192.168.22.201:2379,http://localhost:2379
advertise-client-urls: http://192.168.22.201:2379
initial-cluster: patroni1=http://192.168.22.201:2380,patroni2=http://192.168.22.202:2380,patroni3=http:
//192.168.22.203:2380
```

Listing 4: etcd.conf-Datei

```
su -
cat /etc/systemd/system/etcd.service

[Unit]
Description=dbi services etcd service
After=network.target

[Service]
User=postgres
Type=notify
ExecStart=/u01/app/postgres/local/dmk/bin/etcd --config-file /u01/app/postgres/local/dmk/etc/etcd.conf
Restart=always
RestartSec=10s
LimitNOFILE=40000

[Install]
WantedBy=multi-user.target
```

Listing 5: etcd-Service

nach gewähltem Betriebssystem *(siehe Listing 1)*.

Im nächsten Schritt benötigt es Einträge im /etc/hosts-File, hierzu werden alle Cluster-Knoten mit IP ergänzt *(siehe Listing 2)*. Alternativ dazu sind die entsprechenden Einträge im DNS.

Sind die Pakete in *Listing 1* installiert, wird mit der Installation des Key Value Store beziehungsweise etcd fortgefahren. Das Paket für etcd kann dazu von der GitHub-Seite von etcd-io heruntergeladen und anschließend entpackt werden *(siehe Listing 3)*.

All das wird von dem Benutzer gemacht, dem der Cluster später gehört, nicht als root. Wo genau die Binaries entpackt werden, lässt sich individuell entscheiden. Es gibt keinen festen beziehungsweise vorgeschriebenen Platz.

Für die Konfiguration wird die etcd.conf-Datei erstellt *(siehe Listing 4)*.

Dabei muss darauf geachtet werden, dass in Zeile 1 der Hostname des Servers korrekt ist, zum Beispiel patroni1 für Knoten 1, patroni2 für Knoten 2 und so weiter. Die Datei kann an jedem beliebigen Ort abgelegt werden. Ich empfehle, die Berechtigung auf 0600 zu setzen. Anschließend wird der etcd-Service erstellt, in dem die Konfigurationsdatei referenziert wird *(siehe Listing 5)*.

Sobald dieser erstellt ist, wird die systemd-Konfiguration neu geladen und alle benötigten Services können gestartet werden *(siehe Listing 6)*.

Hiermit sind alle Vorbereitungsschritte abgeschlossen, es kann mit der Installation von Patroni selbst gestartet werden. Dies ist vermutlich der heikelste Teil der Installation, da beachtet werden muss, welches Kommando mit welchem Benutzer ausgeführt wird. Sobald es hier zu Verwechslungen kommt, funktioniert die Installation nicht wie gewünscht *(siehe Listing 7)*.

Beim letzten Komando wird angegeben, welcher Key Value Store verwendet wird. Per Default werden die Patroni Binaries im Home-Verzeichnis des Owners unter ~/.local/bin abgelegt. Dieser Pfad sollte dementsprechend in die PATH-Variable mit aufgenommen oder in einen

```
systemctl daemon-reload
systemctl enable etcd
systemctl enable watchdog
systemctl start watchdog
systemctl start chronyd
systemctl start etcd
```

Listing 6: Starten aller benötigten Services

```
sudo su -
python3 -m pip install --upgrade pip
sudo su - postgres
python3 -m pip install --upgrade --user setuptools
python3 -m pip install --user psycopg2-binary
python3 -m pip install --user Patroni[etcd]
```

Listing 7: Installation Patroni

```
scope: PG1
name: patroni1

restapi:
  listen: 192.168.22.201:8008
  connect_address: 192.168.22.201:8008

etcd:
   hosts: 192.168.22.201:2379, 192.168.22.202:2379, 192.168.22.203:2379

bootstrap:
  dcs:
      ttl: 30
      loop_wait: 10
      retry_timeout: 10
      maximum_lag_on_failover: 1048576
      postgresql:
          use_pg_rewind: true
          use_slots: true
          parameters:
              wal_level: 'hot_standby'
              hot_standby: "on"
              wal_keep_segments: 8
              max_replication_slots: 10
              wal_log_hints: "on"
              listen_addresses: '*'
              port: 5432
              logging_collector: 'on'
              log_truncate_on_rotation: 'on'
              log_filename: 'postgresql-%a.log'
              log_rotation_age: '1440'
              log_line_prefix: '%m - %l - %p - %h - %u@%d - %x'
              log_directory: 'pg_log'
              log_min_messages: 'WARNING'
              log_autovacuum_min_duration: '60s'
              log_min_error_statement: 'NOTICE'
              log_min_duration_statement: '30s'
              log_checkpoints: 'on'
              log_statement: 'ddl'
              log_lock_waits: 'on'
              log_temp_files: '0'
              log_timezone: 'Europe/Zurich'
              log_connections: 'on'
              log_disconnections: 'on'
              log_duration: 'on'
              client_min_messages: 'WARNING'
              wal_level: 'replica'
              hot_standby_feedback: 'on'
              max_wal_senders: '10'
              shared_buffers: '128MB'
              work_mem: '8MB'
              effective_cache_size: '512MB'
              maintenance_work_mem: '64MB'
              wal_compression: 'off'
              max_wal_senders: '20'
              shared_preload_libraries: 'pg_stat_statements'
              autovacuum_max_workers: '6'
              autovacuum_vacuum_scale_factor: '0.1'
              autovacuum_vacuum_threshold: '50'
              archive_mode: 'on'
              archive_command: '/bin/true'
              wal_log_hints: 'on'
#         recovery_conf:
#             restore_command: cp ../wal_archive/%f %p
```

Listing 8, Teil 1: patroni.yml

Siehe nächste Seite ->

```
   initdb:
   - encoding: UTF8
   - data-checksums

   pg_hba
   - host replication replicator 192.168.22.0/24 md5
   - host all all 192.168.22.0/24 md5

   users:
       admin:
           password: admin
           options:
               - createrole
               - createdb
       replicator:
           password: postgres
           options:
               - superuser

postgresql:
   listen: 192.168.22.201:5432
   connect_address: 192.168.22.201:5432
   data_dir: /u02/pgdata/13/PG1/
   bin_dir: /u01/app/postgres/product/13/db_2/bin
   pgpass: /u01/app/postgres/local/dmk/etc/pgpass0
   authentication:
       replication:
           username: replicator
           password: postgres
       superuser:
           username: postgres
           password: postgres
   parameters:
       unix_socket_directories: '/tmp'

watchdog:
   mode: automatic
   device: /dev/watchdog
   safety_margin: 5

tags:
       nofailover: false
       noloadbalance: false
       clonefrom: false
       nosync: false
```

Listing 8, Teil 2: patroni.yml

Ordner verlinkt werden, der bereits in der PATH- Variable aufgeführt ist.

Im letzten Schritt werden nun die Patroni-Konfiguration und der Patroni-Service erstellt. Hierzu wird in einem beliebigen Verzeichnis (zum Beispiel / etc/patroni) auf allen drei Servern eine YAML-Datei erstellt. Diese enthält alle notwendigen Details über den Aufbau des etcd-Clusters und auch die Parameter für die PostgreSQL-Instanzen *(siehe Listing 8)*.

Mit der Erstellung des Patroni-Service *(siehe Listing 9)* und anschließendem Start des Service *(siehe Listing 10)* wird der PostgreSQL-Cluster mit den in *Listing 8* konfigurierten Parametern gestartet und die Installation des Patroni-Clusters ist abgeschlossen.

Sobald der Service auf allen (drei) Servern gestartet ist, können der Patroni und der etcd-Status überprüft werden *(siehe Abbildung 2)*.

Patroni Operations

Die wohl wichtigsten Operationen bei einem Patroni-Cluster sind definitiv der Switchover und der Failover. Beide werden mit einem sehr ähnlichen Befehl ausgeführt *(siehe Listing 11)*.

Abbildung 3 gibt eine Übersicht darüber, wie ein Switchover von Node 1 auf Node 2 aussehen kann. Bei einem Reboot des Primary Node wird sofort ein Failover gemacht; der ehemalige Leader wird, sobald er wieder gestartet ist, als neue Replica wieder eingebunden und der WAL (write ahead log) Lag sollte nicht zu groß sein.

Patroni – „Enterprise Grade"?

Was genau macht Patroni jetzt aber zu der Open-Source-Enterprise-Grade-Lösung? Dafür gibt es mehrere Punkte, die genannt werden können.

```
/etc/systemd/system/patroni.service

[Unit]
Description=dbi services patroni service
After=etcd.service syslog.target network.target

[Service]
User=postgres
Group=postgres
Type=simple
ExecStartPre=-/usr/bin/sudo /sbin/modprobe softdog
ExecStartPre=-/usr/bin/sudo /bin/chown postgres /dev/watchdog
ExecStart=/u01/app/postgres/local/dmk/bin/patroni /u01/app/postgres/local/dmk/etc/patroni.yml
ExecReload=/bin/kill -s HUP $MAINPID
KillMode=process
Restart=no
TimeoutSec=30

[Install]
WantedBy=multi-user.target
```

Listing 9: patroni.service

```
systemctl daemon-reload
systemctl enable patroni
systemctl start patroni
```

Listing 10: Starten und Initialisieren des Patroni-Clusters

```
patronictl -d etcd://192.168.22.203:2379 switchover PG1
patronictl -d etcd://192.168.22.202:2379 failover PG1
```

Listing 11: Switchover and Failover des Patroni-Clusters

Sollte die Verbindung aufgrund eines Switchover oder Failover verloren gehen, gibt es eine kurze Meldung, dass die Verbindung fehlgeschlagen ist. Anschließend wird mit dem nächsten SQL Statement die Verbindung sofort wieder neu aufgebaut. Voraussetzung hierfür ist lediglich die Anmeldung über die im HAProxy definierte Host-Port-Kombination.

Für den Fall, dass eine Replica für eine bestimmte Zeit nicht mit der Primary kommunizieren kann (zum Beispiel aufgrund einer Netzwerkunterbrechung), wird die Replica automatisch wieder nachgefahren. Sollte der Unterschied zwischen Primary und Replica zu groß geworden sein, ist es allerdings möglich, dass die Replica sich nicht mehr automatisch aktualisiert. Dann muss die alte Instanz gelöscht und die Replica neu initialisiert werden. Dies erfolgt mit dem Restart des Patroni-Service. Ich empfehle vor dem erneuten Reinitialisieren zu überprüfen, welche Parameter seit dem initialen Setup geändert wurden.

Anders als bei anderen Lösungen wird die alte Primary nach einem Failover beziehungsweise Switchover automatisch zu einer Replica. Hierfür werden keinerlei manuelle Schritte benötigt, wie zum Beispiel einen recovery_command ins postgresql.conf zu schreiben, damit die Instanz im Recovery Mode gestartet wird. Auch dies gilt, wie oben, solange der WAL Gap nicht zu groß geworden ist.

Patroni-Cluster sind horizontal skalierbar. Eine weitere Instanz kann problemlos in das bereits bestehende Cluster aufgenommen werden.

Besteht bereits ein etcd-Cluster auf einem Server, kann parallel dazu ohne großen Aufwand ein zweiter Patroni-Cluster aufgebaut werden. Hierzu kann die

```
11:46:02 postgres@patroni1:/etc/haproxy/ [PG1] etcdctl member list
2858e6e2f3bcb0f8: name=patroni1 peerURLs=http://192.168.22.201:2380 clientURLs=http://192.168.22.201:2379 isLeader=false
d9eb1eacbdd866d0: name=patroni2 peerURLs=http://192.168.22.202:2380 clientURLs=http://192.168.22.202:2379 isLeader=true
e79ed70c10a3a842: name=patroni3 peerURLs=http://192.168.22.203:2380 clientURLs=http://192.168.22.203:2379 isLeader=false
11:46:06 postgres@patroni1:/etc/haproxy/ [PG1] etcdctl cluster-health
member 2858e6e2f3bcb0f8 is healthy: got healthy result from http://192.168.22.201:2379
member d9eb1eacbdd866d0 is healthy: got healthy result from http://192.168.22.202:2379
member e79ed70c10a3a842 is healthy: got healthy result from http://192.168.22.203:2379
cluster is healthy
11:46:12 postgres@patroni1:/etc/haproxy/ [PG1] patronictl list PG1
+ Cluster: PG1 (6961737994372400376) -+---------+----+-----------+
| Member   | Host           | Role    | State   | TL | Lag in MB |
+----------+----------------+---------+---------+----+-----------+
| patroni1 | 192.168.22.201 | Leader  | running |  4 |           |
| patroni2 | 192.168.22.202 | Replica | running |  4 |         0 |
| patroni3 | 192.168.22.203 | Replica | running |  4 |         0 |
+----------+----------------+---------+---------+----+-----------+
11:46:19 postgres@patroni1:/etc/haproxy/ [PG1]
```

Abbildung 2: Statusabfrage Patroni und etcd (© Julia Gugel, dbi services)

```
11:46:12 postgres@patroni1:/etc/haproxy/ [PG1] patronictl list PG1
+ Cluster: PG1 (6961737994372400376) -+---------+----+-----------+
| Member   | Host           | Role    | State   | TL | Lag in MB |
+----------+----------------+---------+---------+----+-----------+
| patroni1 | 192.168.22.201 | Leader  | running |  4 |           |
| patroni2 | 192.168.22.202 | Replica | running |  4 |         0 |
| patroni3 | 192.168.22.203 | Replica | running |  4 |         0 |
+----------+----------------+---------+---------+----+-----------+
11:46:19 postgres@patroni1:/etc/haproxy/ [PG1] patronictl -d etcd://192.168.22.201:2379 switchover PG1
Master [patroni1]:
Candidate ['patroni2', 'patroni3'] []: patroni2
When should the switchover take place (e.g. 2021-06-01T12:46 )  [now]:
Current cluster topology
+ Cluster: PG1 (6961737994372400376) -+---------+----+-----------+
| Member   | Host           | Role    | State   | TL | Lag in MB |
+----------+----------------+---------+---------+----+-----------+
| patroni1 | 192.168.22.201 | Leader  | running |  4 |           |
| patroni2 | 192.168.22.202 | Replica | running |  4 |         0 |
| patroni3 | 192.168.22.203 | Replica | running |  4 |         0 |
+----------+----------------+---------+---------+----+-----------+
Are you sure you want to switchover cluster PG1, demoting current master patroni1? [y/N]: y
2021-06-01 11:47:05.76614 Successfully switched over to "patroni2"
+ Cluster: PG1 (6961737994372400376) -+---------+----+-----------+
| Member   | Host           | Role    | State   | TL | Lag in MB |
+----------+----------------+---------+---------+----+-----------+
| patroni1 | 192.168.22.201 | Replica | stopped |    |   unknown |
| patroni2 | 192.168.22.202 | Leader  | running |  4 |           |
| patroni3 | 192.168.22.203 | Replica | running |  4 |        16 |
+----------+----------------+---------+---------+----+-----------+
11:47:05 postgres@patroni1:/etc/haproxy/ [PG1] patronictl list PG1
+ Cluster: PG1 (6961737994372400376) -+---------+----+-----------+
| Member   | Host           | Role    | State   | TL | Lag in MB |
+----------+----------------+---------+---------+----+-----------+
| patroni1 | 192.168.22.201 | Replica | running |  5 |         0 |
| patroni2 | 192.168.22.202 | Leader  | running |  5 |           |
| patroni3 | 192.168.22.203 | Replica | running |  5 |         0 |
+----------+----------------+---------+---------+----+-----------+
11:47:26 postgres@patroni1:/etc/haproxy/ [PG1]
```

Abbildung 3: Switchover Patroni (© Julia Gugel, dbi services)

bestehende etcd-Konfiguration genutzt werden. Es benötigt einzig einen eindeutigen Eintrag im patroni.yml *(siehe Listing 12)* des bestehenden Patroni-Clusters, ein zweites patroni.yml mit eindeutigem Namen und einen zweiten Service, ebenfalls mit einem anderen Namen.

Durch den einfachen Switchover von einem Node auf einen anderen können Minor-Version-Updates ohne Downtime durchgeführt werden. Es kann ein Knoten nach dem anderen aktualisiert und immer auf den Knoten gewechselt werden, der gerade nicht im Fokus des Upgrades steht. Es sollte darauf geachtet werden, ob sich Postgres-Parameter geändert haben, zum Beispiel beim Wechsel von PostgreSQL Version 12 auf 13.

Grenzen

Wie auch bei PostgreSQL generell ist eine Primary-Primary-Architektur auch mit Patroni nicht möglich. Des Weiteren kann es auch bei einem entsprechend großen WAL Gap nicht mehr automatisch nachgefahren werden und die Replica muss neu aufgebaut werden. Ich empfehle ein entsprechendes Monitoring des WAL Gap, um schnell reagieren zu können.

```
Namespace: /service/
```

Listing 12: Eintrag für parallele Patroni-Cluster

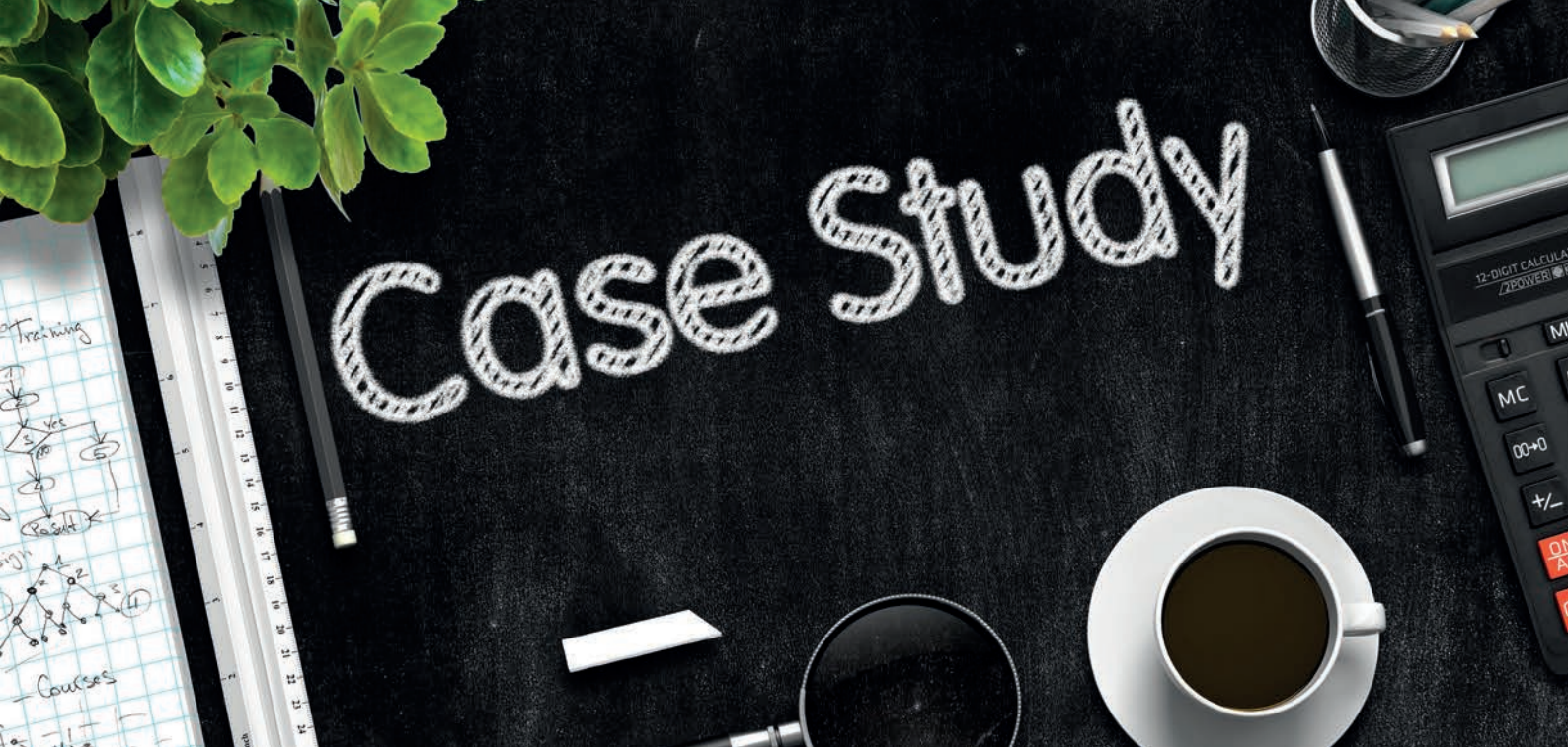
Zusammenfassung

Patroni ist mit seinem Aufbau und der einfachen Administration ein stabiles Werkzeug zur Erstellung einer hochverfügbaren Datenbankumgebung im Open-Source-Bereich. Es verwendet dabei bereits etablierte Linux-Programme. Mag die Installation etwas aufwendiger sein, läuft das System anschließend sehr zuverlässig. Patroni ist defintiv in der Lage, den wachsenden Anforderungen des Business standzuhalten. Speziell aufgrund des unproblematischen Switchover und Failover zu einer anderen Instanz ergibt diese kostenfreie Lösung, meiner Meinung nach, auch für große Datenbanklandschaften Sinn.

Über die Autorin

Julia Gugel ist Consultant im Open-Infrastructure-Team und spezialisiert auf die Bereiche PostgreSQL und Patroni sowie Linux, davor war sie im Bereich Oracle-Datenbanken tätig.

Julia Gugel
julia.gugel@dbi-services.com



expdp/impdp – was so alles passieren kann

Rainer Schaub, Allianz Technology / O IT DA

In den letzten Jahren hat der Autor immer wieder Datenbankmigrationen mit expdp und impdp durchgeführt. Obwohl es dieses Tool seit der Oracle-Version 10g und somit fast zwanzig Jahre gibt, trifft man immer wieder auf Problematiken und sogar Bugs. Dies ist kein Wunder, da die Datentypen erweitert werden und das Datenvolumen wächst. Zuerst wird jedoch in diesem Artikel eine Begriffsdefinition von Datenbank-Upgrade und Datenbank-Migration vorgenommen. Danach dann einige Beispiele dafür, was beim Export und Import so alles schiefgehen kann. Gegen Ende des Artikels noch ein paar „skurrile" Fälle und deren pragmatische Lösungen. Hinweise, wie expdp und impdp getunt werden können, runden den Artikel ab.

Terminologie: Upgrade versus Migration

Abbildung 1 kann der Unterschied zwischen Upgrade und Migration entnommen werden.

Das Upgrade einer Oracle-Datenbank bedeutet, den Datenbank-Katalog so zu verändern, dass er mit einer höheren Datenbankversion kompatibel ist. Typische Aktionen, die Teil eines Datenbank-Upgrades sein können, sind:

- Hinzufügen, Verändern oder Modifizieren von Spalten der Systemtabellen und Systemviews
- Erstellen neuer System-Pakete oder Prozeduren oder Verändern bestehender System-Pakete oder Prozeduren
- Erstellen, Verändern oder Löschen von Datenbank-Benutzern, Rollen und Privilegien
- Verändern von Oracle-Seed-Daten, die von Oracle-Komponenten genutzt werden

Alle diese Aktionen betreffen ausschließlich das Data Dictionary der Datenbank. Sie betreffen keinerlei Applikationsdaten. Daraus folgt auch, dass die Größe der Datenbank keinen oder nur minimalen Einfluss auf die Dauer eines Upgrades hat.

Hingegen bezieht sich der Begriff „Migration" auf mehrere unterschiedliche Arten von Veränderungen, die gegen eine Oracle-Datenbank erfolgen können. Zusätzlich zu einer Datenbankversion kann

sie sich auf eine, mehrere oder alle der folgenden Änderungen beziehen:

- Server
- Storage
- Zeichensatz (character set)
- Betriebssystem
- Schema (z.B. Partitionierung)
- Verschlüsselung
- Komprimierung

Eine Datenbank-Migration unterscheidet sich von einem Datenbank-Upgrade auf zweierlei Art und Weise. Erstens beinhaltet eine Datenbankmigration das Verschieben oder Ändern von Benutzer- oder Applikations-Daten der Datenbank. Das bedeutet, dass die Größe der Datenbank einen erheblichen Einfluss (Laufzeit) auf das Datenbank-Projekt hat. Zweitens kann jede der oben genannten Migrationsarten auf einer Datenbank ausgeführt werden, ohne sie auf eine neuere Version zu heben. *[1]*

NFS-Problematiken

expdp und impdp kann durch einen Dump-File erfolgen oder mittels DB-Link direkt über das Netz ohne Dump-File; dann braucht es nur einen Befehl, und zwar nur impdp. Wenn der Weg eines Dump-Files gewählt wird, nutzt man üblicherweise einen NFS-Mount, um ein Kopieren des Dump-Files vom Quellserver auf den Zielserver zu umgehen und vor allem um Laufzeit zu sparen. Jedoch müssen die Mount-Optionen sowohl auf der Quelle als auch auf dem Ziel richtig gesetzt sein. Ansonsten erhält man eine Fehlermeldung ähnlich der folgenden in *Abbildung 2*.

Anbei in *Abbildung 3* noch die Information, wie die Parameter auf einer IBM AIX und einer Oracle Exadata zu setzen sind.

Zeichensatz Problematiken (I)

Leider treten Zeichensatz-Problematiken immer wieder auf. Deshalb ist die eindrückliche Empfehlung, **jede Produktionsmigration mindestens einmal vorher mit den echten Produktionsdaten zu testen!** *Abbildung 4* zeigt einen Fall, bei dem der Import gegen eine DB mit einem Zeichensatz, der eine Übermenge des Export-Zeichensatzes darstellt, gemacht wurde. Eigentlich

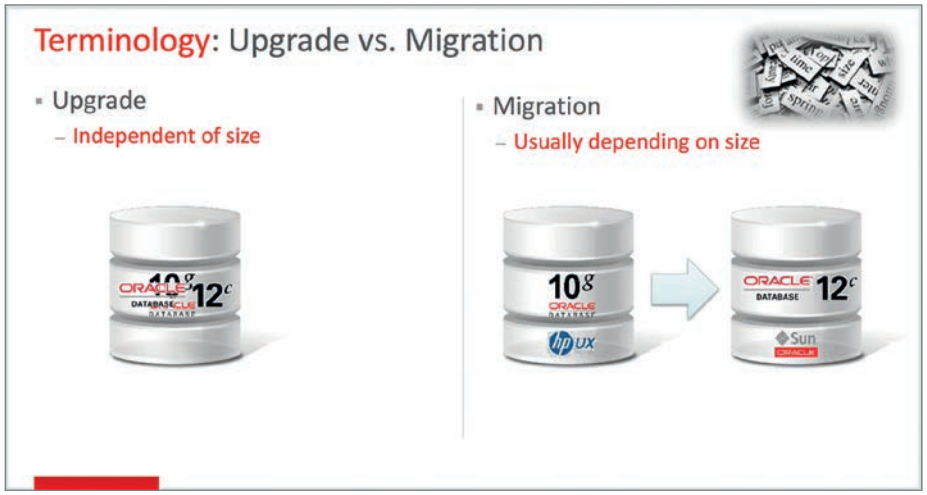


Abbildung 1: Der Unterschied zwischen Upgrade und Migration (Quelle: Oracle)

```
Connected to: Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
ORA-39001: invalid argument value
ORA-39000: bad dump file specification
ORA-31641: unable to create dump file "/nas/examig/DATABASE/exp_DB_20180430_U_U.dmp"
ORA-27054: NFS file system where the file is created or resides is not mounted with correct options
Additional information: 5
Additional information: 18
ORA-27037: unable to obtain file status
IBM AIX RISC System/6000 Error: 2: No such file or directory
Additional information: 3
```

Abbildung 2: Fehlermeldung bei falscher Setzung von Mount-Optionen (Quelle: Rainer Schaub)

```
Standard Mount-Options on AIX:
bg,soft,intr,sec=sys,rw

Necessary Mount-Options on AIX:
rw,bg,vers=3,proto=tcp,noac,hard,nointr,timeo=600,rsize=32768,wsize=32768

Mount-Options on exadata
rw,bg,hard,nointr,rsize=32768,wsize=32768,vers=3,timeo=600
```

Abbildung 3: Setzen der Parameter auf einer IBM AIX und einer Oracle Exadata (Quelle: Rainer Schaub)

```
Import: Release 12.1.0.2.0 - Production on Thu May 10 00:49:43 2019

Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights reserved.

Connected to: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
and Real Application Testing options
Master table "SYSTEM"."SYS_IMPORT_FULL_01" successfully loaded/unloaded
import done in AL32UTF8 character set and UTF8 NCHAR character set
export done in  AL16UTF16 character set and  UTF8 NCHAR character set
WARNING: possible data loss in character set conversions
Starting "SYSTEM"."SYS_IMPORT_FULL_01":  system/********@TARGETPDB
parfile=par_P_imp_DB3.file
```

Abbildung 4: Import gegen eine DB mit einem Zeichensatz, der eine Übermenge des Export-Zeichensatzes darstellt (Quelle: Rainer Schaub)

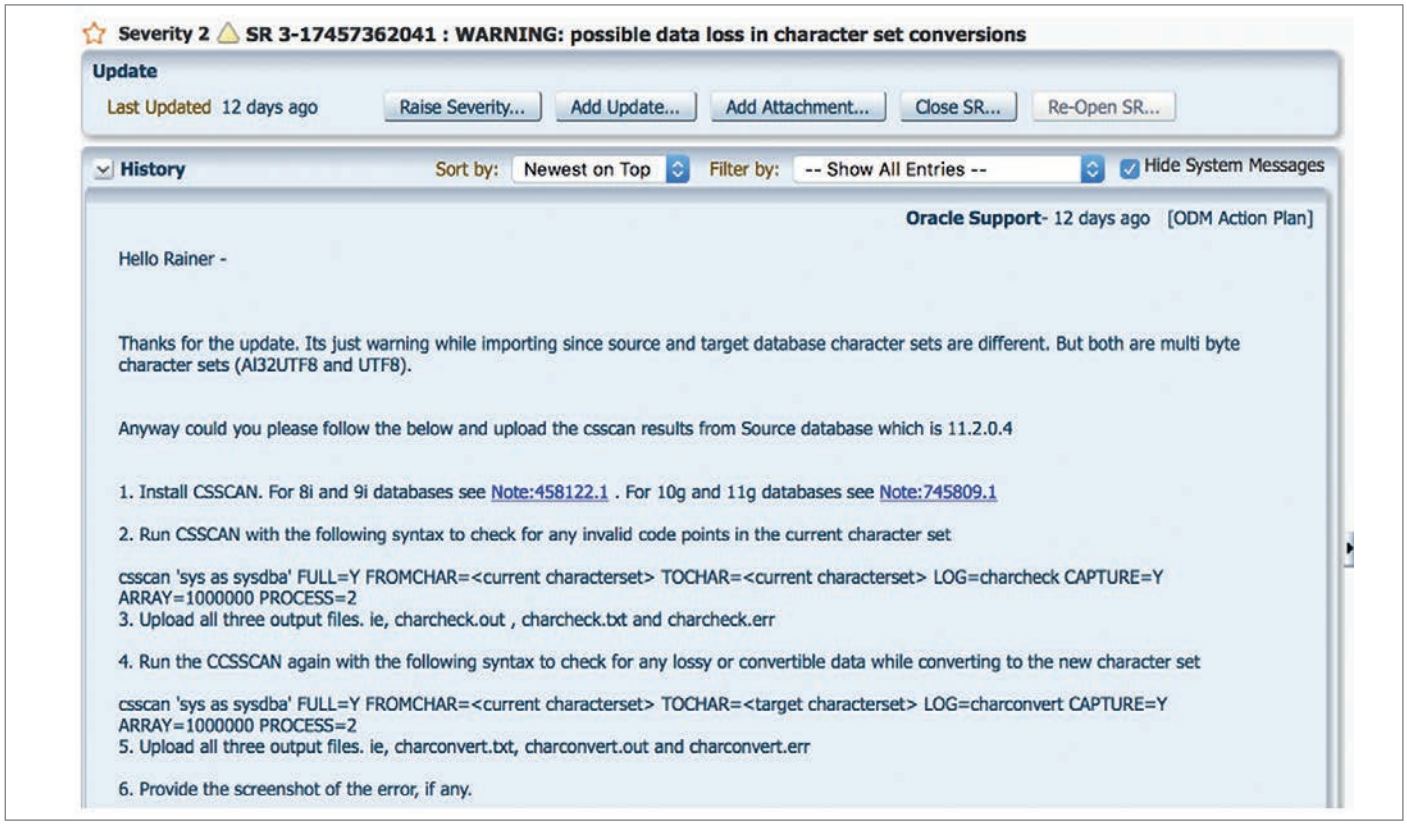


Abbildung 5: Antwort von Oracle auf den eigens erstellten SR (Quelle: Oracle)

```
Import: Release 12.1.0.2.0 - Production on Fri May 18 17:54:52 2019
Copyright (c) 1982, 2014, Oracle and/or its affiliates.  All rights reserved.
Connected to: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options
Master table "SYSTEM"."SYS_IMPORT_FULL_01" successfully loaded/unloaded
Starting "SYSTEM"."SYS_IMPORT_FULL_01":  system/********@PDBTARGET parfile=par_G_imp_DB1.file
Processing object type SCHEMA_EXPORT/USER
Processing object type SCHEMA_EXPORT/SYSTEM_GRANT
Processing object type SCHEMA_EXPORT/ROLE_GRANT
Processing object type SCHEMA_EXPORT/DEFAULT_ROLE
Processing object type SCHEMA_EXPORT/PRE_SCHEMA/PROCACT_SCHEMA
Processing object type SCHEMA_EXPORT/SEQUENCE/SEQUENCE
Processing object type SCHEMA_EXPORT/SEQUENCE/GRANT/OWNER_GRANT/OBJECT_GRANT
Processing object type SCHEMA_EXPORT/TABLE/TABLE
Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA
Processing object type SCHEMA_EXPORT/PROCEDURE/PROCEDURE
ORA-39346: data loss in character set conversion for object SCHEMA_EXPORT/PROCEDURE/PROCEDURE
Processing object type SCHEMA_EXPORT/PACKAGE/COMPILE_PACKAGE/PACKAGE_SPEC/ALTER_PACKAGE_SPEC
```

Abbildung 6: Fehlermeldung bei Datenbankmigrationen von AIX nach Exadata (Quelle: Rainer Schaub)

dürfte diese Meldung gar nicht erscheinen, eben wegen der Übermenge.

Die Antwort von Oracle auf den eigens erstellten SR ist etwas unbefriedigend *(siehe Abbildung 5)*. Es wird auf den mühsamen, fast „kryptischen" CSSCAN verwiesen, den es noch in der Version 11g gab. Ab der Version 12c gibt es den komfortableren Database Migration Assistant for Unicode (DMU).

Nach Rücksprache mit dem Kunden wurde das Risiko, ohne den CSSCAN zu migrieren, als vertretbar erachtet; dies auch im Hinblick auf den Migrationstermin, der keine Verschiebung erlaubte. Die Migration war erfolgreich.

Zeichensatz-Problematiken (II)

Der in *Abbildung 6* dargestellte Sachverhalt trat interessanterweise bei zwei etwa zeitgleich stattfindenden Datenbankmigrationen auf. Eine war von AIX nach Exadata, während die andere von Windows nach der Oracle Database Appliance (ODA) auftrat.

Data Loss hört sich auf den ersten Blick fast beängstigend an. *Abbildung 7* kann man jedoch entnehmen, dass Quell- und Ziel-DB die identischen Zeichensätze haben.

Die Erläuterung zum Oracle Error trägt auch nicht wirklich zu einer Lösung bei;

```
-      SQL*Plus: Release 11.2.0.4.0 Production
-      Copyright (c) 1982, 2013, Oracle.  All rights reserved.
-      Connected to:
-      Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
-      With the Partitioning, OLAP, Data Mining and Real Application Testing options
-
-      SQL> SELECT * FROM NLS_DATABASE_PARAMETERS where PARAMETER like '%CHARACTERSET%';
-      PARAMETER              VALUE
-      ---------------------- ----------------------------------------
-      NLS_CHARACTERSET       AL32UTF8
-      NLS_NCHAR_CHARACTERSET UTF8
-
-      SQL*Plus: Release 12.1.0.2.0 Production
-      Copyright (c) 1982, 2014, Oracle.  All rights reserved.
-      Last Successful login time: Fri May 18 2019 18:01:02 +02:00
-
-      Connected to:
-      Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
-      With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics
-      and Real Application Testing options
-
-      SQL> SELECT * FROM NLS_DATABASE_PARAMETERS where PARAMETER like '%CHARACTERSET%';
-      PARAMETER              VALUE
-      ---------------------- ----------------------------------------
-      NLS_CHARACTERSET       AL32UTF8
-      NLS_NCHAR_CHARACTERSET UTF8
```

Abbildung 7: Quell- und Ziel-DB haben identische Zeichensätze (Quelle: Rainer Schaub)

eher zu noch mehr Verwirrung *(siehe Abbildung 8)*.

Jedoch half die Eröffnung eines SR, da der Oracle Engineer die in *Abbildung 9* dargestellte Query bereitstellte.

Das Ergebnis der Query auf der Quell- und der Ziel-DB kann der *Abbildung 10* entnommen werden.

Im Erläuterungstext von Prozeduren haben sich – vermutlich durch eine unglückliche Einstellung des Client-Zeichensatzes – Zeichen „eingeschlichen", die beim expdp/impdp zu dieser Problematik führten. Es bestand somit kein Migrationsrisiko.

Der Vollständigkeit halber noch die Fehlermeldung sowie Analyse bei der vorhin schon erwähnten Problematik beim Import auf die Oracle Database Appliance *(siehe Abbildung 11)*. Die Fehlermeldung unterscheidet sich leicht und ist informativer. Dies liegt vermutlich an der etwas höheren Version (12.2.0.1.0 gegenüber der 12.1.0.2.0).

Besonderheiten bei RENAME_SCHEMA

Der Kunde wünschte im Rahmen der geplanten Migration eine Bereinigung (anderer Name) der Schemata-Namen auf der Ziel-DB. Das kann zu einem Fehler führen, falls es Trigger innerhalb des Schemas gibt. Hier löst Oracle den neuen Schemanamen nicht rekursiv auf. Die Fehlermeldung sieht dann wie in *Abbildung 12* aus.

Die Lösung ist einfach. Nach dem Import sind die fehlgeschlagenen „CREATE TRIGGER"-Befehle mit dem neuen

```
oracle@exadatadbnode:/nas/examig/ESB/ [CDBTEST] oerr ora 39346
39346, 00000, "data loss in character set conversion for object %s"
// *Cause:    Oracle Data Pump import converted a metadata object from
//            the export database character set into the target database
//            character set prior to processing the object. Some characters
//            could not be converted to the target database character set and
//            so the default replacement character was used.
// *Action:   No specific user action is required. This type of data loss can
//            occur if the target database character set is not a superset of
//            the export databases character set.
```

Abbildung 8: Erläuterung zum Oracle Error (Quelle: Rainer Schaub)

```
set serveroutput on declare cursor c_text is select owner,name,text from dba_source where owner not in
('APEX_050100','APPQOSSYS','AUDSYS','CTXSYS','DBSNMP','MDSYS','ORDSYS','PERFSTAT','SYS','SYSTEM','WMSYS','XDB')
and type='PROCEDURE'; beginfor i in c_text loop for j in 1..length(i.text) loop if ascii(substr(i.text,j,1))>128 then
dbms_output.put_line(i.ownerll'.'lli.namell' 'lli.text); end if; end loop; end loop; end; /
```

Abbildung 9: Eröffnung eines SR mit einer vom Oracle Engineer bereitgestellten Query (Quelle: Rainer Schaub)

Schemanamen zu ersetzen und auszuführen *(siehe Abbildung 13)*.

Tablespace Tools zu klein?

Recht häufig trat im Rahmen einer Migration von 200 Datenbanken der in *Abbildung 14* dargestellte Sachverhalt auf.

Das Tablespace Tool war zu klein. Verwirrend ist dabei, dass keinerlei Benutzerdaten dieses Tablespace zu migrieren waren. Vermutlich benötigt Oracle dieses Tablespace für expdp/impdp-interne Abläufe. Die Lösung ist selbstredend das Vergrößern des Tablespace wie *Abbildung 15* entnommen werden

```
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Indices l?schen
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Materialized Views l?schen
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Tables l?schen
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Sequences l?schen

M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Indices l□schen
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Materialized Views l□schen
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Tables l□schen
M_AMPSR.MDT_DROPSCHEMASEGMENTS -- Sequences l□schen
```

Abbildung 10: Ergebnis der Query auf der Quell- und der Ziel-DB (Quelle: Rainer Schaub)

```
Import: Release 12.2.0.1.0 – Production
Copyright (c) 1982, 2017, Oracle and/or its affiliates.  All rights reserved.
Connected to: Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options

ORA-39346: data loss in character set conversion for object TRIGGER:"D742_EARTH_DATA"."TRG_CURRENCY_YEAR_AIUD"
```

File was loaded in the wrong encoding: 'UTF-8'

```
1  create or replace TRIGGER "TRG_CURRENCY_YEAR_AIUD" AFTER INSERT OR UPDATE OR DELETE
2  ON DT865
3  --------------------------------------------------------------------------------
4  -- Statement Trigger
5  -- □bertr□gt □nderungen in den Wechselkursen in die Tabelle CURRENCY_YEAR
6  -
7  -- MODIFICATION HISTORY
8  -- Person                Date        Comments
9  -- --------------------  ----------  ----------------------------------------
```

Abbildung 11: Fehlermeldung sowie Analyse beim Import auf die Oracle Database Appliance (Quelle: Rainer Schaub)

```
ORA-39083: Object type TRIGGER:"U_SCHEMA"."AFTER_LOGON_TRG" failed to create with error:
ORA-00942: table or view does not exist
Failing sql is:
CREATE TRIGGER "U_AMPSR"."AFTER_LOGON_TRG"
AFTER LOGON ON U_AMPSR_X.SCHEMA
BEGIN
  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=M_AMPSR_X';
END;
```

Abbildung 12: Fehlermeldung bei RENAME SCHEMA (Quelle: Rainer Schaub)

```
CREATE TRIGGER "U_AMPSR"."AFTER_LOGON_TRG"
AFTER LOGON ON U_AMPSR.SCHEMA
BEGIN
  EXECUTE IMMEDIATE 'ALTER SESSION SET current_schema=M_AMPSR';
END;
/
```

Abbildung 13: Fehlgeschlagene „CREATE TRIGGER"-Befehle werden mit dem neuen Schemanamen ersetzt und ausgeführt (Quelle: Rainer Schaub)

kann. Da dieser Sachverhalt auch beim Import (impdp) auftreten kann und im Rahmen dieses großen Migrationsprojektes auch auftrat, ist die Empfehlung klar: Bei allen Quell- und Ziel-Datenbanken sollte dieses Tablespace adäquat vergrößert werden. Nach Abschluss der Migration wird in der Regel die Quell-DB sowieso entfernt und bei der Ziel-DB kann die Größe dieses Tablespace wieder reduziert werden.

Test-Migration der Produktionsdatenbank

Wie schon erwähnt, wird eindringlich empfohlen, die Produktionsdatenbank vor dem eigentlichen Migrationstermin mindestens einmal testweise zu migrieren. Dies aus mindestens zwei Gründen:

1. Die Dauer der Migration kann nur so zuverlässig ermittelt werden.
2. Problematiken, die bei der Migration der Testdatenbanken nicht auftraten, jedoch bei der Produktions-DB vorhanden sind, werden rechtzeitig „erlebt" und es kann noch gegengesteuert werden.

Jedoch kann bei einer testweisen Migration der Produktionsdatenbank folgende berechtigte Fehlermeldung ausgeworfen werden *(siehe Abbildung 16)*.

```
expdp
ORA-39171: Job is experiencing a resumable wait.
ORA-01691: unable to extend lob segment OPS$ORACLE.SYS_LOB059256C00045$$ by 128 in tablespace TOOLS
```

Abbildung 14: Fehlermeldung bei einer Migration von 200 Datenbanken (Quelle: Rainer Schaub)

```
SQL> select FILE_NAME,FILE_ID,TABLESPACE_NAME,BYTES/1024/1024 MB from dba_data_files;

FILE_NAME                                                  FILE_ID TABLESPACE_NAME                        MB
---------------------------------------------------------- ---------- ------------------------------ ----------
/u03/data/ora/001/ORASID/data/dbf/system01.dbf                      1 SYSTEM                           2000
/u03/data/ora/002/ORASID/data/dbf/sysaux01.dbf                      2 SYSAUX                           2000
/u03/data/ora/002/ORASID/data/dbf/undotbs01.dbf                     3 UNDOTBS                          5000
/u03/data/ora/001/ORASID/data/dbf/audit_daten01.dbf                 4 AUDIT_DATEN                      3000
/u03/data/ora/002/ORASID/data/dbf/tools01.dbf                       5 TOOLS                              50
/u03/data/ora/002/ORASID/data/dbf/patrol01.dbf                      6 TS_PATROL                          40
/u03/data/ora/002/ORASID/data/dbf/users01.dbf                       7 USERS                              20
/u03/data/ora/002/ORASID/data/dbf/USER01_DATA_01.dbf                8 TS_API_DATA                       100
/u03/data/ora/002/ORASID/data/dbf/USER02_DATA_01.dbf                9 TS_DAS_DATA                     30000
/u03/data/ora/002/ORASID/data/dbf/USER03_DATA_01.dbf               10 TS_DSS_DATA                       100
/u03/data/ora/002/ORASID/data/dbf/USER04_DATA_01.dbf               11 TS_E2_DATA                        100

SQL> alter database datafile '/u03/data/ora/002/IFITEX/data/dbf/tools01.dbf' resize 120m;

Database altered.
```

Abbildung 15: Vergrößerung des Tablespace bei der Ziel-DB (Quelle: Rainer Schaub)

```
Export: Release 11.2.0.4.0 – Production Copyright (c) 1982, 2011, Oracle and/or its affiliates.  All rights reserved.
Connected to: Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
Legacy Mode Active due to the following parameters:
Legacy Mode Parameter: "consistent=TRUE" Location: Parameter File, Replaced with: "flashback_time=TO_TIMESTAMP('now')"
Legacy Mode has set reuse_dumpfiles=true parameter.
Starting "OPS$ORACLE"."SYS_EXPORT_SCHEMA_01":  /******** directory=exp_exa parfile=par_P_exp_DB3.file
reuse_dumpfiles=true
Estimate in progress using BLOCKS method...
Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA
Total estimation using BLOCKS method: 481.0 GB
ORA-31693: Table data object "M_DASP_X"."ANX___7LHTCNF0_" failed to load/unload and is being skipped due to error:
ORA-02354: error in exporting/importing data
ORA-01466: unable to read data - table definition has changed
```

Abbildung 16: Fehlermeldung bei testweiser Migration der Produktionsdatenbank (Quelle: Rainer Schaub)

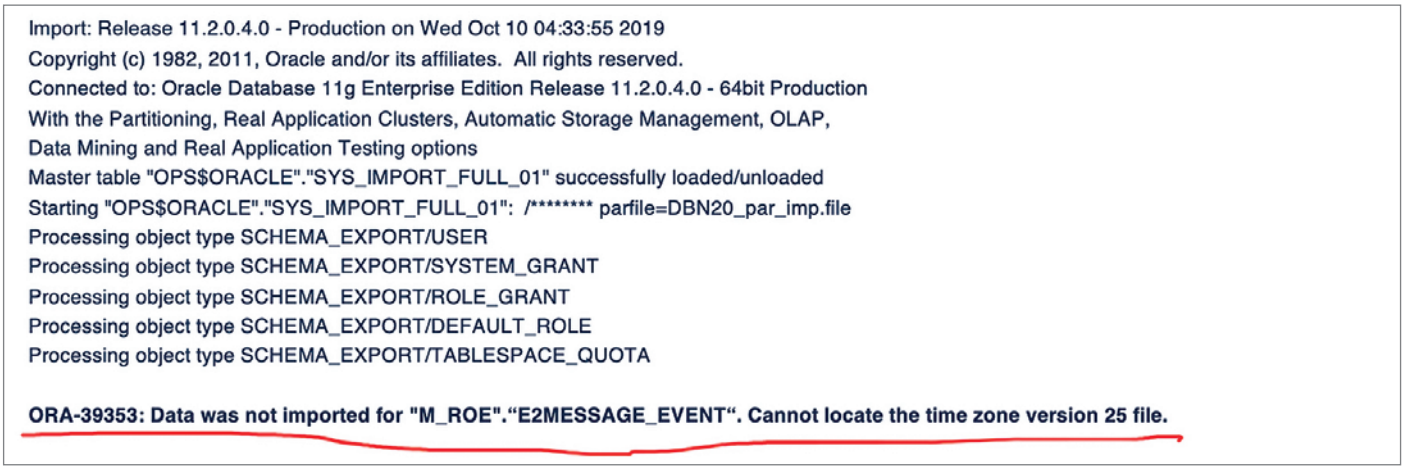


Abbildung 17: Oracle-Fehlermeldung zu Zeitzonen bei einer Migration (Quelle: Rainer Schaub)

Diese Meldung besagt, dass die Struktur eines zu exportierenden Objektes sich während des Exports geändert hat, was auch den Tatsachen entsprach. Dennoch konnten die recht genaue Dauer des Exports und auch nachfolgend des Imports ermittelt sowie weitere allfällige Migrationsproblematiken frühzeitig erkannt oder ausgeschlossen werden.

Time-Zone-Sachverhalte

Die Time Zone ist etwas ganz Spezielles und vom Menschen gemacht/erfunden. In der Informatik wird dieser Sachverhalt noch auf die Spitze getrieben. Es muss nicht nur abgebildet werden können, dass es etwa in St. Petersburg eine Stunde später als in Wien ist, sondern auch, in welchem Zeitraum dies so ist. Deshalb gibt es immer wieder zusätzliche Informationen, die in die Zeitzonen von Datenbanksystemen eingebaut werden müssen. Im Rahmen einer weiteren Migration gab es diesbezüglich die folgende in *Abbildung 17* dargestellte Oracle-Fehlermeldung.

Auch die zugehörige Erläuterung des Oracle-Fehlers hilft nicht wirklich zu verstehen, was die eigentliche Ursache ist *(siehe Abbildung 18)*.

Bei dieser Migration wurde die Hardware-Plattform gewechselt und als Zielversion der Datenbanksoftware auf die damals recht neue 12c R1 migriert, während die Quellversion 11g R2 war. Jedoch hat der Kunde vorbildlich auf allen aktiven Oracle-Datenbanken die „Time Zone" regelmäßig um die neuesten Versionen ergänzt. So kam es, dass die Zieldatenbank, die noch nicht produktiv war, eine etwas ältere Zeitzonendatei hatte. Die Lösung war selbstredend, die neueste Zeitzonendatei auf den Zieldatenbanken einzuspielen. Der Weg dazu ist in folgender MOS beschrieben: (Doc ID 1680065.1).

```
oerr ora 39353
39353, 00000, "Data was not imported for %s. Cannot locate the time zone version %s file."
// *Cause:    This table contains TIMESTAMP WITH TIME ZONE data and Oracle Data Pump needed
//            to load the source version of the time zone file. This version cannot be located.
// *Action:   Install the latest time zone version files.
```

Abbildung 18: Erläuterung des Oracle-Fehlers (Quelle: Rainer Schaub)

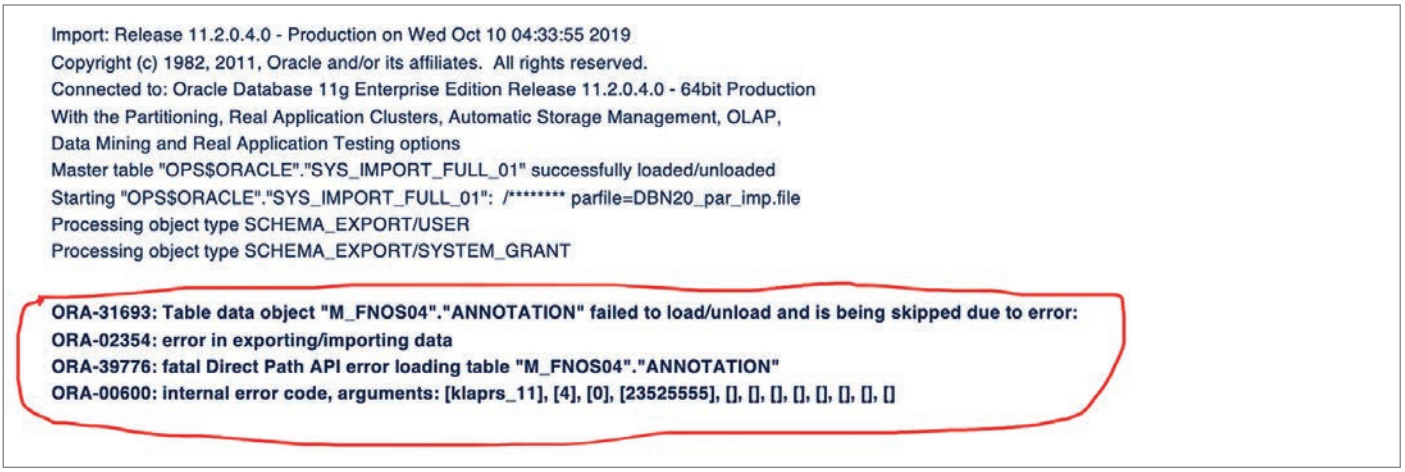


Abbildung 19: ORA-00600-Meldung im Alert-File (Quelle: Rainer Schaub)

ORA-00600 auch bei impdp?

Wenn ORA-00600-Meldungen im Alert-File erscheinen, springt auch der gemächlichste Datenbankadministrator und hat einen (leicht) erhöhten Puls. Dass beim impdp solch eine Meldung auftreten kann, war dem Autor damals nicht bekannt. Zum Glück war diese Meldung eine Eintagsfliege und nicht reproduzierbar und somit auch schon gelöst *(siehe Abbildung 19)*.

„Skurrile" Fälle und pragmatische Lösungen

Hier nun zwei Beispiele, die man als „skurril" bezeichnen kann. Der erste Fall stammt aus dem Jahr 2013 und ist somit etwas älter. Der Lösungsweg ist jedoch interessant und kann gegebenenfalls auch noch heute zur Fehlereingrenzung genutzt werden:

- Es sollten mittels expdp von einer Oracle-EE-Datenbank die zehn vorhandenen Applikationsschemata exportiert und dann auf einem anderen Server (Migration) importiert werden. Der expdp stürzte mit einem Core Dump ohne Fehlermeldung ab. Einen Service-Request (SR) zu eröffnen, erschien als zu aufwendig und eine allfällig von Oracle bereitgestellte Lösung wäre vermutlich nicht mit dem gewünschten Migrationszeitpunkt zu vereinbaren gewesen. Die pragmatische Lösung, um die Problematik einzugrenzen, war, jedes der zehn Applikationsschemata einzeln zu exportieren – davor wurden alle zehn in einem Schritt exportiert. Und tatsächlich, neun der zehn Applikationsschemata ließen sich anstandslos exportieren. Beim zehnten Schema kam wieder ein Core Dump ohne Fehlermeldung. Sodann wurde jede Tabelle dieses „fehlerbehafteten" Schemas einzeln exportiert und alle Tabellen bis auf eine ließen sich exportieren. Bei der Analyse der Feldtypen der fehlerbehafteten Tabelle stellte sich heraus, dass ein Feld vom Typ LONG war. Seit der Version Oracle 8i sollte dieser Datentyp nicht mehr genutzt werden und Oracle empfiehlt die Konvertierung zu CLOB oder NCLOB *[2]*.
- Der zweite Fall ist deutlich neueren Datums und stammt aus dem Jahr 2021. Auch hier handelt es sich um eine Oracle-EE-Datenbank. Diese hat gegen 100 Schemata, ist mehrere Terabyte groß und läuft auf der Version 18.11. Sie sollte auf die Version 19.9 „gehoben" werden. Beim Import warf der impdp folgende Meldungen für alle zu migrierenden Schemata in Unmengen aus *(siehe Listing 1)*.

Nach einer kurzen Analyse der Fehlerlogik und einer Recherche in Metalink bestand der Verdacht auf einen Bug von Oracle. Da auch hier der Migrationszeitpunkt eine rasche Lösung verlangte, war ein pragmatischer Ansatz notwendig. Es wurde ein Testschema ohne Daten, mit einigen wenigen Tabellen und Rechten sowie Rollen der „echten" Schemata auf der Quelle erzeugt und auf die Zielversion migriert. Es kamen dieselben Fehler. Eine Analyse des Quell- und Ziel-Schemas ergab jedoch, dass beide identisch sind. Eine weitere maschinelle Analyse der 100 „echten" Schemata brachte das gleiche Ergebnis zutage. Das bedeutet, dass die Fehlermeldung falsch ist. Die Migration konnte unter „Missachtung" dieses Fehlers erfolgreich durchgeführt werden.

Lange Laufzeit und dennoch das Tool der Wahl?

Eine große Schweizer Bank präsentierte 2019 an einem von Oracle Schweiz durchgeführten Kundenevent das Ergebnis ihrer erfolgreichen Migration der Kernapplikation (einer Oracle-EE-Datenbank)

```
25-JAN-21 13:01:46.465: W-2 Processing object type DATABASE_EXPORT/SCHEMA/ROLE_GRANT
25-JAN-21 13:01:49.550: ORA-39083: Object type ROLE_GRANT failed to create with error:
ORA-01919: role 'DELETE_CATALOG_ROLE' does not exist

Failing sql is:
   GRANT "DELETE_CATALOG_ROLE" TO "DBA"
25-JAN-21 13:01:54.481: W-4     Completed 849 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 1 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 5 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 6 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 7 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 8 49 ROLE_GRANT objects in 0 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 9 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 10 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 11 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 12 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 13 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.481: W-4     Completed by worker 14 80 ROLE_GRANT objects in 1 seconds
25-JAN-21 13:01:54.709: W-4 Processing object type DATABASE_EXPORT/SCHEMA/DEFAULT_ROLE
25-JAN-21 13:01:56.686: ORA-39083: Object type DEFAULT_ROLE:"VERTIGO" failed to create with error:
ORA-01919: role 'NONE' does not exist

Failing sql is:
   ALTER USER "VERTIGO" DEFAULT ROLE  ALL EXCEPT  NONE
```

Listing 1: impdp-Meldungen beim Import für alle zu migrierenden Schemata (Quelle: Rainer Schaub)

```
SQL> select sum(bytes)/1024/1024/1024 GB, a.name from v$datafile b, v$tablespace a where a.TS#=b.TS# and a.name like 'TS_%' group by a.name order by a.name;

        GB NAME
---------- ------------------------------
632        TS_DB1_DATA
190        TS_DB2_DATA
100        TS_DB1_INDEX
1160       TS_DB1_LOB

4 rows selected.

SQL> select sum(bytes)/1024/1024/1024 GB, a.name from v$datafile b, v$tablespace a where a.TS#=b.TS# and a.name like 'TS_%' group by a.name order by a.name;

        GB NAME
---------- ------------------------------
192        TS_DB1_DATA
139        TS_DB2_DATA
  7        TS_DB1_INDEX
103        TS_DB1_LOB

4 rows selected.
```

Abbildung 20: Diskplatzgewinn bei IMPDP bei frischem Aufbau von BLOB-Daten (Quelle: Rainer Schaub)

von AIX nach Exadata. Als Migrationstool wurde expdp/impdp ausgewählt und das trotz der nicht unerheblichen Laufzeit von ca. 36 Stunden. Wichtig in diesem Zusammenhang zu erwähnen ist, dass die Datenbank vor der Migration acht TB Diskplatz belegte und danach nur noch sechs TB. Das ist ein nicht ganz unerheblicher Nebeneffekt und hängt unter anderem damit zusammen, dass die Indizes beim impdp neu aufgebaut werden und somit kompakter als zuvor sind. Zudem werden auch BLOB-Daten frisch aufgebaut und auch hieraus kann ein nicht unerheblicher Diskplatzgewinn resultieren, wie man *Abbildung 20* entnehmen kann. Wäre die Migration mit Tools wie

- Transportable Tablespaces
- RMAN Incremental Backups
- Full Transportable Export/Import

erfolgt, so hätte die Dauer wohl nur einige Stunden betragen, jedoch wäre die Ziel-DB als physisches Abbild der Quell-DB wieder acht TB groß gewesen.

An dieser Stelle scheint es angebracht zu sein, prinzipielle Migrationsoptionen aufzuzeigen *(siehe Abbildung 21)*. Die gerade erwähnten drei Optionen bedingen als Quell-DB-Version mindestens 11.1, haben je nach Situation kürzere Migrationszeiten als expdp/impdp. Beim Einsatz von GoldenGate erzielt man eine „Near-Zero Downtime".

Zu erwähnen sind noch die beiden Optionen Data Guard und Transient Logical Standby, mit denen auch eine „Near Zero Downtime" erreicht wird, falls die Methode in der jeweiligen Kundensituation technisch möglich ist.

Erwähnenswert bei der erwähnten Migration der Schweizer Bank ist noch die Parallelität. Die Exadata hatte erheblich mehr CPU als die AIX und da der Import länger dauert als der Export – die Indizes werden beim Export selbstredend nicht exportiert, müssen jedoch beim Import neu aufgebaut werden –, gab der Zielserver die optimale Parallelität vor. Diese war bei 96 erreicht, obwohl der Quellserver ab einer Parallelität von 36 keinen weiteren Durchlaufzeit-Gewinn hatte.

Tuning

Hier noch kurz einige Tipps zum Tuning von expdp/impdp.

Wie gerade eben erwähnt, ist der Parameter **parallel** für die Durchlaufzeit vom expdp und auch vom impdp von größter Wichtigkeit. Der beste Wert hängt zum einen von der Anzahl vorhandener CPUs ab. Falls es eine sehr große Tabelle gibt, so „bremst" diese den Export und den Import aus, da nur ein Job diese Tabelle bearbeiten kann. Dies ist ein weiteres Beispiel dafür, dass Partitionen aus Performancesicht schneller sind, da ja eine Partition einen Export-Job exportieren kann.

Die zu wählende **sort_area_size** hängt natürlich mit der Größe der jeweiligen Tabellen zusammen. Für den Import ist jedoch die Empfehlung, diese auf mindestens 64 MB zu setzen.

Auch die Größe der **streams_pool_size** kann eine Performanceverbesserung bringen. Hier ist die Empfehlung, diesen Wert auf 128 MB für die Migration zu setzen.

Dass die Ziel-DB während des Imports auf **noarchivelog** gesetzt werden soll, versteht sich von allein. Wichtig ist natürlich, den Parameter nach erfolgreicher Migration wieder auf **archivelog** zurückzusetzen und vor Freigabe der Ziel-Datenbank einen vollständigen Fullback gezogen zu haben.

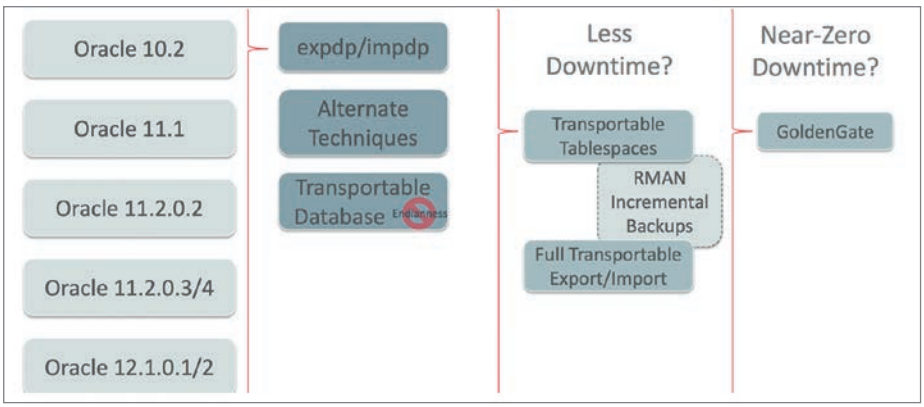


Abbildung 21: Migrations-Optionen (Quelle: Oracle)

Wenn viele große Schemata einer DB zu migrieren sind, empfiehlt es sich, jedes Schema mit je einem eigenen Skript zu migrieren. Ob mehrere Schemata gleichzeitig migriert werden, hängt dann von dem zu wählenden **parallel**-Wert ab. Der Hauptgrund, weshalb mehrere Skripte zu wählen sind, liegt an der Arbeitsweise des Imports. Erst wenn alle Tabellen und Partitionen aller in einem impdp-Aufruf aufgeführten Schemata geladen sind, wird mit dem Aufbau der Indizes begonnen. Wenn jedoch schemaweise importiert wird, werden die Indizes jedes einzelnen Schemas erheblich früher aufgebaut.

Apropos Indizes: Ob und wann beim Aufbau von Indizes der Parameter parallel zieht, ob es besser ist, **parallel** mehrere Indizes aufzubauen, versus Index für Index mit höherer Parallelität, wie man die Indizes aus dem Import-Skript ausgliedern kann und sie dann „händisch" laden und wie die Index-Aufbau-Parallelität im Bereich der PDBs aussieht, hierzu verweise ich auf Mike Dietrichs Blogs. *[3]*, *[4]*

Primary Note

Die Primary Oracle Note for Data Pump ist: (Doc ID 1264715.1).

Danksagung

Mein besonderer Dank gilt Mike Dietrich von Oracle, der mich über Jahre hinweg immer wieder mit Tipps und Tricks bei Migrationen mit expdp/impdp unterstützte. Dank auch an Sven Hilmer von der Hilmer Informatik GmbH, von dem ein Beispiel dieses Artikels stammt.

Quellen

[1] *http://www.oracle.com/technetwork/database/upgrade/upgrading-oracle-database-wp-12c-1896123.pdf*
[2] *https://www.orafaq.com/wiki/LONG*
[3] *https://mikedietrichde.com/2015/04/10/parallel-index-creation-with-data-pump-import/*
[4] *https://mikedietrichde.com/2020/10/15/does-data-pump-import-only-serially-into-pdbs/*

Über den Autor

Rainer Schaub hat schon 1988 eine Migration von DL1 nach DB2 durchgeführt, seine Diplomarbeit 1991 mit Informix realisiert und arbeitet seit 1992 schwerpunktmäßig mit Datenbanksystemen. Seit 1997 arbeitet er hauptsächlich mit Oracle-Datenbanken und sein Steckenpferd ist das Tuning. In den letzten Jahren hat er rund zwanzig Oracle-Zertifizierungen erworben sowie diverse IT-Artikel in England, Deutschland und der Schweiz veröffentlicht. Ab und zu hält er auch Schulungen wie zum Beispiel auf der DOAG 2018 und 2019 in Nürnberg.

Rainer Schaub
rainer.schaub@allianz-suisse.ch

Oracle vereinfacht Lizenzierung bei Migration

DOAG Online

Oracle hat Anfang Juli 2021 im Oracle Partner Network in einem Dokument darüber informiert, dass die Lizenzierung bei Migration rückwirkend zum 2. Juli 2021 vereinfacht wird.

Damit sollen Kunden die gewünschte Version in der Oracle Software Delivery Cloud einfach herunterladen können. Die Lizenzbedingungen der Oracle DB SE 2 können dann durch Anklicken einer Checkbox entsprechend akzeptiert werden. Daraus folgt, dass die bisher durchgeführte Verteuerung des Supports um 20 Prozent, wenn man von der DB SE1 zur DB SE2 migriert hat, entfällt. Eine offizielle Meldung seitens Oracle ist für Oracle-Partner verfügbar. Michael Paege, Leiter des Competence Center Lizenzierung und Mitglied des Vorstands der DOAG sagt: „Aus Kundensicht ist diese Neuerung grundsätzlich positiv zu bewerten, da ein formalbürokratischer Akt entfällt, der mit Aufwand und Kosten verbunden ist."

Weiterführende Informationen
https://www.doag.org/de/home/news/oracle-vereinfacht-lizenzierung-bei-migration/detail/

Data Exchange with PostgreSQL – Teil 2

Michael Kloker, Boehringer Ingelheim / IT RDM

Aufgrund der Lizenzpolitik von Oracle und des allgemeinen Kostendrucks in der IT überlegen momentan viele Firmen, ihre Anzahl an Oracle-Datenbanken deutlich zu reduzieren und auf alternative Datenbanken umzusteigen. Was sich zwischenzeitlich immer stärker als Oracle-Alternative etabliert hat, ist PostgreSQL. Sind Applikationen im Einsatz, die auch PostgreSQL unterstützen, können diese migriert werden. Aber ist die Datenbankmigration das Einzige, was berücksichtigt werden muss? Die wenigsten Datenbanken sind Stand-alone-Datenbanken, die allermeisten haben Schnittstellen zu anderen Datenbanken. Wie geht man mit diesen Schnittstellen um? In einer homogenen Oracle-Umgebung lässt sich der Datenaustausch einfach mit DB-Links realisieren, aber wie kann dieser über Technologiegrenzen hinweg aussehen?

Im Zuge dieser Entwicklung habe ich mich mit der Schnittstellenthematik beschäftigt und untersucht, wie PostgreSQL in eine bereits bestehende Datenbankumgebung aus Oracle-Datenbanken und MSSQL-Server passt und welche Möglichkeiten des Datenaustausches es zwischen den verschieden Datenbanktechnologien gibt *(siehe Abbildung 1)*.

Im ersten Teil des Artikels „Data Exchange with PostgreSQL" ging ich auf den Postgres Foreign Data Wrapper und den Dblink Foreign Data Wrapper ein, mit denen der Datenaustausch und das Ausführen von Remote-Funktionen und Prozeduren zwischen PostgreSQL-Datenbanken möglich ist.

Im zweiten Teil gehe ich auf den Oracle Foreign Data Wrapper ein, mit dem

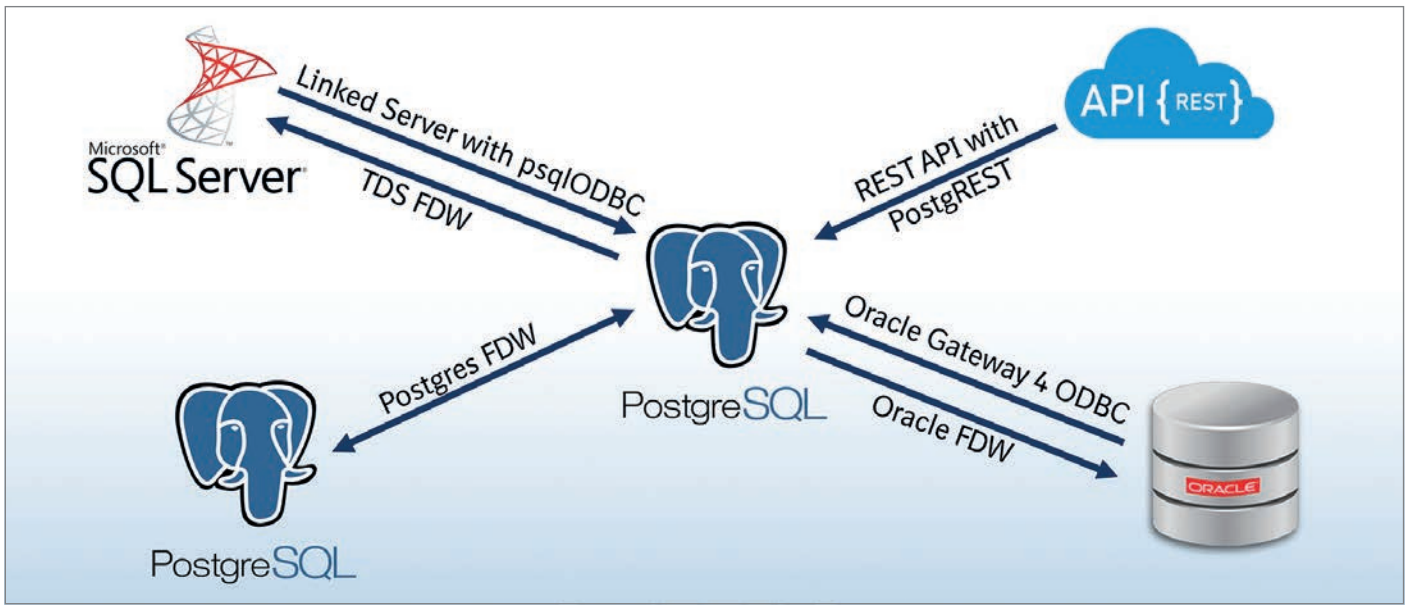


Abbildung 1: Dataexchange-Möglichkeiten mit Postgres (Quelle: © Oracle, Microsoft und PostgreSQL)

der Zugriff von PostgreSQL auf Oracle-Datenbanken ermöglicht wird, sowie auf das Oracle Gateway for ODBC für den Zugriff von Oracle auf PostgreSQL.

Der Oracle FDW: Zugriff von Postgres auf Oracle

Wie der Zugriff von PostgreSQL auf PostgreSQL funktioniert, haben wir im ersten Teil von „Data Exchange with PostgreSQL" ausführlich betrachtet. Nun wollen wir den Oracle FDW, mit dem man von PostgreSQL auf Oracle zugreifen kann, kennenlernen. Im weiteren Text wird PostgreSQL nur noch mit Postgres bezeichnet.

An dieser Stelle möchte ich auf den sehr guten Artikel „Getting Data from Oracle to PostgreSQL and vice versa" von Daniel Westermann im Red Stack Magazin Januar 2021 verweisen, in dem auch schon auf den Oracle FDW eingegangen wurde. Zusätzlich werden wir hier aber noch die Oracle-FDW-Funktionen ORACLE_DIAG und ORACLE_EXECUTE kennenlernen.

Der Oracle FDW unterstützt SELECT-, INSERT-, UPDATE- und DELETE-Statements auf Oracle-Tabellen. Man kann mit dem Oracle FDW auch aus Postgres heraus Funktionen, Prozeduren, Packages und auch DDL-Statements in Oracle ausführen. Allerdings gibt es beim Zugriff von Postgres auf Oracle einen wichtigen Punkt zu beachten, nämlich die Kompatibilität der Datentypen. Beim Erstellen der Foreign Tables werden Oracle-Datentypen auf Postgres-Datentypen gemappt und diese sind nicht immer kompatibel. Ein Beispiel ist der Datentyp DATE. DATE in Oracle beinhaltet Datum und Uhrzeit, DATE in Postgres beinhaltet nur das Datum, für die Uhrzeit gibt es den eigenen Datentyp TIME. Zusätzlich gibt es in Postgres den Datentype TIMESTAMP, der Datum und Uhrzeit kombiniert. Das heißt, es muss darauf geachtet werden, dass das Mapping der Datentypen passt.

Die Installation und Konfiguration des Oracle FDW erfolgt, analog zur Installation und Konfiguration des Postgres FDW, in zwei Teilen, Teil 1 auf Betriebssystemebene, Teil 2 in der Datenbank.

Zunächst wird das Postgres Developer Package installiert *(siehe Listing 1)*. Zusätzlich benötigt der Oracle FDW einen Oracle Client, entweder den Oracle-Full- oder den Instantclient. Entscheidet man sich für den Instantclient, muss auch das Instantclient SDK installiert werden *(siehe Listing 1)*. Die sqlnet.ora und tnsnames.ora werden entsprechend konfiguriert, um auf die gewünschte Oracle-Datenbank zugreifen zu können. Die Installation vom Instantclient sqlplus *(siehe Listing 1)* für einen Oracle-Verbindungstest ist auch empfehlenswert. Im Anschluss werden die Umgebungsvariablen ORACLE_HOME und LD_LIBRARY_PATH für den Postgres-User auf Betriebssystemebene gesetzt *(siehe Listing 1)*. Danach wird ein Neustart

```
# yum install rh-postgresql12-postgresql-devel.x86_64
# su - postgres
$ cd /opt/postgres/instantclient_19_5
$ unzip instantclient-basic-linux.x64-19.5.0.0.0dbru.zip
$ unzip instantclient-sdk-linux.x64-19.5.0.0.0dbru.zip
$ unzip instantclient-sqlplus-linux.x64-19.5.0.0.0dbru.zip

$ export ORACLE_HOME=/opt/postgres/instantclient_19_5
$ export LD_LIBRARY_PATH=/opt/postgres/instantclient_19_5:$LD_LIBRARY_PATH
$ pg_ctl restart -D /data/postgres/pgcl1
```

Listing 1: Vorbereitungen für den Oracle FDW

```
$ export ORACLE_HOME=/opt/postgres/instantclient_19_5
$ unzip oracle_fdw-2.3.0.zip
$ cd /tmp/oracle_fdw-ORACLE_FDW_2_3_0
$ make
$ make install
```

Listing 2: Installation Oracle FDW auf dem Betriebssystem

```
pgdb1=# select name, installed_version, comment
          from pg_available_extensions
          where name like '%oracle%';
  name      | installed_version  |  comment
------------+--------------------+-------------------------
 oracle_fdw | 1.2                | foreign data wrapper for
            |                    | Oracle access
```

Listing 3: Test, ob der Oracle FDW in der Postgres-DB verfügbar ist

```
pgdb1=# CREATE EXTENSION oracle_fdw schema public;
pgdb1=# \dx
                List of installed extensions
  Name      | Version | Schema |    Description
------------+---------+--------+---------------------------
 oracle_fdw | 1.2     | public | foreign data wrapper for
            |         |        | Oracle access
```

Listing 4: Create Oracle FDW Extension

```
pgdb1=# CREATE SERVER xepdb1
       FOREIGN DATA WRAPPER oracle_fdw
       OPTIONS (dbserver ,xepdb1.noborders.com‘);
pgdb1=# \des
       List of foreign servers
 Name   | Owner  | Foreign-data wrapper
--------+--------+----------------------
 xepdb1 | admin1 | oracle_fdw
```

Listing 5: Create Foreign Server für den Oracle FDW

des Postgres-Clusters durchgeführt, damit die neuen beziehungsweise geänderten Umgebungsvariablen gültig werden *(siehe Listing 1)*. Die Umgebungsvariablen sollten permanent gesetzt werden, etwa im .bash_profile des Postgres-Users.

Sind die Vorbereitungen getroffen, wird der Oracle FDW *(https://github.com/laurenz/oracle_fdw)* heruntergeladen, entpackt und mit make/make install installiert *(siehe Listing 2)*. Dabei wird der Oracle FDW gegen den Oracle Client kompiliert und die Oracle FDW Files im Postgres-Extensions-Verzeichnis erstellt.

Der zweite Teil der Installation und Konfiguration des Oracle FDW erfolgt in der Postgres-Datenbank. Das Vorgehen ist gleich wie beim Postgres FDW. Zuerst wird die Extension, dann das Foreign Server Object, anschließend das User Mapping und zum Schluss die Foreign Table erstellt.

```
pgdb1=# CREATE USER MAPPING FOR admin1
       SERVER xepdb1
       OPTIONS (user 'orauser', password ,*******');
pgdb1=# \deu
   List of user mappings
      Server    | User name
----------------+-----------
      xepdb1    | admin1
```

Listing 6: Create User Mapping für den Oracle FDW

```
pgdb1=# CREATE FOREIGN TABLE ft_xepdb1_ot1 (
          pid        integer,
          ptext      character varying(100)
      )
      SERVER xepdb1
      OPTIONS (schema 'orauser', table 'OT1');
pgdb1=# \det
   List of foreign tables
 Schema |     Table     | Server
--------+---------------+--------
 admin1 | ft_xepdb1_ot1 | xepdb1
```

Listing 7: Create Foreign Table mit dem Mapping auf die Oracle-Tabelle

```
pgdb1=# select * from ft_xepdb1_ot1;
 pid |    ptext
-----+---------------------
   1 | Oracle DB XEPDB1
   2 | Oracle Schema test1
   3 | Oracle Table ot1

pgdb1=# insert into ft_xepdb1_ot1
          values (20, 'Greetings from Postgres');
pgdb1=# update ft_xepdb1_ot1
          set ptext='Warm Greetings from Postgres'
          where pid=20;
pgdb1=# delete from ft_xepdb1_ot1 where pid=20;
```

Listing 8: SELECT / INSERT / UPDATE / DELETE von Postgres auf eine Oracle- Tabelle

```
pgdb1=# \df
                        List of functions
Schema |      Name       | Result     | Argument data types
       |                 | data type  |
-------+-----------------+------------+-----------------------
public | oracle_diag     | text       | name DEFAULT NULL::name
public | oracle_execute  | void       | server name, statement
                                      | text
```

Listing 9: Funktionen des Oracle FDW

Wir prüfen zunächst, ob die Betriebssysteminstallation des Oracle FDW erfolgreich war und die Extension in der DB verfügbar ist *(siehe Listing 3)*.

Mit CREATE EXTENSION wird die Extension in der DB im Schema „public" erstellt *(siehe Listing 4)*. Der psql shortcut \dx zeigt die installierten Extensions.

Im Anschluss wird der Foreign Server mit der Referenz auf die Oracle FDW Extension und dem Oracle-TNS-Namen erstellt *(siehe Listing 5)*. Ist die tnsnames.ora nicht richtig konfiguriert, wird der Zugriff auf die Oracle DB nicht funktionieren. Der psql Shortcut \des zeigt die erstellten Foreign Server.

Nun wird das User Mapping mit der Referenz auf den oben erstellten Foreign Server im Schema „admin1", mit den Oracle-Authentifizierungsinformationen Username und Passwort, angelegt *(siehe Listing 6)*.

Zum Schluss erfolgt das Mapping der Oracle-Tabelle auf die Postgres Foreign Table, in unserem Beispiel FT_XEPDB1_OT1 genannt *(siehe Listing 7)*. Die Oracle-Tabelle OT1 besitzt 2 Spalten, Spalte 1 ist vom Datentyp INTEGER, Spalte 2 vom Datentyp VARCHAR2(100). Entsprechend werden die Datentypen auf Postgres-Datentypen in der Foreign Table gemappt. Mit dem psql Shortcut \det werden die Foreign Tables angezeigt.

Ist die Foreign Table erstellt, können SELECT-, INSERT-, UPDATE- und DELETE-Statements ausgeführt werden *(siehe Listing 8)*.

Der Oracle FDW bringt zwei interessante Funktionen mit *(siehe Listing 9)*, die ORACLE_DIAG- und die ORACLE_EXECUTE-Funktion. Mit dem psql Shortcut \df werden die Funktionen angezeigt.

Die ORACLE_DIAG-Funktion zeigt Informationen zur Oracle-FDW-Konfiguration an *(siehe Listing 10)*. Dies kann bei der Fehlersuche hilfreich sein, wenn der Oracle FDW nicht so funktioniert wie erwartet, wenn zum Beispiel TNS_ADMIN nicht oder falsch gesetzt wurde.

Mit der ORACLE_EXECUTE-Funktion können beliebige Statements von Postgres auf Oracle ausgeführt werden. Es können

Funktionen/Prozeduren/Packages *(siehe Listing 11)* oder auch DDL-Statements *(siehe Listing 12)* in Oracle ausgeführt werden. Parameter 1 gibt das Foreign Server Object an, in unserem Beispiel XEPDB1, Parameter 2 beinhaltet das in einen PL/SQL-Block eingebettete Statement.

```
pgdb1=# SELECT oracle_diag();
                          oracle_diag
-------------------------------------------------------------
 oracle_fdw 2.3.0,
 PostgreSQL 12.1,
 Oracle client 19.5.0.0.0,
 ORACLE_HOME=/opt/postgres/instantclient_19_5,
 TNS_ADMIN=/opt/postgres/instantclient_19_5/network/admin
```

Listing 10: Ausgabe der ORACLE_DIAG-Funktion

Oracle Gateway for ODBC: Zugriff von Oracle auf Postgres

Mit dem Oracle Gateway for ODBC bietet Oracle die Möglichkeit, auf Postgres-Datenbanken zuzugreifen. Es können SELECT-, INSERT-, UPDATE- und DELETE-Statements auf Postgres-Tabellen ausgeführt werden. Zusätzlich können mit dem Oracle Package DBMS_HS_PASSTHROUGH-Funktionen und -Prozeduren in Postgres ausgeführt werden. Der große Vorteil am Oracle Gateway for ODBC: Die Verwendung ist kostenlos *[1]*.

Wie schon beim Oracle FDW muss auch beim Oracle Gateway for ODBC auf die Datentypenkompatibilität geachtet werden. Nutzt man beispielsweise in Postgres den Datentyp TEXT, kann dieser beliebig lange

```
pgdb1=# SELECT oracle_execute(
          'xepdb1',
          'BEGIN f_write_ot1(11,
             ''function executed from postgres'');
          END;'
      );
```

Listing 11: Ausführen einer Funktion von Postgres in Oracle mit ORACLE_EXECUTE

```
pgdb1=# SELECT oracle_execute(
          'xepdb1',
          'BEGIN execute immediate
             ''create table test1 (id Number)'';
          END;'
      );
```

Listing 12: Erstellen einer Tabelle von Postgres in Oracle mit ORACLE_EXECUTE

```
# yum install unixODBC.x86_64
# yum install postgresql-odbc.x86_64
```

Listing 13: Installation ODBC Manager und ODBC-Postgres-Treiber

```
# cat /etc/odbcinst.ini
...
[PostgreSQL]
Description      = ODBC for PostgreSQL
Driver           = /usr/lib/psqlodbcw.so
Setup            = /usr/lib/libodbcpsqlS.so
Driver64         = /usr/lib64/psqlodbcw.so
Setup64          = /usr/lib64/libodbcpsqlS.so
FileUsage        = 1
...
```

Listing 14: odbcinst.ini mit Postgres ODBC Libraries

```
# su - oracle
$ odbcinst -j
unixODBC 2.3.1
DRIVERS............: /etc/odbcinst.ini
SYSTEM DATA SOURCES: /etc/odbc.ini
FILE DATA SOURCES..: /etc/ODBCDataSources
USER DATA SOURCES..: /home/oracle/.odbc.ini
```

Listing 15: Installation ODBC-Treiber für User Oracle

Zeichenketten beinhalten. Möchte man diese in den Oracle-Datentyp VARCHAR2 schreiben, kommt es zu Problemen, da VARCHAR2 eine Längenbeschränkung von 4000 Zeichen hat. Hier muss überlegt werden, wie man damit umgeht.

Die Installation und Konfiguration des Oracle Gateway for ODBC erfolgt auf dem Oracle-Datenbankserver in 3 Teilen.

- Betriebssysteminstallation des ODBC-Treibers und Konfiguration für den Oracle-User
- Oracle-Konfiguration außerhalb der DB, das heißt Konfiguration des Oracle Gateway und Konfiguration des Listener und der tnsnames.ora
- Oracle-Konfiguration innerhalb der DB, mit der Erstellung eines DB-Links auf die Postgres-DB

Auf diese Punkte werden wir nun detailliert eingehen.

In *Listing 13* werden der ODBC Manager und der Postgres-ODBC-Treiber installiert.

Unter anderem wird dabei die Datei odbcinst.ini installiert *(siehe Listing 14)*, in der im Abschnitt PostgreSQL die Biblio-

theken aufgeführt sind, die der Postgres-ODBC-Treiber verwendet.

Nun wird der ODBC-Treiber für den User Oracle mit dem Befehl odbcinst installiert *(siehe Listing 15)*. Der Output zeigt, welche Files für die ODBC-Konfiguration benutzt werden.

Im Home-Verzeichnis des Oracle-Users wird nun die Datei .odbc.ini mit den Postgres-Data-Source-Informationen erstellt *(siehe Listing 16)*. Zeile 1 zeigt den Data Source Name, in unserem Beispiel PGDB1. Der Parameter Driver wird auf PostgreSQL gesetzt und verweist auf den Abschnitt PostgreSQL in der Datei /etc/odbcinst.ini *(siehe Listing 16)*. Mit den Parametern Servername, Port, Database werden die Verbindungsinformationen für die Postgres-DB angegeben. Die Parameter Username und Password sind die Authentifizierungsinformationen für die Postgres-DB. Das Passwort wird nur für den isql-Test *(siehe Listing 17)* benötigt. Mit Protocol wird die unterstützte Postgres-Version angegeben, in unserem Beispiel alle Versionen größer Postgres 7.4. Mit ReadOnly=No wird Lesen und Schreiben ermöglicht. Die Beschreibung der weiteren Parameter kann im Internet nachgelesen werden *[2]* und *[3]*.

Ist die Data Source konfiguriert, kann mit dem Befehl isql unter Angabe der oben definierten Data Source PGDB1 eine Verbindung auf die Postgres-DB aufgebaut und ein SELECT abgesetzt werden *(siehe Listing 17)*. Ist der Verbindungsaufbau erfolgreich, ist die Data Source richtig konfiguriert und sichergestellt, dass der Zugriff auch von Oracle heraus funktioniert. Nach diesem Test kann das Passwort aus der Datei .odbc.ini wieder gelöscht werden.

Die ODBC-Installation und Konfiguration ist so weit abgeschlossen, nun kommen wir zur Oracle-Konfiguration außerhalb der Datenbank.

Zunächst erstellen wir die Konfigurationsdatei für das Oracle Gateway. Dazu wechseln wir in das Verzeichnis $ORACLE_HOME/hs/admin. Dort wird eine Kopie des Files initdg4odbc.ora mit dem Namen initDATASOURCE.ini erstellt, in unserem Beispiel initPGDB1.ini *(siehe Listing 18)*. In dem File werden folgende Parameter gesetzt:

- HD_FDS_CONNECT_INFO wird mit der oben definierten Data Source konfiguriert
- HS_FDS_SHAREABLE_NAME zeigt auf die ODBC-Treiber-Manager-Library
- HS_LANGUAGE wird auf LANGUAGE_TERRITORY der Oracle-DB gesetzt, sowie den Postgres-Zeichensatz, in unserem Beispiel UTF8

```
$ vi /home/oracle/.odbc.ini
[PGDB1]
Description          = PGDB1
Driver               = PostgreSQL
Trace                = No
Database             = pgdb1
Servername           = pghost
UserName             = admin1
Password             = ****
Port                 = 5432
Protocol             = 7.4+
ReadOnly             = No
RowVersioning        = No
ShowSystemTables     = No
ShowOidColumn        = Yes
FakeOidIndex         = No
```

Listing 16: Postgres-ODBC-Parameter

- Der Parameter HS_NLS_NCHAR wird auf UCS2 gesetzt, dadurch werden die Oracle-Daten UCS2-codiert, der Zeichensatz, den der ODBC-Treiber erwartet
- Bei ODBCINI wird auf die .odbc.ini im Oracle Home Directory verwiesen, die oben angelegt wurde

Im nächsten Schritt wird die listener.ora angepasst. Es wird ein neuer SID_DESC-Abschnitt für die Postgres-DB erstellt.

- Der SID_NAME wird mit dem Namen der Data Source konfiguriert, in unserem Beispiel PGDB1.
- PROGRAM wird mit dg4odbc konfiguriert, dies ist das Database Gateway Executable for ODBC im $ORACLEHOME/bin-Verzeichnis.
- Die Umgebungsvariable LD_LIBRARY_PATH wird mit den Pfaden auf die ODBC- und Oracle-Bibliotheken konfiguriert.

Danach wird der Listener neu gestartet. Die Ausgabe des Listener zeigt nun den neuen Service PGDB1 an *(siehe Listing 19)*.

Die tnsnames.ora wird um einen Eintrag für die Postgres-DB erweitert *(siehe Listing 20)*.

- Ein Alias wird definiert, im Beispiel PGDB1.noborders.com.
- Der Host wird mit dem Namen des Oracle-Servers konfiguriert.
- SID wird mit der ODBC Data Source konfiguriert.
- Durch den Parameter HS (Heterogenous Services) = OK bekommt Oracle die Info, dass es sich hier um keine Oracle-Verbindung handelt.

```
$ isql PGDB1
+---------------------------------------+
| Connected!                            |
+---------------------------------------+

SQL> select * from pt1;
+------------+--------------------------+
| id         | text                     |
+------------+--------------------------+
| 1          | Host pghost              |
| 2          | Postgres DB pgdb1        |
| 3          | Schema admin1            |
| 4          | Table pt1                |
+------------+--------------------------+
```

Listing 17: Verbindungstest mit isql auf Postgres

```
$ cd $ORACLE_HOME/hs/admin/
$ cp initdg4odbc.ora initPGDB1.ini
$ cat initPGDB1.ini
HS_FDS_CONNECT_INFO = PGDB1
HS_FDS_SHAREABLE_NAME = /usr/lib64/libodbc.so
HS_LANGUAGE = AMERICAN_AMERICA.UTF8
HS_NLS_NCHAR = UCS2
set ODBCINI=/home/oracle/.odbc.ini
```

Listing 18: Oracle Gateway for ODBC Config File

Damit ist die Konfiguration außerhalb der Oracle-DB abgeschlossen. Den Rest kennen wir aus der Oracle-Welt. Es wird ein Oracle-DB-Link erstellt *(siehe Listing 21)*. Dabei wird der Postgres-User mit dem Passwort angegeben, mit dem wir uns an der Postgres-DB authentifizieren, sowie der Connection String, der oben in der tnsnames.ora definiert wurde.

Und schon sind wir so weit, und können DML-Statements auf Postgres-Tabellen ausführen *(siehe Listing 22)*. Noch eine kurze Anmerkung zur Syntax. Die Postgres-Tabellen- sowie die Spaltennamen müssen in den DML-Statements in doppelten Hochkommas geschrieben werden, sonst kommt es zu Fehlermeldungen.

Oracle bietet mit dem DBMS_HS_PASSTHROUGH Package auch die Möglichkeit, Funktionen und Prozeduren in Postgres auszuführen. Nähere Informationen können bei Oracle nachgelesen werden *[4]*. *Listing 23* zeigt, wie die Postgres-Funktion F_WRITE_PT1 aus Oracle in Postgres aufgerufen wird. Der Funktion werden zwei Parameter übergeben, die in eine Postgres-Tabelle geschrieben werden.

Zusammenfassung

Der Zugriff von Postgres auf Oracle mit dem Oracle FDW funktioniert sehr gut. Nicht nur der Datenaustausch kann sichergestellt werden, es können Funktionen, Prozeduren, Packages und auch DDL-Statements von Postgres in Oracle ausgeführt werden.

Gleiches gilt für das Oracle Gateway for ODBC. Mit diesem stellt Oracle ein sehr gutes Werkzeug für die Integration von Postgres zur Verfügung, das keine Wünsche offenlässt. Der Datenaustausch ist möglich und mit dem DBMS_HS_PASSTHROUGH können Funktionen und Prozeduren von Oracle in Postgres ausgeführt werden.

Ausblick

Im dritten Teil von „Data Exchange with PostgreSQL“ werden wir den Table Data Stream FDW, für den Zugriff von Postgres auf MSSQL-Server, und den Linked-Server mit psqlODBC für den Zugriff von MSSQL-Server auf Postgres kennenlernen. Wir werden auch noch einen Blick

```
SID_LIST_LISTENER=
   (SID_LIST=
       (SID_DESC=
           (SID_NAME=PGDB1)
           (ORACLE_HOME=/opt/oracle/product/18c/dbhomeXE)
           (PROGRAM=dg4odbc)
           (ENV="LD_LIBRARY_PATH=/usr/lib64:
               /opt/oracle/product/18c/dbhomeXE/lib")
       )
   )

$ lsnrctl status LISTENER
...
Service "PGDB1" has 1 instance(s).
   Instance "PGDB1", status UNKNOWN, has 1 handler(s) for this service...
...
```

Listing 19: Konfiguration listener.ora und Ausgabe des Postgres Service

```
PGDB1.noborders.com =
   (DESCRIPTION=
       ADDRESS=(PROTOCOL=tcp)(HOST=oraclehost)(PORT=1521))
       (CONNECT_DATA=(SID=PGDB1))
       (HS=OK)
   )
```

Listing 20: Anpassung tnsnames.ora

```
CREATE DATABASE LINK pgdb1
  CONNECT TO "pguser"
  IDENTIFIED BY "***************"
  USING 'pgdb1.noborders.com';
```

Listing 21: Anlegen eines DB-Links auf eine Postgres-DB

```
SQL> select * from “pt1”@pgdb1;
  id text
---- --------------------------------------------------
   1 Host pghost
   2 Postgres DB pgdb1
   3 Owner admin1
   4 Schema admin1
   5 Table pt1

SQL> insert into "pt1"@pgdb1 values (20, 'Grüße von Oracle');
SQL> update "pt1"@pgdb1 set "text"='Update von Oracle' where "id"=20;
SQL> delete from "pt1"@pgdb1 where "id"=20;
```

Listing 22: SELECT / INSERT / UPATE / DELETE von Oracle auf eine Postgres- Tabelle

```
SQL> DECLARE
          num_rows INTEGER;
      BEGIN
          num_rows := DBMS_HS_PASSTHROUGH.EXECUTE_IMMEDIATE@pgdb1
              ('select f_write_pt1(21, ''function executed from
oracle'');');
      END;
```

Listing 23: Ausführen einer Postgres-Funktion mit DBMS_HS_PASSTHROUGH

auf PostgREST werfen, eine Möglichkeit, REST- Schnittstellen für Postgres bereitzustellen.

Quellen

Oracle_FDW

- *https://laurenz.github.io/oracle_fdw/*
- *https://github.com/laurenz/oracle_fdw*
- *https://pgxn.org/dist/oracle_fdw*

Oracle Gateway for ODBC

[1] *https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dblic/Licensing-Information.html#GUID-0F9EB85D-4610-4EDF-89C2-4916A0E7AC87*

[2] *https://www.enterprisedb.com/edb-docs/d/edb-postgres-odbc-connector/user-guides/odbc-guide/12.0.0.1/edb-odbc_connection_properties.html*

[3] *https://www.zabbix.com/documentation/current/manual/config/items/itemtypes/odbc_checks/unixodbc_postgresql*

[4] *https://docs.oracle.com/database/121/ARPLS/d_hspass.htm#ARPLS66494*

https://frankgerasch.de/2018/05/zugriffe-von-oracle-auf-postgresql/

Über den Autor

Michael Kloker arbeitet seit 20 Jahren bei Boehringer Ingelheim in der IT. In dieser Zeit hat er an einer Vielzahl unterschiedlicher Themen gearbeitet und verfügt über ein sehr breites und tiefes Wissen zu Betriebssystemen, Datenbanktechnologien, Virtualisierungslösungen, Applikationsservern, Verzeichnisdiensten, Authentifizierungsmethoden, Applikations- und Prozesswissen. Heute kümmert sich Michael Kloker um die Implementierung, den störungsfreien Betrieb, Systemupdates und die Weiterentwicklung neuer und bestehender Computersysteme für die pharmazeutische Entwicklung sowie den Datenaustausch und die Schnittstellenthematik unterschiedlicher Computer- und Datenbanksysteme.

Michael Kloker
michael.kloker@boehringer-ingelheim.com

Lockdown oder: Wie ich lernte, die Cloud zu lieben – Teil 2

Dr. Jörg Domaschka, Institut für Organisation und Management von Informationssystemen
Steffen Moser, School of Advanced Professional Studies (SAPS)
Thomas Nau, Kommunikations- und Informationszentrum (kiz)
Simon Volpert, Institut für Organisation und Management von Informationssystemen
Alle Autoren arbeiten an der Universität Ulm.

Die COVID-19-Pandemie hat im vergangenen Jahr oft schmerzhaft gezeigt, wie grundlegend wichtig eine stabile, durchgehende, sichere und zeitgemäße Versorgung mit IT-Services im täglichen Leben ist. Auch die Hochschulen bilden hier keine Ausnahme. Dabei spielt „die Cloud", obwohl schon lange als nächster Schritt der IT-Evolution gehandelt, in diesem Bereich oft nach wie vor nur eine Nebenrolle. Dies ist aus mehreren Gründen verständlich: Zum einen existieren vielfältige unterschiedliche Definitionen und Ansichten über das, was eine Cloud ist beziehungsweise ausmacht. Zum anderen ist die IT oft sehr eng mit lokalen Prozessen und Anforderungen verwoben, die eine On-Premises-Lösung – das scheinbare Gegenteil einer Cloud – geradezu erzwingen.

Dieser Artikel fasst die Geschehnisse in den Wochen vor und nach der Anordnung des Lockdowns an der Universität Ulm im März 2020 zusammen. Ziel ist es, den Lesern die insbesondere technischen Voraussetzungen und Entscheidungen aufzuzeigen, die es letztendlich erlaubt haben, die Arbeitsfähigkeit von Lehre, Verwaltung und Forschung an der Universität Ulm in sehr hohem Maße zu gewährleisten. Dieser Artikel zeigt das Spannungsfeld auf und fasst die Entstehungsgeschichte unserer Cloud-Lösung für unser Videokonferenzsystem sowie die gemachten Erfahrungen in der Hoffnung zusammen, anderen als Anregung für eigene interne Diskussionen zu dienen.

Teil 2: Konzeption und Umsetzung

Der erste Teil der Serie *(siehe Heft 03/2021)* fokussierte sich auf die Darstellung der organisatorischen und technischen Hintergründe und stellte die Video-Konferenz-Software BBB vor. Der vorliegende zweite Teil nimmt eine technischere Sichtweise ein und konzentriert sich auf betriebliche Aspekte von BBB, seine Skalierung und die Automatisierung des Betriebes. Der anschließend folgende Teil 3 beschäftigt sich dann mit dem Konfigurations-Management.

Überblick

Wie in Teil 1 detailliert dargestellt, handelt es sich bei BigBlueButton (BBB) um eine Client-/Server-basierte Videokonferenz-Software. Typischerweise ist BBB als On-Premises-Lösung gedacht, die von der nutzenden Einrichtung selbst auf einer Server-Infrastruktur gehostet wird. Architektonisch besteht BBB aus einem Server-Teil und einem Client, wobei Letzterer seit Version 2.2.0 (erschienen im November 2019) in einem HTML5-fähigen Webbrowser abläuft. Entsprechend werden auf Seiten der Nutzer weder Plug-ins noch Browser-Extensions benötigt.

Beim Server-Teil von BBB handelt es sich um einen Verbund aus einer Vielzahl von Modulen für die unterschiedlichen Aufgaben in einem Videokonferenzszenario. Neben Eigenentwicklungen des BBB-Teams kommen hier auch andere Open-Source-Komponenten zum Einsatz wie FreeSWITCH zur VoIP-Telekommunikationslösung und Kurento als Medienserver.

Skalierbarkeit von BBB

Die verteilte Architektur von BBB erlaubt es prinzipiell, die Komponenten einer BBB-Installation auf mehrere Server zu verteilen. Dieses Vorgehen ist jedoch nicht dokumentiert und entsprechend wird von einem solchen Betriebsmodus abgeraten. Stattdessen wird sowohl von den Entwicklern als auch von der Community empfohlen, das Ubuntu-basierte BBB-Installationsskript zu verwenden, das dafür Sorge trägt, alle Module auf einen Server zu installieren und miteinander zu verbinden.

Das Skript setzt Ubuntu 16.04 voraus und installiert die als Ubuntu-Pakete bereitgestellten BBB-Komponenten sowie externe Pakete wie nodejs, Redis, MongoDB, aber auch FreeSWITCH und Kurento. Durch die vielen gegenseitigen Abhängigkeiten der Module ist eine Migration auf andere Distributionen als Ubuntu, oder sogar auf eine modernere Version als die offiziell unterstützte 16.04, als sehr schwierig einzustufen.

Auf Grund des Single-Server-Setups begrenzt die Kapazität des (physischen) Servers die Leistungsfähigkeit der BBB-Installation. Insbesondere setzt der Server eine harte Grenze für die maximale Größe eines Meetings. Um diese Grenze zu erhöhen, kann eine BBB-Installation nur klassisch vertikal, also durch Vergrößern des Servers, skaliert werden. Aber auch hier sind der Skalierbarkeit Grenzen gesetzt: Zwar profitieren sowohl FreeSWITCH als auch Kurento inzwischen in hohem Maße von einer parallelen Architektur, jedoch stellt in der derzeitigen stabilen Version von BBB nodejs einen Flaschenhals dar, da es nur einen Rechenkern ausnutzen kann.

Eine horizontale Skalierung ist insofern möglich, als dass durch Hinzunahme weiterer Server eine größere Zahl an Meetings unterstützt werden kann. Die maximale Größe einzelner Meetings ist jedoch nach wie vor durch die Größe der Server begrenzt, da ein Meeting nicht über mehrere Server verteilt werden kann. Eine horizontale Skalierung lässt sich am einfachsten durch die Verwendung des Scalelite-Load-Balancers realisieren *(siehe Abbildung 1)*. Hier werden neben dem Load-Balancer mehrere unabhängige BBB-Instanzen betrieben, wobei der Load-Balancer bei jedem neu zu startenden Meeting einen der BBB-Server auswählt. In der Standard-Konfiguration erfolgt diese Auswahl basierend auf der Anzahl der derzeit laufenden Meetings sowie der aktiven Audio- und Videoströme. Die jeweiligen Statistiken erfragt der Load-Balancer periodisch von den Instanzen. So ermittelt er nicht nur deren Last, sondern kann auch feststellen, ob

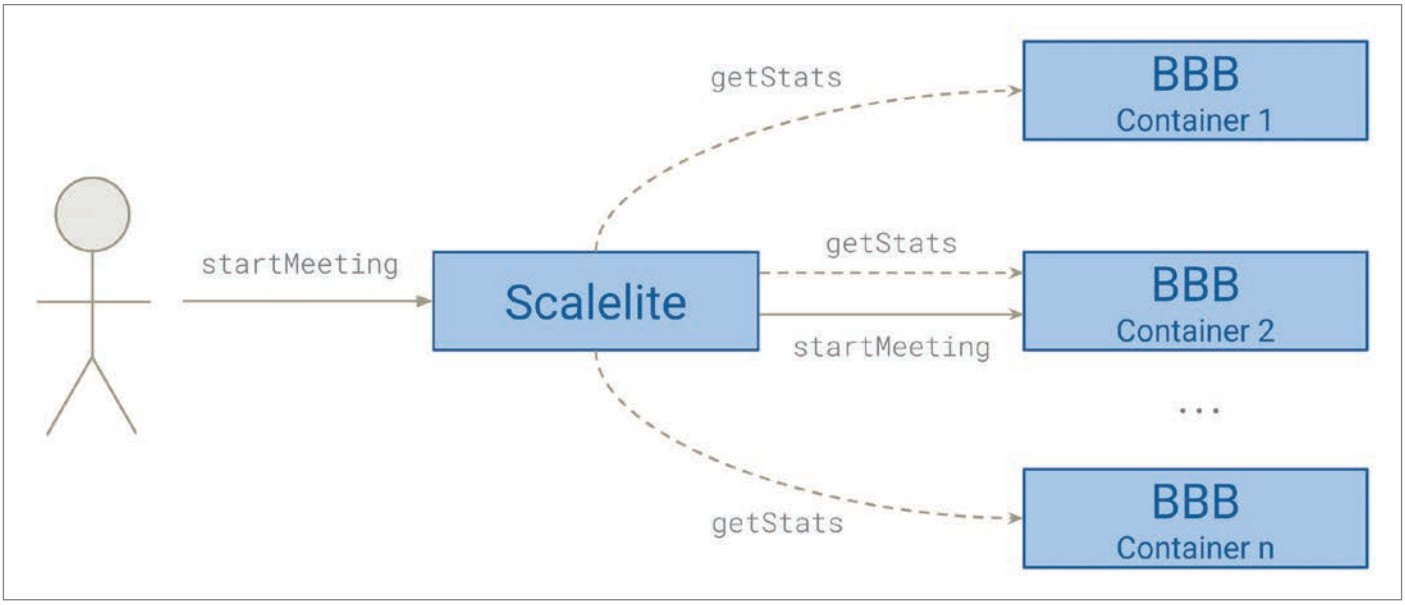


Abbildung 1: Skalierte BBB-Installation mit Scalelite (Quelle: Thomas Nau)

BBB-Instanzen ausgefallen – im Sinne von nicht erreichbar – sind, und diese als Ziel ausschließen.

Releases und Release Management

Die Komponenten von BBB werden in Form mehrerer .deb-Pakete für Ubuntu 16.04 herausgegeben. Ein Release von BBB wird also durch eine Komposition verschiedener Versionen von .deb-Paketdateien definiert. Ein installiertes Release gilt nur dann als konsistent und korrekt installiert, wenn alle .deb-Files auf die richtige Version gebracht werden. Spielraum für Administratoren, nur Teilkomponenten zu aktualisieren, ist nicht vorgesehen.

Mit dem operativen Alltag schwierig in Einklang zu bringen ist das Release-Management von BBB. Bedingt durch die Pandemielage explodierte die Zahl der Nutzer in kürzester Zeit und damit auch die Zahl der Feature-Wünsche und Pull-Requests, die an die Entwickler gerichtet wurden. Dies führte dazu, dass eine große Zahl benötigter Merkmale, die ursprünglich für die kommende Version 2.3 geplant waren, in Version 2.2 zurückportiert wurden. Zwischenzeitlich wurde sogar die Produktivversion 2.2.x zum Hauptentwicklungszweig, wodurch sich die Freigabe von Version 2.3 deutlich verzögerte.

Eine Trennung zwischen der Bereitstellung neuer Merkmale, dem Korrigieren von Bugs und der Beseitigung von Sicherheitslücken fand demnach kaum noch statt. Zu Beginn der Pandemielage wurden teilweise bis zu fünf Minor-Releases pro Monat freigegeben, die aufgrund der enthaltenen Sicherheitskorrekturen zeitnah in das Produktivsystem zu überführen waren.

Die Vermischung der Herausgabe von neuen Features sowie Bug- und Sicherheits-Fixes erschwerte den Betrieb enorm, da es einen reinen Wartungsbetrieb unmöglich machte. Die Änderungen innerhalb von Minor-Releases waren teilweise so signifikant, dass invasive Anpassungen der Konfiguration notwendig wurden.

Lösungskonzept

Kern unseres Umsetzungskonzeptes ist die Wiederverwendung von Funktionsblöcken und Tools, die sich bereits in der Vergangenheit bewährt haben. Hierzu zählen der Verzicht auf die grafische GUI der bwCloud, die Versionierung von Software-Artefakten mithilfe von Containern und der Einsatz eines Container-Orchestrierers zum Ausbringen von versionierten Software-Artefakten und deren ebenfalls versionierter Konfiguration.

Zum Betrieb von BBB sind somit die folgenden Schritte notwendig

1. Containerisierung von BBB, insbesondere
   a. Containerisierung einer BBB-Single-Node-Instanz
   b. Containerisierung und damit Versionierung der BBB-Konfiguration
2. Beschreibung eines BBB-Systems für einen Orchestrierer bestehend aus
   a. Scalelite und Scalelite-Konfiguration
   b. BBB-Container und BBB-Konfiguration
   c. Monitoring
3. Automatisierte Bereitstellung von virtuellen Maschinen und Orchestrierer.

Ein besonderer Fokus lag hierbei darin, alle Schritte weitestgehend zu automatisieren und möglichst keine veränderlichen Elemente zu erlauben. So können unter anderem schnelle Deployment-Iterationen und eine angemessene Wartbarkeit erreicht werden.

Von 0 auf 100 in 12 Tagen

Mit Beginn des Lockdows standen der Video-Conferencing-Task-Force zwölf Kalendertage zur Verfügung, um eine BBB-Installation bereitzustellen, die in Stoßzeiten von damals geschätzt 5.000 Studierenden gleichzeitig genutzt werden kann, die Nutzungszeiten zwischen 05:00 Uhr morgens und 23:00 Uhr nachts hat und deren Ausfall und Störung massive Nutzerbeschwerden nach sich ziehen und entsprechend First- und Second-Level Support-Ressourcen von anderen Diensten abziehen würde.

Zu diesem Zeitpunkt war bereits durch die SAPS Know-how im Betrieb von BBB vorhanden, anzumerken ist jedoch, dass die Nutzung des Tools in der Weiterbildung aus Betreibersicht keine besondere Herausforderung an die technische Infrastruktur stellte. So waren es bis Frühjahr 2020 doch üblicherweise abendliche Webinare und Sprechstunden mit wenigen kleinen Übungsstunden von jeweils ca. 5-25 Studierenden, die die Infrastruktur bewältigen musste. Diese Last war problemlos mit einer virtuellen Maschine (6 vCores, 16 GB RAM) auf Grundlage eines Oracle-Solaris-11.4-Servers zu stemmen. Hostübergreifende Parallelisierung war hier also nicht relevant.

Uns war klar, dass wir für den Betrieb während des Semesters deutlich mehr Ressourcen benötigen würden. Deren Menge und Ausprägung war jedoch noch unbekannt. Ebenso war klar, dass wir während des Semesters Verbesserungen und Patches einspielen werden müssten, da keine Zeit bestand, das System im Vorfeld ausreichend zu testen und zu härten. Eine Beschaffung von neuer Hardware stand wegen der kurzen Zeitspanne außer Frage und machte die Nutzung einer Cloud-Infrastruktur zur naheliegenden Alternative.

Unter anderem wegen der Echtzeit-Anforderungen von BBB stand die Verwendung einer Public Cloud nicht zur Debatte, da wir durch den europaweiten Lockdown mit einer erhöhten Last und damit erhöhten Interferenz auf diesen Services rechneten. Stattdessen konnten wir auf die regionale bwCloud am Standort Ulm ausweichen *[1]*. Dies ermöglichte es uns unter anderem, ein besonderes Scheduling von BBB-VMs zu realisieren, sodass hier immerhin nicht mit Interferenzen durch andere Workloads zu rechnen war.

Nichtsdestotrotz musste eine Lösung gefunden werden, die es uns erlaubte

- ein Flotte von damals geschätzten 20 BBB-Servern zu betreiben (im Wintersemester 2020 betrug die Zahl der eingesetzten BBB-Server tatsächlich 30),
- in dieser Flotte zeitnah und im laufenden Betrieb Software-Updates einzuspielen und neue Versionen zu testen (Canary Releases),
- fehlerhafte Updates problemlos zurückzurollen und fehlerhafte Konfigurationen auf die einfachste mögliche Art und Weise zu beheben, nämlich durch ein Neu-Erstellen einer virtuellen Maschine.

Das Institut für Organisation und Management von Informationssystemen (OMI) der Universität Ulm hat diese Themen als Arbeitsschwerpunkte und seine Mitarbeiter haben in den letzten Jahren praktisch

anwendbare Konzepte entwickelt, um den Betrieb noch weit größerer Software-Cluster durch weitreichende Automatisierung stark zu vereinfachen *[2]*. Auf dieses Vorwissen und passende Software-Tools konnten wir zurückgreifen.

Anforderungen

Um von Beginn an eine solide Lösung zu betreiben, standen für uns drei technische Aspekte im Vordergrund: Reproduzierbarkeit, Skalierbarkeit und Wartbarkeit. Dieser Fokus bewährte sich bereits in der Vergangenheit und ermöglicht es, flexibel und agil zu bleiben. Insbesondere das Aufrechterhalten der Flexibilität war ein zentrales Ziel für dieses Projekt, da sich Details in der Installation und Konfiguration erst durch eine Wechselwirkung zwischen Betrieb und Nutzern herausstellen.

Reproduzierbarkeit nimmt eine Schlüsselrolle bei der Automatisierung ein. Ist jeder Schritt ausgehend vom Deployment der ersten VM bis hin zur Konfiguration vollständig dokumentiert und jederzeit reproduzierbar, stellt dies die Basis für eine vollständige Automatisierung dar. Zudem reduziert dieses Vorgehen die Gefahr des „Configuration Drift", also des Vorgangs, durch manuelles Aktualisieren und Patchen der Systeme Dokumentation und Wirklichkeit schleichend inkonsistent werden zu lassen.

Automatisierung wiederum ist essenziell für die **Skalierbarkeit** des Systems. Hauptaugenmerk ist im Falle von BBB das Skalieren der „Worker Nodes", in *Abbildung 2* als „BBB VM" und „BBB Container" dargestellt. Meetings werden nach bestimmten Regeln auf diese Nodes verteilt *(siehe Skalierbarkeit von BBB)*. Diese Verteilung wird von der ebenfalls in *Abbildung 2* dargestellten „Scalelite"-Komponente umgesetzt. Sollten alle Nodes gesättigt sein, muss ein neuer Node zur Verfügung gestellt werden, um den Betrieb aufrecht erhalten zu können. In diesem Fall ist ein rechtzeitiges und zügiges Vorgehen äußerst wichtig. Dieses Vorgehen ermöglicht zudem, das Potenzial der Elastizität auszuschöpfen. Insbesondere wäre es denkbar, dynamisch Nodes bei geringerer Gesamtauslastung zu stoppen oder gar zu löschen. Dieses Vorgehen wurde für BBB allerdings nicht umgesetzt, weil dem Mehraufwand kein entsprechender Nutzen gegenüberstand.

Auch die **Wartbarkeit** steht in großem Zusammenhang mit der Reproduzierbarkeit. Wir erreichen eine ausreichende Wartbarkeit durch die Identifikation von zustandsbehafteten Teilen des Gesamtsystems. Dies wird Thema des dritten Teils der Artikel-Serie sein.

Deployment

Für das Deployment (Ausbringen) der Anwendungen auf der Cloud ist eine Automatisierung auf zwei Ebenen nötig: Zum einen muss die Anwendungs-Spezifikation samt Konfiguration auf die virtuellen Maschinen ausgebracht werden. Dies geschieht in unserem Fall mithilfe eines Orchestrierers. Zum anderen müssen die benötigten virtuellen Maschinen gestartet, das dort verwendete Betriebssystem konfiguriert und die VMs an den Orchestrierer angebunden werden. Für beide Schritte sind eine Vielzahl von Tools vorhanden.

Virtuelle Maschinen mit Ansible

Aufgrund von positiven Erfahrungen in der Vergangenheit haben wir uns zur Automatisierung der Interaktion mit dem Cloud API für Ansible *[3]* entschieden.

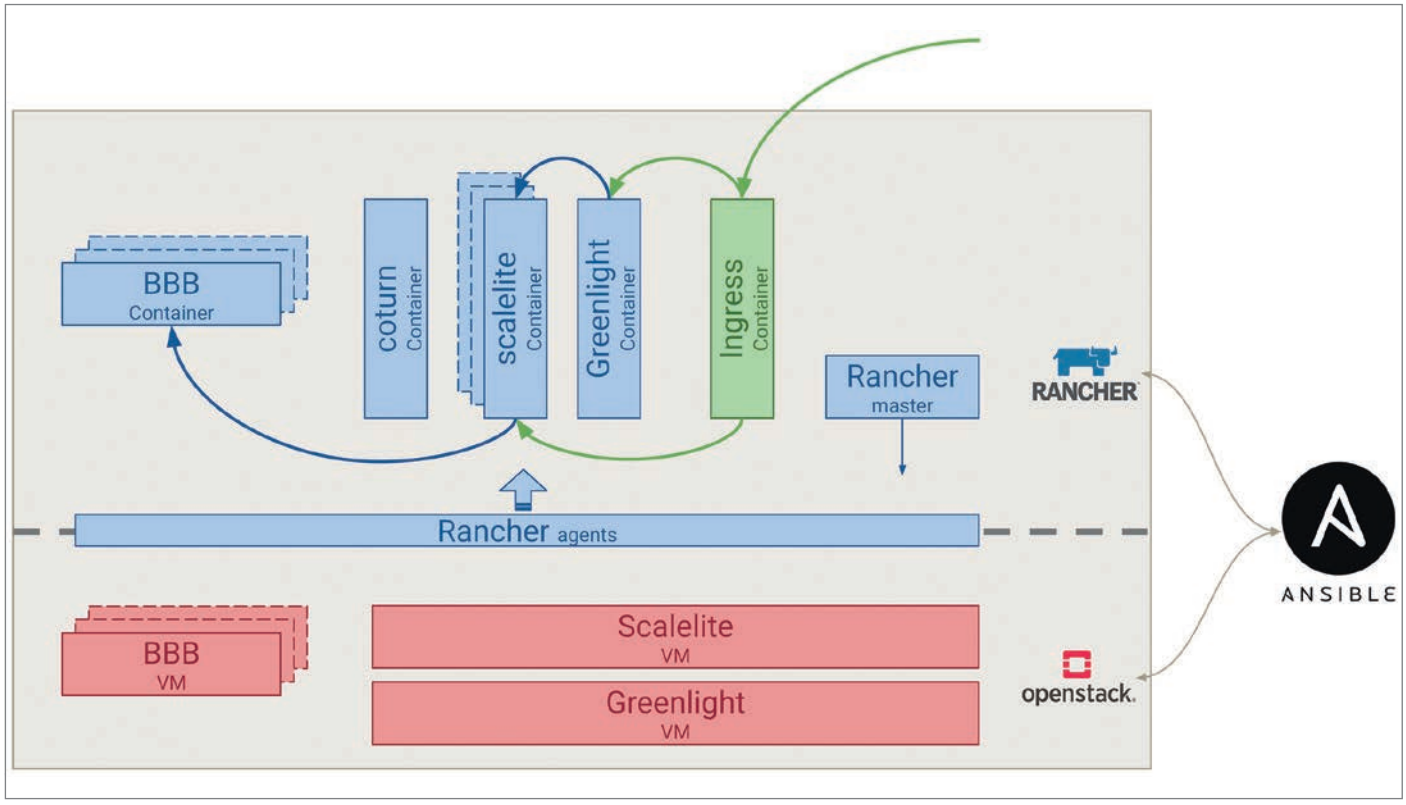


Abbildung 2: Deployment-Ebenen inklusive Zugriffsablauf (Quelle: Thomas Nau)

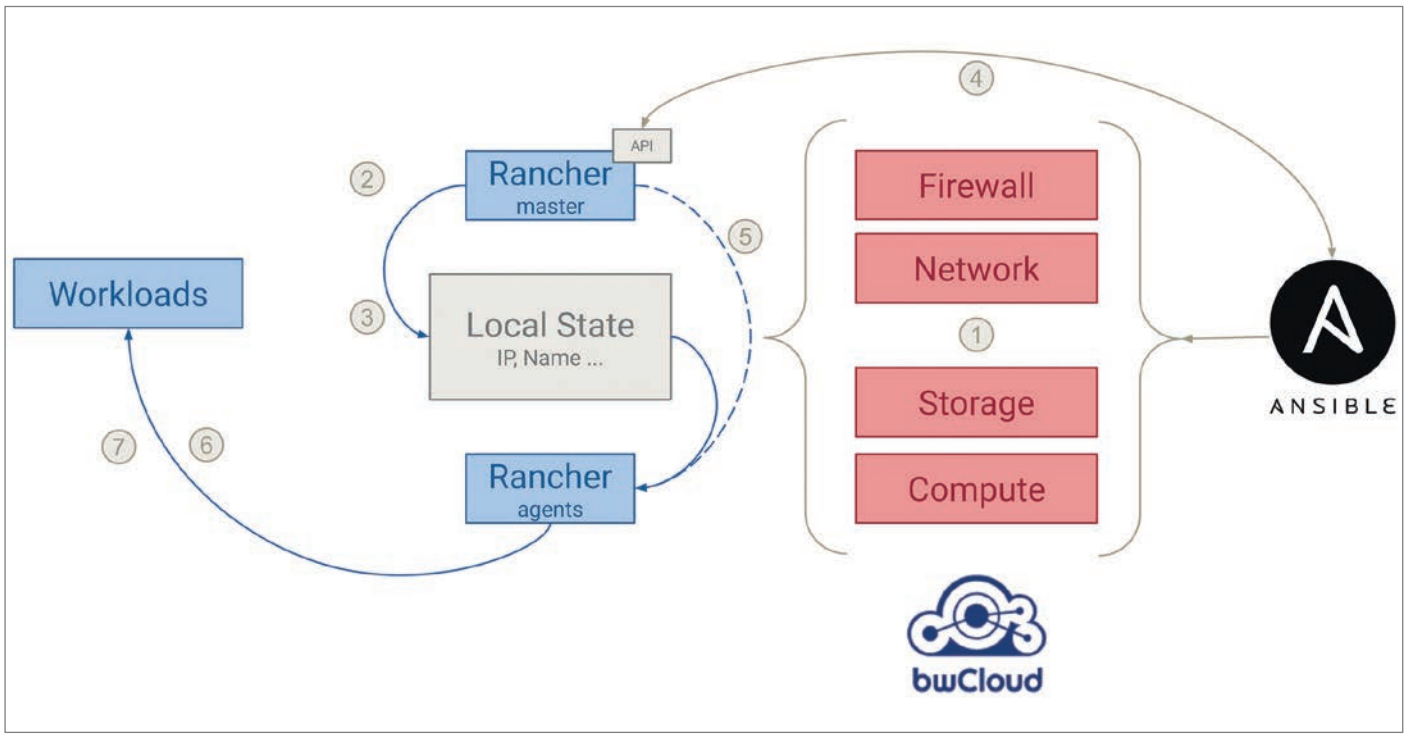


Abbildung 3: Schrittweises Deployment der BBB-Anwendung in bwCloud (Quelle: Thomas Nau)

Ansible ist niederschwellig, aber gleichzeitig mächtig genug, um alle unsere Anforderungen zu erfüllen. Zudem bietet es Module für die Verwaltung von virtuellen Maschinen in OpenStack (bwCloud).

Eine vollständig auf Ansible basierende Lösung wäre zwar umsetzbar, ist in der Praxis jedoch unkomfortabel. Insbesondere das Verwalten der Container (mehrere Hundert) über Konfigurations-Dateien, deren Verbindung auf Netzwerkebene ist mühsam, fehleranfällig und potenziell sicherheitskritisch. Außerdem erfordert das Aktualisieren eines Containers in diesem Fall ein erneutes Ausbringen der virtuellen Maschinen, auch wenn sich auf Betriebssystem-Ebene keine Änderungen ergeben haben.

Container mit Rancher

Ein Container-Orchestrierer vereinfacht das Management von verteilten, containerisierten Anwendungen. Bei der Verwendung eines Orchestrierers sorgt Ansible also lediglich dafür, dass ein Orchestrierer-Master gestartet wird sowie alle virtuellen Maschinen, auf denen BBB zur Ausführung kommen soll, mit diesem verbunden werden. Der Orchestrierer kümmert sich dann um die Verteilung der Container.

Auch hier steht eine Vielzahl von Tools zur Verfügung, von denen Kubernetes *[4]* sicherlich das derzeit Bekannteste ist. Kubernetes hat jedoch Probleme bei der Unterstützung von WebRTC. Zudem hatten wir zum damaligen Zeitpunkt keine wesentliche Betriebserfahrung damit. Die Wahl fiel entsprechend pragmatisch auf Rancher *[5]* (v1.6), weil wir damit bereits deutlich mehr Betriebserfahrung in kritischen Bereichen hatten und Rancher eine wesentlich geringere Komplexität als andere Orchestrierer aufweist.

Synthese

Der Orchestrierer beziehungsweise Rancher stellt das Bindeglied zwischen VMs und Containern dar. Rancher erstellt dynamisch virtuelle Netzwerke und Tunnel zwischen den Containern. Zudem stellt Rancher einen DNS-Server zur Verfügung, wodurch sich Container über ihre jeweiligen Namen Host-übergreifend erreichen können. Daneben stellt Rancher ein API zur Verfügung, über das alle Aspekte von Containern verwaltet werden können. Dadurch muss somit nicht mehr jeder Container Teil der Betriebssystem-Konfiguration sein, sondern kann dynamisch von Rancher verwaltet werden. Im Rückschluss bedeutet das für unser Gesamtkonzept, dass eine VM nicht gelöscht werden muss, wenn sich ein Container ändert, da Rancher dafür Sorge trägt, die Änderungen umzusetzen.

Der einzige Container, der in diesem Fall noch mittels Betriebssystem-Konfiguration gestartet wird, ist ein Adapter-Container, der einen „Rancher Agent" implementiert. Dieser meldet sich am „Rancher Master" an, der wiederum das API zur Konfiguration der Anwendung zur Verfügung stellt. Zum Ansprechen dieses API steht ebenfalls ein Ansible-Modul zur Verfügung.

Die horizontale Skalierung der VMs und Container für die Worker-Nodes wird von Ansible und nicht vom Orchestrierer umgesetzt. Dieses Vorgehen erleichtert den Canary Rollout und ermöglicht ein dediziertes Eingreifen in spezifische Deployments auf Worker Nodes. Teil der Ansible-Konfiguration ist ein Skalierungsparameter, der den Einfluss auf die Skalierung des Deployments bestimmt. So werden im Falle eines Skalierungsparameters von „20" unter anderem 20 Worker VMs gestartet und dort jeweils eine BBB-Instanz installiert.

Das schrittweise Deployment in der finalen Umsetzung sieht entsprechend wie folgt aus und wird durch *Abbildung 3* veranschaulicht:

1. Deployment der virtuellen Maschinen
2. Deployment des Rancher-Master-Servers
3. Rancher-Master-Daten werden an Ansible übermittelt
4. Rancher-Master-API ist verfügbar
5. Rancher Agents melden sich bei Rancher an
6. Deployment der funktionalen Anwendungen (Scalelite, BBB) und deren Konfiguration
7. Deployment der nicht-funktionalen Anwendungen, insbesondere des Monitorings

Zusammenfassung und Ausblick

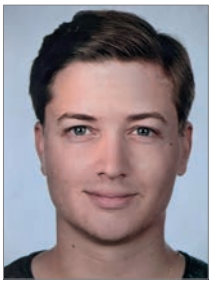
Nach etwa einem Jahr Produktiv-Betrieb blicken wir sehr zufrieden auf die getroffenen Entscheidungen und die umgesetzte Lösung zurück. Unser technisches Konzept hat sich während der letzten 12 Monate sehr bewährt. Wir waren immer dazu in der Lage, schnell auf wechselnde Anforderungen zu reagieren und Änderungen umzusetzen. Aus Mangel an Erfahrungswerten bezüglich großer BBB-Installationen erwies sich insbesondere die flexible Skalierung von Vorteil.

So war es eine Sache von ca. 30 Minuten, die Anzahl der Server von 20 auf 30 zu erhöhen und in Betrieb zu nehmen. Auch die Änderung des Hardware-Flavor zum Wintersemester (16 statt 8 Cores pro VM) konnte mittels Canary Release ohne großen Aufwand und ohne Unterbrechung im Betrieb vonstattengehen. Der dritte Teil dieser Beitragsserie widmet sich dem unserer Installation zugrunde liegenden Konzept der Immutability und vertieft die technischen Konzepte von Teil 2.

Quellen

[1] Siehe auch Red Stack Magazin Nr. 6 - 12/2019 „Die eigene Cloud – Wann eine On-Premises-Lösung Sinn macht“
[2] *https://medium.com/omi-uulm/the-vertical-immutable-infrastructure-pattern-ecd24b8af882*
[3] *https://www.ansible.com/*
[4] *http://kubernetes.io/*
[5] *https://rancher.com/docs/rancher/v1.6/en/*

Thomas Nau
thomas.nau@uni-ulm.de



Simon Volpert
simon.volpert@uni-ulm.de

Dr. Jörg Domaschka
joerg.domaschka@uni-ulm.de

Steffen Moser
steffen.moser@uni-ulm.de

„Mach mal schnell schneller“: Mythen über SQL-Performance

Dani Schnider, Trivadis

Kurze Antwortzeiten von SQL-Abfragen, Vermeidung von lang laufenden Verarbeitungsschritten: Gute Performance ist eine wichtige Voraussetzung in allen Datenbankapplikationen. Doch leider erfolgt Performanceoptimierung in vielen Projekten anhand von Annahmen und Gerüchten, die nicht oder nur teilweise stimmen. Einige dieser Mythen über SQL-Performanceoptimierung sollen hier geklärt werden.

Bei der Entwicklung von Datenbankapplikationen wird das Thema Abfrageperformance oft ausgeklammert oder zu wenig beachtet. Wichtig ist vorerst nur die Funktionalität der Applikation. Ob die SQL-Abfragen effizient sind, spielt ja während der Entwicklung noch keine Rolle. Der DBA (oder der Query Optimizer) richtet es dann schon. Notfalls können immer noch ein paar Indizes erstellt, Hints ergänzt oder Datenbankparameter angepasst werden. Und neuerdings macht ja die Oracle-Datenbank sowieso alles automatisch und autonom.

Wirklich? Ganz so einfach ist Performanceoptimierung in der Realität nicht. Für gute Antwortzeiten von SQL-Befehlen müssen ein paar Mythen zum Thema SQL-Performance widerlegt werden. Beginnen wir mit dem ersten weitverbreiteten Mythos:

„Performance-Tuning können wir später machen“

Der Query Optimizer von Oracle ist mit den aktuellen Datenbankversionen in der Lage, auch für sehr komplexe SQL-Queries gute Ausführungspläne zu berechnen. In den meisten Fällen, aber eben nicht immer. Wenn aber Execution Plans „kippen“ und somit zu langen Antwortzeiten führen, liegt das nicht „an der Datenbank“ oder „am schlechten Optimizer“, sondern meistens an der Applikation beziehungsweise dem ausgeführten SQL-Befehl.

Viele Performanceprobleme werden durch ein ungeeignetes Applikationsdesign, unpassende Datenmodelle oder ineffiziente SQL-Befehle verursacht. Solche Fehler nachträglich zu korrigieren, ist oft mit viel Aufwand verbunden. Wenn sich herausstellt, dass die Abfrage, die mit 10 Datensätzen wunderbar funktioniert hat, mit 100.000 Datensätzen viel zu lange läuft, lässt sich dies meistens nicht mit ein paar Konfigurationsänderungen beheben.

Deshalb ist es wichtig, in jeder Phase eines Projekts die Performanceanforderungen im Auge zu behalten. Die Architektur des Systems, der Aufbau der Applikation und des Datenmodells sowie eine grobe Abschätzung des Mengengerüsts spielen eine maßgebliche Rolle für die Effizienz der späteren Abfragen. Auch ist es sinnvoll, von

Worksheet | Query Builder

```
1  SELECT emp_id, first_name, last_name, dept_code, dept_name
2    FROM employees e
3    JOIN departments d ON (e.dept_id = d.dept_id)
4   WHERE e.last_name = 'Bond';
5
```

Autotrace

SQL HotSpot | 0.311 seconds

OPERATION	OBJECT_NAME	CARDINALITY	LAST_OUTPUT_ROWS	LAST_ELAPSED_TIME	COST
SELECT STATEMENT			1	169	3
NESTED LOOPS		1	1	169	3
NESTED LOOPS		1	1	114	3
TABLE ACCESS (BY INDEX ROWID BATCHED)	EMPLOYEES	1	1	59	2
INDEX (RANGE SCAN)	EMP_LAST_NAME	1	1	29	1
INDEX (UNIQUE SCAN)	DEPT_PK	1	1	15	0
TABLE ACCESS (BY INDEX ROWID)	DEPARTMENTS	1	1	17	1

Abbildung 1: Selektive Abfrage auf zwei Tabellen mit zugehörigem Execution Plan (Quelle: Dani Schnider)

Anfang an festzulegen, was für Anforderungen an die Performance notwendig und realistisch sind. Für eine Online-Applikation im Mehrbenutzerbetrieb kann eine Antwortzeit von einer Sekunde „langsam" sein, während ein Ladejob oder eine Tagesendverarbeitung schon als „schnell genug" gilt, wenn sie in wenigen Stunden durchläuft. Die Performanceanforderungen haben einen wesentlichen Einfluss auf die Systemarchitektur und das Applikationsdesign.

Aber ist das heute überhaupt noch relevant? Schließlich wird ja Hardware immer schneller und Memory immer billiger. Weshalb sollen wir uns da noch Gedanken zur Performance machen? Damit sind wir beim zweiten Mythos:

„Performanceprobleme können mit schneller Hardware gelöst werden"

Ja, das stimmt! Tatsächlich gibt es viele Beispiele, in denen zusätzliche CPUs, mehr Memory und schnellere Disks die Performance massiv verbessern. Ich stelle das regelmäßig fest: Es wird immer schwieriger, für Schulungen und Vorträge Beispiele von normalen SQL-Abfragen zu konstruieren, mit denen man überhaupt noch Performanceunterschiede aufzeigen kann. Mit moderner Hardware, SSD-Disks oder Datenbanken in der Cloud treten viele Performanceprobleme gar nicht mehr auf, auch wenn die Execution Plans nicht optimal sind.

Doch es gibt auch andere – teilweise sehr hässliche – Gegenbeispiele. Bei Performanceanalysen in meiner Rolle als Consultant werde ich immer wieder mit SQL-Queries konfrontiert, die auch leistungsfähige Plattformen an den Anschlag bringen. Wenn eine Query auf einer Exadata mehrere Stunden läuft oder wenn ein Ladejob in ein Data Warehouse tagelang dauert, hat dies kaum mit ungenügender Hardware zu tun. Fehlende Joinbedingungen, unnötige Subqueries, verschachtelte Aufrufe von PL/SQL-Funktionen, die wiederum SQL-Queries ausführen – die Liste von solchen „Horror-SQL"-Statements lässt sich fast beliebig fortsetzen.

Schnelle Hardware ist sicher eine gute Voraussetzung für optimale Performance. Aber schlechtes SQL wird dadurch nicht besser. Nicht mal mit zusätzlichen Indizes – womit wir beim nächsten Mythos wären:

„Indexzugriffe sind besser als Full Table Scans"

Sei es aus Unwissen oder Verzweiflung, für viele Leute ist „CREATE INDEX" der typische (oder einzige) Lösungsansatz, um eine langsame Query schneller zu machen. Das Ergebnis: Viele Datenbanken sind „überindexiert". Nicht jeder Index ist hilfreich, er kann in bestimmten Fällen sogar hinderlich sein. Oft ist ein Full Table Scan die bessere Wahl. Doch woher kommt der Mythos, dass Index Scans schnell und Full Table Scans langsam seien?

Ein Index ist ein hervorragendes Hilfsmittel, um eine kleine Menge von Datensätzen aus einer großen Tabelle zu lesen. Hier kommt die sogenannte Selektivität einer Abfrage ins Spiel. Sie gibt an, welcher prozentuale Anteil der Daten für eine Abfrage gelesen werden muss. Bei einer selektiven Abfrage werden nur wenige Daten gelesen. In diesem Fall ist ein Indexzugriff eine perfekte Wahl. Für eine unselektive Abfrage, in der ein großer Prozentsatz der Daten gelesen wird, ist ein Full Table Scan effizienter.

Abbildung 1 zeigt eine selektive Abfrage auf die Tabellen EMPLOYEES (6453 Rows) und DEPARTMENTS (27 Rows). Sie liest eine Person (James Bond) aus der Tabelle EMPLOYEES. Das ergibt für die Tabelle EMPLOYEES eine Selektivität von 1/6453, also ca. 0.015 %. Der Optimizer entscheidet sich deshalb für Indexzugriffe und einen Nested Loops Join der beiden Tabellen.

Dies ist ein typischer und sehr effizienter Execution Plan, wie er meistens in OLTP-Systemen verwendet wird. Für solche Abfragen sind Indizes perfekt, meistens in Kombination mit Nested Loops, der optimalen Joinmethode für kleine Datenmengen.

In Batchjobs (z.B. Tagesendverarbeitungen), aber auch in Abfragen über größere Datenmengen, haben wir es oft mit Queries zu tun, die einen höheren Prozentsatz der Daten lesen. Im zweiten Beispiel *(siehe Abbildung 2)* werden alle Mitarbeiter des Departements MI6 gelesen und ermittelt, wie viele davon eine „Licence to Kill" besitzen. Im MI6 (zumindest in unserem Beispiel) arbeiten 239 Personen. Die Datenmenge ist zwar auch hier bescheiden, aber die Selektivität für die Tabelle EMPLOYEES beträgt 239/6453, also ca. 3.7 %. Hier entscheidet sich der Optimizer für einen Execution Plan mit Full Table Scans und einem Hash Join der beiden Tabellen.

Diese Art von Execution Plans ist typisch für Ladeprozesse in Data Warehouses, für analytische Abfragen und Aggregationen in Reporting-Systemen. Weil hier der prozentuale Anteil der Daten höher liegt, ist ein Full Table Scan effizienter als ein Indexzugriff. Die magische Grenze der Selektivität liegt bei… Stopp! Wir möchten ja Mythen

Worksheet | Query Builder

```
1  SELECT e.licence_to_kill, COUNT(*)
2    FROM employees e
3    JOIN departments d ON (e.dept_id = d.dept_id)
4   WHERE d.dept_code = 'MI6'
5  GROUP BY e.licence_to_kill;
```

Autotrace

SQL HotSpot | 0.31 seconds

OPERATION	OBJECT_NAME	CARDINALITY	LAST_OUTPUT_ROWS	LAST_ELAPSED_TIME	COST
SELECT STATEMENT			2	2551	19
HASH (GROUP BY)		2	2	2551	19
HASH JOIN		239	254	2141	18
TABLE ACCESS (FULL)	DEPARTMENTS	1	1	72	3
TABLE ACCESS (FULL)	EMPLOYEES	6453	6453	474	15

Abbildung 2: Unselektive Abfrage auf zwei Tabellen mit zugehörigem Execution Plan (Quelle: Dani Schnider)

vermeiden, deshalb ist es keine gute Idee, hier eine konkrete Prozentzahl zu nennen. Ab welcher Selektivität ein Full Table Scan effizienter ist als ein Index Scan, hängt von verschiedenen Faktoren ab. Aber die Grenze liegt tiefer, als meistens angenommen wird – irgendwo im einstelligen Prozentbereich.

Ob ein Indexzugriff oder ein Full Table Scan die effizientere Wahl ist, hängt von der Selektivität der Abfrage ab. Doch wie ermittelt der Optimizer diese Selektivität? Dafür stehen die Optimizer-Statistiken zur Verfügung. Zum Glück müssen wir uns in den aktuellen Oracle-Datenbankversionen nicht mehr darum kümmern, denn...

```
BEGIN
   dbms_stats.gather_schema_stats
       ( ownname       => USER
       , method_opt    => 'FOR ALL COLUMNS SIZE SKEWONLY'
       , no_invalidate => FALSE);
END;
```

Listing 1: Berechnung von Optimizer-Statistiken mit DBMS_STATS

„Statistiken werden automatisch berechnet"

Auch dieser Mythos stimmt nicht immer. Zwar ist das Berechnen von Optimizer-Statistiken heute deutlich einfacher als in früheren Oracle-Versionen. Lange Jahre waren die häufigsten Ursachen für Performanceprobleme fehlende oder veraltete Statistiken. Inzwischen nimmt uns hier die Oracle-Datenbank die meiste Arbeit ab. Bereits seit Oracle 10g steht ein automatischer Statistikjob zur Verfügung, der jede Nacht fehlende und veraltete Statistiken für Tabellen und Indizes neu berechnet. Die Default-Einstellungen sind so gewählt, dass sie für viele Anwendungsbereiche genügen. Seit Oracle 12c werden außerdem bei einem *CREATE TABLE AS SELECT* und bei einem *Direct-Path INSERT* in eine leere Tabelle die Statistiken sofort berechnet. Mit Oracle 19c wurden für Exadata-Plattformen gleich zwei neue Features zum automatischen Berechnen von Optimizer-Statistiken eingeführt: „*High-Frequency Automatic Statistics Collection*" und „*Real-Time Statistics*".

All diese Erweiterungen haben das gleiche Ziel: Die Aktualisierung von Statistiken soll so weit wie möglich vereinfacht und automatisiert werden, um Performanceprobleme aufgrund falscher oder fehlender Statistiken zu vermeiden. Trotzdem gibt es nach wie vor Situationen, in denen wir uns selbst um die Statistikberechnungen kümmern müssen und sollen. Dies soll an zwei Beispielen erläutert werden, die mir in Kundenprojekten begegnet sind:

In einem E-Banking-System werden mehrmals täglich Zahlungsaufträge an eine Buchungsapplikation übermittelt. Für jede übermittelte Zahlung wird der Status von „*erfasst*" auf „*übermittelt*" gesetzt. Umgekehrt liefert die Buchungsapplikation die ausgeführten Buchungen zurück, worauf der Status der zugehörigen Zahlungsaufträge auf „*ausgeführt*" gesetzt wird. Die Datenverteilung für das Status-Attribut ist im E-Banking-System eine wesentliche Information für die Berechnung der Selektivität. Dazu stehen in den Optimizer-Statistiken Histogramme zur Verfügung. Für diesen Anwendungsfall genügt es jedoch nicht, diese einmal täglich zu berechnen. Die prozentuale Verteilung der verschiedenen Statuswerte ändert sich jeweils markant nach

Autotrace

SQL HotSpot | 0.463 seconds

OPERATION	OBJECT_NAME	CARDINALITY	COST	LAST_OUTPUT_ROWS	LAST_ELAPSED_TIME
SELECT STATEMENT			1339	35	177906
HASH JOIN		5353	1339	35	177906
HASH JOIN		5353	1024	35	54319
TABLE ACCESS (FULL)	ADDRESSES	27672	614	27211	23849
NESTED LOOPS		49384	268	324	15163
NESTED LOOPS		49384	268	324	4051
TABLE ACCESS (FULL)	MAILINGS	1	3	1	46
INDEX (RANGE SCAN)	REC_MLG_ID	49384	97	324	1337
TABLE ACCESS (BY INDEX ROWID)	RECIPIENTS	49384	265	324	4186
TABLE ACCESS (FULL)	PERSONS	154235	314	154235	34586

Autotrace

SQL HotSpot | 0.256 seconds

OPERATION	OBJECT_NAME	CARDINALITY	COST	LAST_OUTPUT_ROWS	LAST_ELAPSED_TIME
SELECT STATEMENT			55000	35	25177
NESTED LOOPS		5353	55000	35	25177
NESTED LOOPS		5353	55000	35	24009
NESTED LOOPS		5353	49667	35	22810
NESTED LOOPS		49384	268	324	6891
TABLE ACCESS (FULL)	MAILINGS	1	3	1	59
TABLE ACCESS (BY INDEX ROWID BATCHED)	RECIPIENTS	49384	265	324	4115
INDEX (RANGE SCAN)	REC_MLG_ID	49384	97	324	1451
TABLE ACCESS (BY INDEX ROWID)	ADDRESSES	1	1	35	11773
INDEX (UNIQUE SCAN)	ADR_PK	1	0	324	4564
INDEX (UNIQUE SCAN)	PRS_PK	1	0	35	542
TABLE ACCESS (BY INDEX ROWID)	PERSONS	1	1	35	475

Abbildung 3: Zwei Execution Plans für die gleiche SQL-Abfrage, mit und ohne Hints (Quelle: Dani Schnider)

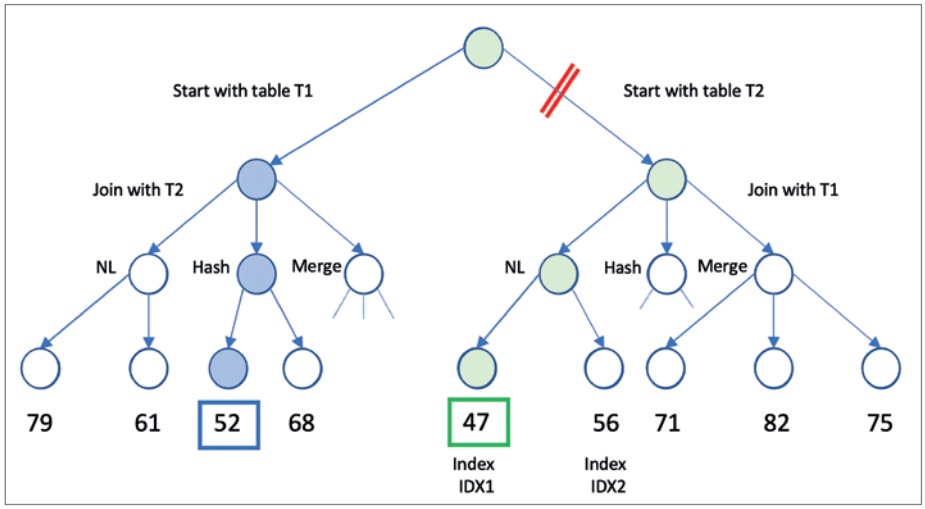


Abbildung 4: Entscheidungsbaum für unterschiedliche Execution Plans (Quelle: Dani Schnider)

jedem Datenaustausch zwischen den beiden Systemen. Deshalb musste das E-Banking-System so erweitert werden, dass jeweils nach dem Datenaustausch mit dem Buchungssystem die Histogramme für das Status-Attribut neu berechnet werden.

In einem anderen Fall ging es um die Migration einer bestehenden Applikation auf einen neuen Datenbankserver. Die Datenbank wurde mit Data Pump exportiert und auf dem neuen Server importiert. Dabei wurden auch die Statistiken neu gerechnet. Alles lief reibungslos, bis am Montagmorgen die ersten Abfragen gestartet wurden. Teilweise katastrophale Antwortzeiten waren die Folge. Als wir einen Tag später die Performanceprobleme analysieren wollten, lief die Applikation wieder einwandfrei. Was war passiert? Die Default-Einstellungen beim Berechnen der Optimizer-Statistiken sind so gesetzt, dass für Attribute mit ungleichmäßiger Datenverteilung Histogramme berechnet werden. Dies jedoch nur, wenn sie zuvor in Abfragen verwendet wurden. Das war natürlich auf der neuen Datenbank unmittelbar nach der Migration noch nicht der Fall. Am Montagabend lief dann erstmals der Default-Statistikjob. Weil tagsüber viele typische Queries ausgeführt wurden, hat dieser nun die fehlenden Histogramme berechnet. Ab Dienstag war die Welt wieder in Ordnung.

Die Performanceprobleme am ersten Arbeitstag hätten vermieden werden können, wenn die Statistiken nach dem Importieren mit einem geeigneten DBMS_STATS-Aufruf berechnet worden wären. *Listing 1* zeigt, wie dies durch Angabe der optionalen Parameter method_opt (Erstellung von Histogrammen) und no_invalidate (neue Statistiken werden sofort verwendet) implementiert werden kann.

In beiden Fällen haben sich die Kunden auf den Default-Statistikjob von Oracle verlassen. Obwohl damit zwar die Statistiken weitgehend automatisiert berechnet werden, funktioniert dies nicht in allen Fällen oder erst, nachdem typische Abfragen auf der Datenbank ausgeführt wurden.

„Hints reduzieren die Kosten eines Execution Plan"

Trotz guten Applikationsdesigns, schneller Hardware, geeigneter Indexierung und aktueller Statistiken: Performanceprobleme und suboptimale Execution Plans können in Ausnahmefällen immer noch auftreten. Für diese Fälle haben wir ein weiteres Werkzeug zur Verfügung, um den Optimizer auf den richtigen Weg zu führen: Hints.

Auch über Hints gibt es zahlreiche Mythen. Ein weitverbreiteter Mythos wird immer wieder genannt: Mit Hints können die Kosten eines Execution Plan reduziert werden. Das stimmt definitiv nicht. Im Gegenteil, Hints erhöhen die Kosten eines Execution Plan. Warum das so ist, soll hier erklärt werden.

Abbildung 3 zeigt zwei Execution Plans für die gleiche Abfrage. Der obere wurde vom Optimizer ermittelt, der untere mithilfe von Hints beeinflusst. Wie in der Spalte LAST_ELAPSED_TIME ersichtlich, ist die Variante mit Hints deutlich schneller, obwohl die Kosten des Execution Plan (Spalte COST) viel höher sind.

Der Query Optimizer von Oracle (auch „Cost-based Optimizer" genannt) berechnet für jedes SQL-Statement unterschiedliche Execution Plans und bewertet diese mit Kosten. Der „günstigste" Plan, also der mit den geringsten Kosten, wird schließlich ausgeführt.

Abbildung 4 zeigt einen (vereinfachten) Entscheidungsbaum für eine Query auf zwei Tabellen T1 und T2. Der Optimizer entscheidet sich, zuerst Tabelle T2 zu lesen und danach einen Nested Loops Join via Index IDX1 mit Tabelle T1 auszuführen. Warum? Weil dieser (grüne) Execution Plan die geringsten Kosten (47) hat.

Mittels Hint /*+ leading(T1) */ geben wir dem Optimizer vor, mit Tabelle T1 zu beginnen. Wir können uns das so vorstellen, dass durch Hints einzelne Äste des Entscheidungsbaums abgetrennt werden und deshalb nicht mehr zur Verfügung stehen. Mit dem so reduzierten Entscheidungsbaum macht der Optimizer, was er immer tut: Er entscheidet sich für den günstigsten Plan – in diesem Fall den (blauen) Execution Plan mit Kosten von 52. Aber diese Kosten sind natürlich höher als die 47 des ursprünglichen Ausführungsplans ohne Hints.

Mithilfe von Hints können wir zwar die Ausführungszeiten einer Query verbessern, nie aber die Kosten eines Execution Plan reduzieren. Das ist auch nicht das Ziel. Die Kosten sind nur ein Hilfsmittel für den Optimizer und werden basierend auf dessen Annahmen berechnet. Hints kommen typischerweise dann zum Einsatz, wenn sich der Optimizer „verschätzt" hat, also bei der Kostenberechnung von falschen Annahmen ausgegangen ist. Denn schließlich gilt:

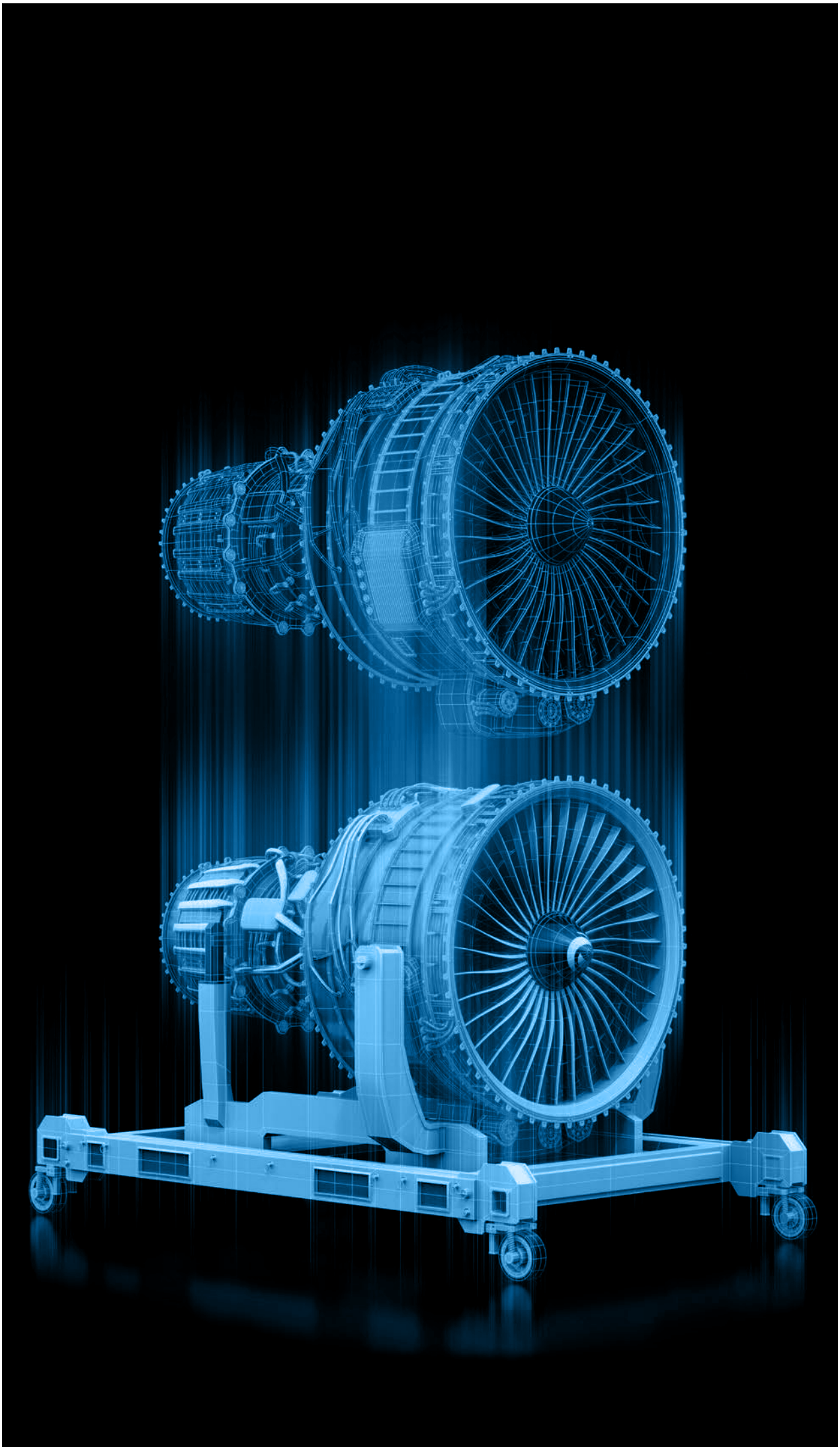
„Der Optimizer ist auch nur ein Mensch"

Dass dieser Mythos nicht stimmt, ist offensichtlich.

Dani Schnider
dani.schnider@trivadis.com

BUSINESS NEWS

04/2021



Was sind digitale Zwillinge?

Andreas Buckenhofer, DaimlerTSS

Der Artikel gibt eine Einführung zu digitalen Zwillingen und deren Nutzen, zeigt typische Use Cases und benennt häufig verwendete Technologien. Diese „virtuellen Doppelgänger" haben das Potenzial, zu einem Baustein in der Datenarchitektur zu werden.

Intro

Ein digitaler Zwilling ist ein virtuelles Abbild eines realen Objekts, das das Verhalten simulieren kann. Das Objekt kann ein Produkt (Häuser, Kühlschränke, Flugzeuge), eine Anlage (Bohranlagen, Werke inkl. Maschinen) oder ein Prozess (Sendungsverfolgung) sein.

Der Begriff wurde erstmalig von Michael Grieves im Rahmen eines Produktlebenszyklus-Managements im Jahr 2002 verwendet *[1]*. Die Idee dagegen ist älter. Für die Apollo-Mission 13 vor fünfzig Jahren wurde ein zweites Raumfahrzeug entwickelt, um während der Mission mithilfe realer Daten Tests durchzuführen *[2]*.

„Market And Market" bewerten den Markt für digitale Zwillinge mit 3.1 Mrd. USD im Jahr 2020 und erwarten bis 2026 ein Wachstum auf 48.2 Mrd. USD *[3]*. Digitale Zwillinge können zu einer wichtigen Komponente der IT-Infrastruktur werden. „Market And Market" sieht das größte Potenzial in den Industrien Gesundheitswesen & Pharmazie, Produktion sowie Luft- und Raumfahrt.

Digitale Zwillinge profitieren von der zunehmenden Digitalisierung in Verbindung mit der verstärkten Nutzung von Software in physikalischen Objekten. Bereits heute stecken in Fahrzeugen rund 100 Millionen Codezeilen. Zum Vergleich: Ein Betriebssystem kommt auf nicht einmal die Hälfte. In Zusammenhang mit digitalen Zwillingen spielen Technologien wie Machine Learning (ML) oder Trends wie das Internet der Dinge (IoT) eine wichtige Rolle *(siehe Abbildung 1)*.

Use Cases

Es existieren verschiedene Use Cases mit unterschiedlichen Zielsetzungen:

1. Erstellung eines digitalen Zwillings für ein noch nicht entwickeltes Objekt. Dies können Flugzeuge, Fahrzeuge, Anlagen und so weiter sein. Mithilfe des Zwillings werden verschiedene Varianten durchgespielt, bevor konkrete Design-Entscheidungen für das reale Produkt getroffen werden. Der

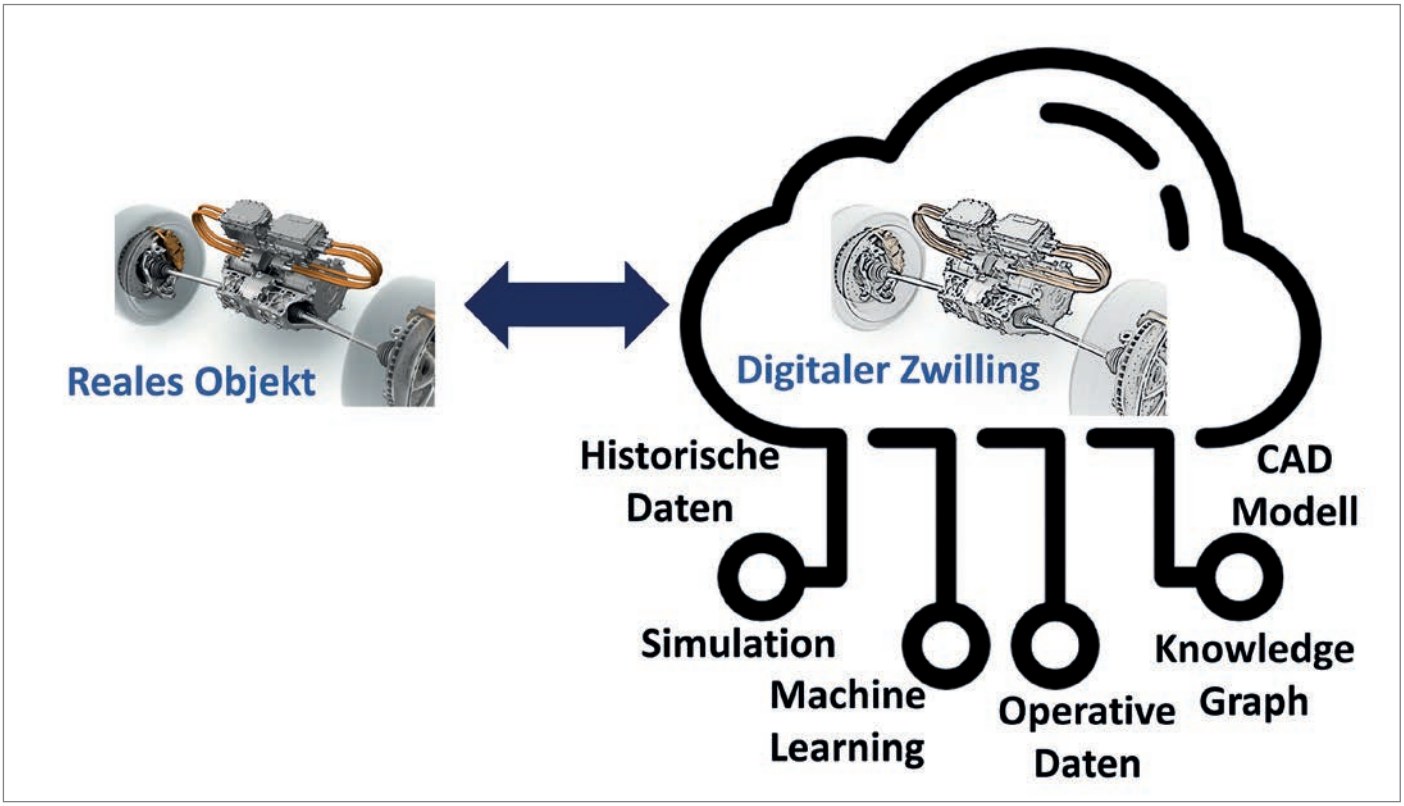


Abbildung 1: Reales Objekt und digitaler Zwilling (Quelle: Andreas Buckenhofer)

digitale Zwilling überwindet während der Konstruktionsphase Silos zwischen verschiedenen Abteilungen. In CAD-Anwendungen werden beispielsweise Nähte als Kurvenverläufe dargestellt. Für andere Datennutzer der rechnerunterstützten Konstruktion muss ersichtlich sein, ob es sich um eine Naht am Lenkrad, am Sitz oder an einer anderen Stelle handelt.

2. Erstellung des digitalen Zwillings parallel zum existierenden Projekt. Der Zwilling wird genutzt, um Sensordaten aufzunehmen und diese auszuwerten. So lassen sich Wartungsintervalle besser planen, ein Werk monitoren oder bei Material- beziehungsweise Produktströmen die Supply Chain verfolgen. Die Daten können über den gesamten Produktlebenszyklus erfasst und gesammelt werden.
3. Digitale Zwillinge können helfen, die hohen Kosten für Zertifizierungen zu verringern. Mithilfe von Modellen werden Simulationen durchgeführt, bevor mit den kostspieligen und aufwendigen Tests am realen Objekt begonnen wird. Außerdem sinkt das Risiko, dass am realen Objekt teure Schäden entstehen.

Ein konkretes Beispiel eines digitalen Zwillings ist ein Fahrzeug. Basis des Modells sind beispielsweise Stammdaten (wie Produktionsdatum, Ausstattungsmerkmale), Stücklisten (Aufbau des Fahrzeugs inklusive aller Bauteile bis zur einzelnen Schraube) und Sensordaten (wie Geschwindigkeit, Batterieladestand). Datenmenge und Datenvielfalt steigen stetig an. Die benötigte Rechenpower sowie benötigte Kommunikationstechnologien stehen zur Verfügung.

Für einen digitalen Zwilling reicht es jedoch nicht, immer mehr und immer bessere Daten zu sammeln. Das Verhalten des Fahrzeugs muss ebenfalls modelliert werden und unterscheidet den digitalen Zwilling von einem Data Warehouse (DWH), Data Lake oder Ähnlichem. Ein großes Potenzial bietet die Modellierung der Physik eines Fahrzeugs. Die Modellierung der Physik bezieht sich beispielsweise auf das Fahrverhalten, das je nach Konstruktion (Antrieb, Fahrzeugart, Radstand etc.) und Fahrsituation (Kurve, Bremsen etc.) unterschiedlich ist. Mithilfe von Simulationen und Prüfständen werden Bauteile auf verschiedene Belastungen ausgelegt bevor, das reale Fahrzeug auf Erprobungsfahrten unterwegs ist.

Nutzen

Ein digitaler Zwilling selbst bringt keinen Nutzen. Erst die konkrete Verwendung des Zwillings durch Simulation oder Datenanalyse erzeugt einen Mehrwert. Ein digitaler Zwilling wird vorrangig verwendet für:

- die Optimierung (zum Beispiel Auslegung von Bauteilen für zu erwartende maximale Belastungen, Reduzierung von Kosten)
- die Transparenz (zum Beispiel Sendungsverfolgung von Paketen)
- das Verständnis (zum Beispiel Erlangung neuer Erkenntnisse, besseres Verständnis der Abläufe in einer komplexen Anlage, Bestimmung von Software-Updates für das reale Objekt) von Produkten und Prozessen.

Um einen monetären Nutzen aufzuzeigen, muss eine Bewertung in Zusammenhang mit dem realen Objekt durchgeführt werden. Am realen Objekt können Kosteneinsparungen erzielt werden, die nur mithilfe des Zwillings zu realisieren sind.

Technologien

Kern eines digitalen Zwillings sind Daten und deren Management. Datenarchitektur, Datenmodellierung, Datenintegration und Datenqualität sind einige der Disziplinen des Datenmanagements. Das Datenmodell muss die Realität abbilden und das Verhalten beschreiben. Aufgrund der Komplexität und der ständigen Änderungen muss das Datenmodell flexibel sein. Graph-Modelle sind eine Möglichkeit, um flexible Erweiterbarkeit zu ermöglichen („think big, start small“) und gleichzeitig eine Struktur zu definieren. Graph-Modelle bilden stark vernetzte Informationen über Knoten und Kanten ab. Die Knoten enthalten die Eigenschaften und die Kanten verbinden die Knoten.

Daten aus verschiedenen dezentralen Systemen müssen referenziert werden. Ein Graph-Modell hilft dabei, Daten in verschiedenen Systemen zu referenzieren, ohne dass alle Daten in einem zentralen Data Lake zusammengeführt werden müssen. Auch die Komponenten von Zulieferern müssen mit einbezogen werden: „Mir ist die durchgängige Kette des digitalen Zwillings wichtig“, betont Daimler-CIO Jan Brecht *[4]*. Ein Datenaustausch zwischen OEM (Original Equipment Manufacturer) und den Zulieferern ist in beide Richtungen nötig.

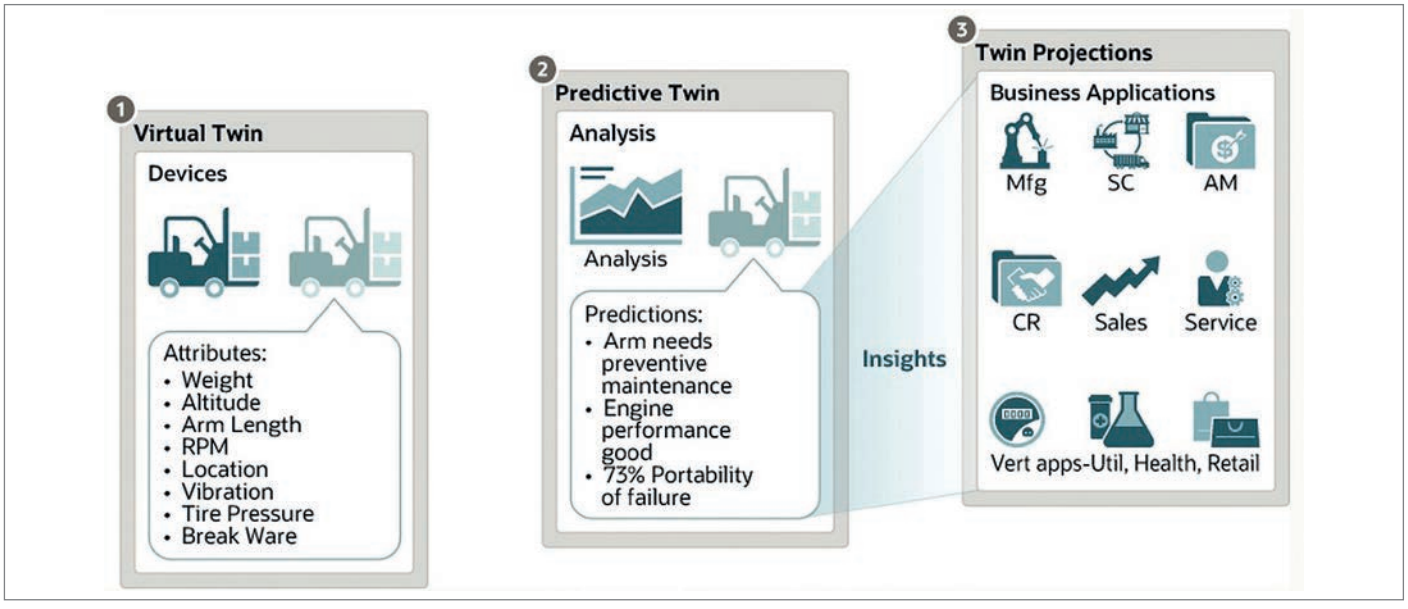


Abbildung 2: Oracle IoT Twin Implementation [5]

Daten beziehungsweise das Datenmanagement allein machen noch keinen digitalen Zwilling aus. In *Abbildung 1* sind weitere Technologien beziehungsweise Trends erwähnt. Die größte Rolle in Zusammenhang mit digitalen Zwillingen spielen:

- Analytics / künstliche Intelligenz: Algorithmen werden verwendet, um zum Beispiel Was-wäre-wenn-Analysen durchzuführen oder allgemein Erkenntnisse zu gewinnen.
- Internet der Dinge / Industrie 4.0 (IoT): Sensoren sammeln Daten des realen Objekts und senden diese an den Zwilling, und umgekehrt können Aktoren Maßnahmen umsetzen, die durch den digitalen Zwilling getriggert werden.

Wirft man auf der Suche nach dem digitalen Zwilling einen Blick in die Oracle Cloud, so findet man entsprechend drei Basiskomponenten *(siehe Abbildung 2)*:

- Virtual Twin: Konkrete Implementierung des digitalen Zwillings, zum Beispiel Datenmanagement.
- Predictive Twin: Erstellung und Ausführung von Algorithmen zur Vorhersage des Verhaltens.
- Twin Projections: Rückkopplung der Ergebnisse in das reale Objekt, zum Beispiel Durchführung von Software-Updates in einem Maschinenpark.

Ausblick Doppelgänger?

Und was ist mit dem Menschen? Jeder Einzelne als digitaler Zwilling? Die Ideen hierzu haben schon längst die Schublade verlassen. In Customer-Relationship-Management-Systemen (CRM) beschäftigt man sich bereits sehr lange damit: Jeder einzelne Kunde als digitales Abbild ist die Vision der nahen Zukunft.

Auch in der Medizin werden digitale Zwillinge betrachtet. Peter Spork beschreibt im Buch „Die Vermessung des Lebens: Wie wir mit Systembiologie erstmals unseren Körper ganzheitlich begreifen – und Krankheiten verhindern, bevor sie entstehen" den virtuellen Menschen, der durch Daten, mathematische Modelle und künstliche Intelligenz definiert ist. „Ein digitaler Zwilling ist etwas, mit dem ich wirklich simulieren kann, was passieren wird. Wie sich zum Beispiel mein Körper verändert, wenn ich die Magnesiumkonzentration in eine bestimmte Richtung ändere" *[6]*.

Die Potenziale in der Medizin sind groß, insbesondere wenn man die Möglichkeit hat, bei Medikamenten zu individualisieren. Heute werden nur grobe Unterscheidungen bei der Medikamentengabe gemacht, dazu zählen Gewicht, Altersgruppen oder Vorerkrankungen, wie aktuell bei COVID-19-Impfstoffen. Das wird sich sicherlich ändern.

Dabei gehören die Gesundheitsdaten zu den besonderen Kategorien personenbezogener Daten. Dementsprechend sind die Anforderungen gegenüber der Datensicherheit hoch. Ein Beispiel für ein zentrales Gesundheitsverwaltungssystem ist Midata *[7]*. Nutzer können dieser Datenplattform ihre Gesundheitsdaten für Forschungsprojekte zur Verfügung stellen und sollen laut Betreiber auch die Hoheit über ihre Daten behalten.

Eine hundertprozentige Datensicherheit gibt es jedoch nicht – es bestehen immer Restrisiken, insbesondere bei zentral gelagerten Daten. Sie sind ein Paradies für Hackerangriffe. Die Gefahren:

- Manipulation der Daten
- Diebstahl der Daten und Erpressung kranker Personen
- Identitätsmissbrauch

Der Hunger nach Daten nimmt weiter zu – egal ob im Gesundheitswesen, in der Produktion oder in einer anderen Industrie. Ein digitaler Zwilling basiert auf Daten und nutzt künstliche Intelligenz zur Vorhersage des Verhaltens. Dennoch klingt die Vorstellung des simulierten „Ich" im Gesundheitswesen unheimlich.

Quellen

Alle Links wurden am 15.06.2021 abgerufen.

[1] Michael Grieves, John Vickers: Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems in Kahlen / Flumerfelt / Alves: Transdisciplinary perspectives on complex systems, Springer 2017: *https://www.researchgate.net/publication/306223791_Digital_Twin_Mitigating_Unpredictable_Undesirable_Emergent_Behavior_in_Complex_Systems*

[2] Apollo 13 – the first digital twin: *https://blogs.sw.siemens.com/simcenter/apollo-13-the-first-digital-twin*

[3] „Market And Market" Studie: *https://www.marketsandmarkets.com/Market-Reports/digital-twin-market-225269522.html*

[4] Digital Twins begleiten Autos ein Leben lang: *https://www.automotiveit.eu/technology/digital-twins-begleiten-autos-ein-leben-lang-105.html*

[5] Oracle IoT Digital Twin: *https://docs.oracle.com/en/cloud/paas/iot-cloud/iotgs/oracle-iot-digital-twin-implementation.html* abgerufen am 04.06.2021

[6] Peter Spork: Die Vermessung des Lebens: Wie wir mit Systembiologie erstmals unseren Körper ganzheitlich begreifen – und Krankheiten verhindern, bevor sie entstehen, deutsche Verlags-Anstalt 2021

[7] *https://www.midata.coop*

Andreas Buckenhofer
andreas.buckenhofer@daimler.com

Andreas Buckenhofer arbeitet bei Daimler TSS in der Business Unit „Vehicle Platforms" und verfügt über mehr als 20 Jahre Erfahrung in datenintensiven Anwendungen. Seine praktischen Erfahrungen gibt er gerne in internen Vorträgen und als Sprecher auf internationalen Konferenzen weiter. An der Dualen Hochschule Baden-Württemberg hält er regelmäßig eine Vorlesung über Data Warehousing und Big Data. Er ist aktives Mitglied in der Datenbank-Community der DOAG und wurde von Oracle zum ACE Associate ernannt.

Life Twins: Fakten und Werte verbinden, um besser zu entscheiden

Dr. Ulrich Vogel, profilingvalues GmbH

Die beobachtbaren Fakten hat die Naturwissenschaft weitgehend im Griff. Werte werden dagegen diffus wahrgenommen und bisher kaum in exakter Weise untersucht. Wie wichtig das Zusammenspiel von Fakten und Werten vor dem Hintergrund der globalen Entwicklungen ist, wird in diesem Artikel deutlich. Analogien zur Unternehmensführung sind schlüssig und weisen den Weg zu konkreten Methoden und Tools. Deren Anwendung führt zu besserem Denken, Entscheiden und Handeln und damit zu nachhaltigem Erfolg.

Fakten und Werte: Zwei Seiten einer Medaille

Seit Galileo Galilei (1564 – 1642) die modernen Naturwissenschaften begründen half, unter anderem indem er die Gleichung v = s/t aufstellte, erscheint der kometenhafte technologische Aufstieg des Menschen unaufhaltsam *[1]*. Galileo widerlegte die aristotelische Physik und formulierte das wichtigste Prinzip in der Welt der Fakten in purer mathematischer Schreibweise: Das Prinzip der Bewegung, das heißt Geschwindigkeit (v = velocity) ist gleich Strecke (s = space) geteilt durch Zeit (t = time). Auf dieser mathematisch exakten Relation ruht unsere gesamte moderne Technologie, die durch Newton, Einstein, Heisenberg und viele weitere Forscher immer weiter verfeinert wurde. Alles ist am Ende Bewegung: von den Orbitalen der Elektronen um die Atomkerne bis hin zur Expansion des Universums. Auch wenn wir uns als Mensch in absoluter Ruhe wägen, bewegt sich alles in uns und um uns herum. Alles ist Bewegung.

In den letzten 400 Jahren hat unsere Technologieentwicklung Enormes erreicht. Der Mensch ist ein technologischer Gigant. Wenn wir Julius Cäsar oder Christoph Kolumbus mit einer Zeitmaschine in die Gegenwart holen könnten, wären sie mehr als beeindruckt. Damit sind die Fakten und ihre Entwicklung knapp beschrieben. Wir können die Sahara zum Blühen bringen, aber auch den Planeten in die Luft jagen.

Die diffuse Welt der Werte

Wir sind zwar technologische Riesen, aber haben wir uns unter Kontrolle? Wir haben es geschafft, Bequemlichkeit zu erreichen, etwa mit Luxuskarossen und Business-Class-Flügen. Auch können wir zum Mond reisen. Auf der anderen Seite lassen wir die Schere zwischen Arm und Reich immer weiter auseinanderdriften. Es mangelt der Menschheit nicht an Talent und Potenzial. Aber wir schaffen es nicht, die humanen Ressourcen so zu allozieren, dass wir die Früchte des menschlichen Potenzials ernten könnten. Wir sind bisher recht kläglich daran gescheitert, aus uns selbst wertemäßig ‚gute', das heißt ethisch-moralisch richtig handelnde Menschen zu machen. Den Beweis für diesen Missstand finden wir täglich in den Medien. Kriege, Folter, Versklavung sowie alle weiteren denkbaren Verbrechen gegen die Menschlichkeit durch Diktaturen, Unternehmen und Einzelpersonen.

Neben der Welt der Fakten gibt es die ‚Zwillingswelt' der Werte. Wir erkennen als Menschen nicht nur die Fakten, sondern wir geben ihnen subjektive Bedeutung – wir beWERTEn sie. Menschliche Wahrnehmung ist also immer eine Kombination aus den Fakten und der subjektiven Interpretation des Wahrnehmenden.

Was haben die ‚Twins' Fakten und Werte gemeinsam und was unterscheidet sie? Sie sind zwar untrennbar verbunden, wenn Menschen auf Fakten treffen. Denn wir bewerten alles, was uns widerfährt. Das fällt uns nur nicht mehr auf. Die Unterscheidung hingegen ist krass: Wir wissen millionenfach mehr über die exakten Fakten als über unsere Werte. Die Welt der Werte wabert im Sinne einer Philosophie durch unsere Gesellschaft und ist so diffus, dass man es kaum glauben kann. In der Welt der Werte liegt aber die ethische Kraft einer Gesellschaft. Leider haben wir keine Ahnung, wie das in wissenschaftlich exakter Weise zu mobilisieren wäre. Religion und Ethikunterricht mögen mitunter helfen, aber es schadet auch, wie man im religiösen Fanatismus erkennen kann. Wir sind also technologische Giganten und gleichzeitig moralische Pygmäen. Eine unschöne und explosive Mischung.

Seit etwa 70 Jahren gibt es erste Ansätze, eine formale Wertewissenschaft zu entwickeln. Sie könnte auf mittlere Sicht unser menschliches Paradoxon vom Giganten und Pygmäen auflösen. Aber der Weg zu einer wissenschaftsbasierten ‚Wertetechnologie' ist weit. Dennoch können wir mit den bereits entwickelten Ansätzen eine ganze Menge erreichen. Dass vor allem auch Unternehmen hiervon enorm profitieren können, ist wenig bekannt.

Von der Wertephilosophie zur Wissenschaft

Den Menschen beschäftigen seine Werte vermutlich schon genauso lange wie sein Drang, sich durch Werkzeuge das Leben zu erleichtern. Als aus der Gattung der Säugetiere hervorgegangene Spezies verfügen wir quer durch weite Gehirnteile über starke emotionale Kompetenzen, die uns in der Natur geholfen haben zu überleben. Der Mensch hat sich als ‚Hordentier' entwickelt und war damit in der Lage, durch geschickte Arbeitsteilung sowie Zusammenhalt von Familie und Sippe im Sinne eines Stammes Verbundenheit und geregeltes Leben zu etablieren. Noah Yuval Harari hat den unter anderem dadurch begründeten Aufstieg des Menschen in seinem berühmten Buch ‚Sapiens' eindrucksvoll beschrieben *[2]*.

Die abendländische Philosophie hat sich seit rund 3.000 Jahren mit dem Thema des Lebenssinns, der Entwicklung der geistig-menschlichen Potenziale sowie dem guten gesellschaftlichen Miteinander auseinandergesetzt. Dabei kamen kluge Köpfe wie Platon und Aristoteles schon früh zu prägenden Schlüssen, haben aber keine ‚ethische Wissenschaft' etablieren können.

Robert S. Hartman hat diesen Missstand schon vor mehr als einem halben Jahrhundert plakativ gemacht *[3]*: Wenn wir nicht mehr gut sehen, dann gehen wir zum Augenarzt oder Optiker. Er misst unsere mangelnde Sehschärfe und gibt uns Hilfe im Sinne von Brille oder Kontaktlinse, sodass wir wieder klarsehen. Wer hilft uns, in der Welt der Werte unsere Unschärfen zu erkennen und wieder Klarsicht herzustellen? Bis heute gibt es diesen ‚Werte-Optiker' nicht an jeder Straßenecke. Aber der Berufsstand beginnt sich langsam herauszuschälen.

Wie integrieren wir Fakten und Werte im positiven Sinne, sodass wir uns persönlich, beruflich und insgesamt in richtiger Weise entwickeln? Wie systematisieren wir die Werte?

Was ist ‚gut'? – Das Axiom der formalen Wertewissenschaft

Wir benutzen das Wort ‚gut' hundertfach am Tag. Aber wissen wir, was es wirklich be-

deutet? Es beschreibt eine Sache, eine Idee oder einen Menschen. Aber nicht so wie ‚rund', ‚intelligent' oder ‚sympathisch'. Es ist irgendwie anders, aber wie?

1949 hat Robert S. Hartman das Axiom der Wertewissenschaft gefunden [4]. Gut ist, was sein Konzept erfüllt. Ein guter Anzug hat die Eigenschaften, die ich ihm grundsätzlich zuschreibe. Ein gutes gekochtes Ei hat die Eigenschaften, die ich mir wünsche, genauso wie die Fernsehsendung oder das betriebliche Meeting. Wenn ich etwas als ‚gut' bezeichne, dann habe ich eine logische Operation im Denken vollzogen. Ich habe das Konzept von einer Sache, also die geforderten oder gewünschten Eigenschaften, die ich mir für das Konzept vorstelle, mit den vorhandenen Eigenschaften eines tatsächlichen Objekts verglichen.

Ich will beispielsweise ein neues Auto kaufen und habe davon eine konkrete Vorstellung im Kopf (Konzept eines guten Autos für mich selbst mit den entsprechenden Eigenschaften). Nun gehe ich in ein Autohaus und vergleiche mein Konzept im Kopf mit den Eigenschaften, die ein real dort stehendes Auto hat. Sind alle vorgestellten beziehungsweise gewünschten Eigenschaften vorhanden, so werde ich sagen, dass dieses Auto gut ist. Ist nur ein Teil erfüllt, so fällt meine Einschätzung weniger positiv aus.

Die drei Wertedimensionen

Wir können schlecht alle Menschen nach ihren spezifischen Konzepten für Autos, Waschmaschinen und vieles mehr fragen. Robert S. Hartman hat tiefer nachgedacht und drei verschiedene Arten von Konzepten herausgearbeitet, mit denen wir viel anfangen können, um wertemäßig systematischer zu werden.

Da ist einmal das genannte Auto, eine Sache, etwas Dingliches. Das Auto hat klare Eigenschaften, die wir abstrahieren können, wenn wir es Stück für Stück beschreiben. Hartman hat diese Konzeptart die ‚extrinsische' genannt, die mit den äußeren Sinnen erfahrbar ist. Es genügt, sie sich als praktische Dimension in der Wertewelt zu merken.

Es gibt eine weitere Konzeptart, die Hartman als ‚systemisch' bezeichnete. Hier handelt es sich nicht um das Konzept für ein reales Objekt, sondern um das Konzept eines Grundsatzes oder Prinzips. Nehmen wir das Beispiel eines geometrischen Kreises. Er hat auch Eigenschaften, nämlich drei an der Zahl: einen Mittelpunkt und eine geschlossene Kreiskurve, die immer den gleichen Abstand zum Mittelpunkt hat. Was ist der Unterschied zum Auto? Die Eigenschaften haben etwas Grundsätzliches, gleichsam Essenzielles. Es gibt keinen ‚fast ganz guten' geometrischen Kreis. Es gibt ihn entweder in Perfektion oder er ist nichtexistent. Die Eigenschaften sind also Bedingungen, die erfüllt sein müssen, damit das Konzept stimmt. Letztlich entsteht der geometrische Kreis nur in unseren Gedanken im Rahmen der mathematischen Logik. Wir Menschen können die Prinzipien hinter den Dingen des Alltags erkennen. Das ist einer unserer wichtigsten Erfolgsgründe.

Schließlich gibt es noch eine dritte Konzeptart – die menschliche. Laut Hartman ist jeder von uns ein ‚kosmisches Ereignis'. Mit unserem einzigartigen genetischen Code und all den Momenten unseres Lebens gleichsam zusammengebunden stellen wir eine Singularität dar. Der Mensch ist eben nicht umfassend beschreibbar durch eine Aufzählung von Eigenschaften. Die Person hat unendlich viele Eigenschaften, die miteinander so verbunden sind, dass Bewusstsein und Kreativität entstehen können, Enthusiasmus und Kooperation, aber leider auch Streit und Hass.

Laut der Wertemathematik von Robert S. Hartman ist das Menschliche stets wertvoller als das Dingliche, was wiederum wertvoller ist als das Grundsätzliche. Demnach wiegen selbst alle Güter dieser Welt kein einziges Menschenleben auf. Kein Gesetz ist wertvoller als die Nahrung, die ein Mensch zum Überleben braucht. Aber man kann auch keine Wertedimension einfach

Explore your potential

Werte-Kompass für Aktivitäten: E-Mail schreiben

Mögliche Struktur der Aktivität	Herz / menschlich (M)	Hand / praktisch (P)	Hirn / grundsätzlich (G)
Zweck & Ziel	Beziehung: Kein geeignetes Mittel, sondern persönlich oder Telefon	Information, Anregung zum Austausch, Faktensammlung, Freundlichkeiten	Information, Regelkommunikation, Faktensicherung, Planung
Betreff	Auf die Menschen bezogen, für wen bringt die Aktivität etwas?	Übergeordnetes Thema und aktueller Bezug	Kontextbezug
Anrede	Möglichst persönlich, ggf. einzeln, menschlich verbindende Wortwahl für eine Gruppe	Verständlich	Korrekt / angemessen
Einleitung	Persönlich-menschlicher Bezug, den Leser individuell abholen und wertschätzen	Anliegen unter Einbindung der Person skizzieren	Kontextbezug, ggf. Termine, Fristen o.ä.
Hauptpunkte	Den persönlichen Blickwinkel des Anliegens transportieren unter Berücksichtigung der anderen Menschen und ihrer Bedürfnisse	Verständlich, klar, dicht, kurz	Auswirkungen auf die Systeme erwähnen
Weiteres Vorgehen & Umgang mit Fragen	Die Menschen explizit einbinden und ihr Engagement anregen	Die nächsten Schritte kurz beschreiben	Nötige Formalia hinzusetzen
Gruß und Signatur	Persönlicher Gruß, mit Vornamen (und Namen) sowie ohne Titel unterschreiben	Dem Leser etwas wünschen mit aktuellem Bezug	Passende Autosignatur nach der persönlichen Signatur

Anleitung zur Bewertung: Jeweils die 3 Werteaspekte auf Skala von 1-9 taxieren und Durchschnitte bilden.

M	P	G	Ø
2	3	4	3
6	8	3	5,7
9	8	4	7
2	3	6	3,7
3	5	7	5
2	8	6	5,3
8	4	3	5
Summe / 7			5

Abbildung 1: Beispiel der Optimierung einer Aktivität durch den Werte-Kompass (© profilingvalues)

‚streichen'. Prinzipien und Theorien sind selbstverständlich enorm wichtig, damit die Menschheit vorankommt. Aber wir müssen die Dimensionen in ihrer Wertigkeit relativ zueinander betrachten.

Mit dieser Differenzierung der drei Wertedimensionen und der Etablierung einer Wertehierarchie über diese Dimensionen hinweg haben wir ein Raster geschaffen für einen Werte-Kompass im Alltag. Der Professor sollte seine Vorlesung eben nicht mit dem reinen Fokus auf seine Wissenschaft beginnen, sondern sich zuallererst in die Schuhe seiner Studenten stellen, um sie geeignet abzuholen und zu inspirieren. Klingt ganz einfach, wird aber häufig so nicht gemacht. Wir können jede Handlung des Alltags mithilfe des Werte-Kompasses ‚zerlegen', um sie dann besser durchzudenken und neu ‚zusammenzusetzen', wie *Abbildung 1* zeigt. Dabei kann man sich oder andere auch bewerten lassen.

In diesem Beispiel ist die Bewertung fiktiv, denn wir haben ja keine konkrete E-Mail analysiert. In der Tabelle stehen lediglich mögliche Adressierungen der jeweiligen Wertedimensionen. Um eine tatsächliche E-Mail zu bewerten, kann man dieses Raster jedoch sehr gut verwenden.

Gut und Böse in der Gesellschaft und im Unternehmen

Gut ist bereits definiert, aber ‚böse'? Robert S. Hartman hat dazu ein eindrucksvolles Buch geschrieben: Die Revolution gegen den Krieg. *[5]* Er ist der Auffassung, dass der Krieg bereits gesät ist, wenn wir beginnen, den Frieden zu verlieren. Wenn wir nicht dagegen vorgehen, wenn Rassen, Religionen oder persönliche Freiheiten verfolgt beziehungsweise genommen werden, dann beginnt der Keim des Bösen sein Werk.

Welche Erkenntnis kann man gewinnen, wenn man diese Aspekte auf Unternehmen überträgt? Klar ist, dass Mobbing schlecht ist, also den Keim des Bösen in sich trägt. Aber es beginnt viel früher. Immer dann, wenn Menschen nicht menschlich behandelt werden, sondern abgewertet oder unmenschlich behandelt werden. Tadel einer Person vor versammelter Mannschaft wäre ein solcher Fall. Oder auch abfällig über eine nicht anwesende Person sprechen. Bevorzugungen aufgrund von Sympathie sind beliebte Varianten. Die Liste lässt sich fortsetzen.

Natürlich haben wir gute Gesetze, die dazu geführt haben, dass unsere Arbeitswelt viel menschlicher ist, als sie beispielsweise im Frühkapitalismus war. Aber verbindlich ist vieles wertemäßig Notwendige nicht.

Der Fisch stinkt vom Kopf her, wie der Volksmund sagt. Wird von oben unethisch geführt, dann setzt sich das im Unternehmen fort. Schließlich verkommt die Unternehmenskultur. Umgekehrt, also aus einem funktionierenden Unternehmen eine großartige Firma zu machen, braucht sehr viel länger und benötigt Konsequenz bei wichtigen Führungsprinzipien, wie Jim Collins in seinem Buch ‚Der Weg zu den Besten' anschaulich herausgearbeitet hat *[6]*.

Wie gehen wir also am besten vor? Wenn wir analog zum Keim des Bösen in der Gesellschaft den Keim des Schlechten in Unternehmen erkennen wollen, dann könnte man folgendermaßen starten: Das Unternehmen ist bestrebt, die individuellen Potenziale der Mitarbeitenden zu erkennen und zu entfalten. Alle Mitarbeitenden genießen sämtliche arbeitsgesetzlichen persönlichen Freiheiten und werden durch das Unternehmen vor abwertender Behandlung geschützt. Abwertung bedeutet unmenschliche Behandlung, die grundsätzliche menschliche Normen wie etwa Respekt, Fairness, Gerechtigkeit, Freiheit oder Solidarität verletzt.

Das klingt zwar edel und gut. Aber wie ist es durchsetzbar? Und wo beginnt der Keim des Bösen im Sinne von ‚Wehret den Anfängen'? Die an klaren menschlichen Werten orientierte Führungskraft hat in der Regel genügend Sensoren, um Fehlverhalten schnell zu erkennen. Oft wird weggeschaut oder nicht konsequent durchgegriffen. Die Belegschaft hat aber ein sehr feines Gespür für Unfairness, Übervorteilung, Ausbremsungen oder das Schüren persönlicher Konflikte.

Es zeigt sich, dass der Teufel im Detail steckt. Während Unternehmensleitungen oftmals stark mit der Strategie beschäftigt sind, vergessen sie das ‚Wer' und das ‚Wie' des Miteinanders. Sie sind nur in der grundsätzlichen und praktischen Wertedimension unterwegs, vernachlässigen aber die menschliche. Und wundern sich dann, dass sie keinen Erfolg haben.

Die gute Nachricht ist: Wir haben es in der Hand. Wir können unseren Kompass der Wertedimensionen benutzen und unseren Berufsalltag verändern. Jegliche Handlung kann in diesem Lichte überprüft und verbessert werden.

Was heißt wertebasiert führen?

Wir befinden uns tagtäglich in herausfordernden Situationen. Deshalb braucht es Instrumente, die Klarheit schaffen und Orientierung geben. Mittlerweile gibt es einige Tools, die helfen, wertemäßig ‚besser zu sehen'. Neben dem oben beschriebenen Werte-Kompass stelle ich hier die „3-Werte-Brille" vor.

Menschliche Bewertungen können in differenzierter Weise ausfallen. Beispielsweise kann man einen Menschen (M) bewerten (z.B. eine bestimmte Staatsangehörigkeit: ja oder nein), also im Sinne von grundsätzlich (G): Die mathematische Formel würde lauten MG. Die Basis M ist der Mensch und der Exponent G ist die „Linse", durch die dieser Mensch bewertet wurde. Man kann ihn aber auch praktisch-funktional bewerten, indem man beobachtet, was er tut (MP), beispielsweise arbeitet sie als Zahnärztin. Schließlich kann man eine Person auch menschlich werten, indem man etwa eine Liebeserklärung ausspricht (MM). Man spricht hier von unterschiedlichen Werteperspektiven.

Wenn man diese Werteperspektiven in ihrer Reihenfolge im Sinne einer Wertehierarchie clustert, so bekommt man drei generelle Aussagen, die über die richtige Werteorientierung im Unternehmen informieren. Man führt das Unternehmen wertebasiert gut, wenn man folgende drei Punkte überall erfüllt, wobei 1. wichtiger ist als 2., was wiederum wichtiger ist als 3.:

1. *Achtsam und sensitiv sein* gegenüber den anderen Menschen und dem gesamten Umfeld sowie gegenüber sich selbst. Sich allem bewusst sein und emotional kompetent und inspiriert vorgehen.
2. *Miteinander das Richtige tun*. Man kooperiert und ist gemeinsam kreativ, tatkräftig und effektiv.
3. *Das Richtige richtig tun und sich ständig verbessern*. Es geht darum, effizient und innovativ zu sein.

Spiegelbildlich dazu kann man in den folgenden drei Punkten Fehler begehen, wobei 4. kleinere Fehler darstellt, 5. schon größere Schwierigkeiten bereitet und 6. in jedem Fall untragbar ist:

4. *Das Richtige nicht richtig tun* und dabei stagnieren. Man wäre also ineffizient und ideenlos. Das ist in der Regel nicht so schwer zu beheben.
5. *Jeder arbeitet für sich, und es wird häufig das Falsche getan*. Es geht also unkooperativ und damit auch kontraproduktiv zu. Man kennt das typische Silodenken in Unternehmen. Hier muss man schon etwas tiefer einsteigen.
6. *Die Menschen und das Umfeld missachten* und damit anderen und letztlich auch sich selbst Schlechtes zufügen. Es geht um Egoismus und Schädlichkeit.

Diese 2 mal 3 Aspekte sind die Kalibrierung der 3-Werte-Brille. Man befindet sich in einer Situation, in der man eine Problemstellung zu meistern hat. Man analysiert, um die richtigen Schritte zu unternehmen. Normalerweise hat man Zahlen, Daten und Fakten zur Verfügung. Aber bekommt man damit allein die vollumfängliche Situation gespiegelt?

Mit der 3-Werte-Brille kommt man dem Geschehen in entscheidender Weise näher. Man sieht die reale ‚Wertelandschaft', in der sich die Szenerie abspielt. Bewegungen können auch aus ihrer emotionalen Intention heraus beobachtet werden. Man nimmt eine tiefere Perspektive ein und kommt daher den dort herrschenden Werten und Bewertungen näher. Diese häufig als „Soft Factors" verunglimpften Strömungen sind im Grunde diejenigen, die über den Erfolg in der komplexen Wirtschaftswelt entscheiden. Sie stellen ‚harte Faktoren' dar, die mit der 3-Werte-Brille erfasst werden können.

Fazit

Fakten werden wissenschaftlich recht gut beherrscht, Werte noch nicht. Es gibt mittlerweile erste Methoden und Tools. Nur die systematische Verbindung von Fakten und Werten gibt den Dingen die richtige Bedeutung und garantiert einen ‚Kompass der Menschlichkeit', der die Arbeit in Unternehmen leiten sollte.

Quellen

[1] Ueli Niederer 1982: Galileo Galilei und die Entwicklung der Physik, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich (1982) 127/3: 205-229.

[2] Noah Yuval Harari 2015: Sapiens: A Brief History of Humankind. Vintage Books, New York.

[3] Robert S. Hartman 2013 (edited by Arthur R. Ellis): Freedom to Live: The Robert S. Hartman Story. Wipf and Stock Publishers, Eugene, Oregon.

[4] Robert S. Hartman 2011: The Structure of Value: Foundations of Scientific Axiology. Wipf and Stock Publishers, Eugene, Oregon.

[5] Robert S. Hartman 2020 (edited by Clifford G. Hurst): The Revolution against War: Selected Writings on War and Peace. Izzard Ink Publishing, Salt Lake City, Utah.

[6] Jim Collins 2001: Good to Great. Harper Collins Publishers, New York.

Dr. Ulrich Vogel
ulrich.vogel@profilingvalues.com

Dr. Ulrich Vogel studierte Politikwissenschaft, Volkswirtschaft und Öffentliches Recht. Seit über 20 Jahren arbeitet er in der Beratung mit dem Fokus auf den Menschen. Er nutzt die Erkenntnisse der formalen Wertewissenschaft, um die Arbeitswelt menschlicher und damit erfolgreicher zu gestalten.

Warum ein digitaler Zwilling in der Organisationsgestaltung sinnvoll ist

Dr. Thomas Karle, Florian Lösch, Horus software GmbH, Ettlingen

Wenn man die Ereignisse und Entwicklungen des letzten Jahrzehnts betrachtet, dann erscheint die Fähigkeit eines Unternehmens, schnell mit sich ändernden Rahmenbedingungen zurechtzukommen, heutzutage überlebenswichtig zu sein, auch für große Konzerne. Entscheidend ist darüber hinaus die Fähigkeit, proaktiv die erforderlichen Veränderungen effizient in der eigenen Organisation umsetzen zu können, um im Wettbewerb langfristig zu bestehen. Hierzu kann ein digitaler Zwilling einer Organisation, bei dem die gesamte Unternehmensorganisation mit ihren Geschäftsprozessen als permanent aktuelles Spiegelbild des Unternehmens bereitgestellt wird, ein zukünftig wichtiges Instrument darstellen, um diese Fähigkeiten in Unternehmen auf- oder auszubauen.

Einführung

Die Fähigkeiten von Unternehmen, mit Veränderungen umgehen zu können oder gar davon zu profitieren, ist eng gekoppelt mit der Qualität des Managements von Anforderungen und Herausforderungen bei den aktuellen Änderungsprojekten und Business-Transformationen. Typische Vertreter für solche Projekte und Transformationen sind:

- die Einführung einer neuen Unternehmenssoftware,
- die digitale Transformation und
- sonstige Geschäftsprozessänderungen aufgrund äußerer oder innerer Einflussfaktoren (wie Krisen, Marktänderungen, neue Technologien, Gesetzesänderungen, Fusionen, Zukäufe etc.).

Eine weitere wichtige Anforderung in diesem Zusammenhang ist das Wissensmanagement bei sich schnell verändernden Rahmenbedingungen kombiniert mit einer Zunahme der Komplexität.

Die genannten Anforderungen können unter dem einen Ziel zusammengefasst werden, Agilität und organisationale Resilienz in einem Unternehmen aufzubauen. Hierbei kann ein Digital Twin of an Organization (DTO) ein zentrales Instrument bereitstellen.

Was ist ein Digital Twin einer Organisation?

Die Grundidee eines Digital Twin (DT) ist die Erstellung und Nutzung einer digitalen Repräsentation eines materiellen oder immateriellen Objekts oder eines Prozesses aus der realen Welt *[1]*. Michael Grieves entwickelte die ersten Grundideen des DT zu einem Konzept weiter, bei dem auch die Kommunikation zwischen dem realen und dem virtuellen Objekt berücksichtigt wird. Die aktuellen Einsatzgebiete dieses Konzepts liegen bisher im Wesentlichen in der industriellen Fertigung, vor allem im Zusammenhang mit dem Einsatz des Internet of Things (IoT).

Gemäß einer Befragung unter 600 Großunternehmen aus sechs verschiedenen Ländern aus dem Jahr 2019 hatten bereits 13 % einen DT in irgendeiner Form in ihrem Unternehmen eingesetzt und 62 % waren in der Einführung oder hatten vor, dies innerhalb des nächsten Jahres umzusetzen *[2]*. Einer weiteren Studie aus dem Herbst 2020 zufolge setzten 31 % der Befragungsteilnehmer einen DT als Teil der Maßnahmen des Unternehmens zur Aufrechterhaltung des operativen Geschäfts im Rahmen der COVID-19-Pandemie ein *[3]*.

Gartner definiert den Digital Twin of an Organization (DTO) und beschreibt eine dreistufige Evolution von diskreten über zusammengesetzte DTs hin zu einem DT einer kompletten Organisation *[4]*. Hierbei wird unter einem diskreten DT die Nutzung der entsprechenden Technologie zur Bewertung und Optimierung einfacher Sachverhalte verstanden. Zusammengesetzte DTs stellen eine Erweiterung der diskreten Version dar, in der weitere externe Ressourcen und Datenquellen eingebunden werden, um ein ausführlicheres Bild des Prozesses, des Produkts oder der beteiligten Rollen zu erhalten. Der DTO wird als Kombination verschiedener diskreter und zusammengesetzter DTs beschrieben. Der hier beschriebene Ansatz geht noch einen Schritt weiter und bezieht auch die strategischen Aspekte wie Ziele, Strategien und Risiken mit ein, die ebenfalls Teil des DTO sind und bei Bewertungen von Änderungen berücksichtigt werden *[5]*. Für das operative Abbild des Unternehmens werden Geschäftsprozesse, Geschäftsobjekte, Systemkomponenten, technische Ressourcen, Organisationsstrukturen und Testfälle betrachtet *[6]*. *Abbildung 1* skizziert einen DTO auf Basis des zuvor beschriebenen Verständnisses als Gesamtheit aller im Unternehmen relevanten prozessbezogenen strategischen und operativen Aspekte. Eine wesentliche Eigenschaft des hier verfolgten Ansatzes ist, dass diese

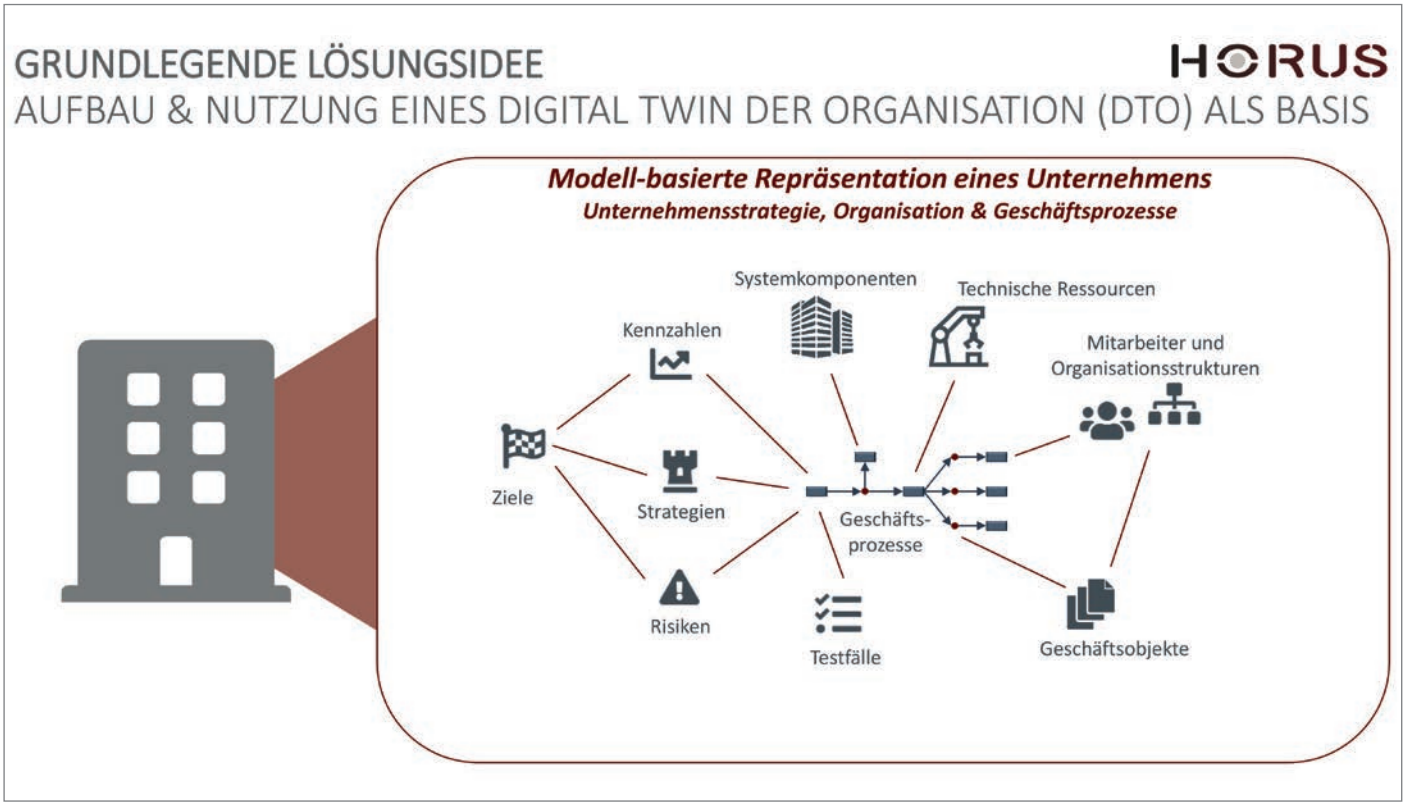


Abbildung 1: Digital Twin of an Organization (DTO) (© Horus software GmbH)

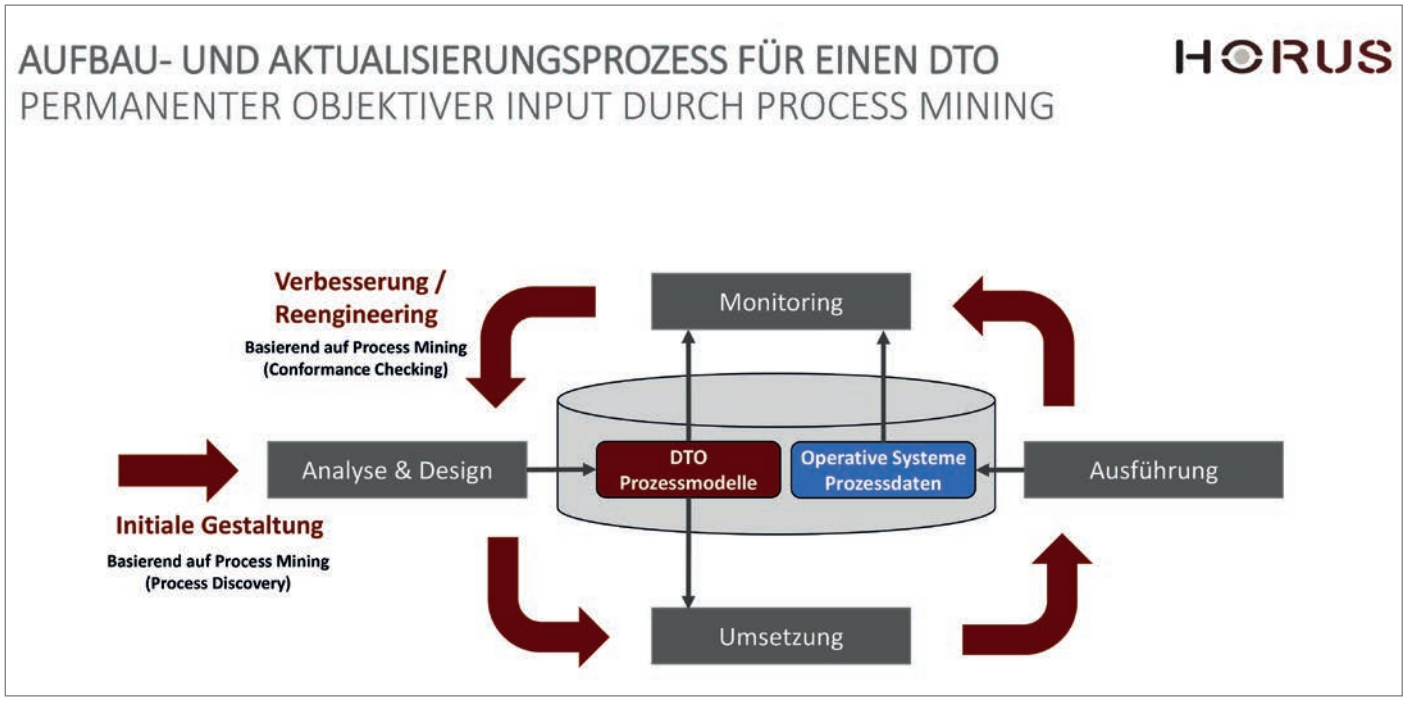


Abbildung 2: Aufbau- und Aktualisierungsprozess für einen DTO (vgl. 5) (© Horus software GmbH)

Aspekte nicht als einzelne, unabhängige Artefakte verwaltet werden, sondern ein zusammenhängendes Informationsnetz aufgebaut wird, das auch die Beziehungen zwischen den einzelnen Artefakten beinhaltet. Der digitale Zwilling einer Organisation kann somit als umfassende Betrachtung und Spiegelung dieser angesehen werden, die deren aktuellen Stand möglichst transparent abbildet.

Um die Aktualität eines DTO zu gewährleisten, muss ein passender Aufbau- und Aktualisierungsprozess umgesetzt werden. Wie in *Abbildung 2* aufgeführt, ist dies ein zyklischer Prozess, der sich in die folgenden Abschnitte unterteilen lässt: initiale Gestaltung (inklusive Analyse und Design), Umsetzung von Änderungen auf Basis des DTO, Ausführung von (geänderten) Prozessen, Monitoring der Ausführungen auf Basis von Prozessdaten und dann wieder Analyse und gegebenenfalls ein Re-Design für weitere Veränderungen.

Eine Basis für die Erstellung und Pflege eines DTO stellt entsprechende Modellierungssoftware bereit *[5]*. Als grundlegende Technologie für eine KI-basierte Unterstützung zur Teilautomatisierung dieses zyklischen Prozesses bietet sich zusätzlich vor allem das Process Mining an, bei dem digitale Datenströme systemseitig analysiert und für die Bewertung von Zuständen und Abläufen nutzbar gemacht werden. Dazu wird spezielle Process-Mining-Software an bestehende operative Systeme, wie beispielsweise ein ERP-System, angeschlossen. Aus den operativen Systemen werden ereignisbasierte Datensätze mit jeweiligem Zeitstempel extrahiert. Die Kombination aus Log-Event in Verbindung mit einem Zeitstempel des jeweiligen Events ermöglicht es der Software, Sachverhalte nachzuvollziehen, zu analysieren und visuell auszugeben. Hierdurch lassen sich die einzelnen tatsächlichen Durchläufe der Unternehmensprozesse transparent darstellen und bewerten.

Bereits bei der initialen Gestaltung kann Process-Mining-Software eingesetzt werden, um über die Möglichkeiten des Process Discovery eines solchen Tools die aktuellen Ist-Abläufe aus der bestehenden Unternehmenssoftware zu ermitteln.

Bei der Anwendung eines DTO können zwei Fälle unterschieden werden: die Umsetzung eines zuvor im DTO erstellten Soll-Zustands in der realen Welt und die Überprüfung der Inhalte des DTO anhand von realen Prozessdaten aus den operativen Systemen. Dementsprechend eignet sich der DTO zum einen für die Weiterentwicklung der bestehenden Organisation, um vorab zu simulieren, wie sich das Unternehmen unter gegebenen Parametern verhält, und bei einem positiven Ergebnis der Simulation dann eine Vorlage für die zukünftige Organisation zu liefern. Zum anderen bietet es ein Mittel, um den Ist-Zustand eines Unternehmens ganzheitlich zu untersuchen und mögliche Abweichungen von einem gewünschten Verhalten frühzeitig zu erkennen. Eine dritte Option ist die Weiterentwicklung einer Organisation auf Basis des DTO mit anschließender Verifikation der durchgeführten Transformation. In den nachfolgenden Abschnitten werden konkrete Anwendungsfälle für den DTO erläutert.

Unterstützung bei der Einführung einer neuen Unternehmenssoftware

Unternehmenssoftware-Projekte – egal, ob Neueinführungen, Erweiterungen oder Ablösungen bestehender Systeme – sind komplexe Veränderungsprojekte für jede Organisation. Sie sind als Transformation der Organisation fordernd für diese selbst und auch für die beteiligten Personen. Eine zentrale Aufgabe stellt hierbei das Anforderungsmanagement dar, bei dem viele verschiedene Forderungen und Wünsche von den diversen Stakeholdern gestellt, anschließend zielgerichtet bewertet und – sofern für das Unternehmen sinnvoll – in das Implementierungsprojekt integriert werden. Die zu berücksichtigenden Anforderungen werden durch einen entsprechenden Soll-Zustand im DTO durch die in *Abbildung 1* dargestellten operativen und geschäftsprozessbezogenen Aspekte beschrieben. An der Stelle wird der DTO als Vorgabe für die anschließende Umsetzung

genutzt. Dies wird in der Regel von den betroffenen Fachbereichen erarbeitet, bildet hierdurch aber zumeist eine sehr subjektive Sicht der Realität innerhalb des Unternehmens ab. Abhilfe kann in diesem Zusammenhang der Einsatz von vorgefertigtem Prozesswissen schaffen, das im DTO als Basis für die Definition der Sollprozesse bereitgestellt wird. Darüber hinaus kann auch das initiale Process Discovery des Process Mining genutzt werden, um die tatsächlichen Ist-Abläufe aus den operativen Systemen zu ermitteln. Auf Basis der hieraus entstehenden Ergebnisse lassen sich objektive Aussagen über die realen Abläufe treffen, um für diese dann die entsprechenden Zielprozesse in der Unternehmenssoftware zu definieren. Am Ende eines Unternehmenssoftware-Projekts bietet ein gepflegter DTO die Möglichkeit der kontinuierlichen Überprüfung, ob die getroffenen Annahmen passen oder ob weitere Transformationen erforderlich sind. Darüber hinaus steht zum Projektende eine umfassende prozessorientierte Dokumentation digital zur Verfügung.

Unterstützung bei der digitalen Transformation

Da in einem DTO alle wesentlichen Geschäftsprozesse eines Unternehmens als Prozessmodelle vorliegen – auch die Prozesse, die aktuell noch nicht komplett oder gar nicht digitalisiert durchgeführt werden –, können diese im DTO leicht identifiziert und bewertet werden. Der DTO liefert dadurch entsprechende Ansatzpunkte für Digitalisierungspotenziale. Durch die im DTO ebenfalls vorhandenen Zusammenhänge mit den strategischen Aspekten im Unternehmen können Digitalisierungsprojekte ganzheitlich, das heißt ausgerichtet an den Zielen und Strategien des Unternehmens und unter Berücksichtigung prozessualer Zusammenhänge aufgesetzt und durchgeführt werden. Bei einer ungesteuerten Agilität ohne diese Transparenz durch einen DTO werden häufig kurzlebige digitale Insellösungen umgesetzt, da Zusammenhänge nicht oder erst nach der Umsetzung erkannt werden.

Unterstützung bei Geschäftsprozessänderungen

Neben dem Vorantreiben der digitalen Transformation können Änderungen an Geschäftsprozessen viele weitere Gründe haben: Fusionen oder Zukäufe von Unternehmen, aber auch ein organisatorischer Umbau innerhalb von Unternehmen, um beispielsweise Probleme und Ineffizienzen bei im Laufe der Zeit gewachsenen Organisationsstrukturen zu beseitigen. Weiterhin können Veränderungen der äußeren Rahmenbedingungen, etwa durch Krisen, Marktänderungen, neue Technologien oder Gesetzesänderungen zu erforderlichen Anpassungen der Geschäftsprozesse führen *[7]*. Als Spezialfall ist hier auch der Trend zur Umsetzung von Nachhaltigkeit in Geschäftsprozessen zu nennen, bei dem neben den ökonomischen Aspekten auch ökologische und soziale Aspekte berücksichtigt, das heißt bewertet und umgesetzt werden *[8]*. Der DTO stellt hier den Ausgangspunkt dar, indem er objektiv den aktuellen Ist-Zustand der Organisation widerspiegelt. Auf Basis des DTO können nun Simulationen der Änderungen durchgeführt werden. Dies geht von organisatorischen Umstrukturierungen über technische Änderungen in einzelnen Geschäftsprozessen bis hin zu einem strategischen Umbau des Gesamtunternehmens. Diese Planspiele werden dann auf dem DTO durchgeführt. Die Ergebnisse führen anschließend zu einer Zielversion des DTO, die als Vorgabe für die Umsetzung der Änderungen dient.

Wissensmanagement mit dem DTO

Bei zunehmender Geschwindigkeit von Änderungen ist das Wissensmanagement im Unternehmen eine weitere wichtige Herausforderung. Da der DTO eine möglichst komplette Dokumentation aller Aspekte des Ist-Zustands beinhaltet, aber im Laufe der Transformationen auch bereits neue Versionen für den Soll-Zustand entstehen, stellt dieser eine solide Basis für das Wissensmanagement speziell für Änderungen im Unternehmen bereit. Die Modelle und sonstigen Artefakte des DTO zu Geschäftsprozessen, Organisationsstrukturen, Systemarchitekturen, Geschäftsobjekten und Testfällen können sowohl im Rahmen eines Self-Service-Portals als auch für die Durchführung von Trainings beim Onboarding und beim organisationalen Lernen verwendet werden.

Zusammenfassung und Fazit

Mit dem vorliegenden Beitrag wurde das Konzept des Digital Twin einer Organisation vorgestellt, der Unternehmen dabei unterstützen soll, den aktuellen Anforderungen und Herausforderungen bei den typischen Änderungsprojekten und Business-Transformationen zu begegnen. Der Kern des DTO ist eine Menge von miteinander verknüpften Modellen, die in ihrer Gesamtheit ein transparentes digitales Abbild des Unternehmens inklusive der Details zu den Geschäftsprozessen darstellt. Darüber hinaus sind auch die strategischen Aspekte des Unternehmens im DTO berücksichtigt. Der Aufbau eines solchen DTO setzt sich im Wesentlichen aus einer Modellierungs-Komponente zum Aufbau und zur Definition der grundlegenden Strukturen des DTO und aus einer Process-Mining-Komponente für einen intelligenten – auf Prozessdaten aus den operativen Systemen basierenden – Austausch zwischen dem realen Unternehmen und dem DTO zusammen. Zusätzlich zum Process Mining kann das Gesamtsystem des DTO auch noch mit Komponenten für Data Mining und Data Analytics ergänzt werden, um eine noch breitere Analyse zu ermöglichen. Durch die aufgeführten Vorteile bei den durch innere oder äußere Einflussfaktoren ausgelösten Änderungsprojekten und Business-Transformationen ist ein DTO ein vielversprechendes Konzept, um Agilität und organisationale Resilienz in einem Unternehmen dauerhaft aufzubauen.

Literatur

[1] Grieves, M.: Digital Twin (2014): Manufacturing Excellence through Virtual Factory Replication, Whitepaper, Florida Institute of Technology.

[2] Costello, K., Omale, G. (2019): Gartner Survey Reveals Digital Twins Are Entering Mainstream Use, *https://www.gartner.com/en/newsroom/press-releases/2019-02-20-gartner-survey-reveals-digital-twins-are-entering-mai*

[3] Goasduff, L. (2020): Gartner Survey Reveals 47% of Organizations Will Increase Investments in IoT Despite the Impact of COVID-19, *https://www.gartner.com/en/newsroom/press-releases/2020-10-29-gartner-survey-reveals-47-percent-of-organizations-will-increase-investments-in-iot-despite-the-impact-of-covid-19-*

[4] Schulte, W. R., Kerremans, M., Lheureux, B., Velosa, A. (2019): What to Expect When You're Expecting Digital Twins, Gartner Research.

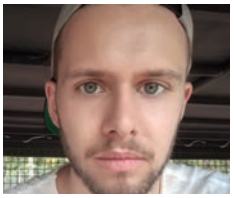
[5] Schönthaler, F., Vossen, G., Oberweis, A. und Karle, T. (2012): Business Processes for Business Communities: Modeling Languages, Methods, Tools, Springer: *https://doi.org/10.1007/978-3-642-24791-0.*

[6] Vossen, G., Schönthaler, F. und Dillon, S. (2017): The Web at Graduation and

Beyond: Business Impacts and Developments, Springer.
[7] Schönthaler, F. (2019): Erfolgreich in der digitalisierten VUCA-Welt: Agilität und atmende Lieferketten, in: DOAG Business News 01/2019 – Willkommen in der VUCA-Welt!
[8] Karle, T., Rivas, A. P. (2021): Wege aus dem ökologischen Lock-in: Gestaltung nachhaltiger Geschäftsmodelle, in: DOAG Business News 02/2021 – Ethik, Green IT, Nachhaltigkeit: Das Business der Zukunft?

Dr. Thomas Karle
thomas.karle@doag.org

Dr. Thomas Karle ist COO und Strategieberater der Horus software GmbH, der Product Company der PROMATIS Unternehmensgruppe. Hier ist er in die Entwicklung von Methoden und Produkten für geschäftsprozessorientierte Ansätze zur Implementierung von Unternehmenssoftware-Lösungen und zu sonstigen Business-Transformationen eingebunden. Darüber hinaus ist er Vorstand Business Solutions der DOAG.



Florian Lösch
florian.loesch@horus.biz

Florian Lösch ist als Senior Consultant Digitized Processes und Projektleiter in der PROMATIS Unternehmensgruppe in verschiedenen geschäftsprozessorientierten Implementierungen Oracle-basierter Unternehmenssoftware aktiv. Er ist Experte für Geschäftsprozessmanagement in Kombination mit modernen Technologien wie Process Mining.

Digitalisierung und neue Arbeitswelten

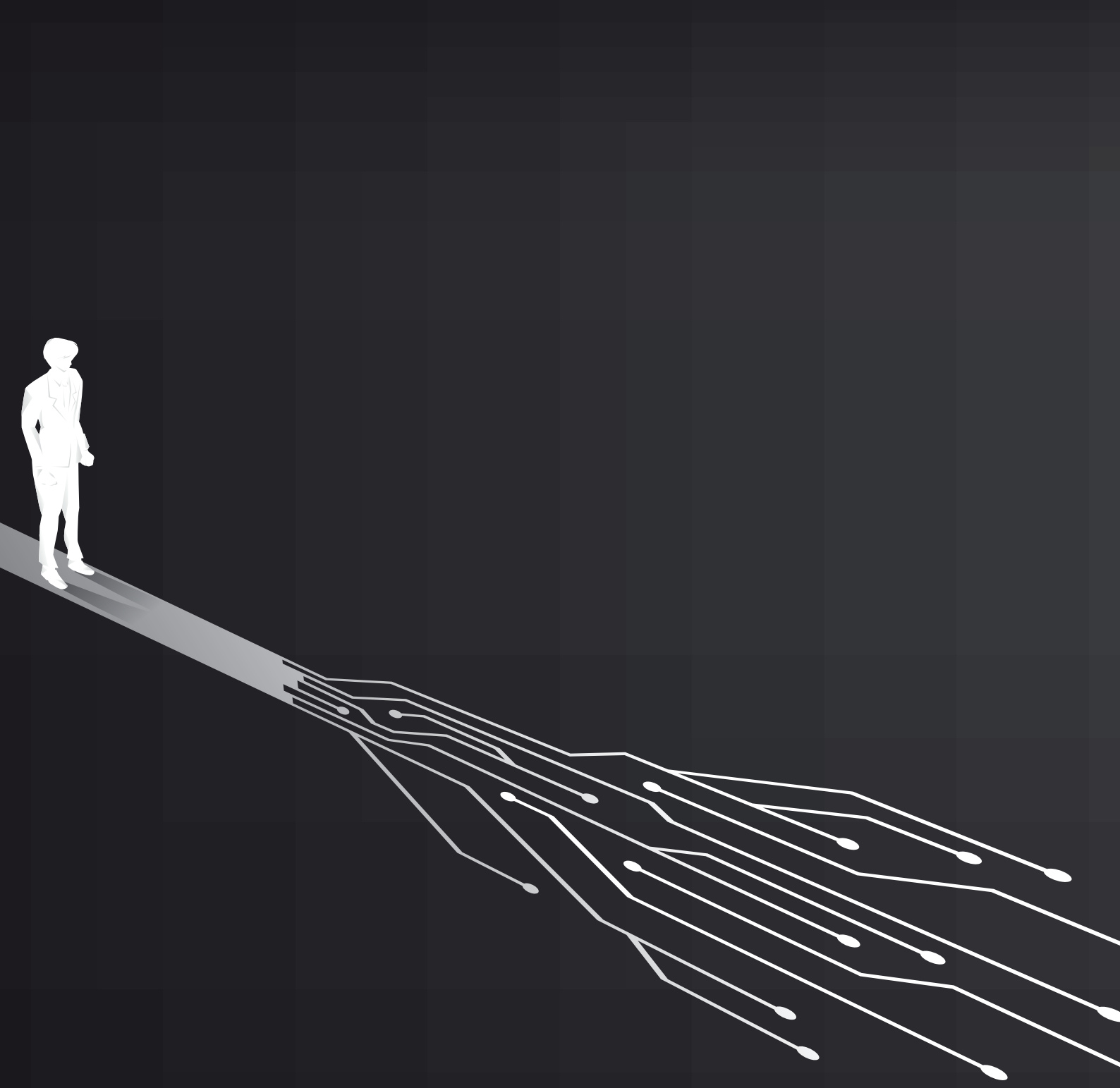
DOAG Redaktion

Unter diesem Motto wird die diesjährige DOAG Konferenz + Ausstellung vom 16. bis 18. November zum zweiten Mal in ihrer langjährigen Geschichte als moderierte Online-Konferenz stattfinden. Nach über 400 Einreichungen im Call for Papers wählte das Programmkomitee über den Sommer rund 180 Vorträge aus, die in den Hauptthemenbereichen „Database & Infrastructure“, „Development & Middleware“, „Data Analytics & KI" sowie „Strategie & Innovation“ präsentiert werden. Ein besonderer Fokus liegt zudem auf den Themen „DevOps“ und – natürlich – „Cloud“.

Das für Furore sorgende Tool Gather.town wird ein einzigartiges Konferenzerlebnis realisieren. Mit einem individualisierten Avatar und dem eigenen Live-Bild im Popup-Fenster können die Teilnehmer im virtuell nachgebauten Nürnberg Convention Center sowohl die Keynotes und Vorträge als auch die Lounges und Stände der Sponsoren und Aussteller besuchen. Dank Gather.town ist das DOAG-typische Networking während der gesamten Konferenz spontan sowie in Relax-Areas oder an Hotspots jederzeit möglich.

Ein spezielles Rahmenprogramm mit interaktiven Formaten und Community-Aktivitäten sowie einer durchgängigen Moderation live aus unserem Studio werden diesen Leuchtturm-Event der DOAG unvergesslich machen. Allen Teilnehmern werden im Nachgang der Konferenz sämtliche Keynotes und Vorträge zur Verfügung gestellt.

Apropos Keynote: Erstmals in der über 30-jährigen Historie der DOAG wird eine Frau eine Keynote halten und zwar Frau Prof. Dr. Yasmin M. Weiß von der Technischen Hochschule Nürnberg Georg Simon Ohm. Thema der Keynote: „New Work & New Skills“. Wir freuen uns auf Ihre Teilnahme!



Die Innovation folgt der Transformation

Lajos Lange, Ströer Digital Publishing / t-online.de

*Innovationskraft ist die Triebfeder eines jeden gesunden Unternehmens, um sich langfristig im Markt zu behaupten. Immer leistungsfähigere Nutzerendgeräte, eine stetig steigende Bandbreite und nahezu endlos wachsende Cloud-Infrastrukturen haben die Innovationszyklen sowie die Erwartungshaltung von Nutzer*innen in den letzten zehn bis fünfzehn Jahren extrem befeuert. Aber was tun, wenn sich Unternehmen technologisch festgefahren haben? Überdimensionierte, monolithische und historisch gewachsene Applikations- und Systemlandschaften sowie eine riesige Anzahl von Übergangslösungen haben sich etabliert. Eine oft notwendige Komplettmodernisierung, um den Anschluss nicht gänzlich zu verlieren, ist teuer, extrem komplex und dementsprechend zeitaufwendig. Hinzu kommt ein verständlicher, jedoch nicht abnehmender Business-Druck an Innovation und Weiterentwicklung. Die Folge: Das Business überdreht und die Technik gräbt sich immer tiefer in einen Komplexitätsgraben von suboptimalen Lösungen. Mit t-online.de haben wir uns entschlossen, aus diesem Muster auszubrechen und die technologische Basis von Grund auf zu erneuern – um eine Produktbasis zu schaffen, auf der wir kontinuierlich innovieren können.*

Transformation vom limitierenden zum ermächtigenden Innovationsfaktor

Damit eine IT nicht komplett handlungsunfähig wird, im schlimmsten Fall sogar das Business schädigt, müssen sich meist grundlegende Dinge in der Technik und Kultur des Unternehmens ändern. Hier gibt es sicherlich keine Patentrezepte, aber zumindest Paradigmen, um eine Transformation anzuschieben und kontinuierlich zum Erfolg zu führen. In unserer aktuellen Transformation bei t-online.de helfen uns die folgenden Bausteine, erfolgreich durch den kräftezehrenden Prozess zu gehen.

Stabilität des Tagesgeschäftes

Transformationen im Enterprise-Umfeld sind meist länger andauernde Phasen von mehreren Jahren, die man nicht unterschätzen sollte. Das Vertrauen des höheren Managements ist eine wichtige Basis, um nicht mitten im Projekt den Boden unter den Füßen zu verlieren. Ein stabiles Bestandsgeschäft muss daher immer gesichert sein! Mein Kredo lautet folglich: Betriebsprobleme gehen immer vor Projektaufgaben.

Bei t-online.de haben wir gut daran getan, uns im ersten halben Jahr genau um diese Absicherung zu kümmern. Failover Testing, Patchmanagement, Refactorings, Prozessautomatisierung und -optimierung, „alte Zöpfe abschneiden“ und aufräumen waren wichtige Maßnahmen, um Komplexität zu reduzieren und mehr Sicherheit im Betrieb zurückzugewinnen. Ein totaler Weiterentwicklungsstillstand über einen längeren Zeitraum ist dabei unrealistisch. Also haben wir uns frühzeitig um ein schlagkräftiges Team von Spezialisten gekümmert, die unseren anderen Teams den Rücken freihalten. An der Stelle sei zu erwähnen, dass dies oft eine undankbare Aufgabe für Mitarbeiter ist. Man muss sich mit alten und „verbastelten“ Systemen herumschlagen, während andere Teams sich mit dem vermeintlichen „hot shit“ auseinandersetzen können. Für mich sind sie die Helden im Hintergrund und so wertschätzend sollte man sie auch immer behandeln!

Neuausrichtung der IT-Strategie

Eine klare Ausrichtung der IT-Strategie ist wichtig, um Orientierung, Halt und die nötige Antriebskraft zu erzeugen. Dabei sollte der Grund für die Veränderung immer an erster Stelle stehen. Technologie ist kein Selbstzweck, sondern löst konkrete Probleme und hilft im besten Fall, sich Wettbewerbsvorteile zu verschaffen.

Cloud only

Infrastructure as a Service (IaaS) mit einer gigantischen Skalierbarkeit ist sicherlich ein wichtiger, aber heutzutage auch ein Hygienefaktor geworden. In Cloud-Transformationsprojekten predige ich immer wieder…

„Agile companies need agile infrastructures!“

So haben wir klar auf eine Cloud-Strategie gesetzt, die den schnellen Entwicklungsprozess unterstützt. Dabei lassen wir die Do-it-yourself-Mentalität hinter uns und setzen auf Platform as a Service (PaaS) mit einer riesigen Vielfalt von gemanagten Diensten, die wir aus eigener Kraft in dieser Qualität niemals selbst betreiben könnten.

Abbildung 1: Produktentwicklungsorganisation der t-online.de (© Lajos Lange)

Dies bedeutet, dass Firmen in kürzester Zeit Applikationslandschaften erschaffen, experimentieren und mit einem Knopfdruck auch wieder terminieren können. Mit diesem Werkzeugkasten besitzen Entwicklungsteams technologisch alles, um sich in einer radikal agilisierenden Wirtschaft zu behaupten. Immer wieder gibt es Widerstände gegen die Einführung fundamentaler Veränderungen wie dem Cloud-Paradigma, die nur allzu menschlich sind. Der Umgang mit Ängsten beziehungsweise Sorgen sollte aktiv begleitet werden: „Ist die Cloud nicht viel zu teuer?", „Werde ich als Systemadministrator überhaupt noch gebraucht?", „Schaffe ich das?" und so weiter. Gerade am Anfang sollte man viel Zeit in die Beantwortung dieser Fragen investieren, um einer andauernden Resistenz vorzubeugen.

Modularisierung

Ein weiterer Faktor, der IT-Mitarbeiter oft verzweifeln lässt, ist die sogenannte Cognitive Overload *[1]*. Gerade in monolithischen Applikationslandschaften ist die Komplexität und auch die Verdichtung an Business-Domänen oft sehr hoch. Diesem Phänomen versucht die IT mittlerweile erfolgreich durch das Aufbrechen in Service-Module entgegenzuwirken. Allerdings sollte dabei nicht nur die technische Modularisierung im Vordergrund stehen, sondern vielmehr eine effiziente Teamorganisation mit klar abgegrenzten Business-Domänen. Dieser Aspekt wird im Management oft unterschätzt und mündet dann in unklaren Systemgrenzen und hohen Abstimmungsaufwänden. Darüber hinaus ist der Systemschnitt auch die Grundlage für einen gut funktionierenden DevOps-Betrieb – getreu dem Motto: „You build it, you run it!"

Bei t-online.de haben wir jedem Team einen klaren Business Purpose (Geschäftssinn) mitgegeben, der im laufenden Prozess auch immer wieder die Systemgrenzen mit definiert. So gibt es beispielsweise ein Content Management System (CMS) Team, mit dem Mantra „tech empowers journalism". Ihre Mission ist es, der Redaktion mit effizienten Lösungen zu helfen, sich auf den kreativen Teil ihrer Arbeit zu konzentrieren und die redaktionelle Leistungskraft zu steigern. Sie bilden eine Basis für unser Content-API-Team, das Inhalte aggregiert und für Ausspielungskanäle transformiert. Unsere Web- und App-Produktteams bilden dann den Rahmen, in dem sich unsere diversen Service-Teams integrieren können.

Es mag im ersten Moment trivial klingen, aber die Organisationsstruktur *[2]* wird gerade bei großen Transformationsprojekten oft vernachlässigt. Es ist also wichtig, im fortlaufenden Prozess immer wieder den Purpose der Teams, die entsprechende Erfolgsmessung mittels Key Performance Indicators (KPIs) und auch die Organisations- und Betriebsform zu optimieren. Mit steigendem Know-how über die Cloud-Dienste im Betrieb und der Modularisierung der Applikationslandschaft gewinnt die IT-Organisation massiv an Geschwindigkeit und erhöht somit konsequent ihren Durchsatz in Time & Quantity to Market sowie ihre Innovationskraft. Mit der Live-Berichterstattung der US-Wahl 2020 als positives Beispiel werden wir noch einmal genauer auf das Thema eingehen.

Enablement & Empowerment

Eine Vision und die darauf abgestimmte IT-Strategie sollten, wie oben beschrieben, immer der Start für den Transformations-

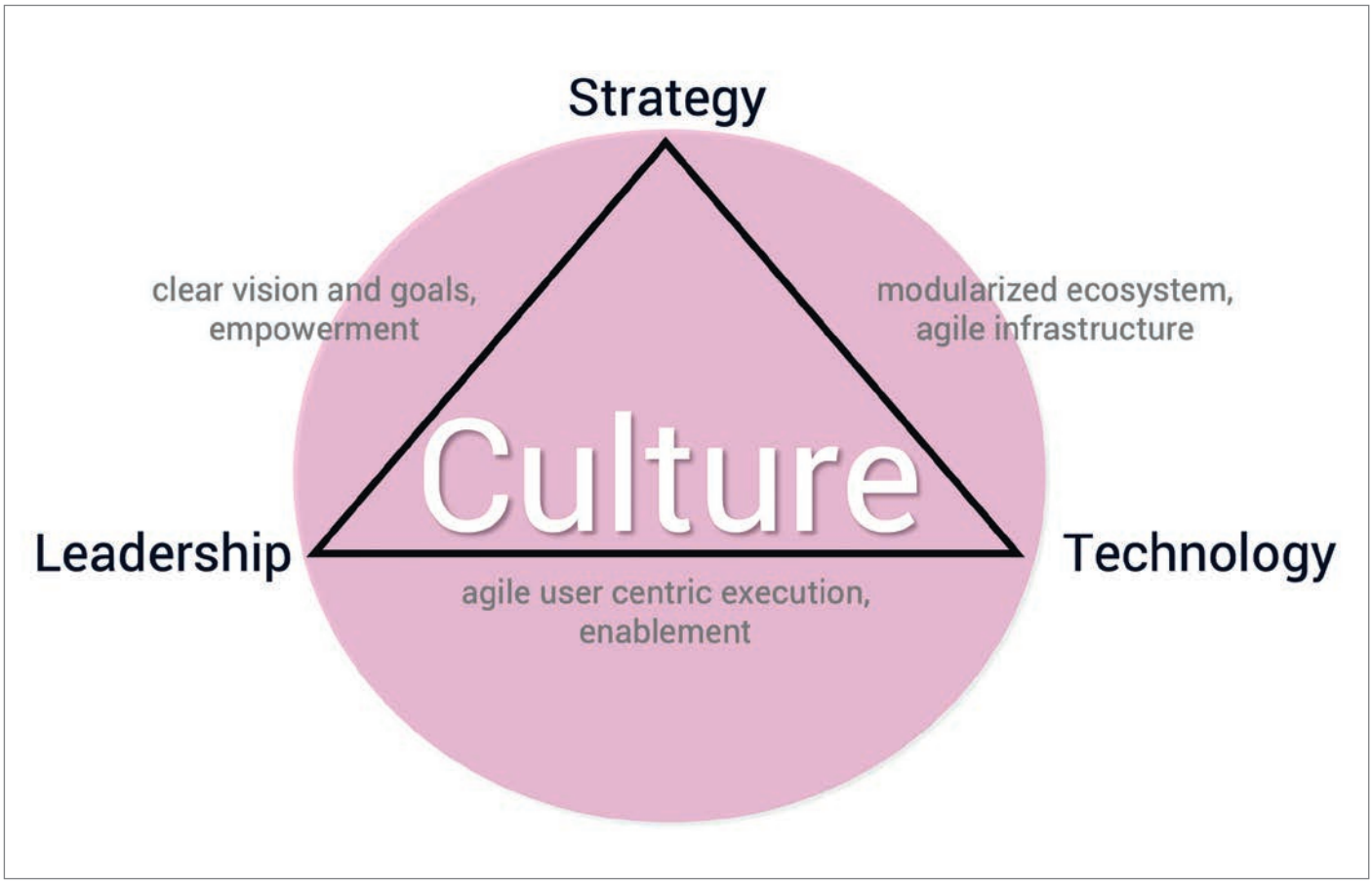


Abbildung 2: Schlüsselfaktoren einer erfolgreichen Transformation (© Lajos Lange)

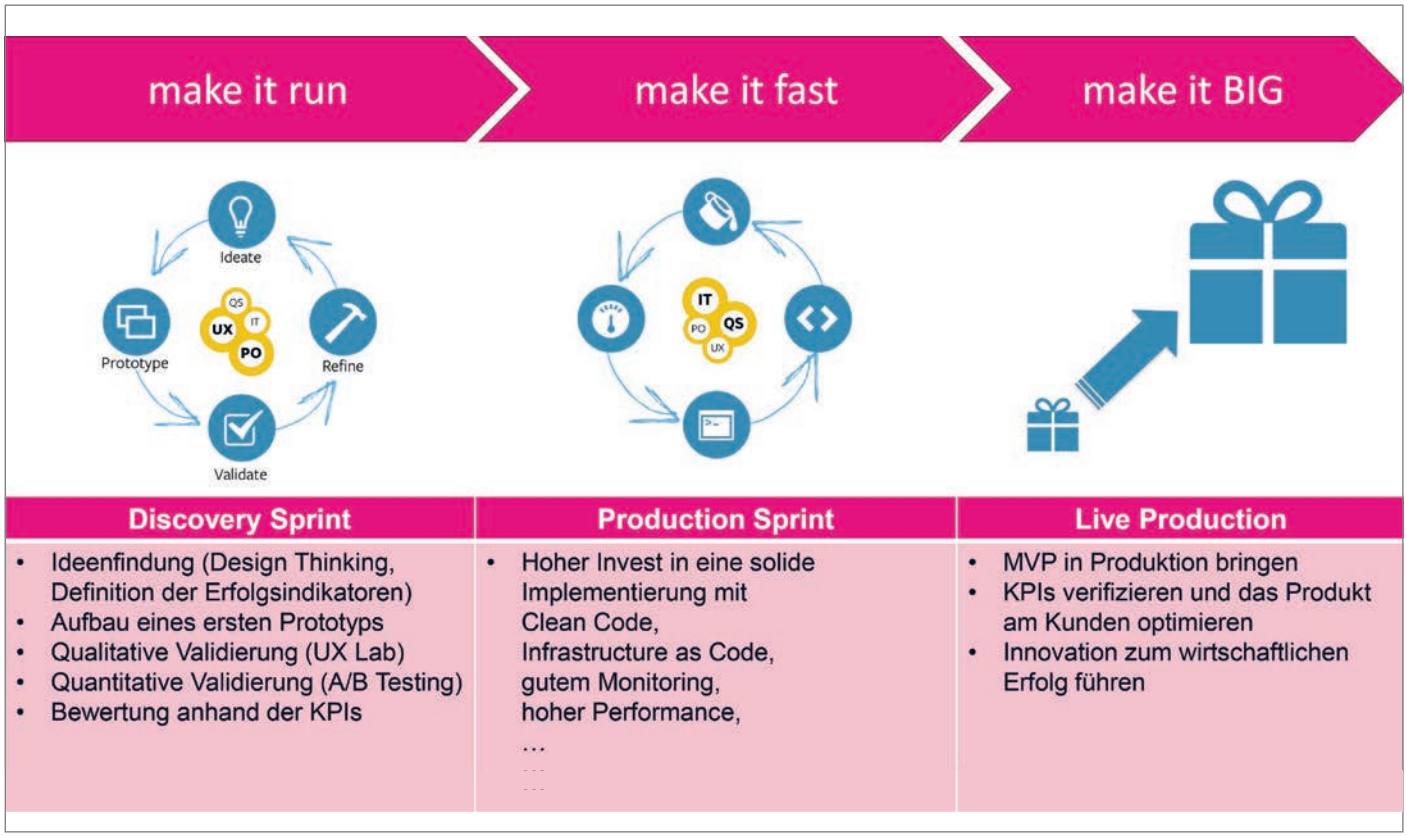


Abbildung 3: Der ideale und agile Produktentwicklungsprozess (© Lajos Lange, Philipp Busse - Head of UX/UI Ebay Kleinanzeigen, Stoyan Stoyanov - Senior DevOps Architect AWS)

prozess sein, die Kraft der vorherrschenden Unternehmenskultur sollte jedoch niemals unterschätzt werden.

Peter Drucker sagte: „Culture eats strategy for breakfast." Damit wies er darauf hin, dass man den Erfolg seiner Unternehmung ins Risiko stellt, wenn man die Kultur von der Strategie trennt. Eine Kultur kann man aber leider nicht am Reißbrett designen, man kann nur mit vielen Impulsen immer wieder darauf einwirken. Somit wird – neben Strategie und Technologie – Führung zu einem weiteren entscheidenden Faktor für den erfolgreichen Wandel. Eine nachhaltige Umstrukturierung in modulare Einheiten und mehr Verantwortung in den einzelnen Teams bedeuten auch ein neues Verständnis von Führung und Management hin zu Befähigung und Ermächtigung der Mannschaft.

Enablement

Die Befähigung von Mitarbeiter*innen, mit den neuen, mächtigen Werkzeugen und Technologien der Cloud umzugehen, ist eine der Hauptaufgaben der Führungsmannschaft. Dabei sind Weiterbildung und ein Seminarprogramm ein guter erster Schritt, der Schlüssel liegt jedoch aus meiner Sicht im Mentoring. Es braucht erfahrene Cloud-Ingenieure in jedem Entwicklungsteam, die mit den Kolleg*innen gemeinsam eine Basis entwickeln und dabei das bestehende Personal konsequent trainieren, um besser zu werden. Es gibt darüber hinaus immer wieder hoch engagierte Mitarbeiter*innen, die den Wandel aktiv mitgestalten wollen und als positive Verstärker, Motivatoren und Treiber den Wandel aktiv mitgestalten. Finde die Treiber des Wandels, unterstütze sie, motiviere und inspiriere sie, kontinuierlich den oft schwierigen Weg weiterzuverfolgen.

Empowerment

Agilität wird zu Anfang meist als eine Art Prozessoptimierung verstanden, es ist allerdings vielmehr eine Kulturrevolution. Wenn Teams die Fähigkeiten entwickelt haben, nachhaltige Lösungen eigenständig zu bauen, liegt es an den Führungskräften, ihren Teams mehr Freiheiten und Verantwortung zu schenken. Dies ist leicht gesagt und erfordert in vielen Fällen ein hohes Maß an Courage, da die Verantwortung für den Gesamterfolg meist noch bei den oberen Führungskräften liegt. Auch der Verlust von Einfluss und Macht hält Führungskräfte oft davon ab, Verantwortung in die Hände ihrer Mitarbeiter zu legen.

Ich selbst beschreibe mich immer wieder gerne als „Physiotherapeuten der Organisation", indem ich Blockaden frühzeitig antizipiere und dann versuche, durch gezielte Maßnahmen die Energie wieder zum Fließen zu bringen. Dabei hilft es, Kolleg*innen immer wieder an die Mission, Vision und Ziele zu erinnern, die Zusammenarbeit in Teams und vielmehr noch zwischen Teams zu fördern und immer wieder inspirierender Treiber von Innovation zu sein. Dies sollte sicherlich das Selbstverständnis einer jeden Führungskraft sein.

Agile Organisationen brauchen agile Infrastrukturen

Natürlich könnte man sagen, dass eine Transformation im besten Falle schon die Innovation in sich selbst ist. Unser Ziel bei t-online.de ist es vor allem, eine neue, agile Infrastruktur zu erschaffen, auf der wir iterieren und unsere Produkte direkt am Kunden innovieren können. So kann Transformation zum kontinuierlichen Innovationsprozess führen. Ein Mantra, das ich in diesem Zusammenhang schon seit vielen

Abbildung 4: Realisierung eines Livestreams zur US-Wahl 2020 – in kürzester Zeit dank eines cross-funktionalen Teams (© Lajos Lange)

Jahren predige, ist: „Make it run, make it fast, make it big."

Ein gutes Beispiel war das größte Medienereignis des letzten Jahres, die US-Wahl 2020. Die Idee war, zur US-Wahl einen Livestream anzubieten, um die Berichterstattung mit Gastbeiträgen aus einem Studio und Live-Schalten zu Politikern und unserem US-Korrespondenten anzureichern. Wir hatten auf diesem Gebiet praktisch keine Erfahrung und das Projektgeschehen gab uns kaum Spielraum für größere Sprünge. Was also tun? Ein cross-funktionales Team zusammenstellen (Journalist & Product & Tech) und durchstarten. Nach zwei Stunden Brainstorming, zwei Tagen Hackathon und zwei Testläufen hatten wir dann eine tragbare Lösung geschaffen.

Dank des Cloud-Streaming-Backbones war die Umsetzung tatsächlich in kurzer Zeit möglich und wir konnten unseren ersten Prototyp für Tausende Nutzer stabil bereitstellen und, was am wichtigsten war: Zahlen, Daten und Fakten sammeln. Auf dieser Basis können wir nun entscheiden, ob wir das Livestreaming Feature in eine solide Implementierung und in die entsprechenden Betriebsprozesse überführen.

Tech Empowers Journalism

Die Zukunftsperspektive bei t-online.de sieht wieder mehr als Magenta aus, da unsere Teams die Herausforderung angenommen haben und mit voller Kraft ein Fundament für eine Innovationsschmiede legen. Technologie muss wieder zum Treiber von Innovation bei t-online.de werden, um einen progressiven Online-Journalismus zu unterstützen. Dafür müssen wir Innovation, wie oben beschrieben, in unseren Alltag verankern und mit Methodiken wie Objectives and Key Results (OKRs) oder Design Thinking weiter etablieren.

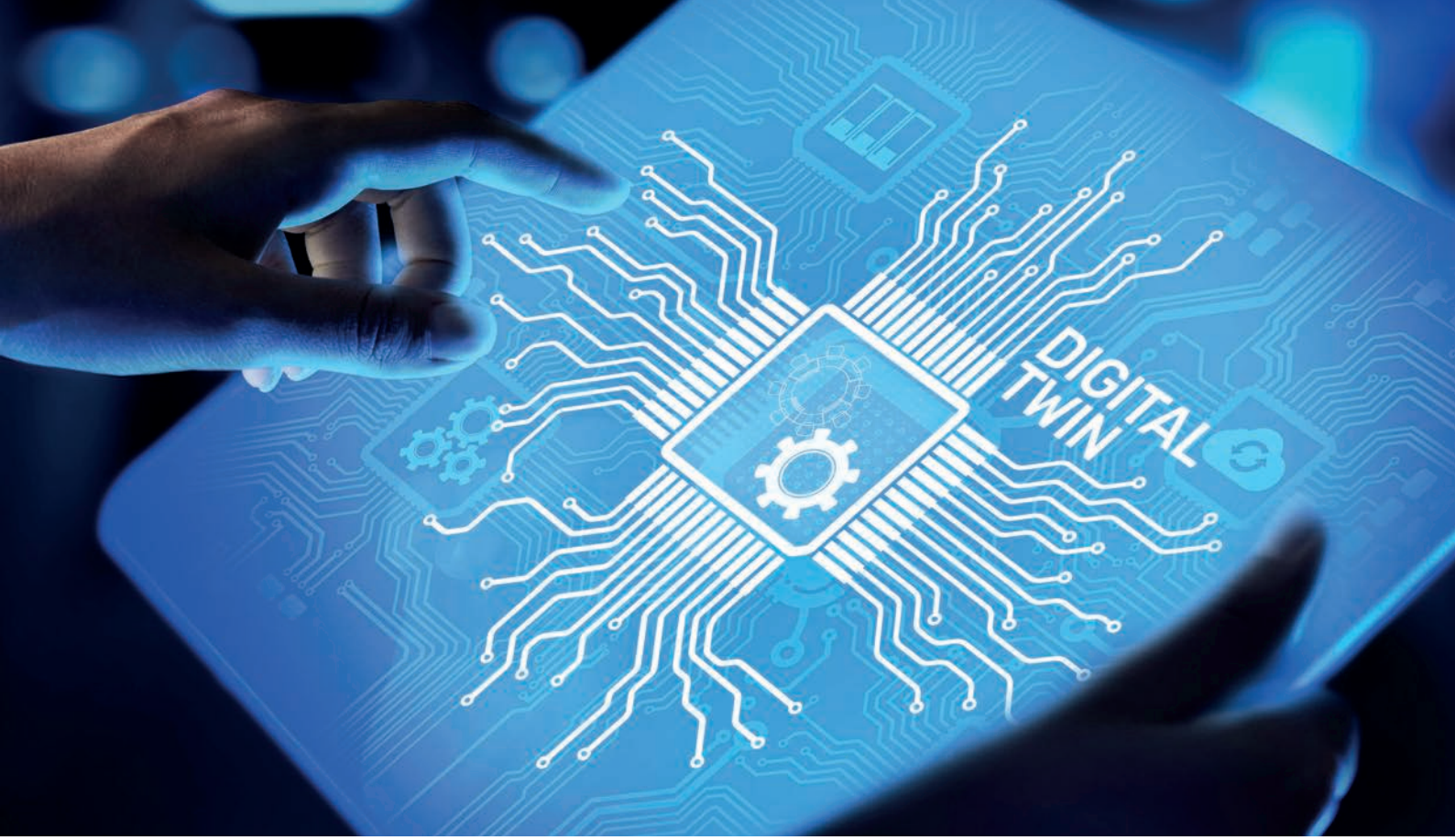
Ein weiterer wichtiger Baustein, an dem wir dafür im Hintergrund schon konzipieren, ist eine Datenplattform als weitere Grundlage für Innovation im Unternehmen. Konkret sammeln wir heute schon viele Daten, die wir aber bisher noch nicht vollumfänglich, automatisiert und mit höchstmöglicher Transparenz allen Fachbereichen zur Verfügung stellen. Diese neu gewonnene Kombination aus einer zugänglichen Datenbasis, einem Machine-Learning-Baukasten der Cloud und unserer modernen Redaktionsplattform soll eine Basis schaffen, um ganz neuartige Produkte und Geschäftsmodelle zu entdecken. Getreu dem bereits oben erwähnten Motto: „Make it run, make it fast, make it big."

Quellen

[1] *https://de.wikipedia.org/wiki/Cognitive_Load_Theory*
[2] *https://de.wikipedia.org/wiki/Gesetz_von_Conway*

Lajos Lange
https://www.linkedin.com/in/lajoslange

Lajos Lange ist CTO der Ströer Digital Publishing und verantwortet in diesem Rahmen die Technik von Deutschlands größter Nachrichtenplattform t-online.de. Davor leitete er die Technik der nationalen Nachrichtenmarken der BILD- und WELT-Gruppe von Axel Springer, Europas führendem Digitalverlag. Nach 10 Jahren Medienindustrie kann er auf viele Erfolge aus diversen Transformations- bzw. Digitalisierungsprojekten zurückblicken. Als Entwickler und Projektleiter begann Lajos Lange seine Karriere im Forschungsbereichs des Fraunhofer Instituts FOKUS und den Telekom Laboratories.



Vom Organizational Twin zur Single Source of Truth

Marcos López, Redaktionsleitung Business News,
in Zusammenarbeit mit Christian Krohn, CONTENT KG

Digitale Transformation, New Work, Workforce Analytics, künstliche Intelligenz... Viele Schlagworte versprechen spannende Ansätze – aber wie steht es um eine konkrete, praktische und vor allem datenbasierte Umsetzung? Und wie steht es um deren Integration, sowohl methodisch als auch technisch? Ein neuer, prämierter Ansatz aus Berlin verspricht viele Probleme mit einem Federstrich zu lösen. Wir wollten wissen, was dran ist, und haben Christian Krohn, den Gründer der Content KG, die sich auf die aufgaben- und datengestützte Unternehmenssteuerung mittels eines weltweit einmaligen relationalen Datenmodells spezialisiert hat, zu dem neuartigen Ansatz aus Deutschland befragt, der Verwendung eines digitalen Zwillings als Single Source of Truth (SSOT) zur Unternehmenssteuerung.

Das Problem – fehlende Transparenz und Daten

„Für unseren Kunden, eine Serviceeinheit eines großen deutschen Unternehmens aus der Branche chemische Industrie, Öl und Gas, begann das Jahr 2016 mit einem Schock", erinnert sich Christian Krohn. Die Geschäftsführung hatte der Serviceeinheit mit knapp 190 Mitarbeiter*innen und einigen Zehntausend betreuten Angestellten unterschiedlicher Tochterfirmen ein zweistelliges Kostensenkungsziel aufgegeben.

„Kostensenkungen und Effizienzsteigerungen sind im Shared-Service-Umfeld ja gang und gäbe. Aber dieses Mal war die Zielvorgabe ungewöhnlich hoch", sagt Krohn. „Und keine gute Nachricht. Die Einheit war schon ziemlich auf Effizienz getrimmt, hatte über die Jahre alle Hausaufgaben gemacht. Das hört dann niemand gern", fügt er hinzu. Krohn hatte selbst acht Jahre bei Siemens im Bereich Business Development & Strategie einer vergleichbaren Einheit Transformationsprojekte begleitet und kennt die Größenordnungen an Einsparpotenzialen aus eigener Erfahrung.

„Das Portfolio der betroffenen Serviceeinheit reichte von einfachen Änderungen der Bankdaten, der Erstellung von Zeugnissen bis hin zur Zeitwirtschaft, der komplexen monatlichen Abrechnung der Mitarbeiter, der Entsendung ins Ausland oder dem Aktien-Management für Mitarbeiterinnen und Mitarbeiter. Eine Servicehotline fungierte sowohl als First-Level-Support als auch als Dispatching-Einheit zur Verteilung

weiterführender Arbeiten. Das gesamte Arbeitsgebiet brachte zu diesem Zeitpunkt knapp 350.000 Anfragen und Aufträge im Jahr aus ganz Deutschland in die Einheit des Kunden.

Man war dort zunächst ratlos. Es gab zwar eine Menge Kennzahlen und auch viele Analysen aus den vorangegangenen Projekten, allerdings reichte diese Transparenz nicht mehr aus, um auch noch die letzten Potenziale sichtbar zu machen. Und dann erinnerte sich die Leitung glücklicherweise an unseren Ansatz und hat uns kontaktiert."

Der Lösungsansatz: Ein digitaler Zwilling auf Arbeitsebene

Ein Jahr zuvor war Christian Krohn, Gründer der Content KG aus Berlin, an die Einheit herangetreten, um sich von den dortigen Experten eine fachliche Einschätzung zu seinem Ansatz der Analyse und Steuerung von Arbeit geben zu lassen. Sie hatten den Ansatz zwar interessant gefunden, zu der Zeit jedoch keine konkrete Verwendung für die entstehenden Daten gesehen.

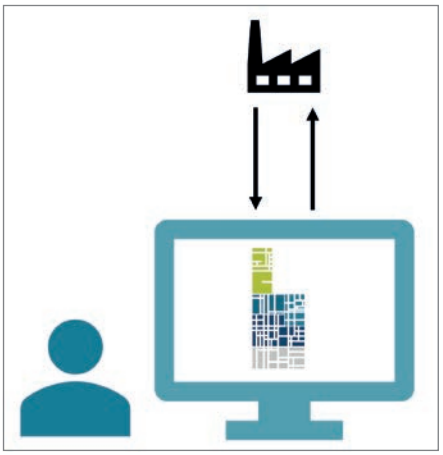


Abbildung 1: Die Abbildung der tatsächlichen Arbeit als digitaler Zwilling zur Organisationssteuerung (Quelle: Christian Krohn & Jens Grundei)

„Ich hatte der Leitung einiges über Geschäftssteuerung, Analysen, Szenarien und Konsistenz von Daten erzählt. Und darüber, dass unsere Datenquelle zu vielen sehr unterschiedlichen Zwecken eingesetzt werden könne. Diese Bedeutung wurde allerdings erst wirklich verstanden, als man dann nach der Implementierung die eigenen Daten zur Verfügung hatte und die Experten diese auch zwei Jahre nach der Einführung zu unterschiedlichen Zwecken kontinuierlich weiter genutzt haben."

Krohn wirkt erfreut: „Eine Führungskraft ist später zu einem mittelständischen Unternehmen der Maschinenbaubranche gewechselt und leitet dort heute eine vergleichbare, jedoch kleinere Einheit. Den Ansatz hatte sie aber mitgenommen, um Transparenz in das Portfolio und die tatsächliche Arbeit zu bekommen. Das aktuelle Portfolio ist zwar mit dem vorherigen vergleichbar, nur vielleicht nicht ganz so breit", weiß Krohn. „Man hat dort zwar deutlich weniger Mitarbeiterinnen und Mitarbeiter zu betreuen und damit auch weniger Transaktionen als in der vorherigen Serviceeinheit. Die Themen sind allerdings nahezu identisch. Nur gibt es in der neuen Einheit größenbedingt deutlich weniger modellierte Prozesse und dokumentiertes Wissen. Die Spezialisten haben einfach weniger Zeit für solche Dinge

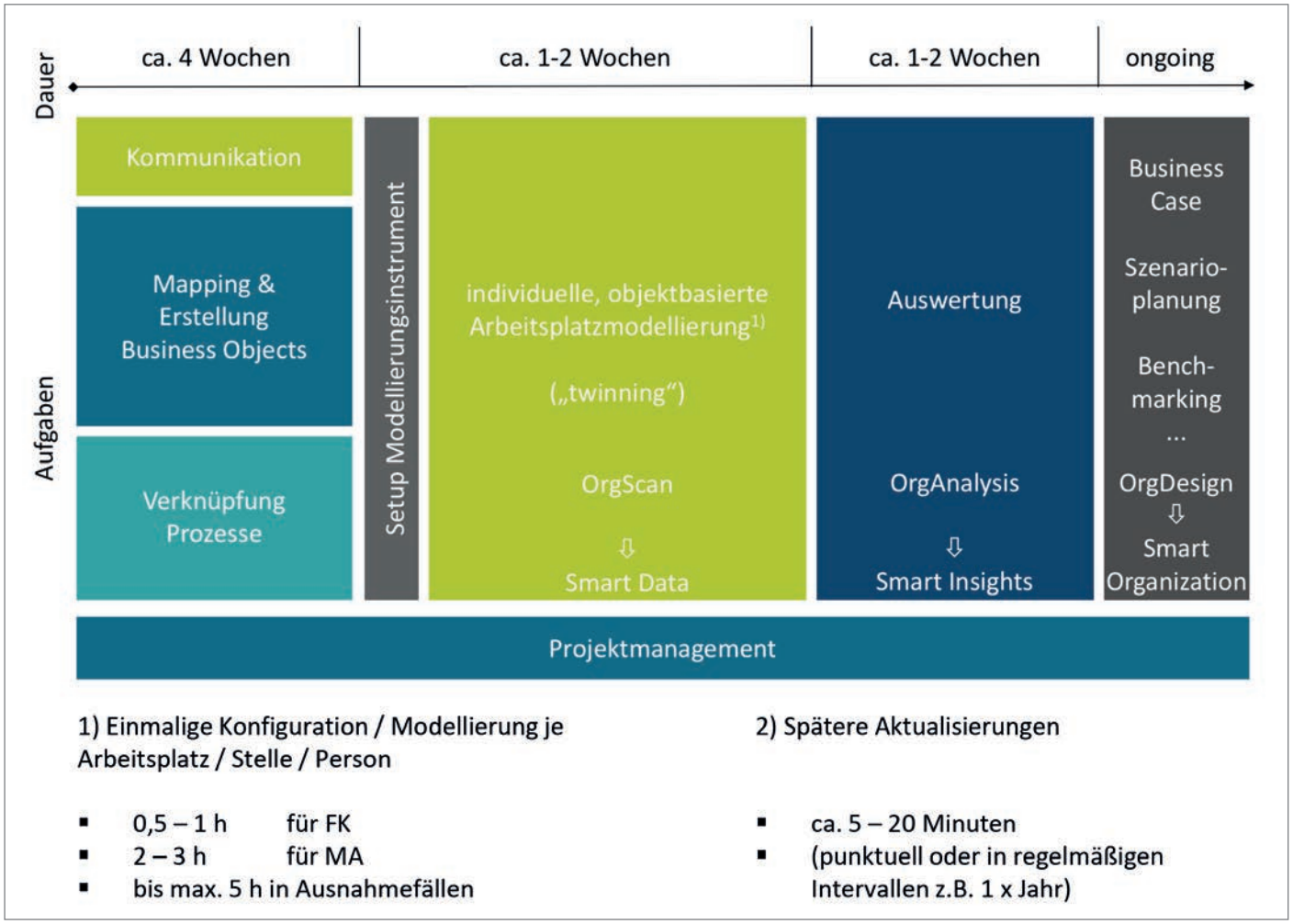


Abbildung 2: Implementierungsphasen zur Erzeugung eines digitalen Zwillings (Quelle: CONTENT KG)

wie Prozessmodellierung oder Wissensdokumentation und sind viel mehr ins operative Tagesgeschäft eingebunden."

Man habe jedoch aufgrund der bereits gemachten Erfahrungen gleich ‚geschaltet' und Herrn Krohn direkt gefragt, ob der Ansatz nicht auch zum Aufbau eines Wissensmanagements nutzbar wäre. „Ich habe dies bejaht, und wir begannen 2020 in der Corona-Pandemie, unter erschwerten Bedingungen und neben dem Tagesgeschäft der Einheit, mit dem Ansatz, Transparenz in das Portfolio und die Organisation des bestehenden Wissens zu bringen. Aktuell weiten wir das Portfolio auf andere Bereiche aus." Krohn ist zufrieden. „Eigentlich müsste man das immer so machen. Keine Ahnung, warum das nicht schon früher erfunden wurde. Ich habe vor Siemens selbst in der Beratung und dann auch Siemens-intern mit Prozessanalysen zu tun gehabt", so Krohn. „Aber der Ansatz ist tatsächlich ganz anders – und macht eine Menge mehr Daten und Zusammenhänge sicht- und nutzbar. Die entstehenden Daten sind quasi zweckfrei, bilden realitätsnah die gesamte Arbeit zum Teil bis auf Datenfeldebene ab."

Mittlerweile werden dieselben Portfolio-Daten beim Mittelständler auch in Hinblick auf Compliance-relevante Fragen in Bezug auf einkommenssteuerrechtliche Aspekte in den Blick genommen: Welche Personaldienstleistungen der Firma berühren in welchem Umfang die steuerrechtliche Verarbeitung? „Hier kann mit einem ‚Flag' in der Library eine eindeutige Zuweisung auf Prozessebene durch Expert*innen erfolgen und den Transparenzanforderungen ist auf Prozessschrittebene genüge getan. Kein großes Projekt, keine wochenlangen Prozessaufnahmen und beratungsintensiven Analysen sind notwendig", erläutert Krohn.

Er erinnert sich: „In der Unternehmensberatung an der Schnittstelle zur Softwareentwicklung habe ich viele Projekte zur Prozessoptimierung und Analyse erlebt. Das hat viel Zeit und Diskussionen gekostet. Und eine Menge Nerven zur Abstimmung der Richtigkeit und Belastbarkeit der Ergebnisse." Er habe sich dann gefragt, ob dies nicht auch anders, viel einfacher und grundsätzlicher ginge. Und man in jedem Projekt tatsächlich immer wieder von vorne beginnen müsse, wo doch das Portfolio, damals im Personalwesen, immer vergleichbar sei. Nach einigen Jahren Forschung und Ausprobieren unterschiedlicher Ansätze habe er dann die zündende Idee gehabt. Er sei damals aus der Beratungsbranche zu Siemens gewechselt und habe dort acht Jahre im Bereich Business Development und Strategie für die neu gegründete Global-Shared-Service-Einheit im Personalbereich gearbeitet und deren Transformation mit vorangetrieben.

„Damals wussten wir nichts über die Prozesse und das Portfolio in den verschiedenen Ländern. Nur Deutschland war eine Insel der Transparenz. Und wir hatten jede Menge Zielvorgaben, um global effiziente Leistungsstrukturen zu etablieren. Das war eine schwierige Ausgangsbasis und die Chance, über einen einheitlichen Ansatz eine globale Transparenz auf Prozessebene zu schaffen. Meine Vorgesetzten haben mich machen lassen, das war ein großes Geschenk. Innenpolitisch sind wir zwar irgendwann stecken geblieben, aber der Ansatz war geboren und wir waren erste Schritte gegangen", erinnert sich Krohn.

„Als wir dann bei Siemens international mit einem Benchmarking-Anbieter zusammengearbeitet haben, wurde die Notwendigkeit belastbarer Daten sichtbarer denn je. Da habe ich das erste Mal den bekannten Ausdruck ‚garbage in – garbage out' leidvoll miterleben müssen. Die vielen erbrachten Arbeitsstunden der Kolleg*innen auf der ganzen Welt und in München, Mitarbeiter*innen, Controller*innen, Führungskräfte. Und auch die Geldsummen, die für die Beratungsleistungen fällig wurden." Krohn schüttelt den Kopf.

Das Projekt – und der Beweis

„Als sich unser späterer Kunde dann meldete, war ich ganz erfreut. Wir haben die Ärmel hochgekrempelt und losgelegt. Vom Anruf bis zum Abschluss des Projektes haben wir gut zwei Monate gebraucht. Es sind nicht immer alle Beteiligten auch verfügbar, wenn man sie braucht. Das Tagesgeschäft hat schließlich Vorrang. Die Erhebung und Gewinnung der Daten selbst hat nur zehn Tage benötigt. Bei einem anderen Kunden tatsächlich sogar nur einen Tag. Darauf bin ich stolz", so Krohn.

Er erläutert weiter: „Die Einführung eines digitalen Zwillings geschieht in vier Abschnitten. Dabei ist die Dauer jeweils abhängig vom Grad der Leistungstransparenz zu Beginn der Einführung – und von der zeitlichen Verfügbarkeit der Portfolioexperten auf Arbeitsebene. Wir gehen nämlich bis auf die konkrete Arbeitswirklichkeit hinunter und extrahieren dort die Leistungsobjekte, an denen Menschen, Software und Maschinen arbeiten. Haben wir bereits einen Katalog, eine Library an Datenobjekten zu den Leistungsobjekten, geht es sehr schnell und wir können innerhalb weniger Tage vollständige Daten produzieren. Beginnen wir bei null, dauert es schon ein paar Wochen. Das hängt vor allem von der Verfügbarkeit der beteiligten Wissensträger*innen und Expert*innen auf Kundenseite ab. Immerhin gibt es auch ein Tagesgeschäft und das hat immer Vorrang."

Projektablauf in vier Phasen:

1. Portfolio, Mapping und Prozesse
2. Datengewinnung
3. Auswertung
4. Szenarien, Business Cases etc.

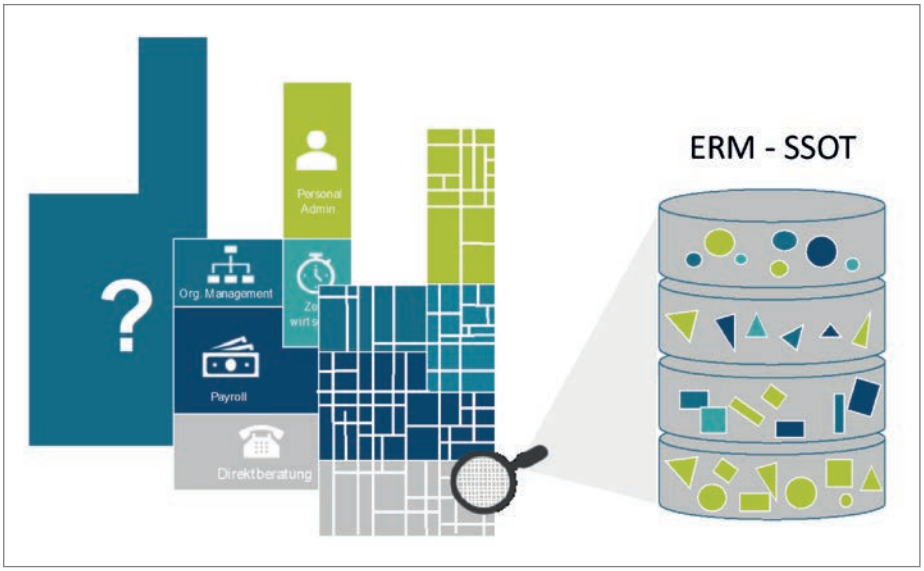


Abbildung 3: Illustration zur vollständigen Zerlegung der Arbeitsleistungen von Organisationen in Datenobjekte (Business Objects) hin zu einer Single Source of Truth in einem relationalen Datenmodell (Quelle: CONTENT KG)

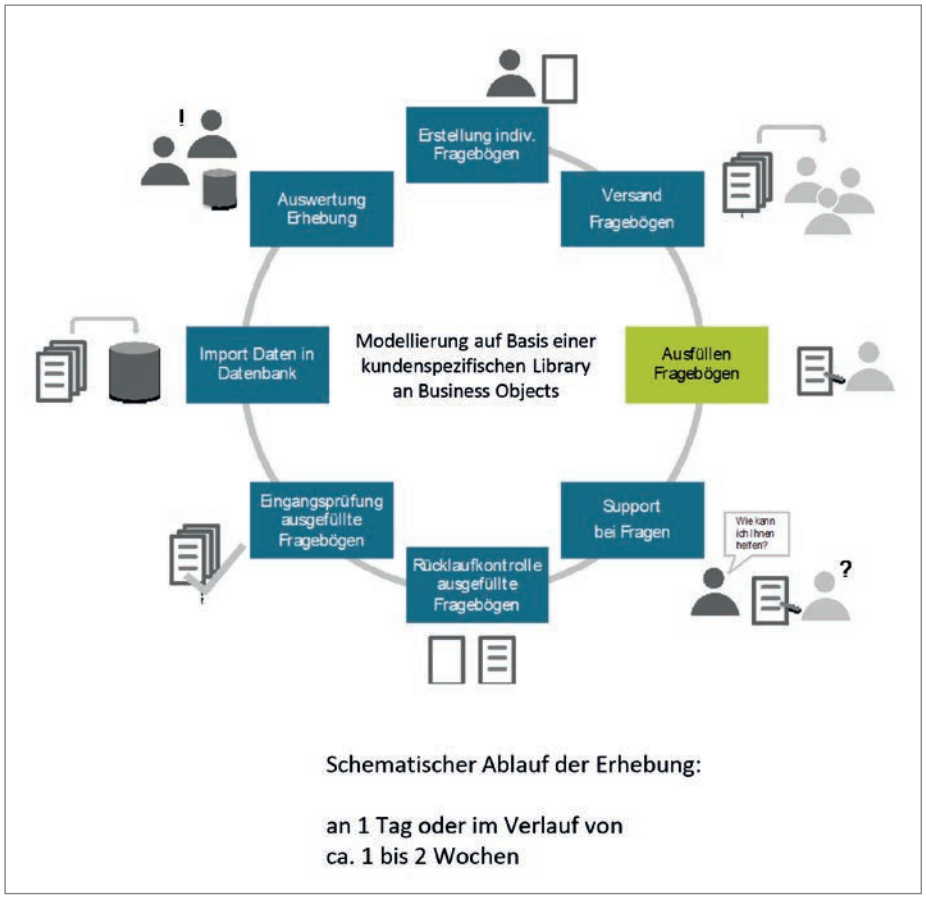


Abbildung 4: Übersicht zum Ablauf der Datengenerierung (Quelle: CONTENT KG)

Erste Phase – Portfolio und Prozesse als Datenobjekte

Krohn führt aus: „In der ersten und wesentlichen Phase geht es allein um die konkreten Leistungsinhalte der Organisation, die untersucht werden und für die ein realitätsgetreues Abbild auf Prozessebene geschaffen werden soll: ein digitaler Zwilling. Diese Arbeit erfolgt mittels einer Library, eines Kataloges von Datenobjekten.

In dieser Library finden sich dann je nach Branche oder Unternehmensfunktion einige Tausend Objekte, die auf Prozessebene allein die Leistung beschreiben. Und das vollständig. Das bedeutet, dass sie auch ohne Prozessmodellierung eine vollständige Transparenz des Outputs einer Organisation generieren – und zwar jeder Organisation. Nicht nur die Leistung der Kernprozesse wird konkret greifbar, sondern die Leistung aus jeder erledigten Aufgabe, jeder Art von Arbeit.

Das Mapping der existierenden Library zu Projektbeginn im Kreis der Fachexperten bei unserem Kunden dauerte einen knappen Tag. Im Anschluss wurden fehlende Datenobjekte mit Expertinnen und Experten erarbeitet und in der Library ergänzt. Damit war die Leistungsseite für den zu schaffenden digitalen Zwilling erarbeitet."

„Ein Großteil bezahlter Arbeit steckt erfahrungsgemäß gar nicht in den beschriebenen Kernprozessen. Denken Sie allein an Führungsaufgaben oder arbeitsorganisatorische Tätigkeiten. Aber auch im Kernportfolio einer Organisation werden meistens nicht alle Arbeiten erfasst oder gar abgebildet und in Prozessen modelliert", sagt Krohn. „Das wird uns bei den Auswertungen zum Ressourceneinsatz und den Aufgabenverteilungen immer wieder deutlich. Genau so etwas wollen Sie als Führungskraft auch sehen."

Krohn ergänzt: „Prozessmanagement ist wahnsinnig aufwendig in der erstmaligen Aufnahme und arbeitsintensiv in der weiteren Pflege und Anpassung der Prozessmodelle. Auch mit datenbankgestützter Software wie Symbio oder Signavio. Den Aufwand muss man sich auch leisten wollen. Und die Granularität und Präzision der Prozessbeschreibungen bleiben dann noch häufig hinter dem, was man eigentlich bräuchte. Gerade beim Thema Digitalisierung, Prozessautomatisierung oder Robotics. Eine Verbindung zu konkreten Kostenstellen, Stellentypen, Teams, Standorten, Kapazitäten oder realen Kosten existiert erst gar nicht. Da ist man im Process Mining schon etwas weiter. Allerdings gilt dies wiederum nur für technische Prozesse innerhalb von Software, ohne personelle Kapazitäten und Kosten. Wir bilden jedoch alles an Leistung ab, 100%, samt aller eingesetzten Kapazitäten und Kosten. Daher auch die Analogie zum Zwilling, dem digitalen Zwilling. So können wir Daten aus Process Mining in diesen integrieren. Andersherum ist das nicht möglich. Process Mining bietet Ausschnitte, unser Ansatz das ganze Bild."

Zweite Phase – die standardisierte Modellierung der individuellen Arbeitssituation

Mittels eines eigenen Ansatzes modellieren dann alle Mitarbeiterinnen und Mitarbeiter ihren Arbeitsplatz auf Basis der Datenobjekte aus der Library. „Das funktioniert ganz einfach sogar in Microsoft Excel oder auf Wunsch webbasiert", sagt Krohn.

Dass dies am Ende tatsächlich so einfach sein würde, hatte der Kunde nicht zu hoffen gewagt. „Sie waren schon skeptisch, das muss ich ehrlich zugeben. Man hatte jedoch angesichts der herausfordernden Vorgaben und der Kürze der Zeit keine andere Wahl, als uns zu vertrauen. Auch die Sorge, vor der Arbeitnehmervertretung oder dem Datenschutz zu scheitern, war groß. Aber

Rahmendaten des Projektes:

- Anzahl erhobener Arbeitsplätze: 192 in sechs Organisationseinheiten (zwei weitere waren zum Projektstart hinzugekommen)
- 177,18 gebundenen FTE (40h/Wo)
- 543 unterschiedliche Ereignisse, Prozessauslöser, Arbeitsanlässe
- 2.500 Datenobjekte (z.B. Erstellung Zeugnis, Erfassung IBAN, Ermittlung Resturlaub)
- 31.747 Datensätze = ø 180 Aufgaben je Arbeitsplatz (von min. 55 – max. 1.650)
- erhoben in einem 10-tägigen Zeitraum April/Mai 2016

Abbildung 5: Ineinandergreifen betriebswirtschaftlicher Strukturen durch die zentrale Verbindung von Business Objects (Quelle: CONTENT KG)

schlussendlich waren die Daten anonymisiert und Leistungskontrollen unmöglich, auch wenn wir bis auf Arbeitsplatzebene Transparenz hatten. Das klingt paradox, wurde aber positiv geprüft."

Dritte Phase – Datenkonsolidierung, Konsistenzprüfung und organisatorische Verknüpfung

Nachdem dann jeder Arbeitsplatz individuell auf Basis der Library modelliert worden war, wurden die Daten kompiliert und in eine Datenbank überführt. Der digitale Zwilling, ein vollständiges digitales Abbild der Organisation auf Arbeitsebene, war geboren:

Sämtliche Arbeitsleistungen auf Prozessebene und darüber hinaus, alle Kapazitäten und vollständigen Arbeitsplatzkosten samt aller verfügbaren Organisationsdaten wie Stellentyp, Team, Abteilung, Standort, Kostenstelle etc. waren nun in einem einzigen Datenmodell konsistent miteinander verbunden.

Vierte Phase – Auswertungen und Nutzung der Daten

„Der Rest war dann fast einfach", erinnert sich Krohn. „Der Kunde konnte nun alles sehen und sich überlegen, mit welchen Maßnahmen er an welche Leistungen wie herangehen wollte. Wo es sich lohnen würde und wo nicht. Aus einer Erkenntnis, nämlich wieviel Zeit in die Erfassung von Daten fließt, wurde sogar eine Portallösung als Leuchtturm-Projekt auf Vorstandsebene vorgestellt und mit einem zweistelligen Millionenbetrag auch positiv entschieden. Das Projekt ist in der Umsetzung. Insgesamt hatte der Kunde 50 Maßnahmen, Ideen und Projekte auf Basis unserer Daten identifiziert und konnte am Ende mit deren Umsetzungen den Zielvorgaben zum Jahresstart Rechnung tragen."

Krohn erinnert sich: „Rückblickend kann ich sagen: Eines der schönsten Erlebnisse dort war, als ein Benchmarking-Anbieter kam und relevante Daten benötigte. Das Mapping zu dessen Struktur dauerte einen Tag und die Daten waren widerspruchsfrei, vollständig und konsistent zugeordnet. Ein Vorgang, der bei Siemens seinerzeit einige Monate beansprucht hatte. Ich kannte damals den Begriff *Single Source of Truth* noch nicht. Das wäre es damals gewesen! Und dass wir heute bei dem erwähnten Mittelständler die Einführung des Wissensmanagements mit unserem Ansatz unterstützen würden, hätte ich mir damals auch nicht träumen lassen. Aber damals waren die Zusammenhänge der Daten zu weiteren Prozessen und Funktionen im Unternehmen auch noch nicht so sichtbar wie heute."

Krohn ist sichtbar zufrieden: „Ich erinnere mich noch, wie wir nach dem Projekt zum Feedback im Büro der Leitung zusammensaßen und eines klar wurde: dass Führungskräfte bei Bedarf auf Knopfdruck nachvollziehen können sollten, was in ihrer Einheit passiert. Und wie die Dinge fachlich, prozessual oder sachlogisch zusammenhängen beziehungsweise in Kapazitäten und Kosten. Diese Transparenz gibt verantwortlichen Führungskräften und Mitarbeiter*innen, gerade im agilen Kontext, jede Menge Entscheidungssicherheit und -geschwindigkeit bei operativen wie strategischen Fragestellungen. Da fällt eine Menge Stress ab von den Schultern. Und so sollte es mit Daten im Jahr 2021 auch sein."

Christian Krohn
christian.krohn@content-b.com

Christian Krohn ist Gründer der CONTENT KG, die sich auf die aufgaben- und datengestützte Unternehmenssteuerung mittels eines weltweit einmaligen relationalen Datenmodells spezialisiert hat.

„Vielleicht die erste Plattformstrategie aus Deutschland auf dem globalen ERP-Markt.“

Interview mit Prof. Dr. Jens Grundei

Dr. Jens Grundei ist Professor für Corporate Governance & Organization und beschäftigt sich intensiv mit Fragen der Effizienzbeurteilung von Organisationsstrukturen. Marcos López, Redaktionsleiter Business News, sprach mit ihm über den innovativen Ansatz des Gründers Christian Krohn, der im Artikel zuvor, „Vom Organizational Twin zur Single Source of Truth" (S. 93-97) geschildert wurde.

Herr Prof. Grundei, wie beurteilen Sie aktuell die datenbasierte Unternehmensführung hierzulande?

Die datenbasierte Unternehmensführung wird zwar seit geraumer Zeit diskutiert, bislang jedoch nur in ausgewählten Unternehmensfunktionen wie Produktion und Marketing auch wirklich schon zur gelebten Praxis gezählt. Für diverse Kernbereiche klassischer Managementaufgaben gilt dies bislang jedoch nicht – insbesondere die schlechte Datenqualität wird dabei als Ursache ausgemacht. Der von mir mitkonzipierte Ansatz eines „Organisations-Controlling" fand bislang ebenfalls seine praktischen Grenzen in Schwierigkeiten der Operationalisierung sowie der Generierung und Vorhaltung geeigneter Daten.

Woran hapert es?

Reorganisationsentscheidungen sind vielfach nicht gut begründet und werden kaum jemals systematisch auf ihre Erfolgswirkungen analysiert; wenn Unternehmen im Kontext von Organisationsgestaltung an so etwas wie „Messen und Auswerten" denken, dann geht es noch immer zumeist um Spans and Layers-Projekte – man misst also gewissermaßen das, was relativ einfach messbar ist, nicht unbedingt das, was Sinn macht. Das erinnert mich immer ein wenig an denjenigen, der nachts unter einer Laterne nach seinem verlorenen Schlüssel sucht – weil dort Licht ist, nicht etwa, weil er seinen Schlüssel tatsächlich dort verloren hätte. Mit der innerorganisatorischen Transparenz sieht es häufig noch ähnlich düster aus; vielfach bekommt man ja noch nicht einmal auf die vermeintlich einfache Frage nach der Mitarbeiterzahl eines Unternehmens eine verlässliche Antwort. Da möchte man nach Details wie „Wie viele Mitarbeiter beschäftigen sich mit Aufgabe X? Wieviel Zeit verwenden Sie darauf und welche Kosten entstehen in verschiedenen Organisationseinheiten dafür?" gar nicht erst fragen. Wird es dennoch getan, so zieht das nicht selten größere, zeit- und kostenintensive Projekte nach sich.

Sie haben eine besondere Verbindung zu Herrn Krohn, dessen methodischer Ansatz, wie im Artikel zuvor beschrieben, relativ schnell Ergebnisse zur organisationalen Transparenz und zu betrieblichen Optimierungspotenzialen liefert. Wie kam die Kooperation mit ihm zustande?

Herr Krohn und ich haben uns zufällig auf einem Kongress getroffen und festgestellt, dass wir beide fachlich tief verbunden sind, sowohl in Bezug auf Gedanken eines der Gründungsväter der Organisationslehre als auch hinsichtlich der Kosten- und Leistungsrechnung.

Wo sind die Schnittmengen Ihrer fachlichen Radien?

Der gemeinsame Kern, an dem Herr Krohn und ich uns fachlich begegnen, ist die strikte Aufgabenorientierung der betriebswirtschaftlichen Organisationslehre, deren Bedeutung wohl niemand so deutlich herausgestellt hat wie Prof. Dr. Erich Kosiol. Kosiol konnte zu seiner Zeit seinen Ansatz allerdings nicht in Daten umwandeln und maschinell verarbeiten. Und es fehlten noch ein paar Kniffe aus der Praxis, die Herr Krohn entwickelt hat. Die heute übliche Sichtweise auf Unternehmen über Prozesse und das Prozessmanagement könnte nun einen völlig neuartigen Impuls bekommen.

Was ist das Besondere an dem Ansatz von Herrn Krohn?

Der Ansatz von Herrn Krohn verbindet Elemente der klassischen betriebswirtschaftlichen Organisationsanalyse mit modernen Formen der Datenhaltung so geschickt, dass nicht nur einfach ein Teilproblem gelöst wurde, sondern die Grundlage für die Datenbasierung von Managemententscheidungen schlechthin geschaffen wurde. Mit der einzigartigen Form der Aufgabenanalyse schafft er gewissermaßen das „Backbone" für die konsistente Zusammenführung aller möglichen Datenbestände, die dann für verschiedenste Analysen und Veränderungen genutzt werden können – von der strategischen Planung über Out-/Insourcing-Entscheidungen und Organisationsfragen bis hin zur Gestaltung von HR-Systemen, um nur einige anzusprechen.

Professor Jens Grundei beim Studienstart an der Quadriga Hochschule Berlin (© Jana Legler)

Analog zur Idee des Digital Twinning, wie wir sie seit einiger Zeit zur Steuerung technischer Systeme kennen, besteht hier also die Möglichkeit, einen „Digital Corporate Twin" zu schaffen. Ein digitales Abbild der Realität der Unternehmung auf Arbeitsebene entsteht. Und es wächst mit jeder neuen Nutzung. Das erlaubt es, die eigene Organisation in einem bislang nicht bekannten Maße analysieren zu können.

Welches Potenzial wohnt digitalen Unternehmens-Zwillingen inne?

Ich glaube, wir können hier von einer echten Sprunginnovation sprechen: Sie ist radikal und kommt aus einer Richtung, mit der niemand gerechnet hat. Sie hat das Potenzial, einige existierende Märkte komplett zu verändern. Ich denke dabei an Geschäftsmodelle wie Benchmarking, Vergütungsberatung, Grading oder das Management von Ressourcen über Job Families, wie wir sie heute kennen. Der Ansatz dürfte aber auch völlig neue Leistungsmöglichkeiten eröffnen und damit auch neue Märkte schaffen. Allein die Automatisierungspotenziale im Bereich des Human Resources Management in Bezug auf Stellenbeschreibungen, Einstufungen oder Rekrutierung dürften beachtlich sein. So man diesen Ansatz zukünftig nutzt, könnte er also viele Beratungsansätze deutlich verändern. So einfach wie der Ansatz im ersten Moment wirkt, so komplex und integriert gedacht sind auf der anderen Seite seine Anwendungsmöglichkeiten. Und damit sein Disruptionspotenzial – unabdingbar für eine Sprunginnovation.

Wo und wie wendet man diese Modellierung an und wie sehen konkrete Use Cases aus?

Im Prinzip müsste es in das breite Feld des Enterprise Resource Planning (ERP) integriert werden und könnte dieses auf den Kopf stellen. Das relationale Datenmodell und auch seine entstehenden Daten in der Anwendung sind einerseits verblüffend einfach konstruiert, andererseits grundlegend und zugleich ergebnisoffen. Sie können somit über ein einfaches Tagging der Datenobjekte Fragestellungen beantworten, die Sie zum Zeitpunkt der Entstehung der Daten noch gar nicht kannten. Beispiel Corona: Welche Aufgaben lassen sich im Home-Office bearbeiten, welche nicht? Und was bedeutet das organisatorisch und in den Kapazitäten?

Aber auch Reorganisationen und Restrukturierungen, strategische Personalplanung, Pricing, Mergers & Acquisitions, Outsourcing-, Offshoring- oder Automatisierungspotenziale sind weitere Use Cases. Die aufgezählten Anwendungsfälle und viele weitere lassen sich sehr einfach abbilden. Zu diesen Fragestellungen des Managements haben wir heutzutage ganz selten überhaupt Daten. Und wenn, sind diese nicht konsistent, recht aufwendig und relativ langsam zu beschaffen sowie oftmals beratungsintensiv – und damit teuer.

Gleichzeitig wird von Führungskräften immer mehr verlangt, eine stetig wachsende Zahl an Entscheidungen in immer kürzeren Abständen rechtssicher und strategisch richtig zu treffen. Ohne saubere Datengrundlage ist dies eigentlich unmöglich. Auf der anderen Seite geht es allen so, dadurch fällt es weniger auf. Der Fisch bemerkt auch nicht, dass er im Wasser schwimmt.

Wie tief greift Herr Krohns Ansatz ins Unternehmen ein?

Die Innovation greift parallel in sehr viele unterschiedliche Mechanismen der Unternehmens-, Arbeits-, Ressourcen-, Prozess- und Organisationssteuerung ein. Allein der Aspekt Compliance wird eine völlig neue Möglichkeit zur Transparenz bei zugleich weniger Aufwand in Organisationen erfahren. Man kann regulatorische Aufgaben außerordentlich präzise den betroffenen Stellen im Unternehmen zuordnen.

Im Übrigen ist der Ansatz durch die strikte Leistungsorientierung auch nicht auf eine Anwendung in Unternehmen begrenzt. Im Grunde lässt sich jede Art von Tätigkeit jedweder Organisation auf diese Weise steuern. Und die Mehrsprachenfähigkeit bei zeitgleicher Eindeutigkeit der Datenobjekte führt zu einem enormen Skalierungspotenzial. Die Objekte in der Datenbank haben einen universellen Charakter und sind somit in jeder Funktion einer Organisation oder eines Unternehmens applizierbar – im Gegensatz zu den doch eher individuellen und wenig kopierbaren Prozessabläufen in Unternehmen. Das macht den Ansatz so charmant und zugleich mächtig – und vielleicht ja auch zur ersten Plattformstrategie aus Deutschland auf dem globalen ERP-Markt.

Herr Grundei, herzlichen Dank für das Gespräch.

Prof. Dr. Jens Grundei
jens.grundei@quadriga.eu

Prof. Dr. Jens Grundei ist Professor für Corporate Governance & Organization an der Quadriga Hochschule Berlin; er forscht und berät im Bereich Organisationseffizienz.

Wir begrüßen unsere neuen Mitglieder

Persönliche Mitglieder

- Rainer Schilling
- Thomas Hoffmann
- Wolfgang Ihde
- Dieter Kasprusch

Firmenmitglieder DOAG

- ADTRAN GmbH, Gunnar Wilsdorf
- GIP Gesellschaft für Innovative Personalwirtschaftssysteme mbH, Andreas Beyg

Termine

September 09

07. - 08.09.2021
Berliner Expertenseminar: Oracle Data Guard mit Christian Pfundtner
Online

09.09.2021
DOAG Dev Talk WebSession: Requirements Engineering für SW-Entwicklung mit Niels de Bruijn
Online

10.09.2021
DOAG Datenbank WebSession: Autoupgrade kann nix dafür mit Ernst Leber
Online

15.09.2021
DOAG Data Analytics WebSession: Data Catalog
Online

16. - 18.09.2021
DOAG 2021 Leitungskräfteforum / Delegiertenversammlung
Bonn

23.09.2021
DOAG Dev Talk WebSession: Forms & APEX? mit Tobias Schweiker
Online

Oktober 10

05. - 06.10.2021
Berliner Expertenseminar: Oracle Datenbank Performance für Entwickler mit Randolf Eberle-Geist
Online

07.10.2021
DOAG Dev Talk WebSession: Objektorientierung in PL/SQL mit Christian Schwitalla
Online

08.10.2021
DOAG Datenbank WebSession
Online

20.10.2021
DOAG Data Analytics WebSession: Stream ETL mit ksql mit Peter Welker
Online

Impressum

Red Stack Magazin inkl. Business News wird gemeinsam herausgegeben von den Oracle-Anwendergruppen DOAG Deutsche ORACLE-Anwendergruppe e.V. (Deutschland, Tempelhofer Weg 64, 12347 Berlin, *www.doag.org*), AOUG Austrian Oracle User Group (Österreich, Lassallestraße 7a, 1020 Wien, *www.aoug.at*) und SOUG Swiss Oracle User Group (Schweiz, Dornacherstraße 192, 4053 Basel, *www.soug.ch*).

Red Stack Magazin inkl. Business News ist das User-Magazin rund um die Produkte der Oracle Corp., USA, im Raum Deutschland, Österreich und Schweiz. Es ist unabhängig von Oracle und vertritt weder direkt noch indirekt deren wirtschaftliche Interessen. Vielmehr vertritt es die Interessen der Anwender an den Themen rund um die Oracle-Produkte, fördert den Wissensaustausch zwischen den Lesern und informiert über neue Produkte und Technologien.

Red Stack Magazin inkl. Business News wird verlegt von der DOAG Dienstleistungen GmbH,Tempelhofer Weg 64, 12347 Berlin, Deutschland, gesetzlich vertreten durch den Geschäftsführer Fried Saacke, deren Unternehmensgegenstand Vereinsmanagement, Veranstaltungsorganisation und Publishing ist.

Die DOAG Deutsche ORACLE-Anwendergruppe e.V. hält 100 Prozent der Stammeinlage der DOAG Dienstleistungen GmbH. Die DOAG Deutsche ORACLE-Anwendergruppe e.V. wird gesetzlich durch den Vorstand vertreten; Vorsitzender: Björn Bröhl. Die DOAG Deutsche ORACLE-Anwendergruppe e.V. informiert kompetent über alle Oracle-Themen, setzt sich für die Interessen der Mitglieder ein und führt einen konstruktiv-kritischen Dialog mit Oracle.

Redaktion:
Sitz: DOAG Dienstleistungen GmbH
(Anschrift s.o.)
ViSdP: Christian Luda
Redaktionsleitung Red Stack Magazin:
Martin Meyer
Redaktionsleitung Business News:
Marcos López
Kontakt: redaktion@doag.org
Weitere Redakteure (in alphabetischer Reihenfolge): Andreas Buckenhofer, Dr. Jörg Domaschka, Markus Flechtner, Prof. Dr. Jens Grunde, Julia Gugel, Dr. Thomas Karle, Wolfgang Klinger, Michael Kloker, Ekaterina Koshkarova, Christian Krohn, Lajos Lange, Florian Lösch, Marco Mischke, Steffen Moser, Thomas Nau, Thomas Petrik, Rainer Schaub, Frank Schneede, Dani Schnider, Sebastian Schreiber, Günther Stürner, Dr. Ulrich Vogel, Simon Volpert

Titel, Gestaltung und Satz:
Alexander Kermas
DOAG Dienstleistungen GmbH
(Anschrift s.o.)

Fotonachweis:
Titel: © ikorch | *www.123rf.com*
S. 11: © maxicam | *www.123rf.com*
S. 12: © gmast3r | *www.123rf.com*
S. 18: © axelbuckert | *www.123rf.com*
S. 21: © mindandi | *www.freepik.com*
S. 29: © artursz | *www.123rf.com*
S. 34: © fullvector | *www.freepik.com*
S. 40: © ThMilherou | *www.pixabay.com*
S. 47: © tashatuvango | *www.123rf.com*
S. 57: © archjoe | *www.freepik.com*
S. 64: © lzflzf | *www.123rf.com*
Titel S. 74: © chesky | *http://stock.adobe.com*
S. 78: © stories | *www.freepik.com*
S. 83: © sifotography | *www.123rf.com*
S. 88: © Panithan | *http://stock.adobe.com*
S. 93: © wrightstudio | *www.123rf.com*
S. 98: © upklyak | *www.freepik.com*
S. 101: © gmast3r | *www.123rf.com*

Anzeigen:
sponsoring@doag.org

Mediadaten und Preise:
www.doag.org/go/mediadaten

Druck:
WIRmachenDRUCK GmbH,
www.wir-machen-druck.de

Inserentenverzeichnis

BERLINER EXPERTENSEMINARE

DOAG

Die Berliner Expertenseminare sind seit über zehn Jahren eine feste Institution im Veranstaltungsangebot der DOAG. An jeweils zwei Tagen vermitteln unsere Experten geballtes Fachwissen inklusive praxisnaher Übungen zu einem bestimmten Themenbereich.

Oracle Data Guard

7. + 8. SEPTEMBER 2021

In diesem Expertenseminar für DBAs widmet sich Christian Pfundtner, Oracle ACE und Oracle Certified Master, der High-Availability-Lösung Oracle Data Guard. Erfahren Sie, wie Sie damit eine aktuelle Kopie Ihrer Datenbank erstellen, auf die Sie dann bei Bedarf umschalten können.

CHRISTIAN PFUNDTNER

www.doag.org/go/expsem_pfundtner

Oracle Datenbank Performance für Entwickler

5. + 6. OKTOBER 2021

Randolf Eberle-Geist ist einer der internationalen Top-Experten im Bereich der Oracle-Optimizer-Technologie und der SQL-Performance-Analyse. In diesem Expertenseminar zeigt er Ihnen, wie Sie als Entwickler die maximale Performance aus der Datenbank holen.

RANDOLF EBERLE-GEIST

www.doag.org/go/expsem_eberle-geist