www.ordix.de € 3,20

1|2018

ORDIX® news

einfach. besser. informiert.

Exadata: Das Flaggschiff von Oracle

SIND SIE STARTKLAR FÜR IHRE ZUKUNFT?

WIR GEBEN IHRER ENTWICKLUNG AUFTRIEB

NEUGIERIG?

Als neuem Mitarbeiter bieten wir Ihnen ein speziell auf Sie zugeschnittenes Start- und Entwicklungsprogramm. Die Themen Weiterbildung und Weiterentwicklung sind ein wesentlicher Teil unserer Unternehmensphilosophie.

STUDENTEN

Wir bieten in Kooperation mit unseren Partner-Fachhochschulen duale Studiengänge für die Standorte Paderborn, Wiesbaden, Köln und Gersthofen an.

Zum Beispiel:

Bachelor of Science
in Wirtschaftsinformatik

Im regelmäßigen Wechsel von Theorie und Praxis steht die Konzeption, das Design und die Entwicklung von modernen Anwendungen im Vordergrund.

BERUFSEINSTEIGER

Wir bieten Ihnen die Möglichkeit, sich in unserem Unternehmen zu entwickeln und ermöglichen Ihnen den optimalen Karrierestart.

Zum Beispiel:

Junior Software-Entwickler – Java

An unseren ORDIX-Standorten arbeiten Sie mit modernen und innovativen Technologien und unterstützen unsere Experten in der Entwicklung von komplexen Applikationen.

BERUFSERFAHRENE

Sie suchen eine neue berufliche Herausforderung? Auf Sie warten spannende und anspruchsvolle IT-Projekte.

Zum Beispiel:

IT-Projektmanager

Die Planung, Organisation und Steuerung interessanter IT-Projekte bei unseren renommierten Kunden stehen im Fokus Ihres Aufgabenfeldes.

Weitere Informationen und Jobangebote finden Sie auf unseren Karriereseiten im Internet.

kununu TOP COMPANY www.kununu.com VON MITARBEITERN EMPFOHLEN!

www.ordix.de/karriere
www.xing.com/companies/ordixag/jobs

Paderborn, Juli 2018

Deutschland 0:2

Eigentlich wollte ich die Überschrift nur 0:1 nennen, weil sie ursprünglich nichts mit der katastrophalen Leistung der deutschen Fußballer zu tun hatte. Jetzt, nachdem gerade das WM-Aus besiegelt ist, habe ich sie auf 0:2 geändert.

Mir ging es mit dieser Überschrift aber mehr um zwei andere Themen, die zurzeit die Schlagzeilen beherrschen: Handelskrieg und DSGVO. Verlierer ist in beiden Fällen Deutschland. Durch die DSGVO verlieren – ähnlich wie bei vielen anderen Gesetzen der letzten Jahre auch – in erster Linie die, die die Umsetzung ernst nehmen und ihr Geschäft in Europa betreiben, nicht aber die, die man eigentlich damit treffen wollte (Google, Facebook …).

Der Handelskrieg, den die USA oder eigentlich nur die Trump-Verwaltung angezettelt haben, wirkt sich natürlich vor allem auf exportorientierte Länder wie uns aus. Und auch wenn man in den USA feststellt, dass die Maßnahmen mittelfristig nur schaden – man wird weitermachen mit nicht nachvollziehbaren Entscheidungen (so erste Reaktionen auf Ankündigungen bei Harley-Davidson).

Aber schon in der Vergangenheit haben die USA durch verkorkste Wirtschaftspolitik (leider bestes Beispiel die Bankenkrise von 2008/2009) erheblichen Schaden angerichtet. Wir hier in Europa sollten uns deshalb einfach etwas von den übermächtigen USA abkoppeln. Wir sind nicht gezwungen, alles mitzumachen, was der große Zampano meint vorgeben zu müssen. Es wird Zeit, dass das auch unsere Politiker lernen zu verstehen.

„EUROPE FIRST“

Ich versuche schon, seitdem die Amerikaner französischen Wein boykottierten, weil u.a. Frankreich nicht in den Irak Krieg eingetreten ist, amerikanische Produkte wann immer möglich zu vermeiden. Auch wenn dies nur eine kleine Maßnahme zugunsten „Europa zuerst“ ist, wenn viele mitmachen und nicht jeden Unfug aus Amerika blind übernehmen, hilft es uns Europäern sehr (wegen „Europa zuerst“ muss ich aufpassen, dass mir unser Marketing nicht eine Trump Tolle verpasst).

Gerade in der IT-Welt sind wir immer noch voll von den USA abhängig, was sich „leider“ auch in unserer Artikelauswahl bemerkbar macht. Nichtsdestotrotz haben wir auch dieses Mal interessante Themen aufgearbeitet und präsentieren Ihnen mit einem Gastartikel neues von der blauen Datenbank sowie zwei Beiträge zu den Premium Produkten der roten Datenbank.

Bei allem Heckmeck um 5 Buchstaben mussten wir natürlich auch was zum Thema (IT-)Security schreiben, allerdings geht es hierbei weniger um die DSGVO. Während es bei Security eher um das „Verstecken“ von Daten geht, geht es bei unserem Artikel über verteilte Dateisysteme unter Linux eher um den schnellen und überall verfügbaren Zugriff auf Daten. Im mittlerweile achten Teil unserer Reihe über Big Data geht es wieder um Security – einer häufig gestellten Frage beim Einsatz dieser Technologien.

Ausnahmsweise haben wir aus dem Entwicklungsumfeld in dieser News-Ausgabe nur etwas zu „altmodischen“ Methoden beim Einsatz von Python. Eine ganz andere Baustelle ist unsere Partnerschaft mit Tegile – wie Sie Speicherkapazitäten einsparen können lesen Sie in einem interessanten Artikel über Komprimierung und Deduplizierung.

Last not least bringen wir mal wieder etwas von Microsoft (auch und immer noch amerikanisch): Wir starten eine Reihe über SharePoint und beginnen mit dem Zusammenspiel mit Office 365. Sicherlich auch für langjährige Leser der News etwas unerwartet, aber durchaus interessant.

Für Ihren Sommerurlaub empfehle ich allen Bürgern der 15 Bundesländer ungleich Bayern, sich sehr gut zu überlegen, ob sie die bayerischen Grenzen überschreiten wollen – nicht dass sie etwa an der Grenze abgewiesen werden. Selbst als Vorstand eines Automobilkonzerns besteht mittlerweile kein Schutz mehr in Bayern und Sie können sogar im Knast landen, wenn Ihre Abgaswerte nicht mehr passen.

Herzlichst Ihr

Wolfgang Kögler

PS: Eigentlich würde mir ein Macron besser stehen. *ORDIX News en marche!*

Quo vadis 2018, CISO?

Exadata: Das Flaggschiff von Oracle?

IT-Security

Betriebssysteme

IBM Datenbanksysteme

Big Data

Oracle

Microsoft

Microsoft SharePoint

OpenVAS

Entwicklung

Storage

Aktuell

Impressum

Herausgeber:	ORDIX AG Aktiengesellschaft für Softwareentwicklung, Beratung, Schulung und Systemintegration, Paderborn
Redaktion/Layout:	Jens Pothmann, Isabell Rosenblatt
V.i.S.d.P.:	Christoph Lafeld, Wolfgang Kögler
Anschrift der Redaktion:	ORDIX AG | Karl-Schurz-Straße 19a | 33100 Paderborn Tel.: 0 52 51 10 63 -0 | Fax: 0180 1673490
Auflage:	7.000 Exemplare
Druck:	Druckerei Bösmann, Detmold
Bildnachweis:	© pexels.com © pixabay.com © istockphoto.com | sturti | Feststecken im Büro © istockphoto.com | RomoloTavani | Nein zur Gewalt...
Autoren:	Manu Carus, Marius Dorlöchter, Thilo Fleischhauer, Michael Hafner, Stefan Hummel, Jan Benedikt Kardinal, Wolfgang Kögler, Patrick Kramer, Nils von Nethen, Isabell Rosenblatt, Adi Schmidt, Michael Skowasch,
Copyright:	Alle Eigentums- und Nachdruckrechte, auch die der Übersetzung, der Vervielfältigung der Artikel oder von Teilen daraus, sind nur mit schriftlicher Zustimmung der ORDIX AG gestattet.
Warenzeichen:	Einige der aufgeführten Bezeichnungen sind eingetragene Warenzeichen ihrer jeweiligen Inhaber. ORDIX® ist eine registrierte Marke der ORDIX AG.
Haftung:	Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden.

Sie können die Zusendung der ORDIX® news jederzeit ohne Angabe von Gründen schriftlich (z.B. Brief, Fax, E-Mail) abbestellen.

Sicherheitsvorfälle, und was wir in der Zukunft für uns ableiten können

Quo vadis 2018, CISO?

In den letzten Jahren wurden einige Sicherheitsvorfälle bekannt, die für die Zukunft der Informationssicherheit wegweisend sind. Wie können wir diesen neuen Gefahren wirksam begegnen? Dieser Artikel gibt einen kurzen Einblick in aktuelle Incidents, Mitigationsmaßnahmen und den Status quo bei deutschen Unternehmen.

Sicherheitsvorfälle

Incidents sind mitunter die wertvollste Wissensquelle in der Informationssicherheit. Wann immer „irgendwo da draußen" ein Sicherheitsvorfall bekannt wird und es gelingt, die Hintergründe zu analysieren und aufzudecken, besteht die Möglichkeit, das eigene Unternehmen weiterzuentwickeln, zu rüsten und vor künftigen Angriffen zu schützen. Vorausgesetzt, man versteht die Natur eines Angriffs und weiß einzuschätzen, welche Mitigationsmaßnahmen wirksam sind.

Viele Kriminelle sind unseren Sicherheitsexperten in ihrem technologischen Know-how weit überlegen, gehen arbeitsteilig vor, agieren international, bleiben unerkannt und bewegen Millionen US-Dollar in haarsträubender Geschwindigkeit zwischen verschiedenen Jurisdiktionen.

Die Aufgabe des Informationssicherheitsbeauftragten (ISO, CISO) besteht darin, das Unternehmen, seine Mitarbeiter und Vermögenswerte zu schützen, Gefahren abzuwenden und ein unvorhergesehenes Ereignis schnellstmöglich unter Kontrolle zu bringen, um entstehenden Schaden eindämmen und den unterbrochenen Betrieb schnellstmöglich in gewohnter Qualität weiterführen zu können. Dazu bedarf es präventiver, detektiver und korrigierender Maßnahmen.

Citadel

Der Online-Banking-Trojaner „Zeus" hatte 2012 eine Variante namens „Citadel" abgeworfen, mit der Kriminelle innerhalb von wenigen Stunden einen Gesamtschaden von einer halben Milliarde US-Dollar angerichtet haben. Dieser Vorfall dient in der Security-Branche als Referenz, um deutlich zu machen, welche Maßnahmen umgesetzt werden müssen, um sich vor üblichen Programmierfehlern und kreativer Energie zu schützen (siehe Abbildung 1).

Ein Cyber-Kriminellen bestellt im Darknet eine Malware für 800 USD und lässt sich diese Software von dem Malware-Autor auf die URLs der 25 größten US-Banken zuschneiden.

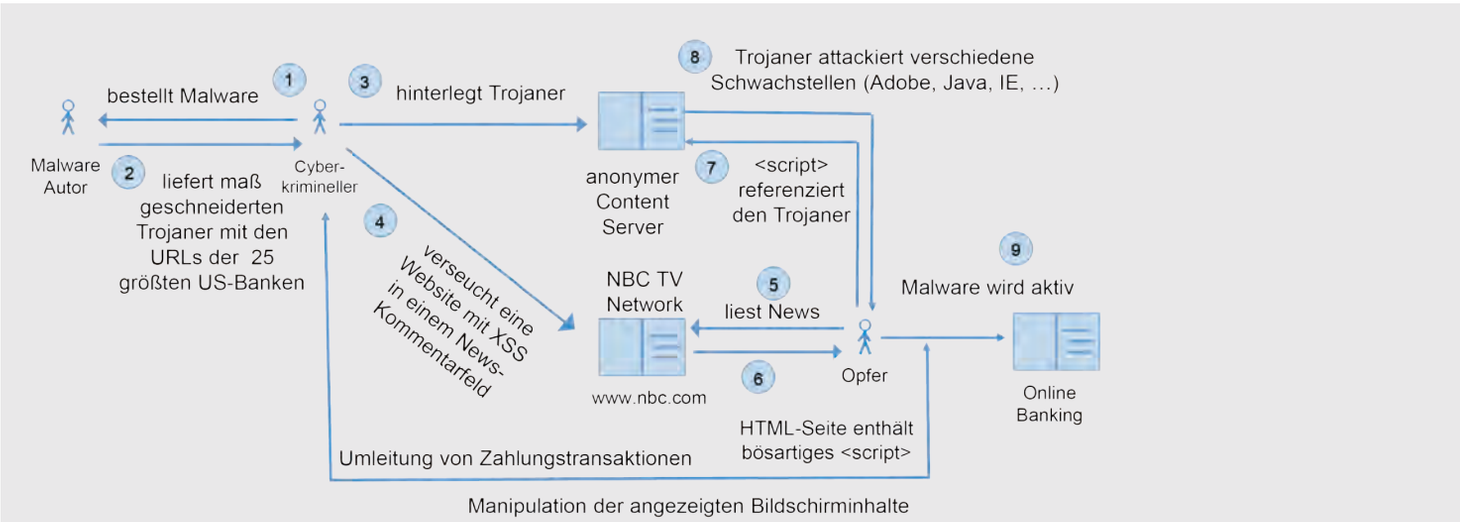

Abb. 1: Funktionsweise des OnlineBanking-Trojaners Citadel (2012)

Der Cyber-Kriminelle hinterlegt den Trojaner auf einem anonymen Content-Server und verseucht anschließend eine häufig frequentierte Website - in diesem Fall die Nachrichtenseite www.nbc.com des amerikanischen NBC TV-Networks, die zu diesem Zeitpunkt anfällig für ein Cross-Site-Scripting (XSS) ist. Ein Angreifer kann also ohne Wissen der NBC ein Kommentarfeld unter den News-Artikeln mit bösartigem JavaScript versehen.

Ein unbedarfter User liest die Nachrichten der NBC auf seinem Browser. Neben Titel, Texten, Fotos und Videos werden ihm eben auch die Kommentare anderer User unter dem Artikel angezeigt, darunter auch der Kommentar des Angreifers. Da das Kommentarfeld aufgrund einer trivialen Sicherheitslücke mit Scripting-Code verseucht wurde, kann das Opfer die Code-Ausführung nicht bemerken. Statt einen Kommentartext anzuzeigen, führt der Browser den vom Angreifer injizierten JavaScript-Code aus, welcher den Online-Banking-Trojaner von dem anonymen Content-Server herunterlädt (Drive-by-Download) und anschließend versucht, verschiedene Sicherheitslücken auf dem Windows-Rechner des Users auszunutzen: Adobe Reader, Java, Internet Explorer, die Liste ist lang. Falls der Rechner anfällig ist, wird der Trojaner installiert, aber erst aktiv, wenn der User über den Browser ins Online-Banking einsteigt. Dann nämlich zweigt der Trojaner die Überweisungen ab und überführt entsprechend große Beträge auf ein internationales Konto des Cyber-Kriminellen.

Ohne weiter auf die Details einzugehen: Die NBC war für ca. 5 Stunden infiziert. In dieser Zeit wurden 80.000 Anwender-PCs von dem Trojaner befallen. Da es der Cyber-Kriminelle aber nicht auf gewöhnliche User abgesehen hatte, sondern auf Firmenmitarbeiter, die in der Buchhaltung oder Rechnungsstelle eines Unternehmens arbeiten, konnten aufgrund der hohen Banklimits insgesamt über 28 Mio. USD umgeleitet werden.

Die Frage, die sich für einen Informationssicherheitsbeauftragten in einem Unternehmen stellt, lautet: Warum hätte dieser Angriff niemals so erfolgreich sein dürfen?

Bei der Analyse stellte sich zunächst heraus, dass die Windows-Rechner der betroffenen User nicht ausreichend gepatcht waren. Die betroffenen Sicherheitslücken waren seit über einem Jahr bekannt und waren nicht behoben worden. Des Weiteren surften die Mitarbeiter ohne technologischen Schutz: es wurden keine Web Application Firewall (WAF) eingesetzt, um vor XSS und SQL Injections zu schützen. Die Mitarbeiter nutzten zudem keinen isolierten Rechner für das Online-Banking, sondern vermischten öffentlichen mit sensiblem Traffic. Eine entsprechende Policy gab es nicht.

Demzufolge gehören Patch Management, physische und logische Segregierung von Netzwerken, Anwendungen und Prozessschritten, Web Security Gateways und strikte Governance-Maßnahmen heute zum Mindestrüstzeug in der Informationssicherheit. Dennoch funktionieren Cybercrime-Märkte auch heute noch wie beschrieben. Erst vor wenigen Monaten konnte Alphabay geschlossen werden, ein Darkmarket mit 40.000 Anbietern von Malware, Drogen, Waffen und gefälschten Ausweisen für über 200.000 Nutzer. Die Anbieter sind seitdem unerkannt auf andere Märkte umgezogen.

Mirai

2016 hatte ein namhafter Security-Experte, Brian Krebs, etwas zu tief im Darknet gegraben und mit den Veröffentlichungen auf seinem Blog [1] einige Player am Markt wohl gründlich verärgert. Es folgte eine einmalige Macht-Demonstration (siehe Abbildung 2). Kreb's Blog wurde über einen Distributed Denial of Service (DDoS) Angriff lahmgelegt, indem seine Server mit einer Wucht von

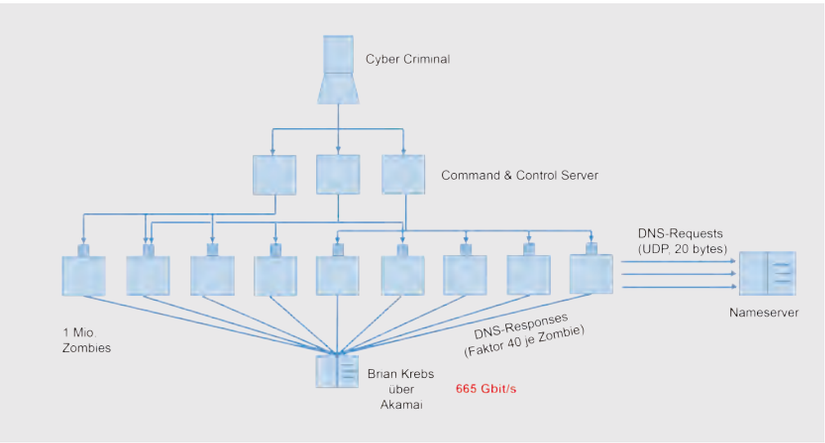

Abb. 2: Distributed Denial of Service Angriff

665 Gbit/s beschossen wurden. Gängige Switches und Router arbeiten mit einem Bruchteil dieser Durchsatzrate.

Die nachfolgende Analyse zeigte, dass die angreifenden Geräte gar keine kompromittierten Server waren, sondern eine Masse von Internet-of-Things-(IoT)-Geräten, die Cyberkriminelle mithilfe von Standard-Passwörtern und einfachsten Sicherheitslücken unter ihre Kontrolle gebracht haben: Webcams, Aufzeichnungsgeräte, Kameraüberwachungssysteme in Firmen. Mini-Computer, die ans Internet angeschlossen sind und wie vollwertige Linux-Rechner funktionieren. Mit einem Unterschied: die meisten dieser Geräte stammen von Billigherstellern, die eine Aktualisierung der Firmware gar nicht erst vorgesehen haben. Einmal kompromittiert, ist das Gerät nicht mehr brauchbar. Nur sehen es so die Kunden nicht. Anstatt die Geräte auszutauschen und gegen hochwertige, patch-bare Systeme auszutauschen, bleiben letzterer in gewohnter Weise konnektiert: anfällig, unter Fremdkontrolle und jederzeit einsatzbereit.

DDoS-Angriffe sind an sich nichts Neues, nur die Wucht dieser neuen Angriffe hat das Potenzial, sogar Großunternehmen vom Netz zu nehmen. Der Blog von Brian Krebs wurde von Akamai gehostet, einem der größten Telekommunikationsunternehmen der Welt. Und selbst diese Firma hätte den Angriff nur unter enormem Einsatz von Geld und Gerätschaft ableiten können.

In diesem Sinne besteht die Verantwortung eines Informationssicherheitsbeauftragten auch über die eingesetzte Technologie hinaus, Einkaufsprozesse zu hinterfragen und Vorgaben für den Einsatz von zertifizierten Geräten im Unternehmen zu schaffen - um zu verhindern, dass eigene Geräte fremdkontrolliert werden und das Unternehmen zum Mittäter wird.

Information Security Management

Die vorliegenden Beispiele sind nur wenige von vielen. Im letzten Jahr hat Ransomware die Runde gemacht. Wegen „WannaCry“ mussten englische Krankenhäuser Lösegeld zahlen und auf den Anzeigetafeln der Deutschen Bahn waren Statements gesetzt. Erst diesen Monat musste ein US-Krankenhaus 60.000 Dollar Lösegeld zahlen ([2]) - es verfügte zwar über Backups, sah sich aber außerstande, diese zeitnah einzuspielen.

Wer Informationssicherheit im Unternehmen steuert, weiß um die Vielfalt der abzudeckenden Themen:

- Information Security Management
- Risk Management
- Asset Security
- Security Engineering
- Kryptographie
- Physische Sicherheit
- Netzwerkkommunikation
- Identity Management und Zugangskontrollen
- Web-Applikationen
- Sichere Software-Entwicklung
- Betrieb und Wartung
- Business Continuity
- Disaster Recovery

Informationssicherheit umfasst die kritischen Erfolgsfaktoren „Management“, „Technologie“ und „physische Sicherheit“ und muss demnach alle Geschäftssäulen gleichermaßen erfassen, alle kritischen Prozesse und daran beteiligten Menschen, Software, Hardware, Netze, Gebäudetechnik und den Betriebsstandort insgesamt.

Eine Herkulesaufgabe, die nur in Kooperation mit allen Business Units gelingen kann. Wie meistern deutsche Unternehmen das?

Lagebericht und Studien

Erst im Herbst 2017 wurden Studien veröffentlicht, die einen interessanten Einblick in die aktuelle Situation bei deutschen Unternehmen ermöglichen:

- Laut Gothaer KMU Studie 2017 [3] haben 20 % der KMUs in Deutschland nicht einmal einen Antivirenschutz im Einsatz. 25 % der KMUs sind ohne Firewall, 33 % fahren keine Backups, und 51 % arbeiten ohne Notfallplan.
- Laut Digitalverband Bitkom 09/2017 [4] ist nicht einmal die Hälfte der (befragten) Unternehmen in Deutschland ausreichend auf einen Cyberangriff vorbereitet. Nur vier von zehn Firmen haben ein Notfallmanagement. Und gerade einmal die Hälfte der Betreiber von kritischen Infrastrukturen haben einen Notfallplan!

Diese Aussagen sind repräsentativ für kleine und mittelständische Unternehmen (KMUs). Es verwundert demnach nicht, warum Ransomware im Darknet so erfolgreich gehandelt wird. Denn ohne Daten, ohne funktionsfähigen Betrieb sind diese Unternehmen tot.

Großunternehmen rüsten sich seit Jahren schon gegen Cyberangriffe und stocken ihre Security-Teams auf. Laut Global Information Security Workforce Study 2017 (GISWS) [5] planen 66 % der Unternehmen in Deutschland,

Österreich und der Schweiz (DACH), ihr Security-Personal in den nächsten 12 Monaten aufzustocken, um teilweise 10 % und mehr Mitarbeiter. Leider kann dieser Bedarf am Markt nicht gedeckt werden. Laut Studie ist es aktuell sehr schwierig, ausreichend qualifizierte Mitarbeiter zu finden. Daher werden Arbeitgeber in die Entwicklung ihres eigenen Personals investieren und Bereitschaft zeigen müssen, weniger erfahrene Kandidaten einzustellen und in Eigenregie auszubilden.

Qualifikation, Training und Zertifikate

Die GISWS stellt sogar einen Mangel von 350.000 Cyber-Sicherheitsexperten in DACH bis 2022 fest.

Um diesen Herausforderungen zu begegnen, hat die ManufakturIT GmbH, ein langjährig bewährtes Security-Beratungsunternehmen in der Region Köln, einen eigenen Trainingsbereich etabliert. Praxiserfahrene Manager und Berater bilden im Schulterschluss mit der ORDIX AG IT-Experten in allen wichtigen Gebieten der Informationssicherheit aus und zertifizieren mit internationaler Anerkennung zum

- Certified Information Systems Security Professional (CISSP) [6]
- Certified Information Security Manager (CISM) [6]
- Certified Information Systems Auditor (CISA) [6]

Absolventen erhalten eine objektive Zertifizierung ihres Wissens auf dem Gebiet der Informationssicherheit, die zunehmend in Deutschland, in Österreich und in der Schweiz nachgefragt und eingefordert wird und ein hohes Ansehen genießt.

Neue Herausforderungen

Die in der Gesellschaft zunehmende Digitalisierung (Stichwort: Industrie 4.0) erfasst die Produktionsprozesse in den Fabriken. Angriffe auf Infrastrukturen werden zunehmen. Für Cyber-Kriminelle wird es ertragreicher, Produktionsabläufe zum Erliegen zu bringen und Lösegelder zu erpressen. Ransomware wird ihren Weg von den Büros in die Fabriken finden.

Immer mehr Alltagsgegenstände werden vernetzt. Intelligente Zähler (sogenannte Smart Meter), Rauchmelder, Türschlösser, Lautsprecher, Kinderspielzeuge kommunizieren miteinander und über die Kommunikationsplattformen der Hersteller. Das sog. Internet of Things (IoT) wird wachsen, und es werden Firmen in die vernetzte Welt drängen, die nicht originär aus der IT kommen und für die das Thema Informationssicherheit nicht wichtig oder auch nicht wirtschaftlich genug ist. Der „Risk Appetite“ dieser Hersteller wird die Angriffsoberfläche unserer Alltagsgegenstände bestimmen.

Autonomes Fahren wird nur durch Sensoren ermöglicht, die miteinander kommunizieren. Die meisten der dabei eingesetzten Protokolle unterstützen keine (oder schwache) Authentisierung und Verschlüsselung. Car Hacking entsteht als Spielfeld für Hacker, Forscher und Neugierige.

Und last but not least verspricht die Blockchain neue Anwendungsmöglichkeiten – dezentrale Intelligenzen, die bestimmen, ob eine Transaktion zustande kommen darf. Anonyme Währungen wie Bitcoin zeigen gerade in diesen Tagen auf dramatische Weise die Chancen (Kurssteigerungen) und Gefahren (Kursverluste) neuer Technologien.

Nur wer im Kern versteht, wie Technik funktioniert, wie Prozesse abgewickelt werden, welche Annahmen dabei getroffen werden und welche Interessen die Player am Markt verfolgen, wird ein erfolgreiches Informationssicherheits-Management betreiben können.

Der Schlüssel zum Gelingen liegt im Wissen und in der Anwendung von Wissen, in Qualifikation und in Trainings.

Manu Carus
(info@manufaktur-it-training.de)

Ihr Referent ist „Official (ISC)² Training Instructor“ und als solcher ein von der (ISC)² autorisierter Partner für deutschsprachige Trainings in Deutschland, Österreich und der Schweiz.

Links/Quellen

[1] Blog von Brian Krebs
https://krebsonsecurity.com/

[2] Golem - IT-News für Profis
https://www.golem.de/news/ransomware-krankenhaus-zahlte-60-000-us-dollar-trotz-backups-1801-132206.html

[3] KMU Studie der Gothaer Versicherung
https://www.gothaer.de/ueber-uns/presse/publikationen/studien/kmu-studie-2018.htm

[4] Branchenverband Bitkom e.V.
https://www.bitkom.org/Presse/Presseinformation/Nur-vier-von-zehn-Unternehmen-sind-auf-Cyberangriffe-vorbereitet.html

[5] GISWS Study 2017
https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

[6] ORDIX IT-Security Seminare:
https://seminare.ordix.de/seminare/it-security.html

Bildnachweis

Eine Übersicht der wichtigsten Systeme unter Linux

Verteilte Dateisysteme unter Linux

Wofür braucht man verteilte Dateisysteme? In Zeiten von Big Data, Cloud Computing und High Performance Clustern können Daten nicht mehr lokal auf einzelnen Systemen gespeichert werden. Die Daten müssen jederzeit auf allen Systemen zur Verfügung stehen und dort auch von allen Systemen bearbeitet werden können. Aus Gründen der Ausfallsicherheit und vor allem der Performance und des parallelen Zugriffs reicht auch ein einfacher Netzwerkspeicher wie z.B. NFS bei Weitem nicht aus. Also verwendet man verteilte bzw. parallele Dateisysteme. Vereinfacht gesagt kann man sich verteilte Dateisysteme wie einen RAID-Verbund im Netzwerk vorstellen. Die Daten werden dabei zwischen den einzelnen Servern verteilt und redundant gespeichert. Verschiedene Mechanismen sorgen dafür, dass die Daten jederzeit konsistent und redundant sind. Aufgrund der Verteilung steigt auch die Performance und je nach Skalierbarkeit der verschiedenen Implementierung können hier I/O-Bandbreiten von mehreren Gigabyte/s erreicht werden.

In der Linux-Welt existieren verschiedene Implementierungen verteilter Dateisysteme, die entweder nativ für und unter Linux entwickelt wurden oder von anderen Plattformen portiert wurden. Die wichtigsten und am häufigsten eingesetzten werden im Folgenden kurz vorgestellt.

Das unter der freien Lizenz LGPL lizensierte Dateisystem Ceph wurde im Zuge einer Doktorarbeit entwickelt und ist seit März 2010 Bestandteil des Linux-Kernels (ab 2.6.34). Der Fokus liegt hier auf Hochverfügbarkeit und hoher Skalierung bis zu mehreren Petabytes. Nutz- und Metadaten können über mehrere Server repliziert werden. Kernkomponente von Ceph ist der Datenspeicher RADOS mit dem Crush-Algorithmus, der die Aufteilung und Verteilung der angelieferten Daten steuert.

Der RADOS-Speicher kann auf den Verbund-Systemen als Block-Device angesprochen werden, was hohe Performance und einfache Administration verspricht. Alternativ kann auch über CephFS, ein POSIX-kompatibles Dateisystem auf den RADOS-Speicher zugegriffen werden. Da der CephFS-Client Bestandteil des Linux-Kernels ist, liegt auch hier im Vergleich zu einer FUSE-Anbindung höhere Performance vor.

GlusterFS wurde 2006 von der Firma Z Research Inc. erstmalig veröffentlicht und steht unter der freien Lizenz GPL v3. 2011 wurde GlusterFS von RedHat gekauft. Die Anbindung im System wird über FUSE realisiert, ein dediziertes Kernel-Modul ist nicht nötig. Vergleichbar ist das Ganze mit einem RAID-Verbund, nur dass die Daten hier nicht lokal, sondern über mehrere Server im Netzwerk verteilt über TCP/IP oder Infiniband verteilt gespeichert werden. GlusterFS ist beliebig skalierbar, mit jedem weiteren Server im Verbund erhöht sich der Datendurchsatz im Dateisystem. Der Aufbau ist modular und bietet diverse Betriebsmodi. Hier die wichtigsten:

- **Standalone Storage**
  Hier stellt ein einzelner Server das FS im Netz bereit, die Funktion entspricht der eines NFS-Servers.
- **Striped Storage**
  Die Daten werden zwischen mehreren Servern gestriped.
- **Replicated Storage**
  Die Daten werden zwischen mehreren Servern gespiegelt.
- **Distributed Storage**
  Die Daten werden auf mehrere Server verteilt.
- **Distributed Replicated Storage**
  Hier werden die Daten verteilt und gespiegelt.

Aufgrund des verteilten Speicherns von Nutz- und Metadaten ist GlusterFS fehlertolerant und Daten können jederzeit auf allen beteiligten Systemen parallel gelesen und geschrieben werden. Im Vergleich zu anderen Implementierungen wird hier auf dedizierte Metadatenserver verzichtet, was eine bessere Skalierbarkeit verspricht. Durch die Anbindung ins System über FUSE ist die Performance im Vergleich zu anderen verteilten Dateisystemen, die direkt mit dem Kernel kommunizieren können, geringer, es eignet sich eher für kleinere Umgebungen, die mehr Wert auf Hochverfügbarkeit als auf Performance legen.

lustre File System

Lustre (Linux Cluster) ist ein hoch performantes und skalierbares parallel verteiltes Dateisystem, das hauptsächlich in großen Cluster-Umgebungen sowie im Umfeld von Supercomputern eingesetzt wird. Entwickelt wird Lustre seit 2003, ursprünglich als Forschungsprojekt an der Carnegie Mellon Universität, zwischenzeitlig von Sun und Oracle und inzwischen von der Firma Xyratex Ltd. Es steht unter der freien Lizenz GPL v2. Lustre setzt auf einen objektbasierten Storage-Ansatz mit eigenen Instanzen für Metadaten (Meta Data Server) und Nutzdaten (Object Storage Server) und einem Management-Server zur Verwaltung des Dateisystems. Dazu kommt noch die Lustre-Network-Komponente, die die Schnittstelle zwischen Meta Data Server und Object Storage Server darstellt. Die Server werden dabei häufig als Failover-Cluster realisiert. Dies ist aus Gründen der Ausfallsicherheit vor allem beim Meta DataServer wichtig, da Lustre von sich aus nur einen MDS pro Verbund vorsieht. Lustre ist das am häufigsten eingesetzte Dateisystem in der Top500 der Supercomputer, was für seine Stabilität und Performance spricht. Für kleinere Umgebungen ist es aufgrund seiner Komplexität eher weniger geeignet.

IBM GPFS

GPFS (General Parallel File System) wurde 1998 von IBM offiziell vorgestellt und entstand aus diversen IBM-Forschungsprojekten zu parallelen Dateisystemen aus der Supercomputer-Welt. Ursprünglich für AIX eingeführt, existiert seit 2001 eine Linux-Implementierung, seit 2008 wird auch Windows unterstützt. 2015 wurde GPFS von IBM in IBM Spectrum Scale umbenannt. Da sich der Name "GPFS" aber über Jahre im Administrator-Wortschatz gefestigt hat, wird das Produkt auch hier weiter als GPFS bezeichnet. Im Gegensatz zu den bisher genannten Lösungen wird GPFS von IBM unter einer proprietären Lizenz vermarktet. Aufgrund der hohen Lizenzkosten ist GPFS unter Linux deshalb nur im kommerziellen Umfeld anzutreffen, hat aber aufgrund des Supports durch IBM und der bewährten Leistung hier durchaus seine Daseinsberechtigung. Eine Besonderheit von GPFS ist die hohe Skalierbarkeit und Ausfallsicherheit im GPFS-Cluster. So können z.B. jederzeit im laufenden Betrieb Server zum GPFS-Cluster hinzugefügt oder entfernt werden. Volumes lassen sich von sehr vielen Clients parallel lesend und schreibend mounten, die Steuerung übernehmen verteilte Lock-Manager. Durch Striping lassen sich sehr hohe Durchsatzraten erzielen, wozu auch die Speicherung von Daten und Metadaten auf unterschiedlichen Datenträgern zählt. Zur einfacheren Administration beinhalten neuere GPFS-Versionen auch eine auf Java basierte GUI (IBM Spectrum Scale management GUI), es können aber natürlich auch weiterhin alle Administrationstasks in der Kommandozeile ausgeführt werden.

Michael Hafner
(info@ordix.de)

Quellen

[1] Linux Magazin: Holger Gantikow -
Leistungsfähige parallele Dateisysteme unter Linux
http://www.linux-magazin.de/ausgaben/2012/06/leistungsfaehige-parallele-dateisysteme-unter-linux/

[2] Linux Magazin: Udo Seidel - Newcomer: Ceph und Gluster-FS
http://www.linux-magazin.de/ausgaben/2013/02/ceph-und-gluster/5/

[3] Linux Magazin: Udo Seidel -
Verteilte Dateisysteme unter Linux im Vergleich
http://www.linux-magazin.de/ausgaben/2013/02/dateisystem-ueberblick/

[4] Erklärung Ceph-Software
https://en.wikipedia.org/wiki/Ceph_(software)

[5] Erklärung Gluster-Software
https://en.wikipedia.org/wiki/Gluster

[6] Erklärung Lustre file system
https://en.wikipedia.org/wiki/Lustre_(file_system)

[7] Erklärung IBM General Parallel File System
https://en.wikipedia.org/wiki/IBM_General_Parallel_File_System

Mit der Datenbank durch die Zeit reisen (Teil II)

Die Datenverwaltung mit Business Time

Mit Business Time lässt sich nachverfolgen, wann bestimmte Geschäftsvorfälle gültig waren, gültig sind oder gültig sein werden. Beispiel: Ein Produkt kostet normalerweise 45 Euro, jedoch während einem Aktionszeitraum von ein Monat nur 39 Euro. Oder auf einen Kredit sind in einem Jahr sechs Prozent und im nächsten Jahr acht Prozent Zinsen zahlbar. Für solche Problemstellungen ist das Konzept Business Time vorgesehen, das die einfache Darstellung von Gültigkeitszeiten ermöglicht.

Wie bei der Bearbeitungszeit ist auch für die Gültigkeitszeit (Business Time) die Angabe einer Periode erforderlich (die Start- und Endzeiten der Gültigkeit). Anders als das Konzept System Time wird für Business Time keine separate History-Tabelle benötigt. Frühere, aktuelle und künftige Gültigkeitszeiten und die zugehörigen Geschäftsdaten werden alle in einer einzigen Tabelle verwaltet. Darüber hinaus ist es der Benutzer, der die Start-/Endwerte für die Business-Time-Spalten bei der Dateneingabe festlegt. Weiterhin wird auch für die Transaktionsstartzeit keine Spalte benötigt.

Erzeugen einer Tabelle mit Business Time

Um eine Tabelle mit Business Time zu erzeugen, sind Spalten für die Start-/Endzeitpunkte des Gültigkeitszeitraums sowie eine **PERIOD BUSINESS_TIME**-Klausel erforderlich. Die Spalten für die Start-/Endzeitpunkte des Gültigkeitszeitraums können vom Typ **DATE** oder **TIMESTAMP** sein.

Im folgenden Beispiel wird eine Tabelle für Kfz-Versicherungspolicen erzeugt, in der auch die Gültigkeitszeiten der jeweiligen Daten hinterlegt sind. Im vorliegenden Beispiel sind die Spalten **bus_start** und **bus_end** vom Typ **DATE**. Mit der Klausel **PERIOD BUSINESS_TIME** wird Db2 angewiesen, diese Spalten zur Nachverfolgung der Start- und Endzeiten für die Gültigkeit von Geschäftsvorfällen in jedem Satz zu nutzen. Um die temporale Integrität der Daten zu gewährleisten, legt Db2 automatisch eine Bedingung (Constraint) fest, die dafür sorgt, dass die Werte in **bus_start** vor denen in **bus_end** liegen.

```
CREATE TABLE policy (
  id              INT NOT NULL,
  vin             VARCHAR(10),
  annual_mileage  INT,
  rental_car      CHAR(1),
  coverage_amt    INT,
  bus_start       DATE NOT NULL,
  bus_end         DATE NOT NULL,
  PERIOD BUSINESS_TIME(bus_start, bus_end),
  PRIMARY KEY(id, BUSINESS_TIME WITHOUT OVER-
LAPS) );
```

Die in der **CREATE TABLE**-Anweisung definierte Bedingung für den Primärschlüssel nutzt die optionale Angabe **BUSINESS_TIME WITHOUT OVERLAPS**. Damit wird Db2 angewiesen, nur eindeutige Primärschlüsselwerte für jeden Zeitpunkt in Gültigkeitszeiträumen anzulegen. Im vorliegendem Beispiel sorgt **BUSINESS_TIME WITHOUT OVERLAPS** also dafür, dass keine zwei Versionen oder Zustände derselben Police gleichzeitig bestehen können.

Mit der Anweisung **ALTER TABLE** lassen sich vorhandene Tabellen für die Darstellung von Gültigkeitszeiten nutzbar machen. Hierzu müssen die oben erwähnten **DATE**- oder **TIMESTAMP**-Spalten eingefügt und **PERIOD BUSINESS_TIME** definiert werden.

Einfügen von Daten in eine Tabelle mit Business Time

Das Einfügen einer Zeile in eine Tabelle mit Business Time ist einfach: Es müssen lediglich gültige Werte für alle Spalten mit der Bedingung **NOT NULL** angegeben werden – auch für die Start- und Endzeitpunkte des Gültigkeitszeitraums. Mit folgenden Anweisungen lassen sich einige Zeilen in der Tabelle **POLICY** mit Business Time einfügen (siehe Abbildung 1). Die Abbildung 2 zeigt das Ergebnis der Operationen.

Die Daten zeigen, dass für Police 1111 im Zeitraum vom 1. Januar 2015 bis zum 1. Januar 2016 eine Deckungssumme von 500.000 € vereinbart war. Ab dem 1. Januar 2016 gilt eine Deckungssumme von 750.000 €. Die Daten zeigen weiterhin, dass vom 1. Mai 2013 bis zum 1. März 2015 für Police 1414 eine Deckungssumme von 750.000 €

für ein Fahrzeug mit einer voraussichtlichen Jahreskilometerleistung von 14.000 km vereinbart war. Vom 1. März 2015 bis zum 1. Januar 2016 galten für diese Police eine Deckungssumme von 600.000 € und eine voraussichtliche Jahreskilometerleistung von 12.000 km . Wie wird die für diese Tabelle (mit der Klausel **BUSINESS_TIME WITHOUT OVERLAPS**) vorgeschriebene zeitliche Eindeutigkeit in der Praxis gewährleistet? Dazu wird folgende **INSERT**-Anweisung eingegeben:

```
INSERT INTO policy
  VALUES(1111,'A1111',10000,
'Y',900000,'2015-06-01','2016-09-01');
```

Db2 wird diese Anweisung nicht ausführen und stattdessen Fehlermeldung ausgeben, weil versucht wurde, eine Zeile für Police 1111 einzufügen, die für einen Zeitraum gilt, für den bereits eine oder mehrere andere Zeilen für diese Police als gültig definiert sind. Es liegt also eine Verletzung der zeitlichen Eindeutigkeit vor. Soll die Deckungssumme für Police 1111 vom 1. Juni 2015 bis 1. September 2016 angepasst werden, ist dafür eine **UPDATE**-Anweisung erforderlich.

Aktualisieren von Daten in einer Tabelle mit Business Time

Auch Tabellen, die Gültigkeitszeiträume vorsehen, können mit herkömmlichen **UPDATE**-Anweisungen aktualisiert werden. Zusätzlich verfügbar ist die Klausel **FOR PORTION OF BUSINESS_TIME** zur Beschränkung der Aktualisierung auf einen bestimmten Gültigkeitszeitraum. Sind von der Aktualisierung auch Sätze betroffen, die nicht vollständig innerhalb des angegebenen Zeitraums liegt, aktualisiert Db2 die innerhalb der Zeitraumbedingung liegenden Daten und fügt zusätzliche Sätze ein zur Protokollierung der alten Werte für Sätze, die nicht innerhalb des angegebenen Zeitraums liegen.

Beispiel: Die Deckungssumme für Police 1111 soll für den Zeitraum vom 1. Juni 2015 bis 1. September 2016 geändert werden. Die entsprechende **UPDATE**-Anweisung könnte so aussehen:

```
UPDATE policy
  FOR PORTION OF BUSINESS_TIME FROM '2015-
06-01' TO '2016-09-01'
  SET coverage_amt = 900000
  WHERE id = 1111;
```

Hierbei ist zu beachten, dass die zeitliche Bedingung für die Abfrage **(FOR PORTION OF BUSINESS_TIME FROM ... TO ...**) hinter dem Tabellennamen steht und nicht Teil der **WHERE**-Klausel ist.

Wie in Abbildung 2 gezeigt, gab es ursprünglich zwei Zeilen für Police 1111. Beide sind von der **UPDATE**-Anweisung betroffen, da der zu aktualisierende Gültigkeitszeitraum teilweise innerhalb der in beiden Zeilen gespeicherten Zeiträume liegt. Diese Überlappung ist im oberen Teil von Abbildung 2 dargestellt. Wenn Db2 die Aktualisierung vornimmt, wird jede der ursprünglichen Zeilen in zwei Zeilen geteilt, wie im unteren Teil von Abbildung 2 dargestellt. Db2 passt die Gültigkeitszeiten der Sätze automatisch an.

```
INSERT INTO policy
 VALUES(1111,'A1111',10000,
'Y',500000,'2015-01-01','2016-01-01');
INSERT INTO policy
 VALUES(1111,'A1111',10000,
'Y',750000,'2016-01-01','9999-12-30');
INSERT INTO policy
 VALUES(1414,'B7777',14000,
'N',750000,'2013-05-01','2015-03-01');
INSERT INTO policy
 VALUES(1414,'B7777',12000,
'N',600000,'2015-03-01','2016-01-01');
```

Abb. 1: Einfügen von Daten in eine Tabelle mit Business Time

POLICY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end
1111	A1111	10000	Y	500000	2015-01-01	2016-01-01
1111	A1111	10000	Y	750000	2016-01-01	9999-12-30
1414	B7777	14000	N	750000	2013-05-01	2015-03-01
1414	B7777	12000	N	600000	2015-03-01	2016-01-01

Abb. 2: Ergebnis der INSERT-Befehle aus Abbildung 1

POLICY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end
1111	A1111	10000	Y	500000	2015-01-01	2015-06-01
1111	A1111	10000	Y	900000	2015-06-01	2016-01-01
1111	A1111	10000	Y	900000	2016-01-01	2016-09-01
1111	A1111	10000	Y	750000	2016-09-01	9999-12-30
1414	B7777	14000	N	750000	2013-05-01	2015-03-01
1414	B7777	12000	N	600000	2015-03-01	2016-01-01

Abb. 3: Die Tabelle POLICY nach dem UPDATE von Police 1111

POLICY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end
1111	A1111	10000	Y	500000	2015-01-01	2015-06-01
1111	A1111	10000	Y	900000	2015-06-01	2016-01-01
1111	A1111	10000	Y	900000	2016-01-01	2016-09-01
1111	A1111	10000	Y	750000	2016-09-01	9999-12-30
1414	B7777	14000	N	750000	2013-05-01	2015-03-01
1414	B7777	12000	N	600000	2015-03-01	2015-06-01

Abb. 4: Die Tabelle POLICY nach dem Löschen von Daten

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end
1414	B7777	14000	N	750000	2013-05-01	2015-03-01
1414	B7777	12000	N	600000	2015-03-01	2016-01-01

Abb. 5: Abfrageergebnis

Abbildung 3 zeigt die Tabelle **POLICY** nach der Aktualisierung. Sowohl der erste als auch der zweite Satz aus Abbildung 2 wird in jeweils zwei neue Sätze geteilt.

Löschen von Daten aus einer Tabelle mit Business Time

Das Löschen von Daten aus Tabellen mit Gültigkeitszeiträumen kann mit der Klausel **FOR PORTION OF BUSINESS_TIME** auf spezifische Zeiträume beschränkt werden. Enthält eine zum Löschen vorgesehene Zeile Daten, die nicht vollständig innerhalb des angegebenen Zeitraums liegen, sorgt Db2 dafür, dass diese Daten erhalten bleiben.

```
DELETE FROM policy
       FOR PORTION OF BUSINESS_TIME FROM
'2015-06-01' TO '2016-01-01'
       WHERE id = 1414;
```

Die Abbildung 4 zeigt das Ergebnis nach dem Löschen der Daten aus dem oben genannten Befehl an. Beachten Sie den letzten Satz (id = 1414), bei dem Db2 die Business Time korrigiert hat.

Abfragen an eine Tabelle mit Business Time

Abfragen an eine Tabelle mit Gültigkeitszeiträumen lassen sich ganz einfach formulieren. Für zeitbezogene Abfragen zur Ermittlung vergangener, aktueller und künftiger Geschäftsvorfälle stehen drei optionale Klauseln zur Verfügung. Natürlich lassen sich Tabellen mit Gültigkeitszeiträumen auch mit herkömmlichen, d.h. nicht-temporalen, **SELECT**-Anweisungen abfragen. Db2 führt solche Abfragen in der gewohnten Weise aus. Ein Beispiel zeigt, wie einfach sich zeitbezogene Abfragen mit dem Konzept Business Time formulieren lassen.

Die Tabelle **POLICY** enthält nun dieselben Daten, die auch Abbildung 2 zeigt, unmittelbar nachdem wir die Tabelle **POLICY** erzeugt und vier Sätze eingefügt hatten.

```
CREATE TABLE policy (
 id             INT NOT NULL,
 vin            VARCHAR(10),
 annual_mileage INT,
 rental_car     CHAR(1),
 coverage_amt   INT,
 bus_start      DATE NOT NULL,
 bus_end        DATE NOT NULL,
 sys_start      TIMESTAMP(12) GENERATED ALWAYS AS ROW BEGIN NOT NULL,
 sys_end        TIMESTAMP(12) GENERATED ALWAYS AS ROW END NOT NULL,
 trans_start    TIMESTAMP(12) GENERATED ALWAYS
                    AS TRANSACTION START ID IMPLICITLY HIDDEN,
 PERIOD SYSTEM_TIME (sys_start, sys_end),
 PERIOD BUSINESS_TIME(bus_start, bus_end),
 PRIMARY KEY(id, BUSINESS_TIME WITHOUT OVERLAPS)
);
```

Abb. 6: Erzeugen einer bitemporalen Tabelle

Für Abfragen nach temporalen Daten muss auch hier analog zu Abfragen mit System Time eine von drei unterstützten Zeitraumangaben in die **FROM**-Klausel aufgenommen werden. Die Zeitangaben können sowohl in der Vergangenheit als auch in der Zukunft liegen:

- **FOR SYSTEM_TIME AS OF ...**
- **FOR SYSTEM_TIME FROM ... TO ...**
- **FOR SYSTEM_TIME BETWEEN ... AND ...**

Mit folgender SQL-Anweisung lassen sich die für Police 1414 vom 1. Januar 2014 bis zum 1. Januar 2016 geltenden Versicherungsbedingungen abfragen. Das Ergebnis ist in Abbildung 5 dargestellt.

```
SELECT *
  FROM policy
  FOR BUSINESS_TIME FROM '2014-01-01' TO
'2016-01-01'
  WHERE id = 1414;
```

Temporale Abfragen an Tabellen mit Gültigkeitszeiträumen werden intern umgesetzt in **WHERE**-Klauseln für die **DATE**- oder **TIMESTAMP**-Spalten, in denen die Start- und Endzeitpunkte der Gültigkeitsdauer abgelegt sind.

Zusätzliche temporale Funktionalitäten

Wie die Beispiele oben zeigen, sind die von Db2 unterstützten temporalen Konzepte System Time und Business Time einfach zu implementieren. Wie bereits erwähnt, bietet Db2 darüber hinaus noch weitere Möglichkeiten zur temporalen Datenhaltung – etwa in so genannten bitemporalen Tabellen. Db2 unterstützt ebenfalls temporale Views und eine Registereinstellung, mit der die jeweilige Datenbank ähnlich wie eine Zeitmaschine arbeitet. Da eine ausführliche Darstellung dieser und anderer erweiterten temporale Funktionen den Rahmen dieses Artikels sprengen würde, sollen sie an dieser Stelle nur kurz vorgestellt werden.

Bitemporale Tabellen

Bitemporale Tabellen ermöglichen die Datenhaltung mit Bearbeitungs- und Gültigkeitszeit und die Ausnutzung der Vorzüge beider Konzepte. So lässt sich die Gültigkeitszeit für die Abbildung logischer Aspekte eines Datenbestands nutzen, wie beispielsweise die Laufzeiten von Versicherungspolicen, und die Bearbeitungszeit zur Nachverfolgung der Änderungen, die an diesen Policen vorgenommen wurden.

Das Erzeugen von Tabellen mit Bearbeitungs- und Gültigkeitszeit ist ebenso einfach wie das Ändern vorhandener Tabellen zur Aufnahme der beiden temporalen Konzepte. Die folgende **CREATE TABLE**-Anweisung definiert eine bitemporale Tabelle mit einer Periode für **BUSINESS_TIME** in den Spalten **bus_start** und **bus_end** sowie mit einer Periode für **SYSTEM_TIME** in den Spalten **sys_start** und **sys_end** (siehe Abbildung 6).

Nach dem Erzeugen der bitemporalen Tabelle muss eine identische History-Tabelle erzeugt und die Versionierung aktiviert werden.

Die bitemporale Beispieltabelle **POLICY** und die zugehörige History-Tabelle sind in den Abbildungen 7 und 8 dargestellt. (Die Spalte **trans_start** wird zur Vereinfachung hier nicht dargestellt.)

Im folgenden Beispiel hat der Kundenservice folgende Handlungen vorgenommen:

- Am 15. November 2016 wird die Police 1111 für das Fahrzeug A1111 angelegt. Als Beginn der Laufzeit der Police mit einer Deckungssumme von 500.000 € wurde der 1. Januar 2017 festgelegt.

```
INSERT INTO policy(id, vin, annual_
mileage, rental_car, coverage_amt, bus_
start, bus_end)
  VALUES(1111,'A1111',10000,
'Y',500000,'2017-01-01','9999-12-30');
```

- Am 1. März 2017 wurden die Bedingungen der Police 1111 mit Wirkung ab dem 1. Juni 2017 geändert: Die Deckungssumme wurde reduziert und die Kostenübernahme für Leihwagen entfernt. Das geschah mit folgender **UPDATE**-Anweisung:

```
UPDATE policy
  FOR PORTION OF BUSINESS_TIME FROM
'2017-06-01' TO '9999-12-30'
  SET coverage_amt = 250000, rental_car='N'
  WHERE id = 1111;
```

  Die Abbildungen 9 und 10 zeigen die Inhalte der Tabellen **POLICY** und **POLICY_HISTORY** nach diesen Operationen. (Der Einfachheit halber sind in den Spalten **sys_start** und **sys_end** nur die Datumswerte gezeigt und nicht der exakte Zeitpunkt)

- Darüber hinaus wird unter der Police 1111 wegen eines Unfalls am 20. Juni 2017 ein Schadenersatzanspruch geltend gemacht. Der zuständige Sachbearbeiter kann die Rechtmäßigkeit des Anspruchs mit folgender Abfrage prüfen:

```
SELECT vin, rental_car, coverage_amt
  FROM policy FOR BUSINESS_TIME AS OF
'2017-06-20'
  WHERE id = 1111;
```

  Db2 gibt die in Abbildung 11 gezeigte Information zurück, aus der hervorgeht, dass eine Versicherungsdeckung für das Fahrzeug besteht, der Kunde aber keinen Anspruch auf kostenlose Nutzung eines Mietwagens hat.

- Am 10. Juli 2017 beschwert sich der Kunde und verlangt eine Aufstellung der in den vergangenen zwei Jahren an seiner Police vorgenommenen Änderungen. Diesem Wunsch kann der Sachbearbeiter mit folgender Abfrage nachkommen:

```
SELECT id, vin, annual_mileage, rental_car,
coverage_amt, bus_start, bus_end, sys_
start, sys_end
  FROM policy FOR SYSTEM_TIME FROM
'2015-07-10' TO '2017-07-11'
  WHERE id = 1111;
```

Db2 gibt die in Abbildung 12 gezeigten Ergebnisse zurück. Der Sachbearbeiter kann dem Kunden nun mitteilen, wann die Änderungen an der Police vorgenommen wurden und ab wann sie wirksam wurden (oder wirksam werden sollten).

POLICY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end	sys_start	sys_end

Abb. 7: Die bitemporale Tabelle POLICY

POLICY_HISTORY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end	sys_start	sys_end

Abb. 8: Die bitemporale Tabelle POLICY_HISTORY

POLICY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end	sys_start	sys_end
1111	A1111	10000	Y	500000	2017-01-01	2017-06-01	2017-03-01	9999-12-3
1111	A1111	10000	N	250000	2017-06-01	9999-12-30	2017-03-01	9999-12-3

Abb. 9: Die bitemporale Tabelle POLICY nach dem UPDATE

POLICY_HISTORY

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end	sys_start	sys_end
1111	A1111	10000	Y	500000	2017-01-01	9999-12-30	2016-11-15	2017-03-0

Abb. 10: Die bitemporale Tabelle POLICY_HISTORY nach dem UPDATE

VIN	rental_car	coverage_amt
A1111	N	250000

Abb. 11: Abfrageergebnis

ID	VIN	annual_mileage	rental_car	coverage_amt	bus_start	bus_end	sys_start	sys_end
1111	A1111	10000	Y	500000	2017-01-01	2017-06-01	2017-03-01	9999-12-3
1111	A1111	10000	N	250000	2017-06-01	9999-12-30	2017-03-01	9999-12-3
1111	A1111	10000	Y	500000	2017-01-01	9999-12-30	2016-11-15	2017-03-0

Abb. 12: Abfrageergebnis (die letzte Zeile stammt aus der HISTORY-Tabelle)

Quellen

[Q1] Cynthia M. Saracco, Matthias Nicola, Lenisha Gandhi:
„A matter of time: Temporal data management in DB2“

[Q2] Db2 auf IBM developerWorks (Technische Artikel, Software, Forum)
https://developer.ibm.com/data/db2/

Views

Db2 stellt für temporale Tabellen zwei Arten von Views zur Verfügung. Solche Views ermöglichen ein flexibles Anwendungsdesign, um bezogen auf eine Datenbanksitzung die Daten für unterschiedliche Zeitpunkte oder Perioden abzubilden.

1. Views können für eine temporale Tabelle mithilfe einer **FOR SYSTEM_TIME**- oder **FOR BUSINESS_TIME**-Klausel definiert werden, um die Sicht auf einen bestimmten Zeitpunkt oder Zeitraum zu beschränken. Anschließend können diese Views mit herkömmlichen SQL-Anweisungen abgefragt werden. Abfragen an solche Views dürfen keine **FOR SYSTEM_TIME**- oder **FOR BUSINESS_TIME**-Klauseln enthalten, weil die zeitliche Bedingung in der Abfrage mit der zeitlichen Bedingung für die Views im Widerspruch stehen oder zu zweideutigen Ergebnissen führen könnte.
2. Die Definition einer View für eine temporale Tabelle ohne eine **FOR SYSTEM_TIME**- oder **FOR BUSINESS_TIME**-Bedingung. Solche Views stellen Daten für alle Zeitpunkte dar und lassen sich mit Anweisungen abfragen, die **FOR SYSTEM_TIME**- oder **FOR BUSINESS_TIME**-Klauseln enthalten. Solche Klauseln werden dann automatisch auf alle Tabellen in der **View**-Definition angewendet, die Perioden für System Time oder Business Time enthalten.

Db2 bietet damit enorme Flexibilität bei der Arbeit mit Views und temporalen Daten. Temporale Bedingungen lassen sich also in der **View**-Definition oder in Abfragen an Views von temporalen Tabellen nutzen.

Globale Einstellungen über Register-Variablen

Db2 Registereinstellungen bieten die Möglichkeit, Datenbestände mit vorhandenen Anwendungen von einem bestimmten Zeitpunkt aus zu analysieren, ohne dass die Anwendung selbst geändert werden muss. Im Folgenden geht es um eine Anwendung, die zahlreiche SQL-Abfragen oder bestimmte Berichtsabfragen enthält, die von Zeit zu Zeit ausgeführt werden müssen. Mit den temporalen Funktionen in Db2 wird man solche Abfragen auch für Bearbeitungszeitpunkte ausführen können, die in der Vergangenheit liegen, oder für vergangene oder künftige Gültigkeitszeiten. Müsste man nun jedoch alle vorhandenen SQL-Anweisungen um eine **FOR SYSTEM_TIME**- oder **FOR BUSINESS_TIME**-Klausel erweitern, wäre das möglicherweise sehr zeitaufwändig. Gleiches gilt für das Erzeugen von Views für alle betroffenen temporalen Tabellen. Deshalb stellt Db2 spezielle Register zur Verfügung, mit denen eine Datenbanksitzung auf einen spezifischen Zeitpunkt eingestellt werden kann.

Beispiel: Mit folgendem **SET**-Befehl wird die Systemzeit der eigenen Sitzung auf den 1. Januar 2013, 10.00 Uhr, eingestellt:

```
SET CURRENT TEMPORAL SYSTEM_TIME = '2013-01-
01 10:00:00';
```

Nun werden alle in dieser Datenbanksitzung an temporale (oder bitemporale) Tabellen gerichteten Abfragen für die Bearbeitungszeit 1. Januar 2013, 10.00 Uhr, ausgeführt. Oder anders ausgedrückt: Alle Abfragen in dieser Datenbanksitzung werden automatisch um die Klausel **FOR SYSTEM_TIME AS OF '2013-01-01 10:00:00'** erweitert. Db2 führt dies automatisch aus. Der Benutzer muss weder an der Anwendung noch an den SQL-Anweisungen irgendetwas ändern.

Mit folgender Registereinstellung lassen sich die Daten für einen Zeitpunkt auswerten, der einen Monat vor der aktuellen Bearbeitungszeit liegt:

```
SET CURRENT TEMPORAL SYSTEM_TIME = current
timestamp – 1 MONTH;
```

Steht im Register **CURRENT TEMPORAL SYSTEM_TIME** ein anderer Wert als **NULL**, sind Datenänderungen wie ändern, einfügen oder löschen an temporalen Tabellen unzulässig.

Für die Business Time lässt sich die Registervariable **CURRENT TEMPORAL BUSINESS_TIME** setzen, um Abfragen, Änderungen, Löschungen usw. an zurückliegenden oder künftigen Gültigkeitszeitpunkten vorzunehmen.
Beispiel:

```
SET CURRENT TEMPORAL BUSINESS_TIME = '2017-06-
01';
```

Nun werden alle Abfragen und Befehle zur Datenmanipulation, die an Tabellen mit Business Time (oder bitemporale Tabellen) gerichtet sind, um die Klausel **FOR BUSINESS_TIME AS OF '2017-06-01'** erweitert. Auch hier nimmt Db2 diese Änderung automatisch vor.

Fazit

Die temporalen Funktionen von Db2 ermöglichen auf einfache Weise sowohl die differenzierte Auswertung historischer Datensätze sowie die Verfolgung zeitlicher Änderungen. Auf der Grundlage der temporalen Erweiterungen des SQL:2011-Standards bietet Db2 eine Umgebung für effektive temporale Datenhaltung, die im Vergleich mit selbst entwickelten Lösungen zur Abbildung temporaler Konzepte in Form von Triggern, Prozeduren oder selbst entwickelten Anwendungen ganz erhebliche Zeit- und Kostenvorteile bietet.

Stefan Hummel, Certified IT Specialist
IBM Deutschland

Python Generator-Funktionen und -Expressions

Ein alter Hut kann auch modern sein

Funktionen wie filter(), map() und zip() geben seit Python 3 keine Liste, sondern einen Iterator zurück. Dadurch muss nicht die gesamte Liste im Speicher gehalten werden, sondern immer nur das aktuelle Objekt. Dies ist wesentlich effizienter und eine gute Vorlage für das Design von eigenem Code. Schon seit Python 2.3 bzw. 2.4 können Generator-Funktionen und -Expressions genutzt werden, um auf einfache und effiziente Weise Iteratoren zu generieren. Trotzdem werden sie viel zu selten eingesetzt. Damit in Zukunft häufiger Generatoren verwendet werden, sollen sie in diesem Beitrag anschaulich erläutert werden.

Wie was – Iterable und Iterator?

Eine Klasse, die gleichzeitig ein Iterable und ein Iterator ist, ist beispielhaft in Abbildung 1 dargestellt. Ein Iterable ist ein Objekt, dass die Methode **`__iter__()`** implementiert. Dies sind alle Sequence-Typen (Listen, Strings usw.) und z. B. Dictionaries oder Dateiobjekte. Die Methode wird aufgerufen, wenn ein Iterator-Objekt des Containers benötigt wird. Dies wird von der Methode zurückgegeben. Das Iterator-Objekt wiederum implementiert die Methode **`__next__()`**, die jeweils das nächste Element in dem Container zurück gibt bzw. die Exception StopIteration generiert, wenn keine weiteren Elemente im Container vorhanden sind. Damit der Iterator weiß, welches das nächste Element ist, speichert er seinen jeweiligen aktuellen Zustand.

Eine Klasse, die gleichzeitig ein Iterable und ein Iterator ist, kann wie folgt aussehen. Dies entspricht der Implementierung von Generatoren und auch den Objekten, die z. B. **`map()`** zurückgibt. Die in dem Beispiel gezeigte Klasse ist ein einfacher Nachbau der Funktion **`range()`**. Beim Aufruf von **`__iter__()`** gibt sie sich selbst zurück und beim Aufruf von **`__next__()`** wird **`self.start`** so lange inkrementiert und zurückgegeben, bis **`self.stop`** erreicht ist.

Iterables können z. B. in **`for`**-Schleifen verwendet werden. Diese ruft implizit die Funktion **`iter()`**, die den Iterator zu einem Iterable zurückgibt, mit dem angegebenen Iterable-Objekt als Argument auf und weist den Iterator einer anonymen Variablen zu. Diese Variable ist temporär und existiert, bis die Schleife beendet ist. In jedem Durchlauf der Schleife wird implizit die Funktion **`next()`** mit dem Iterator als Argument aufgerufen, bis die StopIteration Exception auftritt. Eine **`for`**-Schleife lässt sich somit mit einer **`while`**-Schleife simulieren (siehe Abbildung 2).

Ressourcen? Habe ich doch ausreichend …

Ein Iterator erzeugt ein Ergebnis nur, wenn es angefordert wird, anstatt alle Ergebnisse sofort bereitzustellen. Dieses „faule“ Verhalten kann bei der Verarbeitung großer Datenmengen den benötigten Speicher massiv reduzieren und auch die Performance steigern, wenn komplexe Berechnungen zum Produzieren der Werte notwendig sind. Man kann argumentieren, dass Ressourcen in heutiger Zeit

```
>>> class my_range:...    def __init__(self, start, stop):
...         self.start = start
...         self.stop = stop
...     def __iter__(self):
...         return self
...     def __next__(self):
...         if self.start == self.stop:
...             raise StopIteration
...         self.start += 1
...         return self.start - 1
```

Abb. 1: Iterable- und Iterator-Klasse

```
>>> i = iter(my_range(1, 5))
>>> while True:
...     try:
...         print(next(i))
...     except StopIteration:
...         break
1
2
3
4
```

Abb. 2: StopIteration Exception

in vielen Fällen kein wesentlicher Faktor sind, aber wenn man ihre Nutzung ohne höheren Aufwand auf ein Minimum reduzieren kann, sollte jeder hellhörig werden. In dem folgenden Beispiel wird im ersten Schritt mittels List-Comprehension eine Liste generiert, die Zweierpotenzen der Zahlen von 0 bis 99999999 enthält, und im zweiten Schritt die Summe dieser Zahlen gebildet:

```
>>> sum([n**2 for n in range(100000000)])
333333328333333350000000
```

Für diese Berechnung wird ca. 4 GB Speicher benötigt. Wird anstelle der Liste ein Iterator verwendet, kann der Speicherbedarf, bei vergleichbarer Performance auf ca. 8 MB reduziert werden. Die Implementierung ist im folgenden Beispiel mit einer Generator-Expression gelöst, die in den nächsten Punkten detailliert erläutert wird.

```
>>> sum(n**2 for n in range(100000000))
333333328333333350000000
```

Generatoren

Die Erzeugung eines Iterator-Objektes wie im ersten Beispiel gezeigt ist relativ komplex und der Aufwand wird von vielen Entwicklern gescheut. Mit Generatoren lassen sich Iteratoren auf einfache Weise erstellen und sie machen damit die Einsparung von Ressourcen einfach zugänglich. Ein Generator lässt sich auf zwei verschiedene Arten erzeugen, zum einen mit Generator-Expressions und zum anderen mit Generator-Funktionen.

Generator-Expressions

Einfache Generatoren lassen sich mit Generator-Expressions implementieren. Sie haben, wie im zweiten Beispiel ersichtlich, eine an List-Comprehensions angelehnte Syntax. Ähnlich wie lambda anonyme Funktionen erstellt, erstellen Generator-Expressions anonyme Generator-Funktionen. In der Regel werden die Expressions in runden Klammern geschrieben. Diese können, falls die Expression das einzige Argument einer Funktion ist, weggelassen werden. Im Gegensatz zu einer Liste wird ein Generator „verbraucht“, man kann z. B. nur einmal über ihn iterieren (siehe Abbildung 3). Ebenso kann auf einen Generator nicht über Sequence-Operationen zugegriffen werden. Wird also eine Liste, die mittels List-Comprehension generiert wurde, nicht häufiger benötigt bzw. es müssen keine speziellen Methoden oder Sequence-Operationen auf sie ausgeführt werden, sollte sie durch eine Generator-Expression ersetzt werden.

```
>>> g = (n**2 for n in range(5))
>>> for i in g:
...     print(i)
...
0
1
4
9
16
>>> for i in g:
...     print(i)
...
>>>
```

Abb. 3: Verbrauch von Generatoren

Generator-Funktionen

Es lassen sich mit Generator-Expressions jedoch nicht beliebig komplizierte Generatoren erstellen. An dieser Stelle kommen Generator-Funktionen ins Spiel. Die in den oberen Beispielen dargestellte Expression könnte als Funktion wie folgt definiert werden.

```
>>> def potenz_2(anz):
...     for n in range(anz):
...         yield n**2
...
```

Generator-Funktionen unterscheiden sich somit auf den ersten Blick nicht von „normalen“ Funktionen. Der Unterschied liegt in dem Statement **`yield`**. Es macht eine Funktion zu einem Generator. Wird eine Generator-Funktion aufgerufen, wird sie initialisiert, aber noch kein Code ausgeführt. Dies geschieht erst, wenn der erstellte Iterator genutzt wird (er wird **`next()`** übergeben). Dann wird die Funktion von oben nach unten abgearbeitet, bis das erste **`yield`**-Statement erreicht wird und der Wert der Expression zurückgegeben. Im Gegensatz zu einer normalen Funktion wird diese nun nicht beendet, sondern nur unterbrochen (alle aktuellen Werte bleiben erhalten). Beim nächsten Mal, wenn der Generator **`next()`** übergeben wird, beginnt die Verarbeitung direkt nach dem **`yield`**-Statement, bei dem der Generator das letzte Mal unterbrochen wurde.

Pipelining mit Generatoren

Mit den bisher genannten Beispielen lässt sich zwar das Verhalten von Generatoren gut erklären, aber wirkliche Begeisterung lässt sich damit schwer hervorrufen. Leider hören die Erläuterungen in vielen Python-Büchern an dieser Stelle auf. Dies erklärt eventuell den relativ seltenen Einsatz von Generatoren in Python-Programmen. Folgendes Beispiel zeigt, wie mithilfe von Generator-Expressions und -Funktionen alle Apache-Access-Logfiles in einem Verzeichnis verarbeitet werden können, um eine Liste aller IPs, über die auf den Webserver zugegriffen wurde, zu erstellen (siehe Abbildung 4).

Natürlich fehlt in dem Beispiel das gesamte Exception-Handling, aber es ist auf den ersten Blick ersichtlich, dass der Code durch die Nutzung von Generatoren deutlich eleganter wird. Folgendermaßen läuft die Verarbeitung ab:

1. Der Generator-Funktion **`open_logfiles()`** wird ein Pfad und ein RegEx-Muster übergeben. Er öffnet die entsprechenden Dateien, gibt File-Objekte zurück und nutzt, falls es sich um eine gepackte Datei handelt, die **`open()`**-Funktion des entsprechenden Moduls.

2. **`gen_lines()`** iteriert über die File-Objekte und gibt die einzelnen Zeilen der Dateien zurück.

3. Diese werden in der Generator-Expression verarbeitet, die jeweils die IP-Adresse zurückgibt.

Die genutzte Verknüpfung von Generatoren hat David M. Beazley schon 2008 auf der PyCon als Pipelining beschrieben. Seine Talks zu dem Thema sind die de-facto-Referenz und können als weiterführende Lektüre dienen. Dort erläutert er z. B. auch, wie Co-Routinen auf Basis von Generatoren implementiert werden.

Marius Dorlöchter
(info@ordix.de)

```
#!/usr/bin/env python3

import bz2
import gzip
import lzma
import os
import re

from pprint import pprint

def open_logfiles(path, pattern):
    re_pattern = re.compile(pattern)

    for root, dirs, files in os.walk(path):
      for f in (f for f in files if re_pattern.search(f)):
          if f.endswith('.gz'):
             yield gzip.open(os.path.join(root, f), 'r')
          elif f.endswith('.bz2'):
             yield bz2.open(os.path.join(root, f), 'r')
          elif f.endswith('.xz'):
             yield lzma.open(os.path.join(root, f), 'r')
          else:
            yield open(os.path.join(root, f), 'r')

def gen_lines(fhs):
    for fh in fhs:
        for l in fh:
            yield l.rstrip()

def main():
   apache_logs = open_logfiles('/var/log/apache2',
                               r'^access_log')
   ips = set(l.split()[0] for l in gen_lines(apache_logs))
   pprint(ips)

if __name__ == '__main__':
    main()
```

Abb. 4: Parsen von Apache-Logfiles

Big Data – Informationen neu gelebt (Teil VIII)

Hadoop Security

Zu einem der am meisten genutzten Technologien im Bereich Big Data gehört Hadoop. Das Hadoop-Kernsystem besteht dabei aus dem Hadoop Distributed File System (HDFS), dem Ressourcenmanager YARN (Yet Another Resource Negotiator) und dem MapReduce-Framework. Daneben gibt es noch viele weitere Komponenten, die mit den Hadoop-Kernkomponenten interagieren bzw. diese nutzen. Doch welche Sicherheitsmechanismen gibt es dabei überhaupt? Genau an dieser Stelle setzt der folgende Artikel an.

Einleitung

In diesem Artikel werden hauptsächlich die Punkte Autorisierung und Authentifizierung im HDFS näher betrachtet. Weitere Security-Features wie beispielsweise Data-at-Rest-Verschlüsselung (über den Hadoop Key Management Server (KMS)) oder auch die Data-in-Motion-Verschlüsselung werden nicht behandelt. Neben den Möglichkeiten zur Absicherung der Zugriffe auf das HDFS wird als ein Beispiel für die vielen unterschiedlichen Komponenten aus dem Hadoop-Ökosystem Apache Hive näher analysiert. Hierbei wird insbesondere die Verbindung zwischen Hive und dem HDFS genauer betrachtet.

Rechtevergabe im HDFS

Innerhalb des HDFS können auf Verzeichnisse und auch auf einzelne Dateien verschiedenste Zugriffsrechte vergeben werden. Diese verhalten sich ähnlich wie die Zugriffsrechte im Linux-Betriebssystem. So können beispielsweise Read-, Write- und Execute-Rechte vergeben werden. Diese Rechte können dann noch einmal einzeln für den Besitzer der Datei, für eine spezifische User-Gruppe und für alle restlichen Nutzer vergeben werden. Einen Unterschied zu den POSIX-Rechten gibt es jedoch, und zwar das Verhalten des Execute-Rechts. Im HDFS ist es nicht möglich, eine Datei auszuführen. Somit wird diese Berechtigung ignoriert, sobald sie auf eine einzelne Datei gesetzt ist. Bei Ordnern spielt diese Berechtigung jedoch eine sehr wichtige Rolle, da über diese Berechtigung gesteuert werden kann, ob ein Benutzer Zugriff auf die darunterliegenden Ordner und Dateien hat und beispielsweise ein **ls** ausführen darf. [Q1]

```
hdfs dfs -ls /user/ordix/testdatei.txt

Found 1 items

-rw-r--r--   1 ordix hdfs  34 2018-01-29 14:16 /
user/ordix/testdatei.txt

hdfs dfs -cat /user/ordix/testdatei.txt

Hallo liebe ORDIX News-Leser. :-)
```

Die einzelnen Rechte können dabei über die Kommandos **chown** und **chmod** verändert werden (ein Beispiel ist im nächsten Listing dargestellt). Auch an dieser Stelle verhält sich das HDFS wieder äquivalent zum Linux-Betriebssystem. Somit können die Berechtigungen mittels Okatalnotation oder über die Angabe der Berechtigung (z. B. **+r** für die Leseberechtigung aller User) gesetzt werden. Die Anpassungen können dabei von dem HDFS-Superuser (standardmäßig ist dies der User **hdfs**) oder dem Besitzer der Datei durchgeführt werden. Dabei gibt es allerdings eine kleine Einschränkung: Der Besitzer einer Datei kann nur von dem HDFS-Superuser geändert werden. Falls die **chown**-Operation von einem „normalen“ User ausgeführt wird, bekommt dieser eine Fehlermeldung. [Q2]

```
hdfs dfs -cat /user/ordix/testdatei.txt

Hallo liebe ORDIX News-Leser. :-)

hdfs dfs –chmod 000 /user/ordix/testdatei.txt

hdfs dfs -cat /user/ordix/testdatei.txt

cat: Permission denied: user=ordix, access=READ,
inode="/user/ordix/testdatei.txt":
maria_dev:hdfs:----------
```

Rechtevergabe mittels Access Control Lists (ACL)

Da jedoch eine Vergabe von Rechten auf der Ebene Besitzer, User-Gruppe und Rest der Welt gerade in Hinsicht der Nutzung von Hadoop bzw. genauer des HDFS als sogenanntem Data Lake [Q3] oftmals nicht ausreichend ist, gibt es auch im HDFS das Konzept der ACLs. Die ACLs enthalten standardmäßig immer auch die Berechtigungen, die über die POSIX-Berechtigungen im HDFS für den Besitzer der Datei/des Ordners, einer User-Gruppe und den restlichen Usern vergeben wurden. Zusätzlich bieten die ACLs aber auch noch die Möglichkeit, Rechte für weitere User/User-Gruppen zu vergeben. Damit die ACLs überhaupt genutzt werden können, muss in der HDFS-

Konfiguration der Wert **dfs.namenode.acls.enabled** auf **true** gesetzt werden [Q4]. Ohne diese Änderung werden alle Befehle zum Setzen von ACLs ignoriert (siehe nächstes Listing).

```
hdfs dfs -setfacl -m user:patrick:rw- /user/ordix/testdatei.txt

setfacl: The ACL operation has been rejected. Support for ACLs has been disabled by setting dfs.namenode.acls.enabled to false.
```

Anschließend kann der HDFS-Superuser mittels der ACLs verschiedenste Zugriffsrechte setzen. Dazu muss der Befehl **hdfs dfs -setfacl** genutzt werden.

```
hdfs dfs -setfacl -m user:patrick:rw- /user/ordix/testdatei.txt
```

Mittels **hdfs dfs -getfacl** können die aktuell für diese Datei bzw. Ordner gesetzten ACLs angezeigt werden.

```
hdfs dfs -getfacl /user/ordix/testdatei.txt

# file: /user/ordix/testdatei.txt

# owner: ordix

# group: hdfs

user::r--

user:patrick:rw-

group::r--

mask::rw-

other::r--
```

Zudem wird über ein **+** in der Ausgabe des **ls**-Kommandos symbolisiert, dass eine ACL für diese Datei bzw. diesen Ordner gesetzt wurde.

```
hdfs dfs -ls /user/ordix/testdatei.txt

-r--rw-r--+  1 ordix hdfs  34 2018-01-29 14:16 /user/ordix/testdatei.txt
```

Da pro Datei eine eigene ACL erstellt werden kann und pro ACL 32 Einträge [Q5] erlaubt sind, ist durch die Nutzung der ACLs eine deutlich feingranularere Rechtevergabe möglich. Aber auch 32 Einträge können sehr schnell nicht mehr ausreichen, wenn das Hadoop-Cluster beispielweise als Data Lake genutzt wird. Falls der Data Lake in einem großen Unternehmen aufgebaut wird, kann es sehr schnell dazu kommen, dass mehr als 32 Abteilungen bzw. Personengruppen auf die gleichen Daten zugreifen sollen/wollen. In diesem Fall reicht dann die Möglichkeit zur Rechtevergabe mittels ACLs nicht mehr aus, um solche feingranulare Rechtevergabe zu ermöglichen. An dieser Stelle würde dann eine Komponente wie z. B. Apache Ranger ansetzen.

Kerberos

Kerberos wurde ursprünglich am Massachusetts Institute of Technology (MIT) entwickelt und stellt einen Mechanismus zur eindeutigen Identifizierung des Users bereit (weitere Information zu Kerberos sind in [4] zu finden). Die eindeutige Identifizierung eines Users/Systems wird auch als Authentifizierung bezeichnet [Q6]. Neben dem Authentifizierungsmodus **simple**, bei dem der User-Name im Betriebssystem zur Authentifizierung genutzt wird, bietet Hadoop auch die Möglichkeit zur Nutzung von Kerberos. In diesem Modus ist ein Zugriff auf die, im HDFS gespeicherten, Daten nur noch über ein gültiges Kerberos-Ticket (Kerberos-TGT) möglich. Dieses kann im Linux-Betriebssystem über den Befehl **kinit** erzeugt werden.

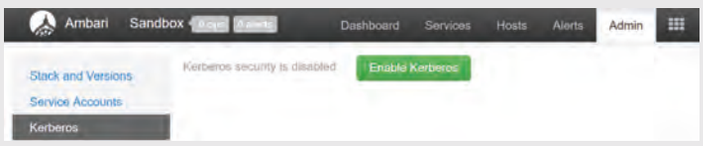

Abb. 1: Button zur Aktivierung von Kerberos in der Apache Ambari-UI

```
hdfs dfs -cat /user/ordix/testdatei.txt

18/01/30 10:00:21 WARN ipc.Client: Exception encountered while connecting to the server : javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)]

[Fehlermeldung ist gekürzt]

kinit ordix@INTERNAL.ORDIX.DE

<Eingabe des Passworts>

hdfs dfs -cat /user/ordix/testdatei.txt

Hallo liebe ORDIX News-Leser. :-)
```

Die Aktivierung von Kerberos in einem Hadoop-Cluster ist jedoch nicht trivial. So müssen beispielsweise für jeden Server die passenden Kerberos Principals und die dazugehörigen Keytabs angelegt werden. Falls eine Distribution wie z. B. die Hortonworks Data Platform (HDP) oder Cloudera's Distribution Including Apache Hadoop (CDH) genutzt werden, dann kann die Kerberisierung des Clusters auch automatisiert über den Cluster Manager (Apache Ambari/Cloudera Manager) vorgenommen werden (siehe Abbildung 1).

Dabei werden durch den Cluster Manager die benötigten Kerberos Principals und die dazugehörigen Keytabs erstellt. Damit dies automatisiert ablaufen kann, muss als Vorbedingung ein Kerberos/AD-Admin-User vorhanden sein. Zudem werden bei der Kerberisierung des Hadoop-Clusters durch den Cluster Manager auch noch die benötigten Einstellungsänderungen bei den einzelnen Hadoop-Komponenten durchgeführt.

Delegation Tokens

Nach der Aktivierung von Kerberos in einem Hadoop-Cluster kommt ein weiterer Sicherheitsmechanismus

von Hadoop zum Tragen. Dies ist die Verwendung von Delegation Tokens. Diese Tokens werden verwendet, um den Zugriff von verteilt ausgeführten Processing-Jobs (wie z. B. MapReduce-Jobs) auf das HDFS abzusichern (siehe Abbildung 2). Um ein Delegation Token nutzen zu können, muss die folgende Abfolge von Operationen ausgeführt werden:

- Der Benutzer authentifiziert sich gegenüber MapReduce/YARN mithilfe von Kerberos.
- Der Benutzer authentifiziert sich gegenüber dem HDFS Namenode und bekommt als Antwort ein Delegation Token.
- Dieses Delegation Token wird anschließend innerhalb des MapReduce-Jobs zum Zugriff auf die HDFS-Daten genutzt.

Delegation Tokens werden eingesetzt, um eine zu hohe Last auf dem Key-Distribution-Center-(KDC)-Server zu verhindern. Die geringere Belastung des KDCs beruht darauf, dass es sich bei den Delegation Tokens nicht

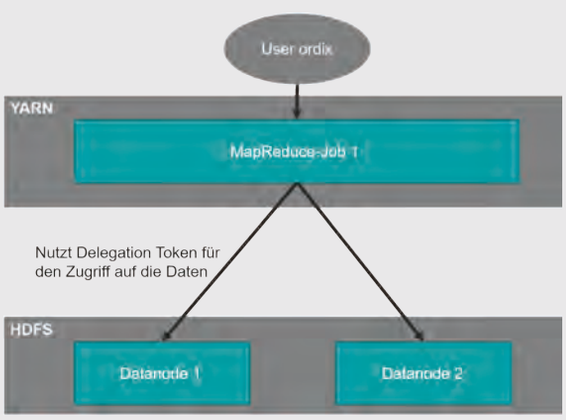

Abb. 2: Verwendung der Delegation Tokens

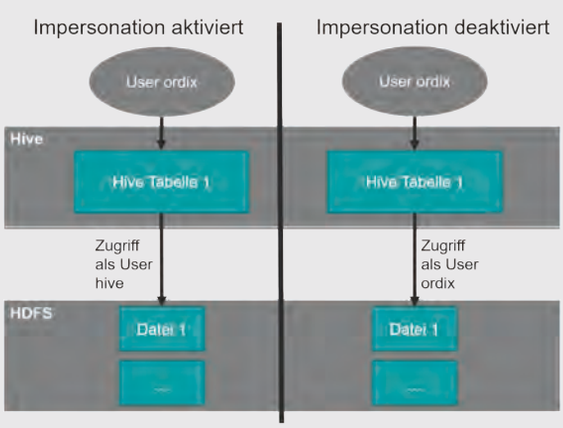

Abb. 3: Unterschiede zwischen den verschiedenen Modi von Hive

um eine Drei-Wege-Authentifizierung (Client, Server, unabhängige Stelle), sondern nur um eine Zwei-Wege-Authentifizierung zwischen dem Client und dem Server handelt. Dadurch wird sichergestellt, dass die Autorisierung des Users/Services immer nur beim Start des MapReduce-Jobs durchgeführt werden muss und nicht bei jedem Zugriff auf die HDFS-Daten bzw. bei der Kommunikation zwischen den beteiligten Komponenten. Gerade bei sehr großen Clustern (> 500 Knoten) würde eine Drei-Wege-Authentifizierung mittels Kerberos zu einer sehr hohen Last auf dem KDC führen. Da das KDC oftmals Bestandteil des unternehmensweiten Active Directorys ist, könnte dies zu einem Ausfall des Active Directorys führen und somit zu einer erheblichen Beeinträchtigung der Unternehmensabläufe.

Des Weiteren ist bei der Nutzung von Delegation Tokens zu beachten, dass diese standardmäßig alle 24 Stunden erneuert werden müssen und nach 7 Tagen auslaufen. Der Ablauf des Delegation Tokens kann gerade bei sehr langlaufenden Jobs zu Problemen führen. Dies muss bei der Entwicklung der Processing-Jobs beachtet werden. Sobald der Processing-Job abgeschlossen ist, wird das Delegation Token automatisch gelöscht und kann dadurch nicht durch einen Angreifer missbraucht werden. Dies ist sowohl nach einem erfolgreichen Abschluss des Jobs der Fall, als auch im Fehlerfall [Q7].

Das Prinzip der Delegation Tokens wird jedoch in einem kerberisierten Hadoop-Cluster nicht nur beim Zusammenspiel von Processing-Jobs mit dem HDFS eingesetzt. Ein weiteres Einsatzgebiet ist beispielsweise der Zugriff von Processing-Jobs auf verschlüsselte HDFS-Ordner. Hierbei kommt das Hadoop KMS Delegation Token ins Spiel. Sobald ein HDFS-Ordner mithilfe des Hadoop KMS verschlüsselt wurde, braucht ein Processing-Job sowohl ein HDFS-Delegation Token als auch ein KMS Delegation Token. Erst dann können die Daten innerhalb des Jobs verarbeitet werden. Weitere Informationen zu den Delegation Tokens sind unter [5] zu finden.

Hive

Apache Hive ist eine oft genutzte Komponente, die sehr eng mit den Hadoop-Kernkomponenten (HDFS, YARN, MapReduce) zusammenarbeitet. Dabei stellt Hive die Möglichkeiten eines Data Warehouse (z. B. die Abfrage von Tabellen mittels SQL-Statements) zur Verfügung. Hive kann zur Speicherung der Daten das HDFS oder andere Technologien wie z. B. HBase nutzen. Oftmals wird jedoch das HDFS genutzt. Durch diese enge Verbindung zwischen Hive und dem HDFS ist eine Rechtevergabe nicht trivial.

So muss bedacht werden, ob Impersonation über die Variable **`hive.server2.enable.doAs`** aktiviert wurde oder nicht. Falls Impersonation aktiviert ist, müssen für den zugreifenden User (in Abbildung 3 ist dies der User **`ordix`**) nur die entsprechenden Rechte in Hive gegeben werden. Dies passiert über den **`GRANT`**-Befehl. Im Folgenden ist ein Beispiel abgedruckt, das einem User die Möglichkeit

gibt, Daten aus einer Tabelle mittels des **SELECT**-Befehls auszulesen.

```
USE ordixdb;

GRANT select ON TABLE mitarbeiter TO USER ordix;

SHOW GRANT ON TABLE mitarbeiter;

OK

ordixdb  mitarbeiter     ordix  USER  SELECT
false  1517327304000  hive

Time taken: 0.089 seconds, Fetched: 1 row(s)
```

Zusätzlich muss in diesem Modus (Impersonation aktiviert) darauf geachtet werden, dass der User, unter dem der Hive-Prozess läuft (standardmäßig ist dies **hive**) im HDFS über die Dateisystemberechtigungen oder ACLs so berechtigt wird, dass er die gespeicherten Daten lesen und bearbeiten darf. Dies muss auch dann beachtet werden, wenn die Daten nicht im per **hive.metastore.warehouse.dir** festgelegten Pfad gespeichert werden. So ist es beispielsweise möglich, beim Anlegen von Schemas individuelle HDFS-Ordner anzugeben (siehe nächstes Listing).

```
CREATE SCHEMA ordixdb LOCATION '/hive-
datenbanken/';
```

Falls Impersonation deaktiviert wird, wird auch die Rechtevergabe noch einmal etwas komplexer. Ein User, der Daten aus einer Hive-Tabelle lesen möchte, braucht jetzt nicht nur die entsprechende Berechtigung in Hive, sondern auch noch zumindest die **Read**-Berechtigung im HDFS (siehe Abbildung 3). Falls mehrere User auf eine Tabelle zugreifen möchten, kann dies im HDFS nur noch über ACLs oder über User-Gruppen, die für jede Tabelle einzeln angelegt werden, gelöst werden. Als weitere Komplexität kommt dann auch noch die Möglichkeit zur Nutzung individueller Speicherorte für einzelne Schemas/Tabellen ins Spiel. Auch bei diesen Ordnern müssen dann immer die entsprechenden Berechtigungen gesetzt werden.

Eine weitere Möglichkeit, auf die mittels Hive im HDFS gespeicherten Daten zuzugreifen, besteht über das Auslesen der im Hive Metastore gespeicherten Metadaten. Weitere Information zu dem Hive Metastore sind unter [6] zu finden.

Ausblick

Wie das Beispiel Apache Hive schon gezeigt hat, macht die Nutzung von weiteren Komponenten aus dem Hadoop Ökosystem und vielen verschiedenen Usern (technische und persönliche) die Rechtevergabe noch komplexer. Dies ist ab einer bestimmten Anzahl an Benutzern irgendwann nicht mehr über die standardmäßigen Mechanismen (z. B. Dateisystemberechtigungen im HDFS) verwaltbar. Aus dieser Problematik haben sich zwei verschiedene Apache-Projekte entwickelt, die den Hadoop-Administrator bei der Rechtevergabe unterstützen. Dies sind Apache Sentry und Apache Ranger.

Ein weiterer Punkt, der nicht durch die Vergabe von Rechten mittels ACLs und der Aktivierung von Kerberos gelöst werden kann, ist der Zugriff des HDFS-Superusers auf alle im HDFS gespeicherten Daten [Q4]. Dies kann erst durch den zusätzlichen Einsatz des Hadoop KMS/Ranger KMS, zur Verschlüsselung des HDFS, verhindert werden.

Patrick Kramer
(info@ordix.de)

Links/Quellen

[1] ORDIX Seminar-Empfehlung: Big Data Seminare
https://seminare.ordix.de/seminare/big-data-und-data-warehouse.html

[2] ORDIX® news 3/2015 -
„Big Data: Informationen neu gelebt (Teil III): Apache Hadoop“
https://www.ordix.de/ordix-news-archiv/3-2015.html

[3] Enabling Kerberos Authentication for Hadoop
Using the Command Line
https://www.cloudera.com/documentation/enterprise/5-6-x/topics/cdh_sg_cdh5_hadoop_security.html

[4] ORDIX® news 4/2012 -
Kerberos (Teil I): Mit dem Höllenhund im Urlaub
https://www.ordix.de/ordix-news-archiv/4-2012.html

[5] Hadoop Delegation Tokens Explained
http://blog.cloudera.com/blog/2017/12/hadoop-delegation-tokens-explained/

[6] Apache Hive Homepage
https://hive.apache.org/

[7] Spark SQL, DataFrames and Datasets Guide - Hive Tables
https://spark.apache.org/docs/latest/sql-programming-guide.html#hive-tables

[8] ORDIX® news 4/2012 - NoSQL vs. SQL -
Hype oder echte Alternative? (Teil IV): HBase - Spaltenorientiert
https://www.ordix.de/ordix-news-archiv/2-2013.html

[Q1] White, Tom: „Hadoop: The Definitive Guide“;
2nd Edition; Sebastopol: O’Reilly Media, 2010

[Q2] FileSystem Shell
http://hadoop.apache.org/docs/r2.7.5/hadoop-project-dist/hadoop-common/FileSystemShell.html

[Q3] Enterprise Hadoop and the Journey to a Data Lake
https://de.hortonworks.com/blog/enterprise-hadoop-journey-data-lake/

[Q4] HDFS Permissions Guide
http://hadoop.apache.org/docs/r2.7.5/hadoop-project-dist/hadoop-hdfs/HdfsPermissionsGuide.html

[Q5] Offizielles HDFS-JIRA-Ticket
https://issues.apache.org/jira/browse/HDFS-7447

[Q6] Authorization and Authentication In Hadoop
http://blog.cloudera.com/blog/2012/03/authorization-and-authentication-in-hadoop/

[Q7] The Role of Delegation Tokens in Apache Hadoop Security
https://de.hortonworks.com/blog/the-role-of-delegation-tokens-in-apache-hadoop-security/

ORDIX® seminare

Seminarzentrum:
ORDIX AG
Kreuzberger Ring 13
65205 Wiesbaden
Tel.: 0611 77840-00

Online-Anmeldung, aktuelle Seminarinhalte und Termine unter:
https://seminare.ordix.de

Unser Seminarstandort ist Wiesbaden.

Die hier angegebenen Termine entsprechen dem ersten Seminartag.

Die Preise gelten pro Seminar pro Teilnehmer in Euro zzgl. ges. MwSt., Inhouse-Preise auf Anfrage.

Big Data und Data Warehouse

BIG Data				
DB-BIG-01	Big Data: Informationen neu gelebt	1 Tag	590,00 €	27.08. | 05.11.
DB-BIG-02	Big Data: Apache Hadoop Grundlagen	3 Tage	1.290,00 €	10.09. | 03.12.
Data Warehouse				
DB-DB-03	Data Warehouse Grundlagen	3 Tage	1.290,00 €	21.08. | 06.11.
DB-NSQL-01	Einführung in NoSQL-Datenbanken	2 Tage	1.090,00 €	13.09. | 06.12.

PostgreSQL

DB-PG-01	PostgreSQL Administration	5 Tag	2.150,00 €	30.07. | 24.09. | 03.12.

Oracle

Entwicklung				
DB-ORA-01	Oracle SQL	5 Tage	1.890,00 €	20.08. | 15.10.
DB-ORA-01A	Oracle SQL Power Workshop	3 Tage	1.290,00 €	17.09. | 26.11.
DB-ORA-02	Oracle Datenbankprogrammierung mit PL/SQL Grundlagen	5 Tage	1.890,00 €	03.09. | 19.11.
DB-ORA-34	Oracle Datenbankprogrammierung mit PL/SQL Aufbau	3 Tage	1.290,00 €	29.10. | 10.12.
DB-ORA-42	Oracle PL/SQL für Experten - Performance Analyse & Laufzeitopt.	3 Tage	1.290,00 €	08.10.
DB-ORA-53	Oracle Text	3 Tage	1.390,00 €	24.09. | 10.12.
DB-ORA-51	Oracle Spatial	3 Tage	1.290,00 €	03.09. | 19.11.
DB-ORA-46	Oracle APEX Anwendungsentwicklung Grundlagen	3 Tage	1.290,00 €	24.09. | 12.11.
DB-ORA-47	Oracle APEX Anwendungsentwicklung Aufbau	3 Tage	1.290,00 €	22.10. | 03.12.
Administration				
DB-ORA-03	Oracle Datenbankadministration Grundlagen	5 Tage	1.990,00 €	24.09. | 12.11.
DB-ORA-04	Oracle Datenbankadministration Aufbau	5 Tage	1.990,00 €	30.07. | 22.10. | 10.12.
DB-ORA-07	Oracle Tuning - Theorie und Interpretation von Reports	5 Tage	2.290,00 €	15.10. | 03.12.
DB-ORA-11	Oracle Troubleshooting Workshop	3 Tage	1.390,00 €	Termine auf Anfrage
DB-ORA-08	Oracle 12c Real Application Cluster (RAC) und Grid Infrastructure	5 Tage	2.290,00 €	10.09. | 26.11.
DB-ORA-49	Oracle 12c Neuheiten	5 Tage	2.090,00 €	25.06. | 06.08. | 08.10.
DB-ORA-49E	Oracle 12c Neuheiten für Entwickler	3 Tage	1.390,00 €	17.09. | 05.11.
DB-ORA-52W	Oracle Lizenz Workshop Webinar	1 Tage	590,00 €	Termine auf Anfrage
DB-ORA-33	Oracle Security	3 Tage	1.290,00 €	27.08. | 05.11.
DB-ORA-35	Oracle Cloud Control	3 Tage	1.290,00 €	10.09. | 29.10.
DB-ORA-55	Oracle ASM für Single Instance	3 Tage	1.390,00 €	06.08. | 12.11.
DB-ORA-56	Oracle Tenant Technologie (Multi/Single Tenant)	3 Tage	1.390,00 €	27.08. | 29.10.
DB-ORA-57	Single Sign On mit Oracle	3 Tage	1.390,00 €	13.08. | 22.10.
Backup und Recovery				
DB-ORA-32	Oracle Backup und Recovery mit RMAN	5 Tage	1.990,00 €	30.07. | 08.10.
DB-ORA-31	Oracle Data Guard	4 Tage	1.690,00 €	20.08. | 15.10.
MySQL				
DB-MY-01	MySQL Administration	3 Tage	1.290,00 €	25.09. | 27.11.

IBM Datenbanksysteme

Informix				
DB-INF-01	IBM Informix SQL	5 Tage	1.790,00 €	18.06. | 24.09.
DB-INF-02	IBM Informix Administration	5 Tage	1.990,00 €	22.10.
DB2				
DB-DB2-01	IBM Db2 für Linux/Unix/Windows SQL Grundlagen	5 Tage	1.890,00 €	17.09.
DB-DB2-02	IBM Db2 für Linux/Unix/Windows Administration	5 Tage	1.990,00 €	08.10.
DB-DB2-05	IBM Db2 für Linux/Unix/Windows Monitoring und Tuning	3 Tage	1.290,00 €	06.08. | 26.11.
DB-DB2-06	IBM Db2 für Linux/Unix/Windows Backup und Hochverfügbarkeit mit HADR	3 Tage	1.390,00 €	30.07. | 12.11.

Microsoft

Entwicklung				
MS-SQL-01	Querying Data with Transact-SQL	5 Tage	1.990,00 €	03.09. | 19.11.
MS-SQL-07	Updating Your Skills to Microsoft SQL Server 2016	5 Tage	1.990,00 €	27.08. | 29.10.
Administration				
MS-SQL-02	Administering a SQL Database Infrastructure	5 Tage	1.990,00 €	10.09. | 26.11.
MS-SQL-05	Implementing a SQL Data Warehouse	5 Tage	1.990,00 €	13.08. | 15.10.
MS-SQL-11	Microsoft SQL Server for Oracle DBAs	4 Tage	1.790,00 €	20.08. | 22.10.
MS-SQL-17W	Microsoft SQL Server 2017 Upgrade Webinar	1 Tag	99,00 €	auf Anfrage

Rechenzentrum

ANSIB-01	Konfigurationsmanagement mit Ansible	3 Tage	1.350,00 €	04.09. | 27.11.
E-Dock-01	Docker DevOps Workshop	1 Tag	405,00 €	29.06. | 03.09. | 26.11.
SM-NAG-01	Systemüberwachung mit Nagios - Workshop	3 Tage	1.190,00 €	15.10.

Web und Application-Server

INT-04	Apache HTTP Server Administration	3 Tage	1.190,00 €	03.09. | 19.11.
INT-07	Tomcat Konfiguration und Administration	3 Tage	1.290,00 €	17.09. | 26.11.
INT-08	WebSphere Application Server Installation und Administration	3 Tage	1.390,00 €	27.08. | 29.10.
INT-12	WildFly Application Server Administration	3 Tage	1.290,00 €	15.10. | 10.12.
DB-ORA-50	Oracle WebLogic Administration Grundlagen	3 Tage	1.390,00 €	10.09. | 05.11.

IT-Security

IT-SEC-01	IT-Sicherheit für Projektmanager und IT-Leiter - ein Überblick	3 Tage	1.590,00 €	30.07. | 24.09. | 03.12.
IT-SEC-02	Certified Information Systems Security Professional (CISSP)	5 Tage	4.240,00 €	27.08. | 22.10.
IT-SEC-03	Certified Information Security Manager (CISM)	3 Tage	1.820,00 €	03.12.
IT-SEC-04	Certified Information Systems Auditor (CISA)	4 Tage	2.130,00 €	06.08.
IT-SEC-05	Security Awareness für Mitarbeiter	1 Tage	1.000,00 €	10.08. | 06.12.

Projekt- und IT-Management

Klassisches Projektmanagement				
PM-01	IT-Projektmanagement praxisorientiert	3 Tage	1.690,00 €	06.08. | 08.10.
PRINCE-01	PRINCE2® Foundation	3 Tage	1.225,00 €	06.08.
PRINCE-02	PRINCE2® Practitioner	3 Tage	1.560,00 €	Termine auf Anfrage
PRINCE-03	PRINCE2® kompakt	5 Tage	2.595,00 €	03.09.
PM-06	Projekte souverän führen - Systemisches Projektmanagement	4 Tage	1.850,00 €	29.10.
PM-05	Projektcontrolling in der IT	2 Tage	1.090,00 €	09.08. | 11.10.
PM-07	Krisenmanagement in Projekten - Projektkrisen vorbeugen & meistern	2 Tage	1.100,00 €	14.06. | 27.09.
PM-14	Anforderungsmanagement in IT-Projekten	2 Tage	1.090,00 €	15.11.
PM-T-01	Testmanagement für agile und klassische Projekte	2 Tage	1.190,00 €	18.10.
Agiles Projektmanagement				
AGIL-01	Agil führen - Neue Konzepte für Ihre Führung im agilen Umfeld	3 Tage	1.190,00 €	03.12.
SCRUM-01	Agiles Projektmanagement mit Scrum - Mit agilem Vorgehen mehr ...	2 Tage	1.190,00 €	27.08. | 19.11.
SCRUM-02	Scrum Vorbereitung zur Zertifizierung - So einfach kann es klappen	1 Tage	690,00 €	29.08. | 21.11.
SCRUM-04	Scrum Product Owner - Produkte erfolgreich entwickeln	3 Tage	690,00 €	17.09.
KB-01	KANBAN in der IT - Prozesse & Projekte mit Hilfe von Kanban optimieren	2 Tage	1.190,00 €	30.08. | 22.11.
IT-Management, IT-Strategie und IT-Organisation				
PM-29	Systemische Führung - Führung unter Berücksichtigung aller Aspekte	3 Tage	1.650,00 €	13.08. | 26.11.
MGM-07	IT-Strategie - strategische IT-Planungen	3 Tage	1.650,00 €	10.12.
MGM-02	IT-Architekturen	3 Tage	1.590,00 €	22.10.
PM-10	IT-Controlling	3 Tage	1.590,00 €	03.09.
MGM-04	Geschäftsprozessmanagement (BPM)	3 Tage	1.590,00 €	20.08. | 15.10.
ITIL-01	ITIL® V3 Foundation	3 Tage	922,50 €	Termine auf Anfrage
ITIL-02	ITIL® V3 Practitioner	3 Tage	1.380,00 €	23.08.
ITIL-03	ITIL® V3 kompakt	3 Tage	2.250,00 €	20.08.
PM-28	IT-Organisation	3 Tage	1.650,00 €	10.09.
Kommunikation und Selbstmanagement				
K-03	Effektive Kommunikation in Projekten - Soft Skills Workshop	2 Tage	1.090,00 €	06.09. | 06.12.
K-04	Konfliktmanagement - Mehr Sicherheit in unsicheren Situationen	2 Tage	1.100,00 €	25.10.
K-05	Zeit- und Selbstmanagement - Mit weniger Stress mehr erreichen	2 Tage	1.090,00 €	08.11.
K-10	Coaching von IT Mitarbeitern - Führungskraft als Coach	3 Tage	1.090,00 €	17.12.
K-11	Kundenorientiertes Verhalten im Service	2 Tage	1.190,00 €	29.08. | 17.10.
K-12	Plötzlich IT-Führungskraft - Von Anfang an richtig führen	4 Tage	1.690,00 €	08.10.
K-20	Beratungs Know-How für IT-Experten - Kunden & Kollegen gut beraten	3 Tage	1.390,00 €	24.09.
MGM-03	IT-Management Einführung - Die IT nachhaltig zum Erfolg führen	3 Tage	1.590,00 €	05.11.
MGM-09	Leadership Skills - Reflektion des eigenen Führungsstils	2 Tage	1.190,00 €	27.08. | 15.10.
PM-CH-01	Change-Management in der IT - Veränderungen reibungslos einführen	3 Tage	1.590,00 €	12.11.

Storage

STORAGE01	Storage Grundlage	2 Tage	1.190,00 €	20.09. | 13.12.

Betriebssysteme & Monitoring

Unix/Linux				
BS-01	Unix/Linux Grundlagen für Einsteiger	5 Tage	1.690,00 €	17.09. | 26.11.
BS-02	Linux Systemadministration	5 Tage	1.690,00 €	06.08. | 15.10. | 03.12.
BS-25	Unix Power Workshop für den Datenbank- & Applikationsbetrieb	5 Tage	1.890,00 €	18.06. | 10.09. | 19.11.
BS-27	Neuerungen SUSE Linux Enterprise Server 12	3 Tage	1.290,00 €	08.10.
BS-09	Linux Hochverfügbarkeits-Cluster	5 Tage	1.890,00 €	03.09. | 10.12.
Solaris				
BS-03-11	Solaris 11 Systemadministration Grundlagen	5 Tage	1.990,00 €	27.08. | 22.10.
BS-04-11	Solaris 11 Systemadministration Aufbau	5 Tage	1.990,00 €	24.09. | 05.11.
BS-06-11	Solaris 11 für erfahrene Unix/Linux-Umsteiger	5 Tage	1.990,00 €	20.08. | 12.11.
BS-24	Solaris 11 Administration Neuheiten	3 Tage	1.290,00 €	30.07. | 29.10.
IBM AIX				
AIX-01	IBM AIX Systemadministration Grundlagen	5 Tage	1.990,00 €	03.09. | 19.11.
AIX-04	IBM AIX Systemadministration Power Workshop	3 Tage	1.290,00 €	10.09. | 26.11.
AIX-02	IBM AIX Installation, Backup und Recovery mit NIM	3 Tage	1.290,00 €	17.09. | 10.12.

Entwicklung

Allgemeines				
OO-01	Einführung in die objektorientierte Programmierung und UML	3 Tage	1.190,00 €	17.09.
E-SWA-01	Softwarearchitekturen	5 Tage	1.890,00 €	03.09. | 10.12.
Script-Sprachen				
P-PERL-01	Perl Programmierung Grundlagen	5 Tage	1.690,00 €	30.07. | 08.10.
P-PERL-02	Perl Programmierung Aufbau	5 Tage	1.690,00 €	13.08. | 22.10.
P-UNIX-01	Shell, Awk und Sed	5 Tage	1.690,00 €	27.08. | 12.11.
P-PYTH-01	Python Programmierung	4 Tage	1.690,00 €	24.09. | 03.12.
XML				
P-XML-01	XML Grundlagen	3 Tage	1.190,00 €	20.08. | 05.11.
Java				
P-JAVA-01	Java Programmierung Grundlagen	5 Tage	1.690,00 €	10.09. | 05.11.
P-JAVA-03	Java Programmierung Aufbau	5 Tage	1.690,00 €	24.09. | 19.11.
P-JEE-08	Java Performance Tuning	3 Tage	1.290,00 €	30.07. | 15.10. | 03.12.
P-JAVA-11	Java 8 Neuheiten	2 Tage	990,00 €	18.10.
Java EE				
P-JAVA-12	Java EE Power Workshop	5 Tage	1.890,00 €	26.11.
J-HIB-01	Java Persistence API mit Hibernate	5 Tage	1.690,00 €	12.11.
INT-05	Java Web Services	3 Tage	1.190,00 €	06.08. | 29.10.
P-JEE-06	Spring Power Workshop	5 Tage	1.590,00 €	13.08. | 10.12.
Web- und GUI-Entwicklung				
P-PHP-01	PHP Programmierung	5 Tage	1.690,00 €	30.07. | 12.11.
P-JEE-05	Rich Internet Application mit JSF und Primefaces	5 Tage	1.590,00 €	08.10. | 10.12.
P-JEE-05A	Webanwendungen mit JavaServer Faces (JSF)	5 Tage	1.590,00 €	20.08. | 22.10.
E-ANG-02	Webanwendungen mit Angular 2	3 Tage	1.590,00 €	24.10.
E-TYPSC-01	TypeScript Grundlagen	2 Tage	1.190,00 €	22.10.
Tools und Verfahren				
P-CI-01	Continuous Integration (CI) Workshop	3 Tage	1.190,00 €	25.07. | 05.09. | 26.11.

Oracle Engineered System

Exadata: Das Flaggschiff von Oracle?

Die Exadata ist ein „Oracle Engineered System“. Die Server-Hardware, das Storage und das Operation System (Oracle Linux) werden von Oracle geliefert. Diese Komponenten sind speziell auf die Oracle-Datenbank abgestimmt. In diesem Artikel beschreibe ich die Vorteile, die exklusiven Features der Exadata und gebe Einblicke aus einem erfolgreichen Exadata-Projekt.

Die Exadata kann in verschiedenen Ausbaustufen (Eighth, Quarter, Half und Full Rack) bestellt werden. Die Exadata X7-2 (2-Socket-Variante pro Datenbank-Server) ist seit Oktober 2017 verfügbar. Die Tabelle 1 zeigt die Basiskonfigurationen der Exadata X7-2. Eine Exadata X7-8 (8-Socket-Variante pro Datenbank-Server) steht ebenfalls zur Auswahl.

Die Anzahl der Datenbank-Server ist bei einem Eighth-Rack auf zwei beschränkt. Auch der Arbeitsspeicher darf nicht voll ausgeschöpft werden. Ab dem Quarter-Rack können alle verfügbaren Ressourcen verwendet werden. Außerdem können weitere Datenbank-Server hinzu konfiguriert werden.

Die Exadata kann in zwei unterschiedlichen Storage-Varianten ausgewählt werden. Die Variante HC (High Capacity) liefert eine hohe Kapazität an physikalischen Platten. Die zweite Variante ist EF (Extreme Flash). Hier besteht das Storage hauptsächlich aus Flash Storage.

Vorteile Exadata

Die Exadata liefert im Zusammenspiel mit der Oracle-Datenbank viele Vorteile und Alleinstellungsmerkmale gegenüber einem selbst konfigurierten Hardware-Stack.

- **Capacity-on-Demand**
  Mit der „Capacity-on-Demand“-Lizenzierung können nur die Cores freigeschaltet und mit Oracle lizenziert werden, die wirklich benötigt werden. Hierbei ist eine Minimum-Freischaltung pro Datenbank-Server zu beachten. Einmal freigeschaltete Cores können nicht wieder reduziert werden. Beim Eighth-Rack können maximal nur die Hälfte der physikalisch eingebauten Cores pro Datenbank-Server verwendet werden.
- **Smart Scan**
  Die Exadata verfügt im Zusammenspiel mit der Datenbank über eine intelligente Storage-Software. Im Storage werden Spalten und Ergebnisse bereits über Storage-Indizes vorgefiltert und damit deutlich weniger Daten in

die System Global Area (SGA) der Datenbank hochgeladen, als ohne den Smart Scan. Das System wird dadurch mit weniger I/O belastet. Und das Beste: es muss für diese Funktionalität nicht extra konfiguriert oder lizenziert werden.

- **Smart Flash Cache**
  Die Storage Server Software der Exadata cached häufig genutzte Datenbank-Blöcke automatisiert in den Flash Cache der Exadata. Die Oracle-Datenbank muss diese Blöcke also nicht mehr von den physikalischen Platten lesen, sondern liest direkt aus dem Smart Flash Cache.
- **InfiniBand**
  In der Exadata sind InfiniBand-Switche (40 Gb/sec) verbaut. Diese realisieren so die Anbindung an die Storage Server, aber auch die Server untereinander kommunizieren über dieses Netzwerk. Daher bietet sich der Einsatz des Real Application Cluster (RAC) an, weil der Interconnect über dieses schnelle Netzwerk realisiert werden kann.
- **Hybrid Columnar Compression**
  Bei dieser speziell für die Exadata entwickelten Komprimierungsart werden die Spalten-Daten in Compression Units abgelegt und spaltenweise komprimiert. Ein Pointer verweist auf die gleichen Werte. Bei dieser Komprimierungsart werden hohe Komprimierungsraten erreicht, ohne dass die Query-Performance sinkt, weil die Daten nicht extra dekomprimiert werden müssen. Die Vorteile liegen auf der Hand: Um diese komprimierten Daten zu lesen, werden weniger I/O-Operationen benötigt. Es wird eine Entlastung des gesamten Systems bis hin zu den Backup-Zeiten erreicht.

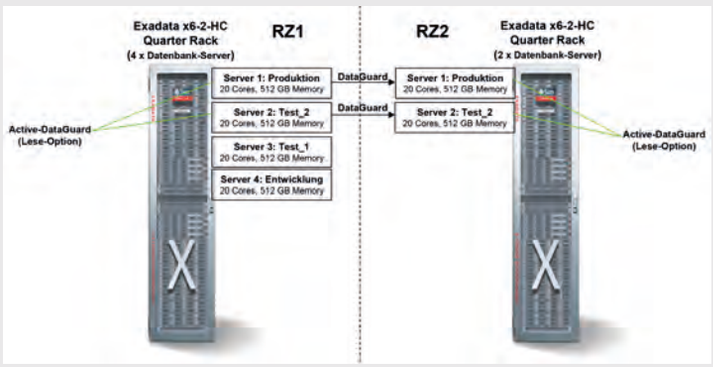

Abb. 1: Zielarchitektur

Exadata im Kundeneinsatz

In den folgenden Punkten berichte ich über ein aktuelles Exadata-Kundenprojekt. Alle Projektspezifikationen kann ich in diesem kurzen Artikel natürlich nicht aufführen, daher erläutere ich nur die wichtigsten Kernpunkte des Projektes.

- **Ausgangslage**
  Die Oracle-Datenbanken des Kunden müssen OLAP- und OLTP-Anforderungen gleichermaßen erfüllen. Ein geshartes SAN in einer virtuellen Umgebung sorgte bei den Lese- und Schreiboperationen zu sehr schwankender Performance und war das Hauptproblem des Kunden. Bei wichtigen OLAP-Operationen waren die Performance-Schwankungen von einer bis sieben

	X7-2 Eighth Rack	X7-2 Quarter Rack	X7-2 Half Rack	X7-2 Full Rack
Datenbank-Server (2x 24-core Xeon 8160 processors (2.1 GHz)	2 Server	2 Server	4 Server	8 Server
Gesamt-Cores der Datenbank-Server	48 Cores	96 Cores	192 Cores	384 Cores
Gesamt-Arbeitsspeicher der Datenbank-Server	384 GB (default) bis 1,5 TB	768 GB (default) bis 3 TB	1536 GB (default) bis 6 TB	3072 GB (default) bis 12 TB
Storage Server	3 Server	3 Server	7 Server	14 Server
HC (High Capacity) Storage Kapazität	180 TB disk, 38.4 TB flash	360 TB disk, 76.8 TB flash	840 TB disk, 179.2 TB flash	1,680 TB disk, 358.4 TB flash
EF (Extreme Flash) Storage Kapazität	76.8 TB flash	153.6 TB flash	358.4 TB flash	716.8 TB flash
HC (High Capacity) Disk Kapatität - ASM Normal Redundancy	68 TB	136 TB	341 TB	681 TB
EF (Extreme Flash) Disk Kapazität - ASM Normal Redundancy	28 TB	56 TB	141 TB	282 TB
HC (High Capacity) Disk Kapazität - ASM High Redundancy	53 TB	107 TB	250 TB	499 TB
EF (Extreme Flash) Disk Kapazität - ASM High Redundancy	22 TB	44 TB	103 TB	206 TB

Tabelle 1: Ausbaustufen Exadata

Stunden der Normalfall. Ebenfalls sollten weitere Datenbanken von Host-Systemen auf das Kundensystem nach und nach migriert werden.

- **Zielarchitektur**
  Die Entscheidung fiel auf das Exadata X6-2 HC Quarter-Rack und die Konfiguration mit zwei zusätzlichen Datenbank-Servern im Rechenzentrum 1 (RZ1). Die Exadata X6-2 ist die Vorgängerversion zur X7-2.

  Mit dieser Konfiguration konnte man die Entwicklungs-, Test_1-, Test_2- und die Produktions-Umgebung in separaten Netzen abbilden. Eine zweite Exadata, ebenfalls ein Quarter-Rack, wurde mit der Basis-Konfiguration mit zwei Datenbank-Servern im Rechenzentrum 2 (RZ2) eingerichtet. Als Disaster-Recovery-Lösung wurde eine synchrone DataGuard-Lösung eingesetzt. Mit der zusätzlichen Option Active-DataGuard wurden die Standby-Datenbanken in RZ2 für die Produktions- und die Test_2-Umgebung lesend geöffnet. Somit konnten Leseanwendungen auf der Standby-Seite arbeiten und Last von der Primary-Seite nehmen. Die Anzahl der Cores wurde in der Anfangskonfiguration mit 20 Cores pro Server limitiert. Die maximale Anzahl der Cores pro Server beträgt hier 44 (Exadata X6-2). Leider müssen die Cores auf allen Datenbank-Servern einer Exadata gleich konfiguriert werden, obwohl eigentlich in der Entwicklungsumgebung nicht so viele Cores benötigt werden. In Abbildung 1 sehen Sie diese Zielarchitektur.

  Diese Zielarchitektur kann auch mit weiteren Datenbank-Servern, z. B. mit weiteren Lesedatenbanken erweitert werden. Auch kann man hier in einer weiteren Ausbaustufe den Real Application Cluster (RAC) konfigurieren, um die Verfügbarkeit weiter zu steigern.

- **Ergebnisse**
  Auf der Exadata konnte man gerade bei den OLAP-Aufgaben durch Erhöhung der Parallelität bei langlaufenden Select-Anweisungen die Leistung der Exadata voll ausnutzen. Dadurch konnte die erwartete Performance und vor allem stabile Laufzeiten erreicht werden. Die OLAP-Aufgaben werden nun bis zu zehnmal schneller erledigt, trotz einer synchronen DataGuard-Konfiguration. Wie dieses Kundenprojekt zeigt, muss auf einer Exadata auch nicht immer RAC eingesetzt werden.

- Bei den OLTP-Abfragen konnte die Performance ebenfalls gesteigert werden, aber bei Weitem nicht so wie für die OLAP-Aufgaben.

Fazit

Die Exadata kann ihre Vorteile und Alleinstellungsmerkmale gerade für OLAP-Aufgaben voll ausspielen. Ebenfalls bietet die Exadata die Möglichkeit, die Ressourcen Schritt für Schritt auszubauen. Die Exadata kann somit auch als Konsolidierungsplattform genutzt werden. Die Verfügbarkeit der Oracle-Datenbanken kann mit dem Einsatz einer Real-Application-Cluster-(RAC)-Konfiguration weiter gesteigert werden.

Wir verfügen über umfangreiche Kenntnisse und Projekterfahrungen mit „Oracle Engineered Systemen“. Gerne beraten wir mit Ihnen gemeinsam eine neue Zielumgebung und ob ein bzw. welches „Oracle Engineered System“ für Ihr Unternehmen die richtige Wahl ist.

Michael Skowasch
(info@ordix.de)

Glossar

Oracle Engineered System
Ein System bestehend aus Hardware, Storage, Operation System und Datenbanksoftware komplett von Oracle.

InfiniBand
Ist eine Spezifikation einer Hardwareschnittstelle zur seriellen Hochgeschwindigkeitsübertragung auf kurzen Distanzen mit geringer Latenz (40 GB/sec). Sie wird bevorzugt in Rechenzentren verwendet, beispielsweise für die Verbindungen der Server in Computerclustern untereinander und zur Verbindung zwischen Servern und benachbarten Massenspeichersystemen wie Storage Area Networks (SAN).

Online-Transaction-Processing (OLTP)
Online-Transaktionsverarbeitung, auch Echtzeit-Transaktionsverarbeitung, bezeichnet ein Benutzungsparadigma von Datenbanksystemen und Geschäftsanwendungen, bei dem die Verarbeitung von Transaktionen direkt und prompt, also ohne nennenswerte Zeitverzögerung, stattfindet.

Online Analytical Processing (OLAP)
OLAP wird neben dem Data-Mining zu den Methoden der analytischen Informationssysteme gezählt. OLAP wird weiterhin den hypothesengestützten Analysemethoden zugeordnet.

DataGuard
Oracle Data Guard ist eine Erweiterung des Datenbankmanagementsystems, die den Betrieb einer Standby-Datenbank erlaubt. Mittels Data Guard ist es möglich, sämtliche Datenänderungen an eine räumlich getrennte Datenbank zu senden.

Real Application Cluster (RAC)
Eine Hochverfügbarkeitslösung von Oracle. Oracle RAC ermöglicht Ausfallsicherheit, indem mehrere Knoten eines Rechnerverbundes auf dieselbe Datenbank zugreifen und für Clientrechner Datenbankdienste zur Verfügung stellen.

Active-DataGuard
Lizenzpflichtige Option, die Standby-Datenbank kann lesend geöffnet werden und wird dennoch von der Primary-Datenbank aktualisiert

Automatic Storage Management (ASM)
Volume Manager von Oracle

SAN
Storage Area Network

Bildnachweis

Neuerungen in der Oracle Database 12.2 (Teil II)

Real Application Clusters

Im zweiten Artikel der Reihe stellen wir Ihnen die wesentlichen Neuerungen von Oracle 12.2 im Bereich Real Application Clusters vor. Wie auch in den vergangenen Releases hat Oracle die Architektur des Real Application Clusters weiterentwickelt und stellt ein neues Cluster-Konzept mit dem Namen „Oracle Cluster Domain" vor. Die Oracle Cluster Domain kann als eine Art private Datenbank-Cloud verstanden werden. In diesem Release wurden auch die Installation der Grid Infrastructure vereinfacht und viele weitere Neuerungen implementiert.

Oracle Cluster Domain

Die Oracle Cluster Domain kann einfach administriert und zentral verwaltet werden. In der Oracle Cluster Domain stellt der Oracle Domain Services Cluster (DSC) zentrale Services für die sogenannten Oracle Member Cluster bereit. Wurde die Basis, ein DSC zur Verfügung gestellt, können unterschiedliche Oracle Member Cluster erstellt werden. Alle Oracle Member Cluster verwenden die zentralen Services des DSC, z. B. den ASM Service. Weiterhin kann auch ein Standalone Cluster für die Installation und Konfiguration eines Real Application Clusters (RAC) ausgewählt werden. Diese Installationsart wird auch weiterhin den Standard für kleinere RAC-Umgebungen mit wenigen Cluster darstellen (siehe Abbildung 1).

Domain Service Cluster (DSC) Komponenten

Ein Domain Service Cluster (DSC) ist das Herz der Oracle Cluster Domain und bildet die Voraussetzung für die Installation und Konfiguration von Oracle Member Cluster. Innerhalb der Oracle Cluster Domain ist das Grid Infrastructure Management Repository (GIMR) das zentrale Repository für die Speicherung von Diagnostic- und Health-Informationen für alle Member Cluster. Hier wird die Management Datenbank MGMTDB zentral vorgehalten. Auf die Informationen des GIMR greifen das Autonomous Health Framework (AHF), der Trace File Analyzer (TFA) und das Rapid Home Provisioning (RHP) zu.

Der IO-Service wird während der DSC-Installation konfiguriert. Der IO-Service stellt indirekt den Shared Storage für die Member Cluster über ein privates ASM Storage-Netzwerk bereit. Der wesentliche Vorteil ist, dass nun sehr einfach Oracle Member Cluster erstellt werden können, ohne ASM separat zu konfigurieren. Neuer Storage wird also im DSC konfiguriert und nicht auf dem Database Member Cluster.

Im DSC stellt Oracle optional einen Rapid Home Provisioning Server (RHP) bereit. Über diesen Server können die Oracle-Datenbanken der Database Member Cluster und der Grid Infrastructure Software Stack gepatcht werden. Der RHP-Server standardisiert somit den Deployment–Prozess über die gesamte Oracle Cluster Domain.

Database Member Cluster

Ein Oracle Member Cluster kann für den Oracle Real Applikation Cluster (Oracle RAC) oder Oracle RAC One Node eingesetzt werden. Dieser Oracle Member Cluster registriert sich mit dem Management Repository Service und nutzt den zentralen TFA-Service. Database Member Cluster können mit lokalem ASM Storage oder mit dem Oracle ASM Storage Management Service des Domain Service Clusters konfiguriert werden. Ein Database Member Cluster muss immer das Grid Management Repository (GIMR) des Domain Service Cluster verwenden. In einem Database Member Cluster können nur Datenbanken > 12.1 erstellt werden.

Application Member Cluster

Innerhalb der Oracle Cluster Domain können normale Anwendungen hochverfügbar integriert werden. Ein Application Member Cluster benötigt eine Verbindung zu den Oracle Cluster Domain Services. Ebenfalls benötigt dieser Oracle Member keinen direkten Zugriff auf das Shared Storage, sondern greift remote auf das ASM-Storage über den IO-Service zu.

Oracle Flex Cluster

Bereits in Oracle 12cR1 führte Oracle eine weitere Variante für den Aufbau eines Clusters ein, das Flex Cluster. Im Oracle Flex Cluster werden zwei Typen von Knoten definiert. Zum einen die sogenannten Hub Nodes, Knoten mit Zugriff auf den Shared Storage, und zum anderen die sogenannten Leaf Nodes, ohne Zugriff auf den Shared

Storage. Diese Variante eines Oracle Clusters als Plattform für flexible Cluster für verschiedene Applikationen neben den RAC-Datenbanken ist ab Oracle 12.2 die Standardkonfiguration, d. h. jedes Standalone Cluster wird als Flex Cluster mit Flex ASM (ebenfalls in Oracle 12cR1 eingeführt) angelegt (siehe hierzu Abbildung 2).

Angedacht ist eine Verteilung der Anwendungen im Cluster, wobei Datenbanken auf den Hub Nodes laufen, andere Applikationen wie Application-Server auf den Leaf Nodes. Auf den Leaf Nodes stehen dann Mechanismen wie

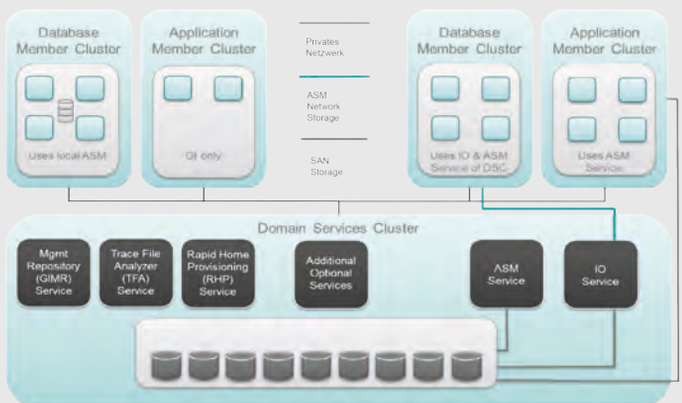

Abb. 1: Oracle Cluster Domain

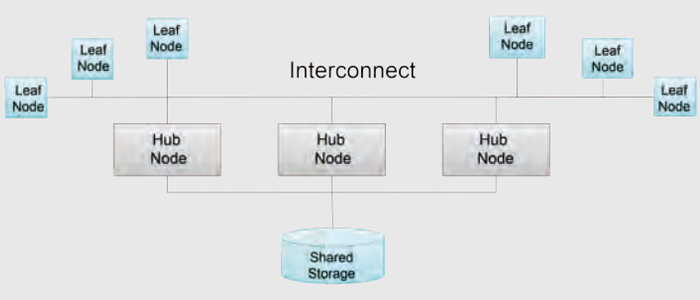

Abb. 2: Oracle Flex Cluster

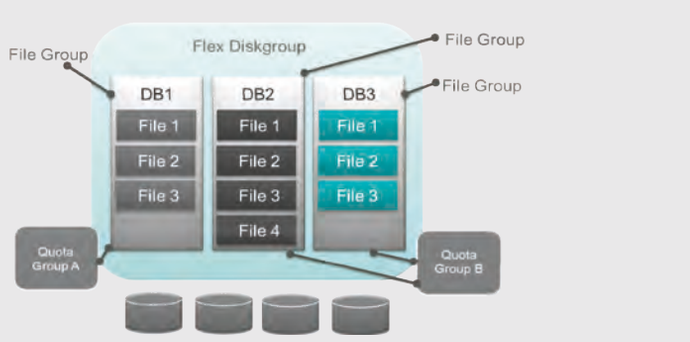

Abb. 3: ASM Flex Diskgroup

Ressourcenverwaltung, automatischer Start bzw. Restart von Ressourcen und Failover von Ressourcen auf andere Knoten zur Verfügung. Selbstverständlich können Standalone Cluster ganz klassisch nur bestehend aus Hub Nodes, d. h. für RAC- oder RAC-One-Node-Datenbanken, angelegt werden. Die Anzahl der Hub Nodes ist nun auf 64 Knoten beschränkt und theoretisch können beliebig viele Leaf Nodes an das Cluster gehängt werden.

Reader Nodes

In Oracle 12.2. ist es nun möglich, Read-Only-Workloads auf den Leaf Nodes in einer Flex-Cluster-Architektur laufen zu lassen, diese nennen sich Reader Nodes. Man kann maximal 64 Reader Nodes pro Hub Node erstellen. Auf den Reader Nodes kann ein lokales Temp-Tablespace erstellt werden und somit die Performance auf den Reader Nodes weiter erhöht werden. Außerdem können auf den Reader Nodes massiv parallele Abfragen ausgeführt werden. Voraussetzung für die Erstellung von Reader Nodes sind Policy-Managed-Datenbanken, also keine „gepinnten" Admin-Managed-Datenbanken.

Grid Infrastructure Management Repository (GIMR)

In Oracle 12cR1 führte Oracle als zentrales Repository für die Daten des Cluster Health Monitors (ora.crf) eine neue Datenbank MGMTDB ein. Die Datenbank lag in der gleichen Lokation/Diskgruppe wie die Oracle Cluster Registry (OCR) und die Voting Disks. Die maximale Größe der Datenbank soll auf 2 GB beschränkt sein. In Oracle 12.2 kann nun eine separate Diskgruppe mit einer Kapazität von mindestens 37,6 GB in der Installationsart Standalone Cluster verwendet werden, alternativ zentral gespeichert im Domain Services Cluster für einen Database Member Cluster. Mit Oracle 12.2 wird deutlich mehr ASM-Kapazität für das Management Repository benötigt – dies muss bei der Planung neuer Cluster-Umgebungen berücksichtigt werden.

Installation und weitere Neuerungen

Die Installation der Grid Infrastructure wurde mit Oracle 12.2 vereinfacht und erfolgt nun als Image-based-Installation in drei Schritten:

- Download der Image-Zip-Dateien
- Entpacken in das **`ORACLE_HOME`** auf dem ersten Knoten im Cluster
- Ausführen **`gridSetup.sh`** vom ersten Knoten

In der Funktionsweise der Grid Infrastructure wurden noch weitere Neuerungen implementiert. Unter dem Schlagwort Server Weight-based Node Eviction können nun über den neuen Parameter **`CSS_CRITICAL`** ein Knoten oder Ressourcen als kritisch eingestuft werden. Bei einem Heartbeat-Problem im RAC-Cluster können Knoten nicht

mehr miteinander kommunizieren. Ein Knoten oder eine Knotengruppe muss gestoppt werden. Bei einem Split Brain-Problem überlebt dann der Knoten oder die Knotengruppe mit der kritischen Ressource.

Automatic Storage Management (ASM)

Auch im Bereich Automatic Storage Management (ASM) gab es einige nennenswerte Änderungen. In früheren Versionen konnten in der Enterprise Edition die zentralen Cluster-Dateien Oracle Cluster Registry (OCR) und Voting Disk auf nicht-ASM-Storage gespeichert werden. Mit Oracle 12.2 müssen nun in allen Editionen die OCR und Voting Disk in einer ASM-Diskgruppe gespeichert werden.

FLEX Diskgruppe

Traditionell können ASM-Diskgruppen EXTERNAL (ungespiegelt), NORMAL (2-fach) oder HIGH (3-fach) redundant angelegt werden. In den Diskgruppen gibt es keine Unterscheidung pro Datenbank. Eine Diskgruppe definierte den Grad der Spiegelung und alle Dateien werden innerhalb der Diskgruppe gleich behandelt.

Mit Oracle 12.2 können Diskgruppen nun datenbankorientiert angelegt werden. Oracle hat einen neuen Diskgruppen-Typ FLEX Diskgroup eingeführt. Eine FLEX-Diskgruppe hat mindestens drei Fehlergruppen und kann auch aus einer NORMAL oder HIGH redundanten Diskgruppe in der RESTRICTED Mount-Phase konvertiert werden (siehe Abbildung 3).

In einer FLEX Diskgroup können nun pro Datenbank die Datenbankdateien verwaltet werden. In einer File Group können Dateien pro Datenbank gruppiert werden. Mit einer Quota Group kann der maximal belegbare Speicherplatz festgelegt werden. Dazu wird eine File Group in eine Quota Group verschoben. Das Vergeben von Quotas ermöglicht es, große konsolidierte Diskgruppen auf Datenbankebene zu verwalten.

Pro File Group ist auch eine individuelle Redundanz einstellbar: HIGH, MIRROR und UNPROTECED. Damit ist es möglich, „unwichtigeren“ Datenbanken eine geringere Redundanz zu konfigurieren. In einer FLEX-Diskgruppe gibt nicht mehr die Diskgruppe, sondern die File Group die Redundanz vor. Dieser neue Aspekt ist in den Betriebskonzepten zu vermerken. Auf jeden Fall werden die Spalten REQUIRED_MIRROR_FREE_MB und USABLE_FILE_MB der View **`v$asm_diskgroup`** für FLEX-Diskgruppen nicht mehr aktualisiert. Auch dies muss in den Betriebskonzepten berücksichtigt werden. Historisch wurden Fehlergruppen zum Schutz vor Hardwarefehlern eingeführt. Mit einer FLEX-Diskgruppe kann die ASM-Redundanz auch für das schnelle Erstellen von Datenbank-Klonen verwendet werden. Dazu wird einfach eine redundante Kopie der File-Extents abgeteilt.

EXTENDED Diskgruppe

Mit Oracle 12.2 wird auch die ASM-Funktionalität für Extended RAC-Konfigurationen, d. h. über zwei Rechenzentren, erweitert. Bisher konnte eine Diskgruppe maximal zwei Fehlergruppen, jeweils eine pro Rechenzentrum, haben. Damit ergab sich ein guter Schutz gegen den Ausfall eines Rechenzentrums. Eine EXTENDED-Diskgruppe ist eine Erweiterung der FLEX Diskgruppe und erlaubt mehrere Fehlergruppen innerhalb einer Site (eines Rechenzentrums). Mit einer EXTENDED-Diskgruppe ist also eine Spiegelung innerhalb eines Rechenzentrums sowie über Rechenzentren hinweg möglich. Zusätzlich unterstützt eine EXTENDED-Diskgruppe nun ASM HIGH Redundanz, d. h. über drei Rechenzentren hinweg.

Fazit

Zusammenfassend kann gesagt werden, dass Oracle 12.2 einige interessante Erweiterungen im Bereich der Real Application Clusters hervorgebracht hat. Oracle hat ein komplett neues Cluster-Konzept mit dem Namen Oracle Cluster Domain vorgestellt. Sie kann als eine Art private Datenbank-Cloud verstanden werden und vereinfacht die Verwaltung großer Cluster-Umgebungen mit mehreren RAC-Umgebungen. Ein Oracle 12.2 RAC kann aber auch ganz klassisch als Standalone Cluster konfiguriert werden. Die in 12cR1 eingeführten Features Flex Cluster und Flex ASM sind nun die Standardkonfigurationen.

Auch im Bereich Automatic Storage Management gibt es Erweiterungen, die die Verwaltung großer Diskgruppen auf Datenbankebene ermöglichen sowie die Verfügbarkeit in Extended RAC-Konfigurationen erhöhen. Mit einer EXTENDED-Diskgruppe können nun auch Extended-RAC-Konfigurationen auf Exadata innerhalb der Limitierungen von InfiniBand implementiert werden.

Die in diesem Artikel vorgestellten Neuerungen der Grid Infrastructure behandeln nur die wesentlichen Aspekte der Oracle 12.2- Erweiterungen. Falls wir Ihr Interesse geweckt haben, dann empfehlen wir Ihnen die Seminare Oracle 12c Real Application Cluster (RAC) und Grid Infrastructure und Oracle ASM für Single Instance.

Thilo Fleischhauer
(info@ordix.de)

Microsoft SharePoint (Teil I):

Plattform für das Informationsmanagement in Projekten

Das Potenzial von SharePoint als Kollaborationsplattform wird in Unternehmen oft nur unzureichend ausgeschöpft. Dabei bieten bereits Bordmittel, insbesondere im Zusammenspiel mit Office 365 vielfältige Kollaborationsmöglichkeiten – gerade auch für die Projektarbeit.

Was sind die Anforderungen?

Projektarbeit – insbesondere, wenn nach klassischen Projektmanagement-Methoden gearbeitet wird – stellt vielfältige Aufgaben/Anforderungen an die Kollaboration in Unternehmen:

- Alle am Projekt Beteiligten müssen stets umfassend über den aktuellen Stand informiert sein, wichtige Termine müssen bekannt sein, alle Beteiligten müssen mit den aktuellsten Dokumenten arbeiten, wesentliche Informationen müssen schnell über geeignete Suchwerkzeuge gefunden werden können. Die Kommunikation muss schnell und unkompliziert und doch verbindlich erfolgen.
- Unter Umständen müssen externe Partner mit in die Kommunikation einbezogen werden.
- Die Zugriffsrechte müssen über Rollenkonzepte geregelt werden können. Gegebenenfalls ist es auch erforderlich, dass Zugriffe direkt durch den Projektverantwortlichen eingerichtet werden können.
- Die im Projekt verwendeten Dokumente müssen zentral abgelegt werden können, idealerweise in einem Dokumentenmanagement-System.
- Zur Vereinfachung der Kommunikation stehen Werkzeuge zum direkten Informationsaustausch außerhalb des Mailsystems zur Verfügung, wie Chats oder Videokonferenzsysteme.
- Im Idealfall stehen die Projektinformationen auch für den Zugriff über mobile Endgeräte zur Verfügung.

Diese exemplarische Auflistung möglicher Anforderungen macht deutlich, dass das Informationsmanagement im Projekt eine Herausforderung darstellt, die in der Praxis meist durch heterogenen Einsatz von Tools und Applikationen gelöst wird. Diese Heterogenität ist in vielerlei Hinsicht nicht produktivitätsfördernd und steht vielfach sogar im Widerspruch zu Anforderungen an die Datensicherheit und

regulatorischen Anforderungen (zum Beispiel Revisionsanforderungen, Aufbewahrungsfristen etc.).

Das Hauptwerkzeug in der Projektarbeit ist nach wie vor das E-Mail-System, was in den meisten Fällen eine Flut von Mails zur Folge hat, in der nicht selten aufgrund der fehlenden Priorisierung Informationen übersehen werden.

Werden in Unternehmen Vorgehensmodelle für die Projektarbeit definiert und Vorlagen für die im Projektverlauf zu erstellenden Dokumente erstellt, so geschieht die Arbeit mit diesen Dokumenten nicht selten in mehr oder weniger komplexen Ordnerstrukturen auf dem Dateisystem. Die Dokumente werden dann an einen (wechselnden) Verteiler geschickt, bevor sie in verschiedenen Versionsständen auf dem Filesystem abgelegt werden.

Diese Vorgehensweise hat Vorteile (zum Beispiel eine strukturierte Ablage), aber auch einige gravierende Nachteile: So umfassen Mailverteiler oft nicht alle Beteiligten. Was den Umgang mit Dokumenten anbelangt, geht schnell der Überblick über den aktuellen Stand verloren (z.B. welche Dokumente zuletzt geändert wurden). Zudem können Sicherheitskonzepte auf Fileserver-Ebene durch den nicht beschränkten Mailversand wieder ausgehebelt werden.

Die Suche nach Lösungsmöglichkeiten führt zu folgendem Dilemma: Werden viele Vorgaben gemacht oder ist die gewählte Plattform zu unflexibel hinsichtlich möglicher Verfahrensweisen, wirkt das Korsett schnell zu sperrig und unterbindet Spontanität und Kreativität. Wird ohne Vorgaben mit Chats oder privaten Social-Media-Kanälen kommuniziert, verliert die Kommunikation u.U. schnell die erforderliche Verbindlichkeit, wird unkontrollierbar und nicht mehr nachvollziehbar gestreut und verletzt schnell sämtliche Vorgaben hinsichtlich Datensicherheit und Aufbewahrungsfristen.

Wie lässt sich dieses Dilemma lösen? Was bieten die Hersteller an Lösungsmöglichkeiten an? Nimmt man das Beispiel Microsoft, das im Fokus dieses Artikels stehen soll, so scheint die Tendenz dahin zu gehen, über die etablierten Basistechnologien Exchange/Outlook und SharePoint hinaus eine breite Palette an Tools und dedizierten Werkzeugen anzubieten, die in der Office-365-Familie zusammengeführt und je nach Kundenanforderung explizit kombiniert werden können.

SharePoint, das mit der Version 2016 von Microsoft neu platziert wurde, spielt auch in der aktuellen Microsoft-Strategie eine zentrale Rolle und stellt über On-Premise- und Hybrid-Szenarien hinaus auch in der Cloud-Version ein Bindeglied zwischen den spezialisierten Einzelanwendungen der Office-365-Familie dar. Einige der grundlegenden Konzepte und Technologien dieser Plattform – auch im Zusammenspiel mit weiteren Office 365-Funktionalitäten – die zur Unterstützung des Informationsmanagements in der Projektarbeit gewinnbringend genutzt werden können, sollen im Folgenden vorgestellt werden. Angesichts der Vielzahl von Möglichkeiten, die diese äußerst vielfältige Plattform bietet, kann dabei nur eine Auswahl getroffen werden.

Wie kann SharePoint die Zusammenarbeit im Projekt unterstützen?

Als webbasierte Kollaborationsplattform bietet SharePoint die Möglichkeit des plattformübergreifenden Zugriffs. Daten bzw. Inhalte können entweder direkt in Form von Listen, Blogs oder Wiki-Seiten erfasst werden oder Dokumente können in Bibliotheken strukturiert abgelegt werden. Dabei können gerade die Möglichkeiten des Dokumentenmanagements – z.B. die „Anreicherung“ mit Metadaten, die Versionsverwaltung, aber auch die Sicherheitsfunktionen wie DRM – für das Informationsmanagement im Projekt sehr gut genutzt werden. Hinzu kommt die sehr leistungsfähige Suchfunktionalität, die auch sehr gezielt in Webparts genutzt werden kann, wenn mit Metadaten und Inhaltstypen gearbeitet wird. SharePoint bietet zudem die Möglichkeit, sofern erforderlich, sehr granular die Zugriffsrechte auf die einzelnen Inhalte zu steuern. Wichtig dabei ist, dass auch die Suche dem Security-Trimming unterliegt, d.h. der Benutzer bekommt als Suchergebnisse nur die Inhalte angezeigt, für die er auch berechtigt ist.

Mit der Version 2016 und insbesondere in der SharePoint-Online-Version wird die Möglichkeit des Zugriffs über mobile Endgeräte stark vorangetrieben. So stehen in der Onlineversion neue, responsive Templates für Seiten, Bibliotheken und Listen zur Verfügung (auch „Modern Experience“ genannt), die mit dem nächsten Feature Release auch in der On-Premise-Variante bereitgestellt werden. Für den mobilen Zugriff stehen zudem Apps für die gängigen mobilen Betriebssysteme zur Verfügung.

Im Folgenden werden zunächst die Möglichkeiten aufgezeigt, die SharePoint in allen Varianten mitbringt und die auch in einer reinen On-Premise-Umgebung genutzt werden können. Dies wird ergänzt durch die Darstellung der Möglichkeiten, die sich im Rahmen eines Microsoft-Office-365-Abonnements zusätzlich noch im Bereich Collaboration ergeben.

Die Möglichkeiten von SharePoint und Office 365

Was macht SharePoint nun zu einer geeigneten Plattform? Aus der Perspektive der Anforderungen an das Informationsmanagement in Projekten betrachtet, können folgende Aspekte/Funktionen/Features von SharePoint angeführt werden.

Listen und Wiki-Seiten

SharePoint bietet vielfältige Möglichkeiten, Inhalte zu erfassen – in Wiki-Seiten und einem der Kernelemente von SharePoint, den Listen in den verschiedensten Ausprägungen, für die zahlreiche vorgefertigte Templates angeboten werden.

Bei „Listen“ handelt es sich in SharePoint um einen etwas weiter gefassten Begriff, neben der flexibel mit Spalten konfigurierbaren „benutzerdefinierten Liste“ fallen hierunter auch zahlreiche bereits vorkonfigurierte Templates wie z. B. Kalender, Aufgabenlisten und Ankündigungen.

Eine insbesondere im Projektmanagement sehr sinnvoll zu nutzende Listenvorlage ist die Aufgabenliste (siehe Abbildung 1).

Die eigentliche Aufgabenliste wird im Beispiel ergänzt durch eine visuelle Darstellung auf einer Zeitleiste. Dabei können wie in MS Project Vorgänge hierarchisch strukturiert werden, Vorgänger definiert und Meilensteine festgelegt werden. Standardmäßig steht auch eine Ansicht als Gantt-Diagramm zur Verfügung, die auch direkt bearbeitet werden kann (siehe Abbildung 2).

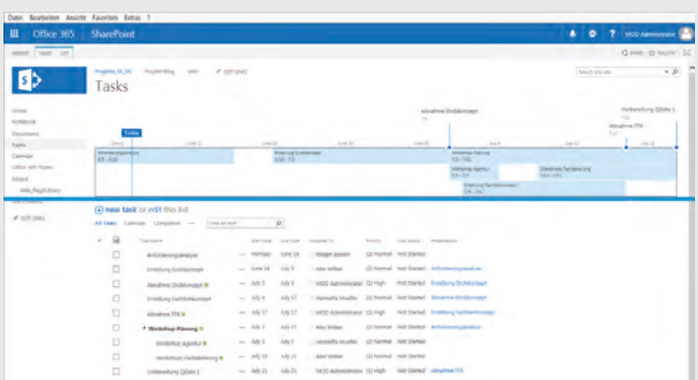

Abb. 1: Aufgabenliste mit Zeitleiste

Abb. 2: Gantt-Ansicht einer Aufgabenliste

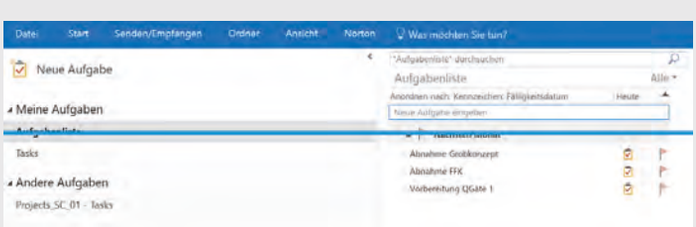

Abb.3: Eigene Aufgaben in Outlook

Zwar verfügt diese App nicht über die umfangreichen Berechnungsfunktionen von MS Project und es kann keine Ressourcenplanung vorgenommen werden. Für die Zeitplanung und als Überblick über die Projektphasen und den aktuellen Stand bietet sie jedoch eine anschauliche und vor allem leicht zu bedienende Option.

Wird die Task-Liste über den bereitgestellten Konnektor zudem mit Outlook verknüpft, kann hierdurch gerade in kleineren Teams mit einfachen Mitteln ein zentrales Aufgabenmanagement konfiguriert werden, das die jeweiligen Verantwortlichen auch außerhalb der SharePoint-Oberfläche über anstehende Aufgaben auf dem Laufenden hält (siehe Abbildung 3).

Dokumentenbibliotheken

Neben den Listen bilden die Dokumentenbibliotheken ein weiteres Kernelement von SharePoint. Bibliotheken bieten die Möglichkeit, Dokumente zu verwalten, wobei zahlreiche Funktionen eines Dokumentenmanagement-Systems zur Verfügung stehen, so z. B. die Versionierung, Verschlagwortung, Informationsverwaltungsrichtlinien und DRM. Bei versehentlichem Löschen von Dokumenten kann die Wiederherstellung aus dem SharePoint-Papierkorb durch den Benutzer selbst erfolgen.

Insbesondere die Versionierungsfunktion kann in der Projektarbeit wertvolle Dienste leisten, indem gewährleistet wird, dass alle Projektmitarbeiter mit dem aktuellsten Stand der Dokumente arbeiten. Die Versions-Historie zeigt zudem transparent die durchgeführten Änderungen auf, im Notfall kann auch mit einfachen Mitteln auf eine frühere Version gewechselt werden.

Um den jeweiligen Spezifika der abzulegenden Items gerecht zu werden, bietet SharePoint auch Templates für weitere Dokumentenarten, so zum Beispiel Bild- und Videobibliotheken.

Eine weitere für die Projektarbeit unter Umständen hilfreiche Funktion stellt die Option dar, Bibliotheken als Mailziel zu konfigurieren, um auf diese Weise Dokumente direkt in SharePoint abzulegen.

Seitentemplates – Cockpits für den Projektarbeitsbereich

Bei SharePoint-Seiten kann grundsätzlich zwischen Wiki-Seiten, auf denen direkt Inhalt erfasst und bereitgestellt werden kann, und Webpart-Seiten unterschieden werden. Webparts bzw. seit SharePoint 2013 auch „Apps“ bieten die Möglichkeit, den Inhalt von Listen oder Bibliotheken in definierten Bereichen auf einer Website darzustellen. Dabei kann der Inhalt über Ansichten gefiltert und struk-

turiert werden, bzw. können über suchbasierte Webparts aktuelle Stände von Inhalten zum Zeitpunkt des Seitenaufrufs dargestellt werden.

Je nach den (projekt-)spezifischen Anforderungen können die zuvor beschriebenen „Bausteine“ (Listen, Bibliotheken) mittels Webparts (bzw. Apps seit SharePoint 2013) auf den Teamsites zusammengestellt und visualisiert werden. Auch hierfür gibt es zahlreiche Templates, die nach Bedarf angepasst werden können. Auf diese Weise können „Cockpits“ für den schnellen Überblick, z. B. für den aktuellen Projektstand erstellt werden.

So kann eine Projekteinstiegsseite beispielsweise Überblicksinformationen, Statusanzeigen, eine Timeline, News etc. bereitstellen.

Folgendes Beispiel zeigt eine Projekteinstiegsseite basierend auf dem Projektwebsite-Template, das um Webparts ergänzt wurde (siehe Abbildung 4).

An zentraler Stelle befindet sich hier die Darstellung der Zeitleiste des Aufgaben-Webparts, das um Informationen zu anstehenden Fälligkeitsterminen und bevorstehende Termine (hier „2 upcoming“) erweitert wurde.

Bei den hinzugefügten Webparts handelt es sich zum einen um gefilterte Ansichten von Listen, die sich auf dieser Website befinden („Meine Tasks“). Zum anderen wurden suchbasierte Webparts konfiguriert („Die nächsten Termine“, „Zuletzt geänderte Dokumente“), in denen auch weitere Datenquellen innerhalb der Seitenstruktur abgefragt werden.

Bei Bedarf können durch die Suchfunktion ab SharePoint 2013 auch Sitecollection-übergreifend Inhalte abgefragt und angezeigt werden, so dass auch projektübergreifende relevante Informationen angezeigt werden können.

Für den schnellen Überblick über die diversen Status innerhalb eines Projekts können auch Dashboards über Statusindikatoren und Berichtsbibliotheken erstellt und eingeblendet werden (hier im Beispiel nicht dargestellt).

Suche

SharePoint bietet zudem eine sehr leistungsfähige Suchfunktion, die nicht nur in der „klassischen“ Ausprägung mit Sucheingabefeld und Ergebnisseiten zur Verfügung steht (und sehr granular und bedarfsgerecht angepasst werden kann), sondern die auch im Hintergrund in Webparts und suchgetriebenen Applikationen genutzt werden kann.

Gesucht werden kann nach Inhalten und Personen, eine gerade im Projektumfeld oft benötigte Funktionalität, wenn Ansprechpartner oder Verantwortliche ermittelt werden müssen. Aufgrund der Leistungsfähigkeit und vielfältigen Anpassungsmöglichkeit der SharePoint-Suche wird die Darstellung in einem eigenen Artikel in dieser Serie erfolgen. Dabei wird es auch darum gehen, wie die SharePoint-Suche im Zusammenspiel mit Delve führt.

Vernetzung mit anderen Office-Produkten

SharePoint als Teil der Microsoft Office-Produktfamilie kann über vorgefertigte Konnektoren mit anderen Office-Produkten verbunden werden, wodurch beispielsweise Projektaufgaben auch in Outlook angezeigt und bearbeitet werden können (s.o.). Darüber hinaus besteht z.B. die Möglichkeit, SharePoint-Listen nach Excel zu exportieren und dort weiterzubearbeiten, gleiches gilt für MS Access.

Wird als Client-Betriebssystem mindestens Windows 7 eingesetzt, so besteht die Möglichkeit, Dokumente per Drag & Drop in Bibliotheken hochzuladen. Bei Verwendung des Internet-Explorers kann zudem im Windows-Explorer eine Web-DAV-Verbindung zur SharePoint-Bibliothek eingerichtet werden, wodurch die Bibliothek als Pfad im Explorer zur Verfügung steht – eine sehr bequeme, aber auch mit großen Nachteilen (keine direkte Metadaten-Eingabe, Aushebelung der SharePoint-Papierkorbfunktion) verbundene Ablageoption.

Über lokal installierte Office-Produkte hinaus sind SharePoint-Teamrooms auch zentrale Bestandteile neuer Produkte der Office-365-Familie wie Microsoft Planner oder Teams, die die Palette der Kollaborationsmöglichkeiten im Projekt ebenfalls erweitern können.

Rollen- und Rechtestruktur

Alle Inhalte, die über SharePoint angeboten werden, werden innerhalb eines definierten Security-Kontextes angeboten, wodurch Benutzer nur die Informationen angezeigt bekommen, für die sie auch berechtigt sind. Dies gilt für Seiten- und Bibliotheken-Inhalte und für Suchergebnisse gleichermaßen. Für den Zugriff von externen Partnern können bei der On-Premise-Version auch andere Authentifizierungsanbieter angebunden werden, sofern in diesem Fall nicht ohnehin die Onlineversion von SharePoint

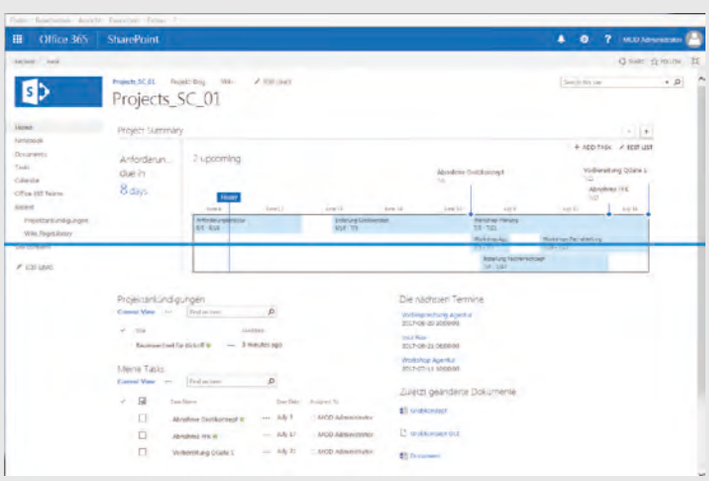

Abb.4: Beispiel für eine Projekt-Einstiegsseite

bevorzugt wird. Je nach Anforderung können sehr vielschichtige und granulare Berechtigungen konfiguriert sowie Rollenkonzepte über Seitenstrukturen und Zugriffsgruppen abgebildet werden.

Wo eine differenzierte und transparente Rechtestruktur erforderlich ist, empfiehlt es sich, mit vielen Sitecollections zu arbeiten, die jeweils einen eigenen Security-Kontext darstellen. Auf diese Weise kann die Rechtevergabe an die Siteowner delegiert werden – eine Rolle, die auch der Projektleiter ausüben kann und der so Zugriffsrechte auch ohne Mitwirkung der IT-Abteilung vergeben kann.

Auch wenn eine Rechtesteuerung sehr granular bis herunter auf Item-Ebene möglich ist, so zeigt die Erfahrung in Kundenprojekten, dass dies in den wenigsten Fällen sinnvoll ist. Empfehlenswert ist vielmehr die Erarbeitung eines passenden Rollen- und Rechtekonzepts und die Definition einer Governance, die noch den erforderlichen kreativitätsfördernden Spielraum lässt, die andererseits aber auch den Security-Erfordernissen genügt.

Wo Vertraulichkeit von Informationen nicht höchste Priorität hat, sondern der spontane Austausch zwischen Projektmitarbeitern (bzw. das spontane Hinzuziehen von Mitarbeitern/Experten auch außerhalb des Projekts) über verschiedene Kanäle (Chat, Videokonferenz, Blog) im Vordergrund steht, kann dieser Rahmen dem einzelnen Mitarbeiter auch viel Spielraum zum Teilen von Informationen lassen.

Hier spielen insbesondere die Office-365-Tools wie „Teams“ oder „Yammer“ ihre Stärken aus. Auf diese Weise spielt sich die Kommunikation immer noch in einem für das Projekt vorgesehenen Rahmen ab (nicht über private WhatsApp-Gruppen etc.) und umfasst einen definierten Teilnehmerkreis (Mitarbeiter mit Firmen-Accounts). Zudem besteht die Möglichkeit der Verknüpfung mit einem SharePoint-Teamroom mit restriktiverer Rechtestruktur für die Ablage oder Pflege vertraulicher Dokumente oder Informationen.

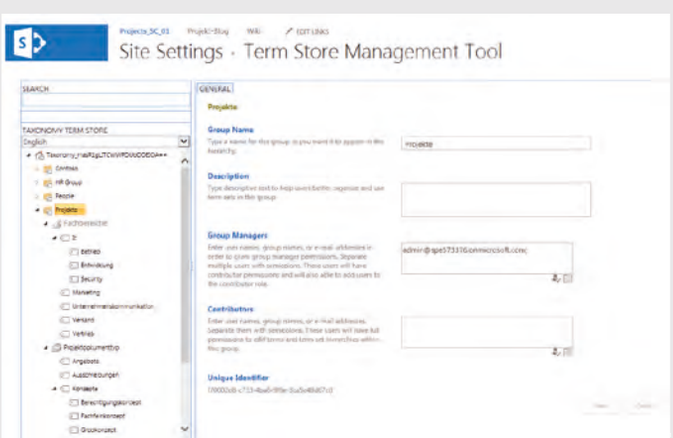

Abb 5: Beispiel für eine Taxonomie

Die Möglichkeiten, die SharePoint auch in Verbindung mit anderen Office-365-Tools für die Kommunikation im Projekt bietet, werden in einem weiteren Artikel dieser Serie ausführlicher beleuchtet.

Personalisierte Bereiche – MySite / Profil in Delve

SharePoint-Benutzern kann auch die Möglichkeit geboten werden, persönliche Bereiche (MySites) einzurichten. Neben Informationen bzgl. der Organisations- oder Abteilungszugehörigkeit, die meist aus dem Active Directory übernommen werden, kann es ermöglicht werden, dass auch persönliche Fähigkeiten, Qualifikationen, aktuelle Projekte etc. durch die Benutzer selbst in ihrem Profil gepflegt und – je nach Firmenphilosophie – auch Social-Media-Features genutzt werden. Indem diese Informationen auch in der Suche angesprochen werden können, bieten sich hier Möglichkeiten zur Suche nach Experten oder Ansprechpartnern.

Funktionen für das Wissensmanagement und die Strukturierung der Daten

Aus anderem Blickwinkel betrachtet, können neben den beschriebenen SharePoint-Tools und Templates auch die folgenden funktionalen Bausteine und Konzepte von SharePoint effektiv in der Projektarbeit eingesetzt werden: Für das Wissensmanagement und die Strukturierung der Daten können in SharePoint die Funktionen des Taggings und das Konzept der Inhaltstypen genutzt werden. Über Managed Metadata können Taxonomien (vorgegeben und fixiert) und Folksonomien (offen, durch Benutzer erstellt) konfiguriert werden, die dann als Metadaten Dokumenten hinzugefügt und auch in der Navigation verwendet werden können (siehe Abbildung 5).

Über Inhaltstypen können SharePoint-Inhalte bereits im Vorfeld mit einem Set an Metadaten versehen werden, die bei der Erstellung z. B. eines Dokuments oder einer Dokumentenmappe hinzugefügt werden. Die Besonderheit liegt darin, dass über Inhaltstypen erstellte Inhalte gezielt von Workflows angesprochen und über die Suche in Webparts oder Apps herausgefiltert und dargestellt oder weiterverarbeitet werden können (u.a. in Informationsverwaltungsrichtlinien).

Ausblick: SharePoint-Projekte sind Organisationsprojekte

Bei all den technischen Möglichkeiten, die SharePoint in den verschiedenen Versionen bietet, muss allerdings immer im Fokus bleiben, dass es sich bei SharePoint-Projekten in erster Linie um Organisationsprojekte handelt. SharePoint kann seine Möglichkeiten nur ausspielen, wenn zuvor die Zielsetzung klar definiert wird: So müssen

die erforderlichen/gewünschten Zugriffsmöglichkeiten und Zugriffsrechte geklärt werden (nur interne Zugriffe, oder auch durch externe Mitarbeiter? Ist ein Rollenkonzept erforderlich?).

Von entscheidender Bedeutung ist, sich bereits im Vorfeld Gedanken zu machen über benötigte Inhaltstypen sowie die erforderlichen Metadaten, über die die Inhalte klassifiziert werden können (teilweise automatisiert im Hintergrund über Inhaltstypen oder manuell durch den Benutzer beim Hochladen). Eine Metadaten-Struktur kann dann in vielfacher Hinsicht genutzt werden, für die Navigation, für die Suche – insbesondere für die Konfiguration von Refinern für Suchergebnisseiten oder auch suchbasierte Apps.

Erst durch Klärung dieser grundsätzlichen Fragen ergibt sich der Mehrwert dieser Kollaborationslösung. Den Benutzern einfach einen Teamraum mit einer Bibliothek zur Verfügung zu stellen, wird zwangsläufig zu Akzeptanzproblemen führen, indem dies nur als kompliziertere Form der Dateiablage empfunden wird – ein Grund, der viele SharePoint-Projekte in der Vergangenheit scheitern ließ.

Strukturierte Planung einer SharePoint- bzw. auch einer Office-365-Umgebung schließt kreativen Umgang mit den technischen Möglichkeiten keineswegs aus. Sie schafft jedoch einen Rahmen, durch den nicht nur ein funktionaler Mehrwert entsteht, sondern durch den auch regulatorischen Anforderungen im Umgang mit Projektdokumenten und -informationen genügt werden kann.

Adi Schmid
(info@ordix.de)

Glossar

Inhaltstypen
Ein Inhaltstyp ist eine wiederverwendbare Sammlung von Metadaten (Spalten), Workflows, Verhaltensweisen und anderen Einstellungen für eine Kategorie von Elementen oder Dokumenten in einer SharePoint-Liste oder Dokumentenbibliothek. Mithilfe von Inhaltstypen können die Einstellungen für eine Kategorie von Informationen zentral und wiederverwendbar verwaltet werden.

Responsive Webdesign
Beim Responsive Webdesign handelt es sich um ein gestalterisches und technisches Paradigma zur Erstellung von Websites, so dass diese auf Eigenschaften des jeweils benutzten Endgeräts, vor allem Smartphones und Tabletcomputer, reagieren können.

Taxonomie
Eine Taxonomie ist eine hierarchische Klassifizierung von Wörtern, Bezeichnungen oder Ausdrücken, die nach Ähnlichkeit geordnet in Gruppen organisiert werden. Eine Taxonomie kann von einer oder mehreren Personen definiert und zentral verwaltet werden. […] Taxonomien sind hilfreich, denn sie ermöglichen eine logische, hierarchische Struktur von Metadaten, mit der Informationen konsistent klassifiziert werden können.

Folksonomie
Eine Folksonomie ist eine Klassifizierung, die sich ergibt, wenn Websitebenutzer dem Inhalt einer Website gemeinsam Wörter, Bezeichnungen oder Ausdrücke zuordnen. Die Verwendung eine Folksonomie für Metadaten kann nützlich sein, da dadurch die Möglichkeit besteht, Wissen und Kompetenzen von Websitebenutzern und Inhaltserstellern gemeinsam zu nutzen. Hiermit kann die Klassifizierung von Inhalten abhängig von Geschäftsanforderungen und Benutzerinteressen weiterentwickelt werden.

Bildnachweis

OpenVAS

Schwachstellenanalyse und -management

Die IT-Sicherheit in Unternehmen ist insbesondere dann wichtig, wenn ein Cyber-Angriff zu hohen Umsatzeinbußen führen kann. Es liegt daher im Interesse der Unternehmen Schwachstellen – und damit Angriffe – erfolgreich vorzubeugen. Ein Hilfsmittel für diese Aufgabe ist das Schwachstellenmanagement-Tool OpenVAS.

Ein fiktiver Angriff

Das fiktive Unternehmen Web AG hat vor wenigen Tagen eine neue Version ihrer Website vor Dutzenden Kunden vorgestellt und auf vielen Kanälen bekannt gegeben. Kurz nach der Veröffentlichung kommt es zu einem Angriff, der dafür sorgt, dass die beworbene Website stundenlang nicht zu erreichen ist. Die Kunden sind verärgert und auch viele potenzielle Neukunden haben gar nicht erst die Möglichkeit, die Web AG als neuen Geschäftspartner kennenzulernen. Später stellt sich heraus, dass der Angreifer durch eine schon länger bekannte Schwachstelle in einer veralteten Version des beliebten Apache Webservers einen sogenannten Distributed-Denial-of-Service-(DDoS)-Angriff durchführen konnte. Hätte dieser verheerende Angriff vermieden werden können?

Täglich werden bis zu 300 neue bekannte Schwachstellen als Common Vulnerability & Exploit (CVE) veröffentlicht, die alle relevanten Informationen präsentieren. Es stellt jedoch eine Mammutaufgabe dar, händisch jedes CVE darauf zu prüfen, ob eine installierte Version betroffen ist und herauszufinden, wie das Problem behoben werden kann. Selbst für einen einzigen Server ist ein Administrator auf diese Weise Tage mit der Absicherung des Servers beschäftigt.

Im Verlauf dieses Artikels werden wir die Web AG bei der Einrichtung des OpenVAS begleiten sowie dabei die Funktionsweise und Fähigkeiten des Systems aufzeigen.

Erkennen von Schwachstellen

Schwachstellen in Systemen können durch gezieltes Testen erkannt werden. Die Grundlage für diese Tests bildet meist eine Checkliste, die vorgibt, welche Tests ausgeführt werden sollen. Handelt es sich um einen Webserver,

werden die entsprechenden Tests ausgewählt. Im Falle der Web AG wird beispielsweise getestet, ob eine veraltete Version des Apache Webservers installiert ist. Ist dies der Fall, wird das Ergebnis vermerkt und mit dem nächsten Test fortgefahren.

Allerdings steigt mit der Anzahl der installierten Anwendungen auch die Zahl der Fragen, die geklärt werden müssen. Ist beispielsweise auch ein Mail Client eingerichtet, muss dieser ebenso überprüft werden. Zusätzlich müssen die Ergebnisse der Tests noch ausgewertet und die entdeckten Sicherheitslücken geschlossen werden.

Viele dieser Sicherheitschecks laufen folglich immer gleich ab, indem eine Schwachstelle mittels dieser gezielten Tests überprüft wird. Vorgegangen wird hierbei immer auf dieselbe Art, was die Frage aufwirft, ob dies automatisiert werden kann.

Das Open Vulnerability Assessment System

Das Open Vulnerability Assessment System (OpenVAS), ein quelloffener Schwachstellenscanner (siehe Abbildung 1), ist in der Lage, diese eingangs erwähnten Tests automatisiert auszuführen. Ein Framework unterschiedlicher Dienste und Werkzeuge, die die Grundlage des Systems bilden, helfen dem System in der aktuellen Versionsnummer 9 vom 8. März 2017, eine Vielzahl von Schwachstellen zu erkennen (vgl. [3]). Es wird von der Greenbone Networks GmbH mit Sitz in Osnabrück entwickelt und vertrieben.

Herzstück des OpenVAS ist der „OpenVAS Scanner“, der die Rolle des virtuellen Penetration Testers übernimmt und die eigentlichen Tests ausführt, indem er die bereitgestellten Werkzeuge, wie beispielsweise den Portscanner nmap nutzt. Kommuniziert wird im gesamten OpenVAS verschlüsselt. Informationen darüber, wie eine Probe auf etwaige Schwachstellen ausgeführt werden soll, liefert ein Feed, der die sogenannten Network Vulnerability Tests (NVTs) zur Verfügung stellt. Dieser Feed ist in einer kostenfreien Variante als Greenbone Community Feed (GCF) und in einer kommerziellen Variante als Greenbone Security Feed (GSF) erhältlich. Der GSF ist konzipiert für das Unternehmensumfeld und bietet spezielle unternehmensrelevante Sicherheitstests, die nicht im Community Feed enthalten sind. Beide Feeds erhalten tägliche Updates.

Funktionsweise des Systems

Den Hauptbestandteil des Systems bilden die NVTs, die Anweisungen für das Erkennen von Sicherheitslücken bereitstellen. Zu Beginn eines jeden Tests wird ein Profil des Systems erstellt. Anhand der erstellten Profile werden Tests ausgewählt, die für das System infrage kommen. Beispielsweise wird ein System nur dann auf fehlende Windows-Updates untersucht, wenn es sich um ein Windows-System handelt. Die Tests werden dann durch den OpenVAS-Scanner effizient anhand der erstellten Profile ausgeführt. Die Profile und Ergebnisse der Tests werden im Hintergrund durch den OpenVAS-Manager abgelegt und verwaltet. Dies geschieht in einer SQLite-Datenbank (vgl. [2]).

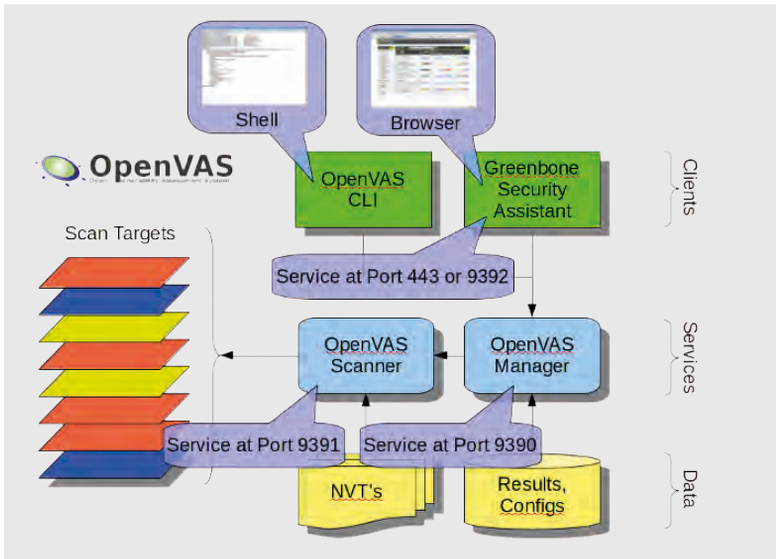

Abb. 1: Architektur des OpenVAS (Quelle: www.openvas.org)

Es ist allerdings auch möglich, den Umfang der Tests vorher zu definieren. Auf diese Weise kann ein System gezielt auf die Umsetzung des durch das BSI vorgeschriebene IT-Grundschutz-Konzept, geprüft werden. NVTs werden durch das OpenVAS nicht automatisch aktualisiert. Es wird jedoch ein Programm bereitgestellt, über das sich die NVTs aktualisieren lassen. Dieses sollte automatisiert, z. B. über Cron aufgerufen werden, um immer auf dem neusten Stand zu sein (vgl. [5]).

Sicherheitslücken werden durch das OpenVAS in sogenannte Severity Classes eingeteilt, die es dem Nutzer ermöglichen, schnell die Schwere einer Lücke zu erkennen. Dazu werden verschiedene Systeme verwendet, die meist nach Low, Medium und High kategorisieren. Allerdings ist es auch möglich, ein anderes System, wie beispielsweise die vom BSI herausgegebene Schwachstellenampel, zu verwenden (vgl. [6]).

Die Greenbone Networks GmbH

Obwohl das OpenVAS quelloffen und damit kostenfrei nutzbar ist, bietet die Greenbone Networks GmbH eine kommerzielle Variante des Tools an. Ein zahlender Kunde erhält dann Zugriff auf den GSF und wie bei den meisten solcher Produkte vor allem Unterstützung durch den Support der Firma.

Zusätzlich bietet das Unternehmen Server an, auf denen das Greenbone OS mit dem OpenVAS-Scanner bereits vorinstalliert ist. Je nach Preiskategorie können so bis zu 50.000 IP-Adressen gescannt werden. Weiterhin werden auch sogenannte virtuelle Appliances zur Verfügung gestellt, die in einem begrenzten Umfang arbeiten.
Für weitere Informationen zu den Produkten:
https://www.greenbone.net/produktvergleich/

Abb. 2: Dashboard des OpenVAS

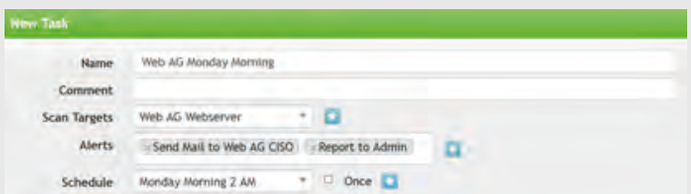

Abb. 3: Scheduling im OpenVAS

Installation des OpenVAS

Das zu Beginn beschriebene Unternehmen Web AG hat aus den Fehlern gelernt und das OpenVAS – damit wir die Installation hier beschreiben können – selbst installiert. Die einfachste Methode, um das System zu installieren, stellen die vorkompilierten Versionen von Drittanbietern dar, die eine schnelle und komfortable Installation ermöglichen. Die Installation läuft dann entsprechend leicht über die Paketverwaltung der entsprechenden Plattform ab. Da es sich hierbei jedoch um Drittanbieter handelt, wird empfohlen, nach der Installation ein Skript auszuführen, welches die korrekte Installation prüft. Das Skript ist unter dem folgenden Link abrufbar: https://svn.wald.intevation.org/svn/openvas/trunk/tools/openvas-check-setup

Sollten Sie während der Installation Fragen oder Probleme haben, hilft der Mailverteiler des OpenVAS (siehe [4]) sehr weiter. Motivierte Anwender und oft auch die Entwickler hinter dem OpenVAS nehmen sich Zeit und beantworten Fragen und geben Hinweise.

Vorbereitung für die Nutzung des OpenVAS

Nachdem das OpenVAS erfolgreich installiert wurde, sind einige Vorüberlegungen notwendig, um das OpenVAS sinnvoll in die Struktur des Unternehmens einzugliedern. Dabei müssen die folgenden Fragen geklärt werden, bevor mit der Einrichtung des Systems begonnen werden kann:

- Welche Systeme benötigen eine Untersuchung?
- Was soll geprüft werden?
- Wie oft sollen die Systeme geprüft werden?
- Was geschieht mit den Ergebnissen?
- Wer soll informiert werden?

Die Web AG hat sich entschieden, nur die Webserver zu untersuchen. Es soll die Umsetzung des vom BSI empfohlenen IT-Grundschutz, geprüft werden. Dies soll jeden Montag um 2 Uhr mit einem umfassenden Scan sowie jeden Tag um 3 Uhr mit einem kleinen Scan geschehen. Legt das OpenVAS kritische Schwachstellen offen, wird der Administrator des Servers informiert (E-Mail) und kann bei Arbeitsbeginn mit der Behebung der Schwachstellen beginnen.

Einrichtung des OpenVAS

Persönliche Erfahrungen haben gezeigt, dass Bedienung und Konfiguration des OpenVAS über die Weboberfläche die komfortabelere Methode gegenüber jener per Kommandozeile darstellt. Der folgende Abschnitt stellt die wichtigsten Komponenten der Weboberfläche vor und gibt einen Einblick in die Vielzahl der Konfigurationsmöglichkeiten des OpenVAS über den Webbrowser.

Zu sehen ist in Abbildung 2 das sogenannte Dashboard, das den Nutzer begrüßt und einige wichtige Informationen zu den bisher ausgeführten Scans und Schwachstellen gibt. Besonders interessant ist die Hosts Topology, die dem Nutzer mittels gefärbter Punkte eine Übersicht über die bereits gescannten Netzwerke mit ihren Systemen anzeigt. Hier ist ersichtlich, wie die Server und PCs in Relation stehen und wie stark oder schwach sie gefährdet sind. Beispielsweise ist ein Knoten besonders gefährdet, wenn er sich in einem Netz mit mehreren rot gefärbten, also unsicheren Hosts befindet. Der Sicherheitsbeauftragte kann sich auf diese Weise schnell einen Überblick über die Infrastruktur und die aktuelle Lage verschaffen.

Automatisierung

Der spannendste Punkt im Einsatz des OpenVAS ist die Automatisierung der Scans. Das System bietet viele verschiedene Möglichkeiten, um ein Netzwerk auf regelmäßiger Basis zu überprüfen. Die Web AG hat sich entschieden, ihre Webserver jeden Montag um 2 Uhr und jeden anderen Tag um 3 Uhr zu prüfen. Dabei wird montags ein vollumfassender Scan ausgeführt, während an anderen Tagen nur ein kurzer Scan durchgeführt wird. Abbildung 3 zeigt, wie eine solche Aufgabe (Task) im OpenVAS eingestellt werden kann.

Im Menü kann festgelegt werden, wann der Task ausgeführt werden soll. Dabei lässt sich einstellen in welchem Intervall der Scan durchlaufen wird. Eine Stunde ist die kleinste Einheit. Die Benachrichtigungen (Alerts) sind in diesem Fall „Send Mail to Web AG CISO“ und „Report to Admin“. Die Alerts lassen sich so konfigurieren, dass nur dann eine Mail an den CISO (Chief Information Security Officer) versandt wird, wenn eine Schwachstelle einen bestimmten Gefährdungsgrad darstellt.

Auswahl der Scans

Die Web AG möchte ihre Webserver nur auf die Einhaltung des IT-Grundschutzes prüfen, da die Nichteinhaltung finanzielle Konsequenzen nach sich ziehen kann. Montagmorgens soll der umfassende Scan ausgeführt werden, während an allen anderen Tagen nur die Einhaltung des IT-Grundschutzes geprüft werden soll.

Die Abbildung 4 zeigt dazu das Konfigurieren einer Scan Config, die vorgibt, wie ein bestimmter Scan ablaufen soll. Die grundlegenden Optionen des IT-Grundschutzes wurden hier ausgewählt. Bei Erstellung eines neuen Tasks kann die erstellte Scan Config dann ausgewählt werden, um die gewählten Tests auszuführen.

Ergebnisse

Die Ergebnisse der Scans werden in Berichten (Reports) zusammengefasst und zusätzlich in Diagrammen visualisiert. Die Web AG hat die Scans für einige Wochen regelmäßig ausgeführt (siehe Abbildung 5). Deutlich zu erkennen ist hierbei der fallende Verlauf des Diagramms in der Mitte, der auf einen Rückgang der Anzahl der gefundenen Schwachstellen hindeutet.

Fazit

Nach dem Einsatz des OpenVAS bei der Web AG konnten einige Schwachstellen gefunden und geschlossen werden. Durch die erstellten automatischen Scans wird die Sicherheit auch in Zukunft gewährleistet, solange die Lücken entsprechend zeitnah geschlossen werden. Mithilfe der automatischen Benachrichtigungen an die zuständigen Administratoren geht keine Zeit verloren, sodass die Sicherheitsrisiken schnell auf ein Minimum reduziert werden können.

Die Web AG hat sich weiterhin für den Kauf eines Produktes der Greenbone Networks GmbH entschieden, um den Greenbone Security Feed zu erhalten. Denn für kleinere Unternehmen, die bereits versierte Sicherheitsspezialisten im Haus beschäftigen und die nötigen personellen Ressourcen zur Verfügung stellen können, steht der Anschaffung des kostenlosen OpenVAS, nichts im Wege. Jedoch benötigt die Web AG auch einen umfassenden Support und möchte dabei auf einen externen Dienstleister vertrauen. Denn größere Unternehmen, die viel Wert auf die Sicherheit ihrer Infrastruktur legen (müssen) und keine personellen Ressourcen für den Betrieb des Systems zur Verfügung stellen können, sollten sich die Produkte der Greenbone Networks GmbH einmal näher anschauen.

Nils von Nethen
(info@ordix.de)

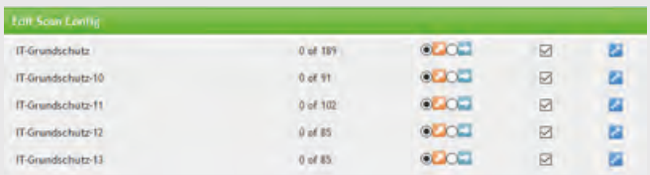

Abb. 4: Editieren der Scan Config im OpenVAS.

Abb. 5: Ergebniss der Scans

Links/Quellen

[1] Webseite von OpenVAS: http://www.openvas.org/

[2] Webseite der Greenbone GmbH: https://www.greenbone.net/

[3] Livedemo des OpenVAS Tools: https://livedemo.greenbone.net/

[4] Dokumentation des Greenbone Security Assistants: http://docs.greenbone.net/GSM-Manual/gos-4/en/

[5] Suchen nach spezifischen Sicherheitstests: https://secinfo.greenbone.net/omp?r=1&token=guest

[6] Produkte der Greenbone Networks GmbH: https://www.greenbone.net/produktvergleich/

[Q1]: Greenbone Networks GmbH: „About OpenVAS Software“ http://www.openvas.org/software.html

[Q2]: Greenbone Networks GmbH: „About OpenVAS” http://www.openvas.org/about.html

[Q3]: Greenbone Networks GmbH: „Openvas-discuss Info Page“ http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

[Q4]: „OpenVAS Compendium – Automatically Updating an NVT Feed” http://www.openvas.org/compendium/automatically-updating-an-nvt-feed.html

[Q5]: Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Gefaehrdungslage/Schwachstellenampel/cs_schwachstellenampel_node.html

Bildnachweis

Unterstützung karitativer Organisationen - Was passiert mit der Spende?

Spende unterstützt Tier- & Musik-therapien für schwerstkranke Kinder

v.l.: ORDIX-Vorstand Benedikt Georgi mit dem Kunstobjekt Sterntaler, Wilhelm Stute mit dem symbolischen ORDIX Spendenschwein

Sterntaler – Hilfe für schwerkranke Kinder e.V.

Zur diesjährigen Spendenübergabe kam der Vorstand des Sterntaler e.V. Wilhelm Stute in die neue ORDIX-Geschäftsstelle in Paderborn. Als Dankeschön für die erneute finanzielle Unterstützung brachte er im Namen von Sterntaler e.V. ein ganz besonderes Geschenk mit – das Lichtkunstobjekt „Sterntaler“, welches von der Glasmalerei Peters in Paderborn hergestellt wurde, um langjährigen Unterstützern des Vereins ein Symbol der Dankbarkeit zu überreichen.

Im Fokus des Gesprächs lag ein ganz besonderes Hilfsprojekt, welches unter anderem durch die Fördergelder der ORDIX AG aus dem letzten Jahr finanziert werden konnte – die tiergesteuerte Therapie für Ben.

Mrs. Marples Gefühle für Ben

Auch wenn sich Herr Stute weiterhin treu bleibt, die Spendenempfänger nicht zu benennen, konnte er mit Zustimmung der Familie über ein interessantes Projekt aus dem letzten Jahr berichten. Aufgrund der hohen finanziellen und zugleich psychischen Belastung, die Familien von langzeiterkrankten Kindern tragen müssen, werden immer häufiger Tiertherapien eingesetzt, um den Kindern eine Art Ablenkung von ihrer Krankheit zu geben. Dies entlastet auch die betroffenen Familien enorm. So auch im Fall Ben, 9 Jahre alt, aus Ostwestfalen-Lippe, bei dem, wie immer häufiger auftretend, die Krankenkasse die Kosten für Tiertherapien nicht mehr übernimmt.

Ben leidet seit einigen Jahren an der neurologischen Krankheit Epilepsie, welche sich unter anderem durch krampfende Anfälle oder Zuckungen sowie durch Bewusstseinspausen bemerkbar macht. Demnach ist auch Bens Mutter komplett ausgelastet, da diese Krankheit vor allem bei Kindern eine permanente Beobachtung fordert.

Durch die finanzielle Unterstützung von Sterntaler im fünfstelligen Bereich war es möglich, den Hundewelpen Mrs. Marple in die Familie zu integrieren und Ben somit nicht nur einen Warnhund, sondern auch einen Kuschelgefährten zur Seite zu stellen. Mrs. Marple begleitet Ben und seine Familie jeden Tag – ob bei Trainings oder seinem motorischen Handicap. Sie ist immer an Bens Seite und kann zum Beispiel bei Epilepsien auch die Notfalltasche bringen und somit in Notsituationen jederzeit auf Ben reagieren.

Durch die Unterstützung von Sterntaler e.V und seinen Förderern kann schwerkranken Kindern und deren Familien, wie auch im Fall Ben, geholfen werden – insbesondere an den Stellen, wo keine Hilfeleistungen von öffentlichen Einrichtungen getragen werden. Laut Aussage von Wilhelm Stute ist leider eine gewisse Zurückhaltung für gemeinnützige Spenden deutlich spürbar, da die Spendengelder deutlich zurück gehen.

Vorstand Benedikt Georgi hat zugesichert, dass ORDIX im nächsten Jahr erneut die großartigen Projekte des Sterntaler e.V. finanziell unterstützen will und hofft zudem, dass weitere Unternehmen in OWL gemeinnützige Institutionen mit Spenden fördern.

Der gemeinnützige Verein Sterntaler unterstützt seit 1999 schwerkranke Kinder und ihre Familien dort, wo öffentliche Ämter nicht greifen. Der Verein arbeitet ausschließlich ehrenamtlich und ohne Verwaltungskosten, weshalb die Spenden zu 100 Prozent an die Betroffenen gehen.

Weitere Informationen zur Sterntaler-Hilfe finden Sie unter http://www.sterntaler-kinder.de/unsere-hilfe/

ORDIX unterstützt Musiktherapie für Bärenherz-Kinder und Angehörige

Zur diesjährigen Spendenübergabe war Matthias Jung, Geschäftsstellenleiter der ORDIX AG in Wiesbaden, erneut zu Besuch im Kinderhospiz Bärenherz, um die Spende für 2018 symbolisch zu überreichen. Im Gespräch mit Frau Anja Eli-Klein, stellv. Geschäftsführerin der Stiftung, kamen insbesondere zwei wichtige Themen zur Sprache – die Musiktherapie und die Geschwisterbegleitung.

Musik schafft klingende gemeinsame Lebenszeit

Die ORDIX-Spende aus dem letzten Jahr wurde hauptsächlich für die Musiktherapie eingesetzt, von dieser Methode wollte sich Herr Jung ein genaueres Bild machen. Frau Heidi Schock-Corall, Musiktherapeutin der Stiftung, lud zu einer Sitzung ein, um gemeinsam vielfältige Instrumente zu entdecken. Für diese Anlässe gibt es im Hospiz einen separaten Raum mit unterschiedlichen Instrumenten. Das Ziel dieser Musiktherapie ist vor allem die Entspannung der kleinen Patienten.

In Musik und Klang kann sich das Leben in all seinen Facetten ausdrücken. Dies ist ein wichtiger Ansatz im Kinderhospiz Bärenherz Wiesbaden. Gefühle wie Trauer, Verzweiflung, Freude und Wut können aufgenommen, hörbar und spürbar werden. Aber auch Getragensein, Geborgenheit, Trost und Gemeinschaft sind darin erfahrbar.

Zudem ermöglicht dies den kleinen Bärenherzbewohnern die Kommunikation, den Ausdruck und das Erleben ohne Worte mit ihren Geschwistern und Eltern in ihrem Kommen, Dasein und Gehen. Seien es Sinneserfahrungen in der Klangwiege, Entspannung mit Klangschalen, Aktivierung durch gemeinsames Trommeln und Singen, Förderung der Wahrnehmung durch spielerisches Experimentieren und gemeinsames Lauschen. Sei es alleine oder in der Gruppe, im Musiktherapieraum, im Kinderzimmer oder im Wohnbereich des Kinderhospizes.

Im Trauerprozess erfahren die erwachsenen Angehörigen musikpsychotherapeutische Begleitung durch Klangentspannung – Atemholen, Ruhe finden, Zeitinseln erleben, Kraft schöpfen. Besondere Erlebnisse sind: Musikreisen und Imagination. Bei diesen inneren Entdeckungsreisen kommt vorwiegend klassische Musik zum Einsatz, und die Einbindung weiterer kreativer Ausdrucksformen wie Malen, Tonarbeit, Bewegung ist möglich. Das reflektierende Gespräch über das Erlebte und Gestaltete rundet die Musikreise ab.

Die Begleitung der Geschwister mit kreativen Angeboten und individuellen Sternstunden – Geschwister werden nicht allein gelassen

Die diesjährige Spende wird für die Geschwisterbegleitung eingesetzt. Neben den eigentlichen Patienten belastet die Diagnose oftmals auch die Geschwister sehr.

Im Kinderhospiz Bärenherz findet neben der Begleitung der erkrankten Kinder und deren Eltern auch eine professionelle Begleitung der Geschwister statt. Ziel dieser Begleitung ist es, den Kindern in ihrer aktuellen Situation Angebote zu machen, um sie zu stärken, sie ernst zu nehmen und sie mit ihrer Trauer nicht alleinzulassen.

Die Diagnose einer lebensverkürzenden Erkrankung des Bruders oder der Schwester verändert im Leben alles. Plötzlich sind Mama und Papa traurig, haben weniger Zeit, der geplante Urlaub kann nicht stattfinden, alles ist anders! In diesen Situationen fühlen sich Kinder oft alleine, wollen den Eltern nicht noch mehr Kummer machen und funktionieren einfach.

Bärenherz unterstützt die Geschwister der stationären wie auch der ambulant betreuten Kinder mit kreativen Angeboten, Ausflügen, Gruppenangeboten und Freizeiten.

Seit Jahren begleitet auch das Harfenspiel der Musiktherapeutin den Weg der Kinder und Familien im Bärenherz. Viele Menschen verbinden mit diesen besonderen Klängen und Melodien eine besondere Lebenszeit.

„Wir sind sehr dankbar, dass Sie keine zweckgebundenen Spenden machen, sondern das Geld frei zu Verfügung stellen."

Anja Eli-Klein im Gespräch mit Matthias Jung.

Besonders wichtig sind die Sternstunden, in denen für ein einzelnes Kind nach seinen ganz speziellen Wünschen ein besonderes Programm erstellt und durchgeführt wird. Hier können die Kinder spüren, dass sie jetzt an der Reihe sind und jemand für sie da ist.

Ein großes Ziel ist auch, die Eltern zu entlasten und ihnen den Rücken freizuhalten für die Zeit mit dem kranken Kind. Und manchmal ist hier auch nur das Organisieren des Alltags wichtig, beispielsweise Fahrten zum Kindergarten und zur Schule.

Im Kinderhospiz Bärenherz wird Raum und Zeit geschaffen, damit auch die Kinder, egal welchen Alters, Abschied nehmen können von Bruder oder Schwester. Den Tod begreifen hat mit greifen – mit verstehen – zu tun. Gemeinsam mit den Geschwistern wird gesehen, welche Rituale zum Abschiednehmen wichtig und stimmig sind. Auch hier begleitet das Bärenherz-Team entsprechende den Bedürfnissen der Kinder.

Viele Eltern erzählen, dass nach dem Verlust eines Kindes der wieder einkehrende Alltag die Lücke, die das Kind hinterlassen hat, richtig spürbar macht. Auch für Geschwister ist dies häufig eine schwierige Situation. Hierzu bietet Bärenherz weiterhin Hausbesuche und eventuell ein Gespräch mit Erziehern im Kindergarten oder Lehrern in der Schule an.

Bei den Hausbesuchen geht es darum, der Trauer Raum zu geben, Erinnerungen zu wahren und dem Verstorbenen einen neuen Platz im Leben zu geben. Dies geschieht im kreativen Tun, im körperlichen Ausdruck oder im Gespräch – je nach Alter des Kindes. Wichtig dabei ist der enge Austausch mit den Eltern, denen Bärenherz auch beratend zur Seite steht. Priorität hat, dass sich jede Familie gut aufgehoben fühlt.

Überblick über Projekte des Elisabethstifts in 2017

Leider konnten wir in diesem Jahr nicht persönlich die symbolische Spende für den Fördervereins des Elisabethstifts in Berlin überreichen.

Dennoch war es ganz besonders interessant zu erfahren, welche Projekte ORDIX durch die jährliche Weihnachtsspende im Jahr 2017 gefördert hat. Ein herzlicher Dank geht deshalb an Herrn Wegner, Geschäftsführer und Leiter des Fördervereins, der uns ausführlich über die tollen Projekte in der Kinder- und Jugendentwicklung des Elisabethstifts informiert hat.

„Der Förderverein des Elisabethstifts hat im letzten Jahr die musik- und freizeitpädagogische Arbeit im Elisabethstift unterstützt. So konnten wir mit Ihrer Hilfe Kindern ermöglichen, am Kochkurs teilzunehmen, in der Märchengruppe mitzumachen und bei einem weihnachtlichen Kindermusical mitzuwirken. Das sind für die Kinder ganz wichtige Erfahrungen."

Neben diesen Aktivitäten bietet das Elisabethstift ein musikpädagogisches Projekt an, bei dem Kinder ein Theaterstück vorspielen. „Zunächst einmal lernten die Kinder Lieder auswendig, organisierten Deko- und Kleidungsutensilien, sodass sie bei der Weihnachtsfeier ihr Theaterstück präsentieren konnten.

„Besonders schön war es zu sehen, dass Kinder, die sonst zurückhaltend erschienen, enorm aufblühten und somit ihren vollverdienten Applaus erhielten. Für ihr weiteres Leben und ihre sozial-emotionale Entwicklung sind solche Momente ungemein wichtig."

Ausblick auf 2018 – Gruppenreise für Kinder

In 2018 plant das Elisabethstift unter anderem eine gruppenübergreifende Reise nach Elbingerode ins dortige Diakonissen-Mutterhaus. In den Osterferien sollen die Kinder die Möglichkeit erhalten, aus ihrem Gruppenalltag herauszukommen. Dort treffen sie auf andere Kinder mit ähnlichen Erfahrungen, sodass neue Freundschaften untereinander geschlossen werden können.

Durch die stetig hervorragende Arbeit des Fördervereins hat sich ORDIX dazu entschlossen, auch in 2018 wieder einen Beitrag für die Kinder- und Jugendhilfeeinrichtung zu leisten und ihn ganz nach dem Leitsatz „Das Elisabethstift will etwas bewegen" weiterhin finanziell zu unterstützen.

Isabell Rosenblatt
(info@ordix.de)

Storage-Komprimierung und Deduplizierung

Darf es vielleicht noch ein bisschen weniger sein?

In einer zurückliegenden Ausgabe der ORDIX® news hat unser Kollege Klaus Reimers einen Artikel zum Thema Oracle-Komprimierung veröffentlicht, der sich mit den verschiedenen Komprimierungs-Optionen einer Oracle-Datenbank auseinandersetzt [1]. Dieser Beitrag betrachtet das Thema Komprimierung aus einem anderen Blickwinkel: In einem Labor-PoC (Proof of Concept) hat ORDIX zusammen mit dem Storage-Hersteller Tegile untersucht, welche Mehrwerte die storage-eigenen Komprimimierungs- und Deduplizierungsoptionen für eine Oracle-Datenbank liefern können. Untersuchungsgegenstand war neben der eigentlichen Effizienz, die sich im tatsächlichen Speicherbedarf und der Performance ausdrückt, auch die Überlegung, ob das Delegieren der Komprimierung vom Server- zum Storagesystem wirtschaftlich einen Nutzen bringt.

Der ORDIX-Partner Tegile Systems Inc.

Nach den Marktanalysten der Dell'Oro Group ist eine Transition des Storage Marktes schon länger in voller Fahrt [2]. Die klassischen Speichersysteme mit drehenden Festplatten, die von einem halben Dutzend seit Jahren etablierter Anbieter angeboten werden, bekommen Konkurrenz.

Junge und innovative Hersteller von Hybrid- oder All-Flash-Lösungen mit hohen Wachstumsraten etablieren sich zunehmend am Markt. Ein solcher Anbieter ist das 2010 gegründete Unternehmen Tegile, mit dem die ORDIX AG im Jahr 2017 eine Partnerschaft begründet hat. Weitere Storage-Trends sind die Adaption von NVMe (Non-Volatile Memory Express) sowie die zunehmende Bedeutung von Cloud-Storage. Auch in diesen Bereichen ist Tegile mit dem Portfolio gut aufgestellt [3].

Natürlich legt die Entscheidung zwischen Flash, HDD oder der Kombination daraus neben weiterer Hardware nur den Grundstein für eine adäquate Architektur. Die Features kommen in der Regel bei allen Herstellern aus einem ausgeklügelten und häufig proprietären Storage-Betriebssystem, welches die eigentliche Differenzierung zu den Wettbewerbern liefert. So bietet Tegile-Storage die Konsolidierung von verschiedensten Workloads aus der File- und Blockwelt sowie auch ausgefeilte Technologie zur Reduzierung des RAW-Speicherbedarfs an, um die nutzbare Kapazität deutlich zu steigern. Neben Thin-Provisioning sind hier auch Deduplizierung und Inline-Komprimierung der Daten herauszustellen. Es sei erwähnt, dass bei dem Aufbau und bei der Durchführung des PoCs die besonders einfache GUI-Bedienbarkeit des Speichersystems aufgefallen ist (siehe Abbildung 2). Alle Workloads des Storagesystems werden durch Projekt-Wizards eingerichtet, wobei für gängige Workloads in den Templates gleich die korrekte Best Practice vorgeschlagen wird. Auch das Monitoring oder der Export von Performance-Daten – bis auf LUN-Ebene – ist ausgesprochen hilfreich.

PoC-Aufbau

Um den Aufwand für eine Testumgebung gering zu halten, wurde, wie in Abbildung 2 zu sehen, ein einzelner x86-Server mit Broadcom-HBA (Dualport, ehemals Emulex) über zwei redundante Brocade-Fabrics mit einem Tegile All-Flash-Storage verbunden. Die Datenbank-LUNs wurden also über Fibre Channel angeschlossen. Über Multipathing (ALUA) wurde sichergestellt, dass zwei Pfade zu jeder LUN aktiv genutzt wurden, um die Bandbreite zwischen Server und Storage zu aggregieren.

Auf dem Server wurde Oracle Linux 7.3 (x64) installiert und eine Oracle-Datenbank der Version 12.2 EE genutzt. Die Verwaltung der LUNs geschah dabei mithilfe von Oracle Grid Infrastructure (GI), ebenfalls in Version 12.2. Den Tegile Best Practices [4] folgend, wurden insgesamt 16

neue LUNs erstellt, 8 pro Controller. Jeder der beiden Controller verwaltete dabei je vier LUNs für Daten (128 GB) und Redologs (64 GB). Aus den LUNs sind anschließend mithilfe von Oracle GI die zwei Disk- Gruppen **DATA** und **REDOLOG** gebildet worden. Den Empfehlungen folgend, setzen sowohl die LUNs, als auch die Oracle-Datenbank eine einheitliche Blockgröße von 8 KB ein. Für die Tests wurden der Oracle-Datenbank zehn 1 GB große Logfiles für Redologs zur Verfügung gestellt und Bigfile Tablespaces genutzt.

Abb. 1: Tegile IntelliFlash OS 3.5 Web-UI Dashboard

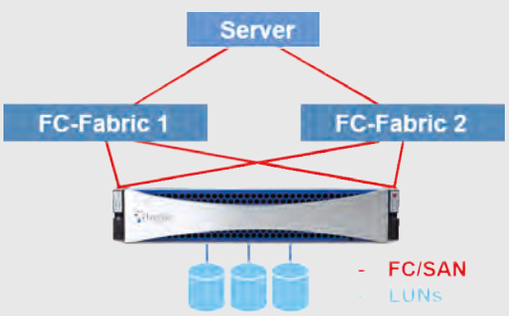

Abb. 2: Schematischer Proof-of-Concept-Aufbau

Szenario/Messgröße	Bedarf der Oracle DB (MB)	Bedarf der Tegile LUNs (MB)
Basiswert	2624 (100%)	2710 (100%)
Tegile Compression	2624 (100%)	800 (30%)
Oracle Compression	568 (22%)	630 (23%)
Oracle Advanced Compression	656 (25%)	730 (27%)
Tegile and Oracle Compression	568 (22%)	400 (15%)
Tegile Compression und Oracle Advanced Compression	656 (25%)	500 (18%)

Abb. 3: Messergebnisse zum Speicherbedarf

Messreihen

Selbstverständlich können Messreihen, die unter Laborbedingungen durchgeführt werden, nicht ohne Weiteres gegen eine Lasttest-Validierung mit echten Produktivdatenbanken verglichen werden.

Ziel der durchgeführten Tests ist lediglich, eine Tendenz in den Messwerten zu erkennen, um eine grundsätzliche Aussage treffen zu können. Die akzeptierte Abweichung der Messungen wurde mit 10% recht groß definiert.

Auf der Datenbank wurden die folgenden Aktionen in unterschiedlichen Szenarios mit jeweils einer Millionen Zeilen durchgeführt:

- Lesen (**SELECT**)
- Änderungen (**UPDATES**)
- Löschungen (**DELETES**)
- Einfügungen (**INSERTS**)

Beim Einfügen der Daten wurde der dadurch verbrauchte Speicherplatz mithilfe von Boardmitteln festgestellt. Es wurde dabei die Größe der Oracle-Datenbank und die der LUNs des Tegile-Systems betrachtet. Daraus ergaben sich die in der Tabelle aufgeführten Ergebnisse.

Auswertung der Messreihen

In Abbildung 3 wird die hohe Komprimierungsrate des Tegile-Systems deutlich. Interessant ist, dass auch im Fall von bereits aktivierter Oracle-Komprimierung immer noch eine signifikante Komprimierung durch den Storage erfolgt. Gleichfalls zeigt die Tabelle auch den Nutzen der Oracle-Komprimierung. Die Differenz aus den Größenangaben aus der Datenbank und dem tatsächlichen Platzbedarf der LUNs auf dem Storage ist durch Metadaten erklärbar. Wird die Komprimierung sowohl auf dem Storage als auch innerhalb der Datenbank aktiviert, führt dies zu einem beeindruckenden Wert von 85%, bezogen auf den Speicherbedarf!

Deduplizierung, von dessen Einsatz Tegile im Zusammenhang mit Oracle-Datenbanken abrät, wurde zusätzlich getestet. Es konnte nachgewiesen werden, dass der Einsatz keinen Vorteil bringt. Dies liegt an der Datenstruktur einer Oracle-Datenbank, die in der Regel keine identischen Blöcke enthält.

Fazit

Zusammengefasst kann gesagt werden: Komprimierung ist sehr gut geeignet, um im Oracle-Umfeld erhebliche

Speicherkapazitäten zu sparen. Im Falle von Tegile Storage geschieht dies kostenneutral, da keine zusätzlichen Lizenzen benötigt werden.

Als Orientierungshilfe lässt sich basierend auf den Messergebnissen daher Folgendes festhalten: die Messergebnisse zeigen, dass die Komprimierung durch Tegile in den getesteten Fällen, ohne auf das Anwendungsszenario der Datenbank achten zu müssen, stets aktiviert sein sollte. Die Aktivierung zeigt insbesondere keine negativen Auswirkungen auf die Performance. Unter bestimmten Bedingungen zeigt sich sogar eine Performancesteigerung sowie eine Verbesserung der Latenzzeiten, da I/O-Operationen im Backend eingespart werden können. Tegiles empfohlene Komprimierung LZ4 erreichte eine Komprimierung von bis zu 70% und liegt damit nur knapp unter der Komprimierungsrate von Oracle mit bis zu 78%.

Tests in realen, großen Kundenumgebungen durch ORDIX haben gezeigt, dass Select / Delete Statements – insbesondere bei Massendaten – in Kombination mit Oracle-Komprimierung immer schneller sind als eine Komprimierung mit Storage-Mitteln. Dies liegt daran, dass Oracle unmittelbar in der System Global Area (SGA) komprimiert bzw. dekomprimiert. Dadurch müssen zwischen Host und Storage weniger Blöcke transportiert werden. Massenänderungen sind hingegen mit Tegile-Technologien etwas schneller. Relativ unentschieden ist das Ergebnis zwischen Oracle- und Tegile-Komprimierung bei Masseninserts.

Die Kombination der beiden Komprimierungs-/Deduplizierungmöglichkeiten zeigt, dass sogar noch zusätzlich Speicherplatz eingespart werden kann. Dabei kann es je nach Anwendungsszenario aber auch sinnvoll sein, auf die Oracle Komprimierung zu verzichten, um so Lizenz- und Hardwarekosten serverseitig zu sparen. Die Komprimierungsrate des Tegile-Systems mit dem empfohlenen Komprimierungsalgorithmus erweist sich auch in Kombination mit der Oracle- Komprimierung als effektiv, wenn auch verständlicherweise weniger als mit unkomprimierten Oracle-Datenbanken. Aus technischer Sicht kann festgehalten werden, dass in der Regel immer noch das tatsächliche, einzelne Speichermedium die langsamste Komponente ist. Dafür ist jede Verminderung von I/O, die im Vorfeld geschieht, nützlich. Natürlich wird diesem Aspekt auch schon durch das geeignete RAID-Layout Rechnung getragen

Aus finanzieller Sicht bietet das Tegile-System Einsparpotentiale durch nicht oder weniger benötigte Oracle-Lizenzen, eingesparten Speicherplatz oder Konsolidierung mehrerer Storages auf ein einziges System. Für das Tegile-System werden auch ansonsten keine zusätzlichen Lizenzkosten fällig; alle Features sind nativ implementiert und der Storage schnell und einfach zu konfigurieren. Es muss natürlich immer die individuelle Situation ganzheitlich betrachtet werden – dafür stehen Ihnen Tegile und ORDIX selbstverständlich gerne zur Verfügung.

Links/Quellen

[1] ORDIX Blog: Oracle Compression - Weniger ist mehr
https://blog.ordix.de/technologien/oracle-compression-weniger-ist-mehr

[2] Marktanalyse der Dell'Oro Group
http://www.delloro.com/other/storage-systems-market-transition

[3] Unternehmensseite Tegile
http://www.tegile.com

[4]Tegile Best Practices
http://pages.tegile.com/rs/568-BVY-995/images/Oracle12cPerformanceT4700v3.pdf

Glossar

NVMe
Non Volatile Memory Express ist eine Schnittstelle, um SSD, also nichtflüchtige Massenspeicher, über PCI Express zu verbinden, ohne dass dafür herstellerspezifische Treiber nötig wären. Sie soll besonders bei parallelen Zugriffen, wie sie bei Multithreading häufig vorkommen, die Geschwindigkeit erhöhen, indem die Latenz und der Overhead durch die Befehle verringert werden.

Deduplizierung
Bei der Deduplizierung, Deduplication (DeDup), oder Daten-Deduplizierung, Data Deduplication (DDD), geht es darum, mehrfach bearbeitete und gespeicherte Dateien, die redundant sind oder sich nur geringfügig unterscheiden, zu erkennen und zu beseitigen. Ziel der Deduplizierung ist die Kapazitätsoptimierung von Speichermedien.

Thin Provisioning
Thin Provisioning (TP), bezeichnet ein kostensparendes Verfahren zur Bereitstellung von Speicherkapazität in virtualisierten Speicherumgebungen (Storage-Virtualisierung). Bei der schlanken Speicherzuweisung wird nur der Speicher reserviert, welcher auch tatsächlich benötigt wird.

ALUA
Asymmetric Logical Unit Access beschreibt ein standardisiertes Protokoll im SCSI Standard für den Zugriff auf ein LUN über mehrere Controller eines Speichersystems.

Jan Benedikt Kardinal
(info@ordix.de)

CISSP- CISM- CISA- ZERTIFIKATE

SCHULEN SIE SICH UND IHRE MITARBEITER HEUTE IN DER IT-SICHERHEIT VON MORGEN

Warum sollte ich mich zertifizieren?

Sie zertifizieren sich mit dem international anerkannten Weiterbildungsstandard auf dem Gebiet der Informationssicherheit – zunehmend in Deutschland eingefordert! Eine objektive Zertifizierung Ihres Wissens durch die Isaca mit weltweiter Relevanz im Bereich der IT-Sicherheit verschafft Ihnen eine hohe internationale Anerkennung, neue Karriere-Chancen und die Differenzierung von Mitbewerbern.

Folgende Zertifizierungen bieten wir an:

Certified Information Systems Security Professional (CISSP)
5 Tage Intensivkurs

Certified Information Security Manager (CISM)
3 Tage Intensivkurs

Certified Information Systems Auditor (CISA)
4 Tage Intensivkurs

Manufaktur IT
Information Security Training for Business

ORDIX® seminare
einfach. gut. geschult.

NEUGIERIG?