www.ordix.de € 3,20

2|2018

ORDIX® news

einfach. besser. informiert.

APEX auf dem Security-Prüfstand

30 | Wie sicher ist Oracle's Webentwicklungstool?

6 | Application Server – Sicherheitsanalyse von Anwendungsservern

14 | Neuheiten Java 9 (Teil II): Java 9 macht schlank, kann aber noch mehr?

22 | OAuth 2.0 und Java Spring – REST-Schnittstellen absichern

40 | ORDIX baut IT-Security Know-how aus – Vier neue CISSP's

»Ready for IT! – gemeinsam Richtung Zukunft«

Möchten Sie erste Praxis-Erfahrungen im Praktikum sammeln? Oder nach Ihrem Studium beruflich durchstarten?
Oder sind Sie bereits Profi und wollen Ihre Laufbahn als Consultant weiter ausbauen?

Ob als Praktikant, Young Professional oder Senior Professional – für Ihre Karriere bieten wir viele Möglichkeiten. Dabei gehen wir auf Ihre individuellen Berufswünsche und Ihre persönlichen Ziele ein. Wir zeigen Ihnen auf, welche spannenden Aufgaben, attraktiven Verdienstmöglichkeiten und vielfältigen Sozial- und Sonderleistungen auf Sie warten.

PRAKTIKUM | STUDIUM

Ready for IT?
Wir gestalten mit dir die Zukunft

DUALES STUDIUM ZUM
BACHELOR OF SCIENCE
IT-SECURITY (W/M)

YOUNG PROFESSIONALS

Als neues Team-Mitglied bekommst
du bei uns viele Chancen

JUNIOR DATENBANKSPEZIALIST
(W/M) – ORACLE

SENIOR PROFESSIONALS

Sie sind erfolgreich im Beruf und
möchten den nächsten Schritt gehen

BIG DATA ADMINISTRATOR (W/M)

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

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

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

Paderborn, Januar 2019

Macht hoch die Tür, die Tor …

Grammatikalisch nicht ganz korrekt, es müsste ja DAS Tor heißen, aber das alte Kirchenlied passt gerade ganz gut auf die Situation der massenweise bestohlenen Politiker und (Pseudo-) Promis.

Ich war vor einigen Tagen im Urlaub und stellte mir vor, ich hätte vor meinem Urlaub im Vorgarten ein Schild aufgestellt „Bis 20.01. im Urlaub“ und die Tür nicht abgesperrt. Wenn Einbrecher eben diese Dämlichkeit von mir ausnutzen und die halbe Bude leer räumen, hätte ich mich dann bei der Polizei beschweren dürfen, dass sie mein Eigentum nicht schützt?

So oder so ähnlich kommen mir die Beschwerden über den „Datenklau“ *) vor. Ich sage nur, das kommt davon, wenn man jeden Mist bei Facebook, Instagram, Twitter oder wo auch immer ins Netz stellt. Ich meine, Privates gehört da einfach nicht hin. Dann wird auch nichts geklaut, so wie bei mir zu Hause, wo ich natürlich kein Schild aufgestellt habe und sowohl Fenster als auch Türen jederzeit vernünftig gesichert sind.

Sie mögen mich für altmodisch halten? Nein bin ich nicht, allein durch dieses im Netz verfügbare Editorial bin ich schon öffentlicher als mir lieb ist. Wenn ich mich also mit Ex-Supertramp Roger Hodgson ablichten lasse, dann muss ich das nicht bei Instagram oder Facebook posten. Das ist privat, auch wenn mich das vielleicht interessanter erscheinen lässt und ich es hier gerade öffentlich gemacht habe. **)

Ich bin aus gutem Grund nicht bei XING (ich suche keinen neuen Job, spioniere nicht meinen Mitarbeitern nach und Geschäftskontakte kann ich auch anders knüpfen, zumindest mache ich das schon nahezu 30 Jahre relativ erfolgreich ohne XING). ***)

Facebook lasse ich eh aus, das ist aus meiner Sicht entweder etwas für pubertierende Teenager, notfalls aber auch etwas in einem kleinen privaten Kreis. Instagram braucht meines Erachtens auch keiner, es sei denn er/sie/es abonniert alle Zeitungen von „Frau im Spiegel“ über „Bunte“ bis hin zur „Gala“. Nur dass m.E. das Niveau der Poster bei Instagram meistens unter dem der in obigen Zeitungen per Artikel erwähnten Personen ist.

Und zu Twitter sage ich gar nichts außer der alten lateinischen Binsenwahrheit: „Si tacuisses, philosophus mansisses“. Obwohl beim Stichwort Twitter fällt mir sofort einer ein, dem würde heute nicht mal mehr Schweigen helfen.

Apropos Artikel, da war doch noch was: Was würde besser zu meinem Editorial passen als ein Artikel über die Sicherheit von Web-Applikationen bzw. Web-Servern? Voilà: Unsere Sicherheitsanalyse von Anwendungsservern und APEX auf dem Sicherheitsprüfstand (natürlich neudeutsch Security).

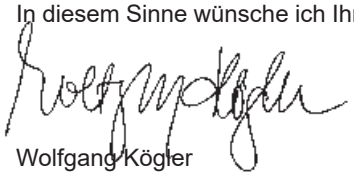
Kleiner Kalauer am Rande: Warum entwickelt sich die Oracle-Aktie besser als die Apple-Aktie? Weil wir nur Artikel über Oracle schreiben, keine über Apple: Zweimal was zu Oracles Directory Services und natürlich etwas zu einer unserer Domäne schlechthin: Oracle AWR Warehouse, Performance Performance Performance. Womit wir auch wieder bei Aktien wären.

Nun sagen Sie sicherlich: Alles halb so wild mit den vielen Oracle-Artikeln, da kommen doch noch Java-Artikel! Aber Java ist leider mittlerweile auch Oracle: Trotzdem aktuell und interessant Teil II zu den Java 9 Neuheiten und gleich zwei Artikel, die sich mehr oder weniger um Microservices drehen.

Gott sei Dank ist da noch ein Apache-Hadoop-Artikel, aber mal schauen, wann sich das Oracle einverleibt. In dieser News haben wir noch einen Oracle freien Blick auf Hadoop 3. Sicherlich rechtzeitig zum Datenklau ließen wir ein paar gut ausgebildete Security-Berater noch zusätzlich zertifizieren.

Genug gezwitschert, Kögler, warten wir ab, was die Briten mit ihrem Brexit noch so alles veranstalten oder ob die Amis wirklich aus ihrem Shutdown-Modus herauskommen. Der orange gefärbten, amerikanischen Blondlocke sei nur gesagt: Keine Mauer – und sei sie noch so hoch – hält Menschen davon ab, auf die andere Seite zu kommen, wenn sie dorthin wollen. Wir Deutschen wissen wovon wir reden.

In diesem Sinne wünsche ich Ihnen ein spannendes Jahr 2019



Wolfgang Kögler

P.S.: Oh wie peinlich, nach Merkel hängt jetzt auch unser Präsident wegen eines Defektes der Regierungsmaschine fest. Kaputte Infrastruktur (Bahn und Straßen), weltweit betrügende Konzerne (Automobil), Flughäfen, die nicht in Betrieb gehen, oh du schönes Germanien, wie tief bist Du gesunken!

*) Hier wurde auch nichts gehackt, nur akribisch eingesammelt, was offen herumliegt, auch wenn die Berichterstattung hartnäckig vom „Hacken“ sprach.

**) Wenn Sie jetzt das Foto erwartet hätten, das stammt von einem professionellem Fotografen (auch wenn er es mit meinem Handy geschossen hat) und da hat er aber auch Roger Hodgson natürlich Rechte daran.

***) Das gilt natürlich auch für LinkedIn, wo übrigens dem Daimler Chef Zetsche Jobs bei BMW vorgeschlagen werden. https://www.automobilwoche.de/article/20171110/NACHRICHTEN/171119997/ueberraschender-karrieretipp-zetsche-veralbert-linkedin

Sicherheitsanalyse von Anwendungsservern

Neuheiten Java 9

Web und Application Server

6 ..... Application Server – Sicherheitsanalyse von Anwendungsservern
Die Sicherheit des Application Server darf bei der Entwicklung von Webentwicklungen nicht vernachlässigt werden. In diesem Artikel zeigen wir, welche sicherheitstechnischen Maßnahmen aktiviert werden können und welche Möglichkeiten die Hersteller bieten.

Oracle

9 ..... Oracle Directory Services (Teil I)
Rollenspiele mal anders – Userverwaltung im Oracle-Verzeichnisdienst
Benutzerauthentifizierung gegenüber Verzeichnisdiensten ist in professionellen IT-Umgebungen unumgänglich. Im ersten Teil zeigen wir, warum die Zentralisierung der Rollen- und Rechteverwaltung entscheidend ist. Und zeigen die Möglichkeit, gezielt und personalisiert zu auditieren.

17 ..... Oracle AWR Warehouse – alles unter einem Dach
Performance-Daten auszuwerten ermöglicht, Engpässe zu vermeiden und die Performance zu optimieren. In diesem Beitrag stellen wir Ihnen die Funktionsweise des Oracle AWR Warehouse vor.

30 ..... Wie sicher ist Oracle's Webentwicklungstool? Oracle Application Express auf dem Security-Prüfstand
APEX bietet die Möglichkeit, Webapplikationen zu erstellen, die äußerst effizient und detailliert Daten auswerten und darstellen können. Doch welche Möglichkeiten bietet eine solche Applikation für Hacker und Wirtschaftsspione, sich an Ihren Daten zu bereichern?

Oracle

36 ..... Oracle Directory Services (Teil II)
Datenbanken & Verzeichnisdienst – ein Bund für's Leben
Ein Verzeichnisdienst bietet die Möglichkeit, Datenbankbenutzer an einem Ort zu bündeln. Dieser Dienst bildet nur die Plattform, die erforderlichen Strukturen hingegen liefert die Enterprise User Security (EUS). Der vorliegende Teil zeigt, wie Oracle-Datenbanken und Verzeichnisdienst auf der Basis von EUS einen Bund eingehen.

Entwicklung

14 ..... Neuheiten Java 9 (Teil II)
Java 9 macht schlank, kann aber noch mehr?
Im zweiten Teil werfen wir einen erweiterten Blick auf die Modularisierung. Wir stellen die Möglichkeit dar, wesentlich schlankere Anwendungspakete schnüren zu können.

22 ..... OAuth 2.0 und Java Spring
REST-Schnittstellen absichern mit Spring, OAuth 2.0 & JSON Web Token
Das Autorisierungsprotokoll OAuth 2.0 bietet bei der Verwendung von Microservice-Architektur-Patterns eine zentrale Instanz zur Verwaltung der Benutzeranmeldeinformationen.

33 ..... Microservices
Mit Eclipse MicroProfile zu leichtgewichtigen verteilten Java EE Microservices
Mit Eclipse MicroProfile steht ein Quasistandard zur Verfügung, der die Implementierung von Microservices erheblich vereinfacht. In diesem Artikel zeigen wir Ihnen den Einstieg in Eclipse Microprofile.

REST-Schnittstellen – OAuth 2.0 und Java Spring

Oracle Application Express

IT-Security

40 ..... ORDIX baut IT-Security Portfolio aus – vier neue CISSP-Berater erhalten Zertifikat

In der Vielfalt der Zertifizierungen für IT-Sicherheits-Profis hat sich in den letzten Jahren der CISSP (Certified Information Systems Security Professional) als besonders anerkannt erwiesen. Durch unsere vier Mitarbeiter, die die CISSP-Prüfung bestanden haben, kann die ORDIX AG ihr Portfolio im Bereich der IT-Sicherheit weiter ausbauen.

Big Data

41 ..... Neuigkeiten im Überblick Apache Hadoop 3

Hadoop 3 ist bereits seit einem Jahr verfügbar. Aber welche neuen Features bietet die neue Version, die bereits Bestandteil der großen kommerziellen Distributionen ist? Wir geben einen Überblick.

Aktuell

12 ..... Rückblick auf die DOAG Konferenz 2018
20 ..... Seminarübersicht 2018
28 ..... Nachhaltigkeit bei ORDIX

Impressum

Herausgeber:	ORDIX AG Aktiengesellschaft für Softwareentwicklung, Beratung, Schulung und Systemintegration, Paderborn
Redaktion/Layout:	Jens Pothmann, Elisabeth Herick
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:	© istockphoto.com | matejmo | Firewall-Schutz-Lock © pexels.com © pixabay.com © istockphoto.com | Cecilie_Arcurs | Lassen Sie uns eintauchen in diesen code © istockphoto.com | alphaspirit | Firewall und antivirus Konzept
Autoren:	Dominik Anielski, Dr. Hubert Austermeier, Uwe Bechthold, Marcel Cossijns, Tobias Flüter, Carsten Griese, Wolfgang Kögler, Dirk Krautschick, Phillip Kürsten, Aron Tigor Möllers, Christian Rädisch, Thomas Trakle
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.
Kontaktadresse:	redaktion@ordix.de

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

Application Server

Sicherheitsanalyse von Anwendungsservern

Webanwendungen erfreuen sich immer größer werdender Beliebtheit. Dies ist vor allem darin begründet, dass mithilfe vieler Frameworks die Möglichkeiten bezüglich Gestaltung und Funktionalitäten schier unendlich sind. Daher bietet Java in der Enterprise Edition (Java EE oder nun Jakarta EE) eine stabile Basis für performante und skalierbare Anwendungen jeglicher Art. Jedoch darf dabei eine zentrale Komponente nicht vernachlässigt werden: der Application Server. In diesem Artikel soll untersucht werden, inwiefern sich sicherheitstechnische Maßnahmen bei ausgewählten Application Servern aktivieren lassen bzw. welche Möglichkeiten der Hersteller bereitstellt.

Was ist ein Application Server?

Ein Application Server stellt primär die Laufzeitumgebung für eine Java EE Anwendung dar [Q1]. Damit es möglich ist, mit dem Benutzer zu interagieren und auf einen Datenvorrat zuzugreifen, muss die Laufzeitumgebung der Java-Anwendung um weitere Elemente erweitert werden. Daher sind aus konzeptioneller Sicht drei Ebenen in einem Informationssystem vorhanden.

Der Application Logic Layer befindet sich im Kern des Informationssystems. Diese Schicht ist dafür zuständig, die Geschäftslogik zu implementieren. Der Application Logic Layer ist somit geeignet, die Geschäftsprozesse eines Unternehmens abzubilden. In diesem Bereich ist die Laufzeitumgebung der Java-Anwendung zu finden. Für die Interaktion mit dem Benutzer ist der Presentation Layer verantwortlich. Dieser bereitet die verarbeiteten Daten aus dem Application Logic Layer entsprechend auf und übermittelt sie an den Client (z.B. Browser).

Zusätzlich brauchen Informationssysteme häufig einen Datenvorrat. Dieser wird im Ressource Management Layer persistent gehalten. [Q2]

Welche Application Server gibt es auf dem Markt?

Das Spektrum an am Markt angebotenen Anwendungsservern ist sehr breit gefächert. Während einige Application Server strengen Lizenzierungsmodellen unterliegen, sind viele Anwendungsserver unter Open-Source Lizenzen verfügbar und werden stetig von der Community weiterentwickelt. Eine Übersicht einiger populärer Modelle und Hersteller ist in Tabelle 1 aufgeführt.

Application Server	Hersteller	Lizenz
WebLogic	Oracle Corporation	Proprietär
TomEE	Apache Software Foundation	Open Source
WebSphere	IBM	Proprietär
Geronimo	Apache Software Foundation	Open Source
WildFly	Red Hat	Open Source
Glassfish	Oracle Corporation	Open Source

Abb. 1: Übersicht über bekannte Application Server

Welche Schwachstellen sollten bei Application Servern geschlossen werden?

Alle oben genannten Anwendungsserver werden vom Hersteller mit Sicherheitsmaßnahmen versehen, um unbefugten Zugang zu sensiblen Daten und Ressourcen zu schützen. Jedoch gilt es zunächst zu klären, auf welche Sicherheitsmaßnahmen ein Administrator im Allgemeinen achten sollte. Dazu können Security Patterns verwendet werden, um die Schwachstellen in einer strukturierten Form vorzuhalten.

Security Patterns sollen helfen, immer wieder auftretende Schwachstellen so zu dokumentieren, dass sie anderen Entwicklern und Administratoren bei der Erstellung eines ganzheitlichen Sicherheitskonzepts unterstützen. Bei einer unzureichend durchdachten Konzeption von Software besteht die Gefahr, dass Sicherheitslücken mit erheblichem Angriffspotenzial entstehen. [Q3]

Benutzung einer gesicherten Verbindung

Ein Administrator eines Anwendungsservers sollte seinen Nutzern unbedingt eine gesicherte Verbindung anbieten. Dadurch stellt er sicher, dass keine sensiblen Daten von Dritten abgefangen und manipuliert werden können. Ein klassisches Beispiel hierfür ist die vertrauliche Benutzername-Passwort-Kombination eines Users. Ein Angreifer hat die Möglichkeit, mit einem speziellen Tool (zum Beispiel `tcpdump`) den Verkehr im Netzwerk abzuhören. Dadurch werden Schutzziele wie Vertraulichkeit und Integrität nicht mehr gewährleistet. Die Lösung für diese Schwachstelle besteht darin, eine TLS/SSL-geschützte Verbindung zu aktivieren. Voraussetzung hierfür ist jedoch, dass ein geeignetes Verschlüsselungsverfahren angewandt wird, um die Gefahr von Brute-Force-Angriffen zu minimieren.

Schutz des Anwendungsservers auf Betriebssystemebene

Um den Application Server weiter abzusichern, müssen die Daten und Ressourcen sowohl nach außen als auch nach innen geschützt werden. Letzteres soll dem Anwendungsserver auf Betriebssystemebene Schutz bieten. Dies bedeutet, dass Deployments, Konfigurationsdateien, Executables und andere wichtige Ressourcen des Application Servers nur einem bestimmten User zugänglich sind. Im Idealfall sollte der Anwendungsserver nur von einem speziell für die Ausführung vorgesehenen User ausgeführt werden. Sollten die Ressourcen nicht geschützt, sondern frei zugänglich sein, haben Angreifer mit Zugang zum Betriebssystem leichtes Spiel, die Ausführung des Application Servers zu stören. Ferner können die Deployments weitere Rückschlüsse auf sensible Geschäftsprozesse preisgeben. Der Administrator muss daher zusätzlich ein durchdachtes Rechtekonzept erarbeiten, um unbefugten Zugriff zu vermeiden.

Deaktivieren von Standardanwendungen und veralteten Passwörtern

Um eine schnelle Installation und anschließende Konfiguration des Anwendungsservers zu gewährleisten, setzen viele Anwendungsserver auf Benutzerfreundlichkeit. Dies setzen einige Modelle z.B. in einer ansprechenden GUI mit Installation-Wizard um. Nach der Erstkonfiguration sind diese Application Server sofort einsatzbereit und lassen das Deployment von benutzerdefinierten Anwendungen zu. Die Gefahr hierbei besteht darin, dass vorinstallierte Inhalte noch aktiviert und abrufbar sind. Deaktiviert der Administrator die vorinstallierten Anwendungen nicht oder ändert er keine Defaults, haben Angreifer auch hier eine Chance: Wenn die Standardanwendungen unter bekannten URLs abrufbar sind, können diese Rückschlüsse auf den Application Server und dessen Version geben. Das nutzen Angreifer aus, um gezielt nach Schwachstellen zu suchen. Ein Beispiel hierfür sind „Welcome-Pages“, die dem Administrator eine erfolgreiche Installation bestätigen – und Angreifern Tür und Tor öffnen. Beide Anwendungsserver bieten jedoch Möglichkeiten, mit denen sich die Schwachstellen schnell und unkompliziert schließen lassen.

Vermeidung von Denial-of-Service-Attacken

Werden auf dem Anwendungsserver unternehmenskritische Anwendungen gehostet, gewinnt er zunehmend an Stellenwert im Unternehmen. Um den Geschäftsbetrieb aufrechtzuerhalten, muss das Informationssystem stets verfügbar sein. Schon kurze, ungeplante Downtimes können erhebliche finanzielle Schäden verursachen. Sollten keine technischen Störungen der Grund für eine Downtime sein, sind es womöglich Angreifer, die einen

Denial-of-Service-Angriff durchführen. Dabei wird der Application Server mit einer hohen Zahl an Requests überschwemmt (SYN-Flood) und kann aufgrund begrenzter Kapazitäten die Anfragen nicht mehr beantworten. Die Folge ist ein nicht mehr erreichbarer Application Server. Daher muss der Administrator Sicherheitsmaßnahmen treffen, die den Zugriff auf den Anwendungsserver reglementieren oder gar verdächtige Anfragen blockieren.

Wie werden die Sicherheitsmaßnahmen aktiviert?

Wie die Sicherheitsmaßnahmen aktiviert werden, hängt stark vom Application Server ab. Bei einigen wenigen Anwendungsservern sind nahezu alle Konfigurationseinstellungen über eine grafische Oberfläche editierbar. Ein Paradebeispiel hierfür ist Oracle WebLogic (im Test Version 12cR2). Die benutzerfreundliche GUI hilft dem Administrator, die notwendigen Häkchen und Parameter zu setzen. Sollte der Administrator die Änderungen eher per Skript (automatisiert) durchführen wollen, ist dies mit dem WebLogic Scripting Tool (WLST) ebenfalls problemlos möglich. Damit kann mit wenigen Klicks eine TLS/SSL-geschützte Verbindung aktiviert werden. Aber Achtung: Nicht nur bei WebLogic sind hierfür Demo-Zertifikate hinterlegt, die ausschließlich für Testzwecke vorgesehen sind. In der Produktion sollten ausschließlich von einer seriösen Certification Authority (CA) signierte Zertifikate verwendet werden. Der Application Server WildFly (ehemals JBoss) von Red Hat bietet in Version 12.0.0 ähnliche Möglichkeiten, eine sichere Verbindung zu aktivieren. Jedoch muss hierfür das Konfigurationsfile editiert werden. Vor allem im Hinblick auf unerfahrene Administratoren ist hier mit einem Mehraufwand zu rechnen.

Was den Schutz auf Betriebssystemebene betrifft, sind die Sicherheitsmaßnahmen eher unabhängig vom Anwendungsserver zu aktivieren. Es ist sehr wichtig, dass Working-Directory mit entsprechenden Rechten zu versehen, damit Unbefugte keine Deployments oder Konfigurationsdateien manipulieren. Ferner sollten die Zugänge zum Betriebssystem (z.B. über SSH) auf die notwendigen User eingeschränkt werden, um bereits einen großen Angriffsvektor auszuschließen. Es sollte zudem darauf geachtet werden, dass dem Application Server stets genügend Systemressourcen zu Verfügung stehen und diese nicht durch andere Nutzer blockiert werden.

Sowohl WebLogic als auch WildFly stellen Standardanwendungen zu Verfügung, welche Informationen über die Version preisgeben. Wird eine WebLogic-Umgebung über den Konfigurationsassistenten mit Default-Werten erstellt, kann ein Angreifer mit einem einfachen Request die Administrationskonsole aufrufen und die Version erkennen. Der Application Server WildFly bietet an dieser Stelle sicherere Defaults. Die Administrationsoberfläche ist nicht von „überall“ aus aufrufbar, sondern lediglich vom Host-System erreichbar. Jedoch bietet auch WildFly-Schwachstellen in diesem Angriffsvektor. Sendet der Angreifer bei unveränderten Defaults einen bestimmten Request an den Application Server, antwortet auch dieser mit einer Website, die Informationen zur Major-Version preisgibt. An dieser Stelle ist es unabdingbar, die unsicheren Defaults zu ändern.

Bei der Abwehr von Denial-of-Service-Attacken bieten beide Application Server gewisse Schutzmaßnahmen. Damit kann ein Administrator verschiedene Konfigurationseinstellungen bearbeiten und somit zum Beispiel die Processing-Time eines Requests verändern oder die maximale Größe eines eingehenden Requests bearbeiten. Um einen besseren Schutz zu gewährleisten, sollte jedoch Gebrauch von weiterer Software gemacht werden. Diese ist speziell darauf ausgelegt, DoS- bzw. DDoS-Angriffe zu erkennen und abzuwehren.

Um die stichprobenartige Bewertung der Application Server abzuschließen, lässt sich ein positives Fazit ziehen. Trotz einiger auf Standardeinstellungen basierender Schwachstellen, lassen sich die Anwendungsserver mit entsprechenden Änderungen in den Konfigurationseinstellungen gegen Angreifer absichern. Die dargestellten Security Patterns stellen jedoch keine vollständige Sammlung an möglichen Schwachstellen dar. Vielmehr sollten sie als initialer Bestandteil eines umfassenden Sicherheitskonzepts betrachtet werden, welches kontinuierlich weiterentwickelt werden muss. Nur so ist es möglich, die Gefahr von aktuellen Bedrohungen unter Kontrolle zu halten.

Quellen

[Q1] IBM Knowledge Center: Anwendungsserver.
https://www.ibm.com/support/knowledgecenter/de/ssw_ibm_i_72/rzahg/rzahgebappserv.htm

[Q2] G. Alonso, F. Casati, H. Kuno und V. Machiraju (2004).
Web Services: Concepts, Architectures and Applications.
Springer Verlag Berlin Heidelberg

[Q3] Gesellschaft für Informatik (2013). Security Patterns.
https://gi.de/informatiklexikon/security-patterns/

Bildnachweis

Dominic Anielski
(info@ordix.de)

Oracle Directory Services (Teil I)

Rollenspiele mal anders – Userverwaltung im Oracle Verzeichnisdienst

Benutzerauthentifizierung gegenüber Verzeichnisdiensten ist in nahezu allen professionellen IT-Umgebungen unumgänglich, lokale Benutzerkonten sind schon lange nicht mehr zeitgemäß. Oracle-Datenbanken stellen aber überraschenderweise sehr häufig die Ausnahme dar, obwohl gerade hier oft hochkritische Sicherheitsbedingungen einzuhalten sind. Nicht zuletzt durch die neue EU-Datenschutzgrundverordnung ist der Bedarf an einer ausnahmslosen Integration der Datenbanknutzer in bestehende zentrale Verzeichnisdienste immer wichtiger. Hierbei ist nicht nur die Zentralisierung der Rollen- und Rechteverwaltung entscheidend, sondern auch die Möglichkeit, erst so gezielt und personalisiert zu auditieren – insbesondere bei Administratoren.

Die Funktionalität, Oracle-Datenbank-User gegenüber einem Verzeichnisdienst grundsätzlich authentifizieren zu können, bezeichnet Oracle als Enterprise User Security und ist ein Feature der Enterprise Edition. Damit ist offiziell mit der Standard Edition oder Standard Edition 2 eine solche Authentifizierung nicht möglich. Immerhin ist dieses Feature seit Version 10.2 kein Teil der Advanced Security Option mehr, sondern ohne weitere Lizenzierung in der Enterprise Edition enthalten. Hierbei ist aber einiges zu berücksichtigen.

Bis einschließlich Version 12.2 gibt Oracle vor, dass als Verzeichnisdienst entweder einer der vorgegebenen Oracle-hauseigenen Dienste verwendet werden muss oder dass dieser als Proxy vorgeschaltet wird, um somit das Konzept der Global- und Enterprise Roles korrekt umsetzen zu können. Details zu diesem Konzept werden in Teil 2 der Reihe genauer erläutert.

Oracle Directory Services

Als Lösungspaket für die Abbildung von Identitäten im Enterprise-Umfeld hat Oracle die Identity Management Suite im Fusion-Middleware-Produktportfolio angesiedelt. Diese Suite unterteilt sich in folgenden Bestandteile:

- Access Management
- Identity Governance
- Mobile
- Directory Services

Im Directory-Services-Paket befinden sich alle Verzeichnisdienste, die Oracle entwickelt oder eingekauft hat und somit selbst vertreibt. Neben den beiden aktuell relevanten Diensten Oracle Internet Directory (OID) und Oracle Unified Directory (OUD) findet man zusätzlich auch noch die Oracle Directory Server Enterprise Edition (ODSEE) und Oracle Virtual Directory (OVD).

Die zwei zuletzt genannten Produkte sind jedoch bereits End of Life und werden nur noch bedingt supported. Sie finden aber immer wieder Erwähnung in Beschreibungen und Dokumentationen und sollten daher zumindest bekannt sein.

Mit den OUD und OID bietet Oracle zwei vollwertig LDAP-v3-kompatible Verzeichnisdienste an, die beide noch langfristig supported werden und für den Einsatz von Enterprise User Security bei Oracle-Datenbanken geeignet sind. Nach heutigem Stand sind beide Dienste offiziell als gleichwertig zu betrachten.

Der aktuell einzige Vorteil vom OID ist die Verbreitung im Markt und der dadurch resultierende bessere Know how-Transfer und Support. Den Signalen aus dem Oracle-Marketing nach gewinnt man aber immer häufiger den Eindruck, dass dem OUD die Zukunft gehört, auch wenn es hierzu aktuell keine offiziellen Angaben gibt. Die Release-Sprünge und Support-Lifetimes sind sowohl beim OUD als auch beim OID zum aktuellen Zeitpunkt identisch. (siehe Abbildung 1).

Oracle Unified Directory

Der vollständig in Java implementierte Verzeichnisdienst Oracle Unified Directory ist das neueste Produkt aus der Reihe von Oracle. Obwohl OID momentan wesentlich mehr Verbreitung in der Praxis findet und dadurch erprobt ist, bietet OUD einige strategische Vorteile. Während bei OID eine zusätzliche Datenbank zur Datenhaltung notwendig ist, bringt OUD eine integrierte Berkeley Database Java Edition (OBDB JE) mit und läuft somit autark.

Oracle Unified Directory (OUD)	Oracle Internet Directory (OID)
LDAP v3 kompatibel	
basiert auf ehemals Sun OpenDS	Eigenentwicklung von Oracle
ausschließlich in Java implementiert	in C und Java implementiert
integrierte Berkeley Database Java Edition (OBDB JE)	zusätzliche Datenbank notwendig
vertikal und horizontal skalierbar (siehe OUD Proxy)	nur vertikal skalierbar
Verwaltung über Kommandozeile oder Oracle Directory Service Manager	

Abb. 1: Vergleich von OUD und OID

Abb. 2: Oracle Directory Services Manager

Die Bezeichnung „Unified“ bezieht sich neben der integrierten Datenbank auch auf die unterschiedlichen Betriebsarten, die unter anderem ältere Produkte obsolet gemacht haben, wie z.B. das Oracle Virtual Directory, welches nur als abstrahierter View auf andere Verzeichnisdienste zugegriffen hat. Zusätzlich bietet die Funktionalität Replication Gateway noch die Möglichkeit, direkt aus dem ODSEE zu replizieren, falls es dazu noch bestehende Verzeichnisse gibt. Oracle will damit eine All-in-One-Directory-Service-Solution propagieren.

Die wichtigsten Betriebsarten beziehen sich jedoch auf die Skalierung, die bei dem OID nur vertikal mit Server-Aufrüstung möglich war. Durch Verwendung des OUD-Proxys kann dieser als zusätzlicher Prozess sowohl für Load Balancing als auch für Failover-Szenarien dienen. Damit hat man die Möglichkeit, jederzeit auch horizontal zu skalieren. In ähnlicher Form ist auch eine Replikation zum Schutz vor Datenverlust möglich. Auch hier wird der OUD als Replication Server Prozess die Kommunikation zwischen den beiden Replikaten verwalten.

Konfiguration und Verwaltung

Grundsätzlich lässt sich die Installation, Konfiguration und auch die Verwaltung über die Kommandozeile durchführen. Aber spätestens bei Letzterem ist dies auf Dauer nicht praxistauglich. Neben den obligatorischen grafischen Installern liefert Oracle darum auch mit dem Oracle Directory Services Manager eine umfangreiche webbasierte Administrationsoberfläche, die ein oder mehrere Verzeichnisdienste verwalten kann und sowohl optisch als

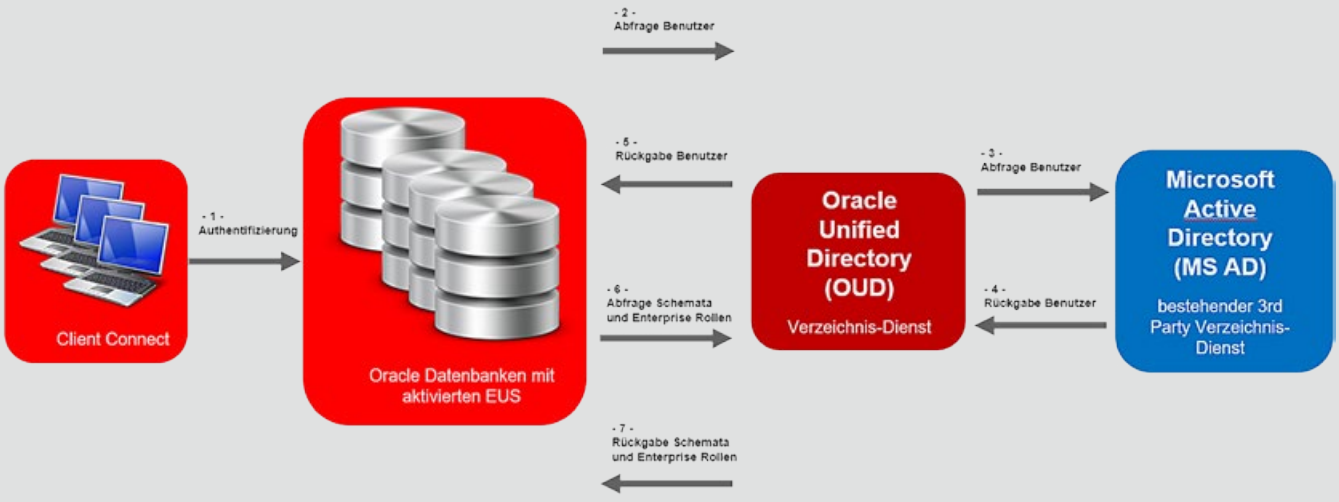


Abb. 3: Gesamtdarstellung einer Authentifizierung mit EUS

auch funktional stark an den Enterprise Manager Cloud Control erinnert. Die hierfür notwendige Grundlage ist ein Weblogic Application Server, den es aber für diese Anwendung auch kompakt als angepasstes Infrastructure Package gibt und man somit auch mit wenig Aufwand den Rollout durchführen kann, ohne sich aufwendig Weblogic-Knowhow aufbauen zu müssen (siehe Abbildung 2).

Synchronisation mit anderen Directories

Da bei den meisten Use Cases bereits ein bestehender Verzeichnisdienst existiert, welcher nicht ersetzt werden soll, kann auch eine Synchronisation durch die Directory Integration Platform (DIP) erfolgen. Mit dieser Zusatzkomponente können Daten von vielen gängigen Verzeichnisdiensten je nach Konfiguration mit dem OUD oder OID synchronisiert und verwendet werden. Dies erleichtert entweder die Übergangsphase bei der Implementierung oder bietet auch die Möglichkeit, die bestehende Infrastruktur und die Oracle-basierte Infrastruktur strikt getrennt zu verwalten, falls eine Vermischung der Benutzerverwaltung der Datenbanken mit dem betrieblichen Verzeichnisdienst nicht erwünscht ist.

Durch die unterschiedlichen Betriebsarten und die optionale Synchronisation mit anderen Verzeichnisdiensten kann man somit alle denkbar möglichen Szenarien abdecken und ein Verzeichnisdienst von Oracle als Komponente in bestehende Umgebungen einbinden. Ob ein OUD bzw. OID dann die Rolle des primären Verzeichnisdienstes jemals übernimmt oder ob man nur den Zwischenschritt für die Modulierung der Enterprise-Rollen und der Shared Schemas nutzt, ist frei wählbar und beides hat eine Daseinsberechtigung. Selbst die Integration in eine produktive Umgebung ist unkritisch. Die Synchronisation über DIP ist unidirektional möglich. Somit ist sie ohne Einfluss auf den bestehenden Verzeichnisdienst. Die Verwendung des OUD/OID wird damit parallel umgesetzt und getestet. Danach kann man die Konfiguration von Enterprise User Security in der bestehenden Datenbank-Landschaft implementieren, bis am Ende die eigentliche Authentifizierung nicht mehr lokal auf der Datenbank, sondern über einen Oracle-Verzeichnisdienst stattfindet (siehe Abbildung 3).

Direkte Integration von Active Directory mit 18c

Mit der neuesten Datenbank Version 18c von Oracle gibt es die Möglichkeit, Enterprise User Security ohne den Umweg über ein Verzeichnisdienst von Oracle zu implementieren. Dies reduziert bei Neuinstallationen den Aufwand der Umsetzung durch Wegfall des OUD oder OID erheblich. Oracle selbst empfiehlt dies aber nur für Organisationen, die eine neue Umgebung implementieren und keine spezielleren Anforderungen haben. Für komplexere Szenarien im Enterprise-User-Security-Umfeld ist die klare Empfehlung immer noch der Zwischenschritt mit einem OID oder OUD.

Lizenzierung

Die Lizenzierung der Verzeichnisdienste ist endeutig und klar definiert. Oracle bietet hierfür ein Lizenzpaket – Oracle Directory Services Plus – an, in dem sämtliche neue und alte, eigen vertriebene Verzeichnisdienste inklusive des Oracle Directory Serivce Manager abgedeckt sind. Die Metriken sind hier entweder Prozessoren oder die Anzahl der Mitarbeiter (mit einer Unterscheidung zwischen internen und externen Mitarbeitern). Der Wortlaut aus dem Lizenzierungs-Guide von Oracle setzt hier auch nicht auf die prinzipielle Verwendung eines Verzeichnisdienstes, sondern auf die Nutzung von Enterprise User Security im Allgemeinen, die ein Verzeichnisdienst implizit voraussetzt. Somit kommt man auch bei Verwendung eines externen Active Directory mit Oracle 18c ohne den Zwischenschritt über die Oracle-eigenen Verzeichnisdienste nicht an dieser Lizenzierung vorbei.

Zusammenfassung

Abgesehen davon, dass Oracle zur Verwendung von OUD bzw. OID im Zusammenspiel mit Enterprise User Security regelrecht und zumindest bis Version 18c verpflichtet, sind diese auch allein betrachtet hochinteressante und erwähnenswerte Produkte, die sich auch mit gängigen aktuellen Verzeichnisdiensten durchaus messen können. Es ist aber kaum vorstellbar, dass man eine Verwendung anstrebt, ohne den eigentlichen Nutzen der möglichen Verwendung von EUS in Datenbanken als Grund und Hauptanwendung zu haben. Der Funktionsumfang, die Integrationsmöglichkeiten und die zeitgemäßen Skalierungsmethoden bieten aber trotzdem kaum Raum, sich aus technischer Sicht gegen eine Umsetzung von EUS mit OUD/OID zu entscheiden.

Dirk Krautschick
(info@ordix.de)

Links

[1] Oracle Web-Präsenz Directory-Services:
https://www.oracle.com/middleware/identity-management/directory-services/

[2] Offizielle Dokumenation OUD
https://docs.oracle.com/en/middleware/idm/unified-directory/12.2.1.3/

[3] Offizielle Dokumentation OID
https://docs.oracle.com/en/middleware/idm/internet-directory/12.2.1.3/

[4] Seminarempfehlung: „Single Sign-On mit Oracle“ DB-ORA-57
https://seminare.ordix.de/seminare/oracle/administration/single-sign-on-mit-oracle.html

DOAG Konferenz + Ausstellung 2018

Neuigkeiten aus der Oracle-Welt

Die DOAG Konferenz 2018 mit vier Referenten der ORDIX AG

Die Konferenz & Ausstellung fand vom 20. - 23. November wie gewohnt im Congress-Center Ost Nürnberg statt. Viele internationale Top-Redner und nationale Oracle Experten teilten Ihr Wissen.

Die ORDIX AG nahm in diesem Jahr mit vier Beiträgen an der Konferenz teil. Neben den beiden bereits erfahrenen Rednern Klaus Reimers und Markus Fiegler konnten in diesem Jahr die Referenten Dirk Krautschick und Raphael Salguero Erfahrungen auf der Konferenz sammeln.

dbms_redefinition – damit kann man Vieles tun (Referent: Klaus Reimers)

Die Reorganisation von Tabellen stellt immer eine große Herausforderung für jeden Administrator dar. Auf der einen Seite sollen die Tabellen wieder besser gefüllt und somit performanter durch eine Reorganisation werden, auf der anderen Seite steht dem immer die Frage des Aufwandes und des Wartungsfensters gegenüber. Mit dem Package dbms_redefinition hat Oracle dem DBA schon mit Version 9i ein Mittel an die Hand gegeben, mit dem ONLINE reorganisiert und auch redefiniert werden kann.

In seinem Vortrag ging Klaus Reimers auf die Möglichkeiten des Packages anhand vieler Demos ein. So zeigte er eine normale Reorganisation, die Umwandlung einer Tabelle in eine IOT oder in eine partitionierte Tabelle. Klaus Reimers beleuchtete, wie mit VPD und Materialized View zu verfahren ist. Des Weiteren erläuterte er die Bulk-Load-Optimierung und demonstrierte die Möglichkeiten einer Wiederaufnahme nach einem Fehler.

Abgerundet wurde der Vortrag mit einem Überblick über die weiteren gängigen Möglichkeiten zur Reorganisation von Tabellen (CTAS/table move/table shrink/datadump).

Fehlerbehandlung bei einer SQL-Bulk-Verarbeitung (Referent: Markus Fiegler)

Sollen Daten schnell und ressourcen-schonend verarbeitet werden, dann ist SQL-Bulk-Verarbeitung im Gegensatz zu einer Einzeldatensatzverarbeitung die erste Wahl. Tritt bei der SQL-Bulk-Verarbeitung allerdings ein Fehler z.B. bei der Datentypkonvertierung auf, so wird die Verarbeitung standardmäßig abgebrochen.

Welche Möglichkeiten gibt es, eine SQL-Bulk-Verarbeitung trotz geworfener Fehler fortzusetzen? In diesem Vortrag wurden Fehlerbehandlungsvarianten für eine SQL-Bulk-Verarbeitung wie Pipelined Table Function, Error Logging Table und Standardwert bei Konvertierungsfunktionen (ab 12.2) vorgestellt und, bezogen auf den Einsatz in der Praxis, bewertet. Darüber hinaus werden diese Varianten unter dem Gesichtspunkt Performance miteinander verglichen.

Oracle Data Guard Observer – der vergessene Helfer (Referent: Dirk Krautschick)

Hochverfügbarkeit mit Oracle Data Guard ist seit einiger Zeit Best Practice und in vielen Unternehmen etabliert. Bei Ausfällen wird aber in den meisten Umgebungen immer noch auf den manuellen Einsatz der Administratoren gesetzt, obwohl ein Einsatz von Fast-Start Failover mit dem Data Guard Observer eine Downtime deutlich verringern kann.

Durch die gesammelten Erfahrungen bei einer Änderung des Hochverfügbarkeitskonzepts einer deutschen Großbank auf Fast-Start Failover wurden die Funktionalitäten, die Möglichkeiten und die Vor- bzw. Nachteile von Data Guard mit und ohne Observer erläutert.

Ziel des Vortrags war es, neben dem Verständnis auch die Inspiration und den Anreiz für den vermehrten Einsatz des Observers zur Erleichterung des DBA-Alltags darzustellen.

APEX-Security – Ein Überblick für Einsteiger (Referent: Raphael Salguero)

Applikationen sind mit Oracle APEX schnell entwickelt, allerdings kommen oft wichtige Sicherheitsaspekte zu kurz. Dass hierbei meist nachlässig mit wichtigen Unternehmensdaten umgegangen wird, ist den Entwicklern oftmals gar nicht bewusst.

So reicht einem potenziellen Angreifer bereits die Ergänzung eines Eingabefeldes um wenige Wörter aus, um mittels SQL-Injection an Datensätze zu gelangen. In diesem Vortrag sensibilisierte der Referent Raphael Salguero die APEX-Entwickler durch das Aufzeigen diverser Sicherheitslücken in der Theorie und in der Praxis.

Gleichzeitig wurden Hinweise geliefert, wie die Sicherheit der Applikationen bereits mit einfachen Mitteln erhöht werden kann.

Die Referenten ziehen eine positive Bilanz

Alle Vorträge waren sehr gut besucht und die anschließenden interessanten Gesprächen führten zu einem durchweg positiven Fazit der diesjährigen DOAG Konferenz & Ausstellung. Somit steht den Planungen für die DOAG 2019 nichts mehr im Wege.

Impressionen von der DOAG 2017

Neuheiten Java 9 (Teil II)

Java 9 macht schlank, kann aber noch mehr?

Im ersten Teil kam das Hauptthema von Java 9, die Modularisierung (Codewort Jigsaw), in Grundzügen zur Sprache. Wir wollen nun einen erweiterten Blick auf dieses Feature von Java 9 nehmen, indem wir Auswirkungen der Modularisierung betrachten. Eine wichtige stellt die Möglichkeit dar, wesentlich schlankere Anwendungspakete schnüren zu können. Aber auch weitere bedeutende Neuerungen sollen hier in den Fokus genommen werden.

Jigsaw – die Auswirkungen?

Modularisierung in Java 9 arbeitet – welch Wunder – mit Modulen, das haben wir in Teil I schon ausgearbeitet. Module ermöglichen eine zusätzliche Gruppierung von Java-Strukturen oberhalb von public. Die Beschreibung findet sich in einer speziellen, modul-spezifischen Datei namens `modul-info.java`. Darin steht der Name/ID des Moduls, die Abhängigkeiten des Modul zu anderen Modulen und die eigenen, für andere nutzbaren APIs.

Das speziell Neue bei Modulen ist die Fortführung der Abkapselung auf JAR-Ebene. Das heißt, anders als bei früheren Java Versionen gibt es es für nicht authorisierte Stellen keine Möglichkeit, auf Modulinhalte in JAR-Dateien zuzugreifen. Das unterscheidet sich fundamental zum alten Reflection-Mechanismus, mit dessen Hilfe es möglich war, auch auf die innersten Strukturen der Java Runtime Zugriff zu erlangen. Eine gewisse Berühmtheit hat dabei die Klasse `sun.misc.Unsafe` erlangt, in der spezifische, betriebssystemnahe Methoden untergebracht sind. Mittels Reflection konnte man auch darauf zugreifen und sich in den Innereien des Betriebssystems austoben – mit unabsehbaren Gefahren für die Sicherheit und die Abwehrmöglichkeit gegen Schadsoftware, Viren und feindliche Attacken.

Gerade diese spezielle Klasse hat allerdings immense Bedeutung für viele Unternehmen, die Frameworks und Tools basierend auf Java anbieten, wie z.B. Hadoop, Cassandra, Spring, um nur einige zu nennen.

Modularisierung bringt Performance-Gewinne – wie das?

Ein weiterer positiver Effekt der Modularisierung ergibt sich durch die Möglichkeit der exakten Schneidung einer Java-Anwendung. Bei Nutzung der Modultechnik ist es unabdingbar, genau zu spzifizieren, was benötigt und was zur Verfügung gestellt wird (siehe **`modul-info.java`**).

Daraus folgt aber auch, dass nicht mehr gebraucht wird als nötig, d.h. der Compiler und Linker kann zur Anwendung genau das – und nur das – packen, was zum reibungslosen Funktionieren erforderlich ist. Das kann zu wesentlich kleineren Installationspaketen und Runtime Images führen, was wiederum Lade- und Ausführungszeiten in der JVM senken kann. Die Mindestgröße früherer Anwendungen (<= Java 8) wurde bestimmt von der Größe der Runtime-Bibliothek **`rt.jar`**, welche praktisch die gesamte Java API beinhaltete und immer mitsamt der Anwendung installiert sein musste (zum Umfang der **`rt.jar`** siehe Abbildung 2).

Performance-Gewinne ergeben sich durch schnelleres Laden von Klassen und viel unkompliziertere Handhabung des Classpath bzw. Modulpath. Der Classpath musste früher aufwendig durchsucht werden und es konnte leicht zu Konflikten führen, wenn Klassen mehrfach auftraten.

Mit jlink zurück zu schlanker Figur

Mit **`jlink`** hat Java 9 genau das Werkzeug bekommen, um zielgenaue Laufzeit-Images erstellen zu können. Was ist damit gemeint? Stellen wir uns vor, eine Java-Anwendung soll mit minimalem Speicher auf der Platte auskommen.

Bisher war es notwendig, dass wenigstens eine vollwertige JRE vorliegt. Mit dem Modulkonzept und **`jlink`** können wir nun ein maßgeschneidertes Paket zusammenstellen. In solche Images gelangen nur genau die Module und Konstrukte, die für den Betrieb der Anwendung benötigt werden. Das stellt eine Abkehr von der alten Java-Strategie dar, nach der nahezu alle Strukturen der Java-Laufzeitumgebung in der **`rt.jar`** (Runtime Jar) untergebracht waren.

Die Aufrufsyntax von jlink ist fast selbsterklärend:

```
jlink [jlink Optionen]
--module-path <Modulpfad>
--add-modules <Liste von Root-Modulen>
--output <Verzeichnisname>
```

`modul-path` bezeichnet den Pfad zu „unseren“ Modulen, also zu den applikationsspezifischen Programmanteilen. Es ist erstaunlich, dass das ausreichen soll, aber durch die explizite Angabe von Abhängigkeiten mittels **`exports`** und **`requires`** kann das System exakt ermitteln, welche Module insgesamt notwendig sind für einen reibungslosen Programmablauf.

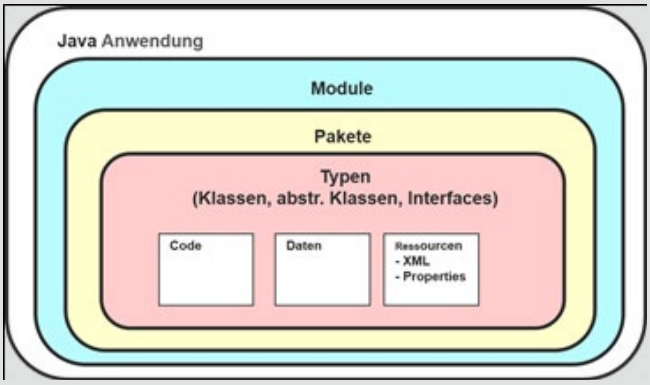


Abb. 1: Grundsätzliche Darstellung der Hierarchiestufen im Java-System. Mit Modulbildung ist eine zusätzliche Gruppierung und Kapselung von Paketen möglich.

```
    1 META-INF/
    2 META-INF/MANIFEST.MF
    3 com/oracle/net/Sdp$1.class
    4 com/oracle/net/Sdp$SdpSocket.class
    5 com/oracle/net/Sdp.class
    6 com/oracle/nio/BufferSecrets.class
    7 com/oracle/nio/BufferSecretsPermission.class
    8 com/oracle/util/Checksums.class
    9 com/oracle/webservices/internal/api/
EnvelopeStyle$Style.class
   10 com/oracle/webservices/internal/api/EnvelopeStyle.
class
   11 com/oracle/webservices/internal/api/EnvelopeStyleFea-
ture.class
   12 com/oracle/webservices/internal/api/databinding/
Databinding$Builder.class
...
19728 java/lang/System.class
19729 java/lang/ClassLoader.class
19730 java/lang/Cloneable.class
19731 java/lang/reflect/Type.class
19732 java/lang/reflect/AnnotatedElement.class
19733 java/lang/reflect/GenericDeclaration.class
19734 java/lang/Class.class
19735 java/lang/CharSequence.class
19736 java/lang/Comparable.class
19737 java/io/Serializable.class
19738 java/lang/String.class
19739 java/lang/Object.class
```

Abb. 2: Ein kleiner Auszug der rt.jar aus JRE 8, der Anfang und das Ende. Es beinhaltet die gesamte Java-API mit insgesamt ca. 19700 class-Dateien, was zur Gesamtgröße von ca. 52 MB führt.

Diese Möglichkeit der Verschlankung kommt dem aktuellen Trend der Verkleinerung entgegen. Neben den immer größer und leistungsfähiger werdenden Serversystemen gibt es zahllose technische IT-Einheiten mit begrenztem Anforderungsprofil, die immer kleiner werden. Zu nennen wäre da beispielhaft Sensortechnik im Maschinenbau, wo es z.B. lediglich um genaue Temperaturmessungen und ggf. daraus abzuleitende Verfahrensschritte gehen könnte. Für solche Aufgaben-

```
Stream.of(2,4,6,8,9,10,12)
    .takeWhile(n->n%2==0)
    .forEach(System.
out::println);

// Ausgabe:
// 2
// 4
// 6
// 8
```

```
Stream.of(2,4,6,8,9,10,12)
    .dropWhile(n->n%2==0)
    .forEach(System.
out::println);

// Ausgabe:
// 9
// 10
// 12
```

Abb. 3: Methode `Stream::takeWhile()`, um Elemente solange zu adressieren, bis eine Bedingung erfüllt ist (hier: `n % 2 == 0`, also die ersten Zahlen, die gerade sind). Auch zu sehen ist die antagonistische Methode `Stream::dropWhile()`.

```
Stream.iterate(1, i -> 2 * i)
   .forEach(System.out::println);
// Ausgabe: 1 2 4 8 ...

Stream.iterate(1, i -> i <= 10, i -> 2 * i)
   .forEach(System.out::println);
// Ausgabe: 1 2 4 8
```

Abb. 4: `Stream::iterate()` erlaubt nun die begrenzte Erzeugung von Stream-Inhalten. Dazu ist eine überschriebene Methode mit drittem Argument hinzugekommen. Dieses Argument stellt eine Abbruchbedingung dar, ähnlich wie einer klassischen For-Loop.

Dr. Hubert Austermeier
(info@ordix.de)

stellungen kommen schmalbrüstig definierte Kleinstcomputer zum Einsatz, für die die absolute Größe eines Laufzeitimages ein entscheidendes Kriterium sein können.

Ein weitere Stream-API: takeWhile, dropWhile

Mit Java 8 kamen die coolen Streams, die mit den gleichzeitig eingeführten Lambdas ein mächtiges Programmierparadigma anbieten. Die Stream-API ist die Java-Anwort auf immer größer werdende Datenmengen und auf das Thema Big Data. Anstatt beispielsweise eine große Datenstruktur (> 10 Mio. Datenelemente) in eine Java-Collection zu packen und sie als Ganzes zu handhaben, kann man einen Stream definieren. Der geht elementweise vor, nimmt sich das erste Element vor, dann das zweite usw. Das erlaubt den effizienten Umgang mit riesigen und mit potenziell unendlichen Datenstrukturen (Beispiel: alle positiven, ganzen Zahlen).

Java 9 hat einige neue Methoden zur Stream API im Gepäck, als da wären:

1. **`Stream::takeWhile()`**
2. **`Stream::dropWhile()`**
3. **`Stream::ofNullable()`**
4. **`Stream::iterate() (`**

Die ersten beiden sind antagonistisch zueinander, beide verarbeiten nur einen Teil eines Streams, wobei **`takeWhile()`** genau die nimmt, die **`dropWhile()`** weglässt. Wir sehen uns das an einem Beispiel genauer an, es sollte dadurch offensichtlich werden (siehe Abbildung 3).

Fazit

Mit der Modularisierung bekommen wir ein mächtiges Werkzeug an die Hand, um Java-Anwendungen sicherer, kompakter und performanter gestalten zu können.

In diesem Artikel lag der Schwerpunkt auf der Kompaktheit, die durch den Wegfall der **`rt.jar`** erreicht wird.

Selbstverständlich gibt es dazu eine Seminarveranstaltung „Java-Neuheiten“. Dort lernen Sie als Seminarteilnehmer die wesentlichen Neuerungen zu Java 8, 9 und 10 kennen.

Oracle AWR Warehouse

Alles unter einem Dach

Mit dem AWR Warehouse bietet Oracle die Möglichkeit, Performance-Daten langfristig an einem zentralen Ort zu speichern. Dieser Artikel erläutert die Funktionsweise eines AWR Warehouse.

Was ist das AWR?

Mit der Oracle Datenbank Version 10 wurde das Automatic Workload Repository (AWR) eingeführt. Es dient als Speicherort für Datenbank-Performance-Daten. Die Daten werden in internen Tabellen im Tablespace **SYSAUX** gespeichert und standardmäßig acht Tage aufbewahrt.

Auf der Grundlage dieser Daten besteht die Möglichkeit, Berichte (sogenannte AWR Reports) zu erstellen. Diese sind hilfreich für allgemeine Performance-Auswertungen sowie zur Erkennung von Engpässen.

Es können Berichte von verschiedenen Zeiträumen erstellt beziehungsweise das Lastverhalten verschiedener Zeiträume miteinander verglichen werden.

Das AWR Warehouse – Überblick

Mit dem Oracle Enterprise Manager 12cR4 führte Oracle das neues Feature "AWR Warehouse“ (AWR WH) ein.

Dieses ermöglicht es dem Administrator, AWR-Statistiken von individuellen Datenbanken in einer zentralen WAR-Repository-Datenbank zu speichern und für Auswertungszwecke bereitzustellen. Durch das zentrale Repository sind die AWR-Daten auch nach einer Datenbankmigration noch vorhanden und zugreifbar.

Das Verlagern der Statistikdaten von einzelnen Quelldatenbanken an einen zentralen Ort eröffnet die Möglichkeit, den Haltezeitraum der Statistikdaten auf den einzelnen Datenbanken zu reduzieren und somit gleichzeitig Platz in den einzelnen Datenbanken zu sparen.

Die Verwaltung der Quelldatenbanken erfolgt über den Enterprise Manager Cloud Control (EMCC). Hier können Quelldatenbanken dem AWR WH hinzugefügt und entfernt werden (siehe Abbildung 1).

Architektur

Als Basis für das AWR WH wird ein EMCC sowie eine Repository-Datenbank benötigt. Oracle empfiehlt, das Repository in einer separaten Datenbank zu erstellen, welche nicht mit der des EMCC identisch ist.

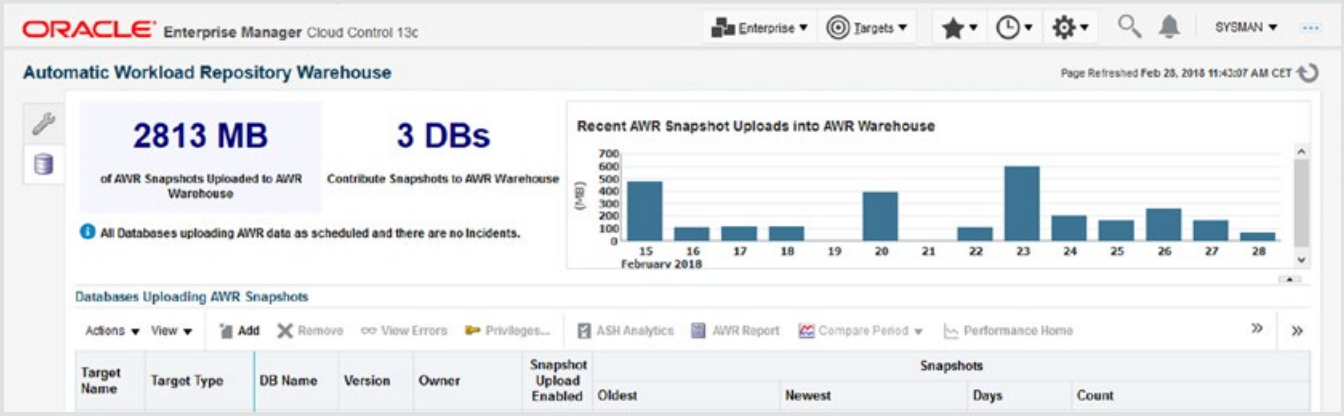


Abb. 1: Automatic Workload Repository Warehouse

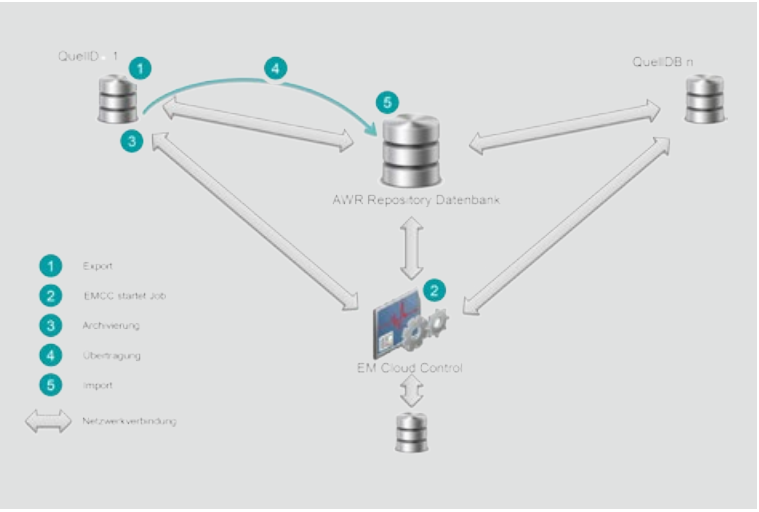


Abb. 2: Netzwerk-Architektur

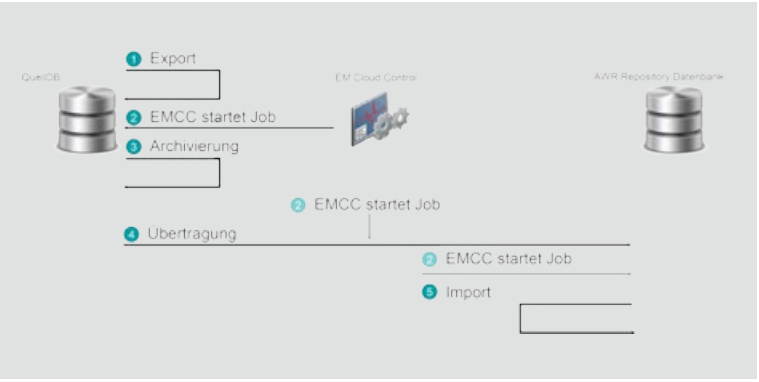


Abb. 3: Ablauf des ETL-Job

Voraussetzung für das AWR WH Repository ist eine Oracle-Enterprise-Edition-Datenbank in der Version 12.1.0.2 oder höher. Alternativ kann die Version 11.2.0.4 mit entsprechenden Patches verwendet werden. Die Repository-Datenbank darf zum jetzigen Zeitpunkt keine Container-Datenbank (NON-CDB) sein.

Der Oracle Management Server (OMS) muss mindestens in der Version 12.1.0.4.3 mit installiertem Patch 19391521 vorliegen.

Quelldatenbanken werden ab der Version 10.2.0.4 unterstützt. Die höchste, unterstützte Version wird durch die WAR-Warehouse-Repository-Datenbank vorgegeben. Es können keine Quelldatenbanken mit einer höheren Version als die der Repository-Datenbank genutzt werden. Dies ist in der Updatepolitik entsprechend zu beachten.

Für das Zusammenspiel zwischen den Quelldatenbanken und der AWR Repository Datenbank ist ein ETL-Job zuständig. Der ETL-Job überträgt die gesammelten Statistikdaten der einzelnen Datenbanken in das AWR WH. Über das EMCC können die Zugriffsrechte für die Benutzer auf Basis der Quelldatenbanken verwaltet werden.

Ablauf des ETL-Prozesses

Der ETL-Prozess ist in drei logische Phasen aufgeteilt:

- Export
- Transport
- Import

Im Folgenden wird von der Funktionsweise der EMCC Version 13c R2 ausgegangen, da die Import-Job-Ansteuerung im Vergleich zur Version 12c verändert wurde. Der Import-Job wird jetzt über den EMCC angesteuert, anstelle über den Scheduler auf der Datenbank.

Der Export-Job wird immer lokal auf den Quell-Datenbanken gestartet. Im Gegensatz dazu müssen Transport und Import-Job über das EMCC gestartet werden. Dieser Vorgang wird in den folgenden Phasen 1 bis 5 genauer erläutert (siehe Abbildung 2 und 3).

1. Phase: Export

Zunächst erstellt der Job **`MGMT_CAW_EXTRACT`** auf der Quelldatenbank einen Data Pump Export der Statistikdaten. Diese werden standardmäßig unter **`$AGENT_INSTANCE_HOME`** gespeichert. Um nicht zu große Exportdateien zu generieren, kann die maximale Anzahl an Snapshots für eine Exportdatei begrenzt werden (default 500). Bei Überschreitung des Wertes werden mehrere Exportdateien erstellt. Die Exportdateien werden im folgenden Format abgelegt: **`<em_id>_<sys_guid>_<dbid>_<von-Snap-ID>_<bis-Snap-ID>.dmp`**.

2. Phase: Start ETL-Prozess

Das EMCC startet periodisch (default alle 24h) den eigentlichen ETL-Prozess. Im EMCC kann der Fortschritt der einzelnen Tasks angezeigt und überwacht werden.

3. Phase: Archivierung

In dieser Phase komprimiert der Agent die Export-Datei auf dem Server der Quelldatenbank.

4. Phase: Übertragung

Die archivierte Datei wird vom lokalen Agenten mittels ssh-Verbindung an den Agenten des Repository-Servers übergeben und dort unter **`$AGENT_INSTANCE_HOME/war_t`** abgelegt.

5. Phase: Import

Mittels der Prozedur **`dbsnmp.mgmt_caw_load.run_master`** werden diese exportierten Daten der Quelldaten-

bank in die AWR-Repository-Datenbank importiert. Dies erfolgt in zwei Schritten. Im ersten Schritt importiert die Repository-Datenbank die Data-Pump-Daten in ein temporär erzeugtes Schema. Anschließend werden die Daten ins SYS-Schema geladen.

Wenn diese Phase beendet ist, sind die Daten aus der Quelldatenbank in der Repository-Datenbank zu Analysezwecken verfügbar.

Unterstützung der Multitenant-Architektur

In der aktuellen Version bietet Oracle AWR WH die Möglichkeit, AWR-Daten auf CDB-Ebene bereitzustellen. Das mit 12c R2 eingeführte Feature von AWR-Reports auf PDB-Ebene wird aktuell noch nicht unterstützt.

Sizing und Kompression

Der benötigte Speicherplatz im AWR hängt von mehreren Faktoren ab. Bei 10 aktiven Sessions fallen ca. 1–2 MB an Daten pro Snapshot an. Daher ist pro Quelldatenbank bei einem Snapshot-Intervall von 60 Minuten (default) mit ca. 24-48 MB pro Tag zu rechnen. Diese Daten werden im SYSAUX-Tablespace gespeichert.

Für eine detaillierte WAR-Analyse können die Skripte **`awrinfo.sql`** und **`utlsyxsz.sql`** verwendet werden.

Sie stellen Inhalte bereit über:

- WAR-Tabellen-Details
- WAR-Retention-Informationen
- WAR-Snapshot-Informationen
- SYSAUX-Tablespace-Belegung

Um einen fehlerfreien Import der Quelldaten in die Repository-Datenbank zu gewährleisten, muss sichergestellt werden, dass im **`SYSAUX`**-Tablespace genügend freier Speicherplatz vorhanden ist. Weiterhin muss auf Filesystem-Ebene (der WAR-Repository-Datenbank) ausreichend Speicherplatz zum temporären Speichern der Dump-Dateien vorhanden sein. Hier empfiehlt Oracle, 50 GB zu reservieren.

Durch den Einsatz von Oracle Advanced Compression kann der benötige Speicherbedarf reduziert werden. Dabei sind die geltenden Lizenzbedingungen zu beachten.

Glossar

Oracle Management Server (OMS)
Im Zusammenhang mit dem Enterprise Manager Cloud Control (EMCC) beziehungsweise dem Oracle Enterprise Manager Cloud Control eine Middleware zwischen dem Oracle Agenten und der Oracle Management Console.

Enterprise Manager Cloud Control (EMCC)
Ein webbasiertes Management Tool mit einer grafischen Oberfläche.

Extract, Transform, Load (ETL)
Beschreibt einen Prozess, welcher die relevanten Daten aus Quellen extrahiert, die Daten in das Format der Zieldatenbank transformiert und diese am Ende in die Zieldatenbank speichert.

Non-CDB
Beschreibt die klassischen Oracle-Architektur im Gegensatz zur neuen Container Datenbank-Architektur (CDB), welche mit der Oracle Version 12c eingeführt wurde.

Fazit

Mit dem AWR WH existiert eine Möglichkeit, Anforderungen der Performance-Analyse zentral und weitestgehend unabhängig von den zu betrachtenden Datenbanken durchzuführen. Ebenso gehen bei einer Datenbankmigration oder einem Plattformwechsel keine AWR-Daten mehr verloren.

Die Analyse von Statistikdaten und deren Vergleich wird mit steigender Anzahl von Datenbanken immer bedeutender. Mit dem AWR WH bietet Oracle ein mächtiges Tool, um diesem Bedürfnis nachzukommen.

In der aktuellen Version können Auswertungen von NON-CDB-Datenbanken als auch von CDB-Datenbanken erstellt werden. Analysen und Vergleiche von WAR-Reports auf PDB-Ebene sind aktuell nicht möglich. Die in EMCC 13c eingeführten Änderungen gestatten eine bessere Überwachung der Prozesse vom EMCC aus, was einen erheblichen Vorteil zur Vorgängerversion darstellt.

Bei der Analyse Ihres Systems und der Implementierung eines WAR-Warehouses unterstützen wir Sie gerne.

Marcel Cossijns
(info@ordix.de)

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 €	18.02. | 06.05. | 26.08. | 04.11.
DB-BIG-02	Big Data: Apache Hadoop Grundlagen	3 Tage	1.390,00 €	18.03. | 24.06. | 23.09. | 02.12.
DB-NSQL-01	Einführung in NoSQL-Datenbanken	2 Tage	1.090,00 €	21.03. | 27.06. | 26.09. | 05.12.
Data Warehouse				
DB-DB-03	Data Warehouse Grundlagen	3 Tage	1.290,00 €	19.02. | 07.05. | 19.08. | 05.11.

PostgreSQL

DB-PG-01	PostgreSQL Administration	5 Tage	1.990,00 €	04.03. | 06.05. | 12.08. | 21.10.

Oracle

Entwicklung				
DB-ORA-01	Oracle SQL	5 Tage	1.990,00 €	04.03. | 20.05. | 29.07. | 23.09. | 04.11.
DB-ORA-01A	Oracle SQL Workshop für Experten	3 Tage	1.490,00 €	04.02. | 13.05. | 01.07. | 07.10. | 02.12.
DB-ORA-02	Oracle Datenbankprogrammierung mit PL/SQL Grundlagen	5 Tage	1.890,00 €	18.03. | 03.06. | 12.08. | 18.11.
DB-ORA-34	Oracle Datenbankprogrammierung mit PL/SQL Aufbau	3 Tage	1.390,00 €	01.04. | 15.07. | 02.09. | 09.12.
DB-ORA-42	Oracle PL/SQL für Experten - Performance Analyse & Laufzeitopt.	3 Tage	1.390,00 €	06.05. | 26.08. | 28.10. | 09.12.
DB-ORA-49E	Oracle 12c Neuheiten für Entwickler	3 Tage	1.390,00 €	25.02. | 08.04. | 19.08. | 21.10. |09.12.
DB-ORA-53	Oracle Text	3 Tage	1.490,00 €	27.03. | 13.05. | 16.09. | 16.12.
DB-ORA-51	Oracle Spatial	3 Tage	1.490,00 €	18.02. | 13.05. | 22.07. | 11.11.
DB-ORA-46	Oracle APEX Anwendungsentwicklung Grundlagen	3 Tage	1.490,00 €	06.05. | 05.08. | 07.10.
DB-ORA-47	Oracle APEX Anwendungsentwicklung Aufbau	3 Tage	1.490,00 €	04.02. | 20.05. | 19.08. | 28.10.
Administration				
DB-ORA-03	Oracle Datenbankadministration Grundlagen	5 Tage	1.990,00 €	11.02. | 08.04. | 24.06. | 09.09. | 25.11.
DB-ORA-04	Oracle Datenbankadministration Aufbau	5 Tage	1.990,00 €	11.03. | 13.05. | 08.07. | 16.09. | 02.12.
DB-ORA-07	Oracle Tuning - Theorie und Interpretation von Reports	5 Tage	2.290,00 €	18.03. | 01.07. | 23.09. | 18.11.
DB-ORA-08	Oracle Grid Infrastructure und Real Application Cluster (RAC)	5 Tage	2.290,00 €	25.02. | 06.05. | 15.07. | 02.09. | 11.11.
DB-ORA-49A	Oracle 12c / Oracle 18c Neuheiten	5 Tage	2.190,00 €	25.03. | 03.06. | 26.08. | 14.10. | 02.12.
DB-ORA-49B	Oracle 18c Neuheiten	2 Tage	1.090,00 €	28.03. | 06.06. | 29.08. | 17.10. | 05.12.
DB-ORA-52W	Oracle Lizenz Workshop Webinar	1 Tag	590,00 €	Termine auf Anfrage
DB-ORA-33	Oracle Security	4 Tage	1.890,00 €	04.03. | 20.05. | 12.08. | 21.10. | 16.12.
DB-ORA-35	Oracle Cloud Control	3 Tage	1.590,00 €	11.03. | 24.06. | 16.09. | 09.12.
DB-ORA-55	Oracle ASM für Single Instance	3 Tage	1.490,00 €	25.03. | 03.06. | 26.08. | 14.10. | 16.12.
DB-ORA-56	Oracle Tenant Technologie (Multi Tenant / Single Tenant)	3 Tage	1.490,00 €	25.03. | 22.07. | 07.10.
DB-ORA-57	Single Sign On mit Oracle	3 Tage	1.490,00 €	01.04. | 08.07. | 28.10.
Backup und Recovery				
DB-ORA-32	Oracle Backup und Recovery mit RMAN	5 Tage	1.990,00 €	01.04. | 29.07. | 21.10
DB-ORA-31	Oracle Data Guard	4 Tage	1.890,00 €	04.02. | 13.05. | 05.08. | 04.11.
MySQL				
DB-MY-01	MySQL Administration	4 Tage	1.490,00 €	11.02. | 08.04. | 15.07. | 21.10.

IBM Datenbanksysteme

Informix				
DB-INF-01	IBM Informix SQL	5 Tage	1.790,00 €	04.03. | 01.07. | 07.10.
DB-INF-02	IBM Informix Administration	5 Tage	1.990,00 €	25.03. | 22.07. | 11.11.
DB2				
DB-DB2-01	IBM Db2 für Linux/Unix/Windows SQL Grundlagen	5 Tage	1.990,00 €	20.05. | 12.08. | 21.10.
DB-DB2-02	IBM Db2 für Linux/Unix/Windows Administration	5 Tage	1.990,00 €	24.06. | 02.09. | 25.11.
DB-DB2-05	IBM Db2 für Linux/Unix/Windows Monitoring und Tuning	3 Tage	1.490,00 €	25.02. | 08.07. | 16.09. | 09.12.
DB-DB2-06	IBM Db2 für Linux/Unix/Windows Backup und Hochverfügbarkeit mit HADR	3 Tage	1.490,00 €	04.02. | 15.07. | 28.10. | 02.12.

Microsoft

Entwicklung				
MS-SQL-01	Querying Data with Transact-SQL	5 Tage	2.190,00 €	18.02. | 05.08. | 18.11.
MS-SQL-07	Updating Your Skills to Microsoft SQL Server 2017	2 Tage	1.290,00 €	28.01. | 11.04. | 29.07. | 28.10.
Administration				
MS-SQL-02	Verwalten einer SQL Datenbankinfrastruktur	5 Tage	2.190,00 €	11.03. | 24.06. | 16.09. | 25.11.
MS-SQL-11	Microsoft SQL Server for Oracle DBAs	4 Tage	1.890,00 €	11.02. | 20.05. | 19.08. | 04.11.
MS-SQL-17W	Microsoft SQL Server 2017 Upgrade Webinar	1 Tag	99,00 €	auf Anfrage

Rechenzentrum

ANSIB-01	Konfigurationsmanagement mit Ansible	3 Tage	1.390,00 €	25.03. | 20.05. | 19.08. | 11.11.
E-DOCK-01	Docker DevOps Workshop	1 Tag	450,00 €	29.03. | 02.07. | 27.09. | 03.12.
SM-NAG-01	Systemüberwachung mit Nagios - Workshop	3 Tage	1.190,00 €	auf Anfrage

Web und Application-Server

INT-04	Apache HTTP Server Administration	3 Tage	1.290,00 €	11.03. | 01.07. | 16.12.
INT-07	Tomcat Konfiguration und Administration	3 Tage	1.290,00 €	18.02. | 08.04. | 05.08. | 21.10. | 09.12
INT-08	WebSphere Application Server Installation und Administration	3 Tage	1.390,00 €	auf Anfrage
INT-12	WildFly Application Server Administration	3 Tage	1.290,00 €	18.03. | 03.06. | 02.09. | 09.12.
DB-ORA-50	Oracle WebLogic Administration Grundlagen	3 Tage	1.390,00 €	11.03. | 11.06. | 02.09. | 25.11.

IT-Security

IT-SEC-01	IT-Sicherheit für Projektmanager und IT-Leiter - ein Überblick	3 Tage	1.690,00 €	11.02. | 10.04. | 03.06. | 02.09. | 18.11
SEC-06	Security Awareness für Mitarbeiter	1 Tag	990,00 €	24.10.
SEC-02	Certified Information Systems Security Professional (CISSP)	5 Tage	3.490,00 €	08.04. | 24.06. | 09.09. | 23.09. | 02.12.
SEC-03	Certified Information Security Manager (CISM)	3 Tage	2090,00 €	25.03. | 02.04. | 13.05. | 21.10. | 29.10.
SEC-04	Certified Information Systems Auditor (CISA)	4 Tage	2.290,00 €	21.05. | 07.10. | 05.11.
Begleitende Coachings zu CISSP (SEC-02C), CISM (SEC-03C), CISA (SEC-04C)			800,00 €	

Projekt- und IT-Management

Klassisches Projektmanagement				
PM-01	IT-Projektmanagement praxisorientiert	3 Tage	1.690,00 €	08.04. | 24.06. | 09.09. | 02.12.
PM-15	Projektmanagement für Führungskräfte - ein Überblick	2 Tage	1.290,00 €	21.02. | 06.05. | 05.08. | 04.11.
PRINCE-01	PRINCE2® Foundation	3 Tage	1.160,00 €	18.03. | 13.05. | 15.07. | 16.09. | 25.11.
PRINCE-02	PRINCE2® Practitioner	3 Tage	1.655,00 €	20.03. | 15.05. | 17.07. | 18.09. | 27.11.
PRINCE-03	PRINCE2® kompakt	5 Tage	2.560,00 €	18.03. | 13.05. | 15.07. | 25.11.
PM-06	Projekte souverän führen - Systemisches Projektmanagement	4 Tage	1.790,00 €	11.02. | 08.07. | 28.10.
PM-05	Projektcontrolling in der IT	2 Tage	1.290,00 €	01.04. | 19.08. | 16.10. | 09.12
PM-07	Krisenmanagement in Projekten - Projektkrisen vorbeugen & meistern	2 Tage	1.290,00 €	07.02. | 23.05. | 17.10.
PM-14	Anforderungsmanagement in IT-Projekten	2 Tage	1.290,00 €	25.03. | 03.06. | 16.09. | 18.11.
Agiles Projektmanagement				
AGIL-01	Agil führen - Neue Konzepte für Ihre Führung im agilen Umfeld	3 Tage	1.490,00 €	18.03. | 17.06. | 04.11.
SCRUM-01	Agiles Projektmanagement mit Scrum - Mit agilem Vorgehen mehr ...	2 Tage	1.290,00 €	13.05. | 23.09.
SCRUM-02	Scrum Vorbereitung zur Zertifizierung - So einfach kann es klappen	1 Tag	690,00 €	15.05. | 25.09.
SCRUM-04	Scrum Product Owner - Produkte erfolgreich entwickeln	3 Tage	1.490,00 €	17.09.
KB-01	KANBAN in der IT - Prozesse & Projekte mit Hilfe von Kanban optimieren	2 Tage	1.290,00 €	28.02. | 04.04. | 16.05. | 26.09.
PM-T-01	Testmanagement für agile und klassische Projekte	2 Tage	1.290,00 €	27.03. | 05.06. | 18.09. | 20.11.
PM-08	Hybrides Projektmanagement	2 Tage	1.290,00 €	20.02. | 08.05. | 14.10.
IT-Management, IT-Strategie und IT-Organisation				
MGM-03	IT-Management - Die IT nachhaltig zum Erfolg führen	3 Tage	1.690,00 €	28.01. | 20.05. | 16.12.
PM-29	Systemische Führung - Führung unter Berücksichtigung aller Aspekte	3 Tage	1.690,00 €	04.02. | 27.05. | 30.09.
K-12	Plötzlich IT-Führungskraft - Von Anfang an richtig führen	4 Tage	1.790,00 €	06.05. | 09.09.
MGM-07	IT-Strategie - strategische IT-Planungen	3 Tage	1.690,00 €	18.02. | 27.05. | 18.11.
MGM-02	IT-Architekturen - Ihre IT-Landschaft sinnvoll gestalten	3 Tage	1.690,00 €	25.02. | 20.05. | 14.10.
PM-10	IT-Controlling - Methoden zur Steuerung der IT	3 Tage	1.690,00 €	24.04. | 02.09.
MGM-04	Geschäftsprozessmanagement (BPM)	3 Tage	1.690,00 €	04.03. | 24.06. | 25.11.
PM-CH-01	Change Management in der IT - Veränderungen reibungslos einführen	3 Tage	1.690,00 €	25.03. | 01.07. | 11.11.
ITIL-01	ITIL® V3 Foundation	3 Tage	952,50 €	11.03. | 06.05. | 08.07. | 09.09. | 04.11.
ITIL-02	ITIL® V3 Practitioner	2 Tage	1.410,00 €	14.03. | 09.05. | 11.07. | 12.09. | 07.11.
ITIL-03	ITIL® V3 kompakt	5 Tage	2.375,00 €	11.03. | 06.05. | 08.07. | 09.09. | 04.11.
PM-28	IT-Organisation - Optimierung Ihrer IT-Organisation	3 Tage	1.690,00 €	11.03. | 21.08. | 25.11.

Kommunikation und Selbstmanagement

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-20	Beratungs Know-How für IT-Experten - Kunden & Kollegen gut beraten	3 Tage	1.390,00 €	24.09.
K-30	Burn-out vorbeugen, bessere Work-Life-Balance erreichen	3 Tage	1.340,00 €	01.04. | 22.07. | 21.10.
K-40	Heikle Gespräche	3 Tage	630,00 €	15.02. | 30.04. | 18.07. | 04.10.

Betriebssysteme & Monitoring

Unix/Linux				
BS-01	Unix/Linux Grundlagen für Einsteiger	5 Tage	1.790,00 €	04.02. | 01.04. | 15.07. | 09.09. | 04.11.
BS-02	Linux Systemadministration	5 Tage	1.790,00 €	11.02. | 08.04. | 29.07. | 23.09. | 11.11.
BS-25	Unix Power Workshop für den Datenbank- & Applikationsbetrieb	5 Tage	1.890,00 €	25.02. | 13.05. | 12.08. | 25.11.
BS-27	Neuerungen SUSE Linux Enterprise Server 12	3 Tage	1.290,00 €	25.02. | 03.06. | 16.09. | 16.12.
BS-09	Linux Cluster mit Pacemaker und Corosync	3 Tage	1.490,00 €	18.02. | 13.05. | 26.08. | 18.11.
Solaris				
BS-03-11	Solaris 11 Systemadministration Grundlagen	5 Tage	1.990,00 €	11.03. | 01.07. | 14.10.
BS-04-11	Solaris 11 Systemadministration Aufbau	5 Tage	1.990,00 €	18.03. | 22.07. | 02.12.
BS-06-11	Solaris 11 für erfahrene Unix/Linux-Umsteiger	3 Tage	1.990,00 €	auf Anfrage
IBM AIX				
AIX-01	IBM AIX Systemadministration Grundlagen	5 Tage	1.990,00 €	04.03. | 06.05. | 16.09. | 09.12.
AIX-04	IBM AIX Systemadministration Power Workshop	3 Tage	1.390,00 €	11.03. | 08.07. | 07.10.
AIX-02	IBM AIX Installation, Backup und Recovery mit NIM	3 Tage	1.390,00 €	18.03. | 22.07. | 11.11.

Entwicklung

Allgemeines				
OO-01	Einführung in die objektorientierte Programmierung und UML	3 Tage	1.190,00 €	18.03. | 24.06. | 23.09.
E-SWA-01	Softwarearchitekturen	5 Tage	1.890,00 €	25.02. | 13.05. | 23.09. | 09.12.
Script-Sprachen				
PSHELL-01	Windows PowerShell Für Administratoren	3 Tage	1.490,00 €	18.02. | 06.05. | 01.07. | 23.09. | 09.12.
P-PERL-01	Perl Programmierung	5 Tage	1.790,00 €	08.04. | 15.07. | 09.09. | 16.12.
P-UNIX-01	Shell, Awk und Sed	5 Tage	1.690,00 €	18.03. | 08.07. | 07.10. | 02.12.
P-PYTH-01	Python Programmierung	4 Tage	1.590,00 €	18.02. | 11.03. | 08.07. | 09.09. | 25.11.
XML				
P-XML-01	XML Grundlagen	3 Tage	1.290,00 €	04.02. | 20.05. | 26.08. | 07.10.
Java				
P-JAVA-01	Java Programmierung Grundlagen	5 Tage	1.790,00 €	01.04. | 29.07. | 14.10.
P-JAVA-03	Java Programmierung Aufbau	5 Tage	1.790,00 €	11.02. | 18.03. | 06.05. | 12.08. | 11.11.
P-JEE-08	Java Performance Tuning	3 Tage	1.490,00 €	18.03. | 15.07. | 14.10. | 02.12.
P-JAVA-11	Java Neuheiten	2 Tage	990,00 €	14.02. | 06.06. | 05.09. | 07.11.
Java EE				
P-JAVA-12	Java EE Power Workshop	5 Tage	1.890,00 €	18.02. | 20.05. | 19.08. | 04.11.
J-HIB-01	Java Persistence API mit Hibernate	5 Tage	1.790,00 €	04.03. | 01.07. | 02.09. | 25.11.
INT-05	Java Web Services	3 Tage	1.290,00 €	25.03. | 29.07. | 28.10.
P-JEE-06	Spring Power Workshop	5 Tage	1.790,00 €	25.03. | 08.07. | 07.10. | 02.12.
MICRO-01	Microservices Workshop mit Spring Boot	5 Tage	1.790,00 €	08.04. | 22.07. | 21.10. | 09.12.
Web- und GUI-Entwicklung				
P-PHP-01	PHP Programmierung	5 Tage	1.790,00 €	11.03. | 20.05. | 16.09. | 18.11.
P-JEE-05	Rich Internet Application mit JSF und Primefaces	5 Tage	1.790,00 €	25.02. | 08.04. | 26.08. | 11.11.
P-JEE-05A	Webanwendungen mit JavaServer Faces (JSF)	5 Tage	1.790,00 €	04.02. | 13.05. | 09.09. | 25.11.
E-ANG-02	Webanwendungen mit Angular	3 Tage	1.590,00 €	03.04. | 07.08. | 20.11.
E-TYPSC-01	TypeScript Grundlagen	2 Tage	1.190,00 €	01.04. | 05.08. | 18.11.
Tools und Verfahren				
P-CI-01	Continuous Integration (CI) Workshop	3 Tage	1.390,00 €	11.02. | 03.06. | 02.09. | 04.11.

OAuth 2.0 und Java Spring

REST-Schnittstellen absichern mit Spring, OAuth2.0 & JSON Web Token

Durch die zunehmende Verwendung des Microservice-Architektur-Patterns ist eine zentrale Instanz zur Verwaltung der Benutzeranmeldeinformationen unabdingbar. Das Autorisierungsprotokoll OAuth 2.0 bietet hierfür im Zusammenspiel mit Java Spring eine perfekte Basis. Dieser Artikel veranschaulicht anhand eines Beispiels, wie sich dies in der Praxis realisieren lässt.

OAuth2.0

Das offene Autorisierungsprotokoll OAuth 2.0 gehört zu den bekanntesten Autorisierungsverfahren der heutigen Zeit. Ziel dieses Protokolls ist es, einem Endnutzer Zugriff zu seinen Ressourcen (bzw. REST-Schnittstellen) zu gewähren.

Das OAuth2.0 Protokoll unterstützt hierbei verschiedene Verfahren zur Autorisierung von Nutzern [1]. Grundsätzlich wird bei den Verfahren immer zwischen dem Resource-Owner, dem Ressource-Server und dem Autorisierungs-Server unterschieden. Der Resource-Owner (oder auch Endnutzer) autorisiert sich mittels Nutzername und Passwort gegenüber dem Autorisierungsserver. Dieser stellt daraufhin ein Access-Token (dt. „Zugriffs-Marke“) aus. Mithilfe dieses Access-Tokens kann der Nutzer nun eine Anfrage an den Ressourcenserver stellen.

Der Ressourcenserver prüft daraufhin die Integrität des Access-Tokens und verarbeitet dann den Aufruf. Das in diesem Artikel verwendete „Password-Credentials“-Verfahren wird in der Abbildung 1 genauer dargestellt. Weitere Informationen zu diesem Verfahren lassen sich der Link-Sammlung entnehmen.

JSON Web Token

Innerhalb des OAuth2.0-Verfahrens wird die Beschaffenheit des Access-Tokens nicht weiter erläutert. Als Standard

hat sich hier das JSON Web Token etabliert, welches sich für JavaScript Clients, wie beispielsweise Angular- oder React-Anwendungen, sehr gut verarbeiten lässt.

Das JSON Web Token (JWT) ist ein JSON-Objekt, dass laut RFC 7519 [2] als sicherer Weg definiert ist, um Informationen zwischen zwei Parteien auszutauschen. Ein JWT ist eine Aneinanderreihung von Header, Payload und Signatur. Diese drei Bestandteile werden durch einen Punkt „.“ voneinander getrennt und enthalten folgende Informationen:

- **Header**
  Der Header enthält Informationen bzgl. des Verschlüsselungsverfahrens.
- **Payload**
  Innerhalb des Payloads werden die Daten des Tokens vorgehalten. Hierunter fallen Informationen wie das Subjekt, für das das Token ausgestellt wurde – also der Nutzer, der Name des Nutzers, wie auch Informationen über die Haltbarkeit des JSON Web Tokens.
- **Signatur**
  Die Signatur ist zur Validierung des Tokens gedacht. Hierdurch lässt sich errechnen, ob der Token kompromittiert wurde. Die Berechnung der Signatur ist abhängig von dem verwendeten Verschlüsselungsverfahren.

Für Testzwecke lassen sich diese JSON Web Tokens auch online valideren. Hierfür kann die Webseite von JWT.io [3] verwendet werden.

Architektur

Um einer Microservice-Landschaft gerecht zu werden, wird für dieses Beispiel auf zwei unabhängige Microservices gesetzt. Beide Applikationen verwenden als Grundlage Java und setzten darüber hinaus das Framework Spring ein. Das Spring-Framework [4] hat sich in den letzten Jahren als De-facto-Standard für die Entwicklung von Microservices im Bereich Java etabliert und bietet eine Reihe von Tools zur Unterstützung in diesem Architektur-Pattern an. Als Paketmanager wird Maven eingesetzt. Die grundlegenden Abhängigkeiten beider Microservices können der Abbildung 2 entnommen werden.

Die Applikationen werden in ihren Funktionalitäten wie folgt geschnitten:

- **Autorisierungsserver**
  Der Autorisierungsserver ist verantwortlich für die Ausstellung der JSON Web Tokens. Darüber hinaus ist er für die Validierung eingehender Anfragen gegen den REST-Service verantwortlich.
- **Ressourcenserver**
  Der Ressourcenserver stellt Endpunkte zur Abfrage von Informationen (Ressourcen) für einen Endbenutzer zur Verfügung. Eingehende Anfragen an diesen Server werden zunächst vom Autorisierungsserver validiert und dann ausgeführt.

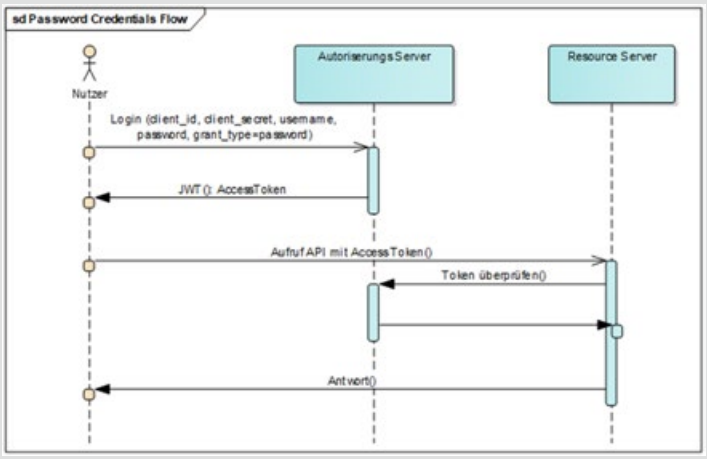


Abb. 1: OAuth2.0 – Password Credentials Flow

```
...
<parent>
   <groupId>org.springframework.boot</groupId>
   <artifactId>spring-boot-starter-parent</artifactId>
   <version>2.0.3.RELEASE</version>
</parent>
<properties>
   <java.version>1.8</java.version>
</properties>
...
```

Abb. 2: Grundlegende Abhängigkeiten beider Applikationen (pom.xml)

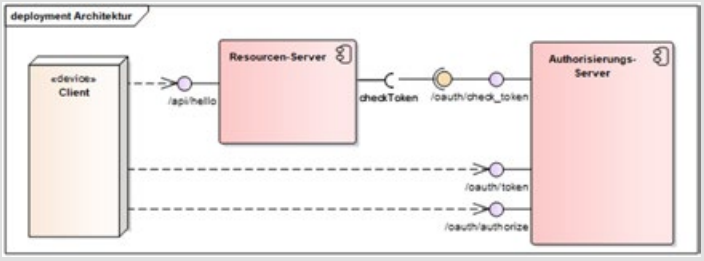


Abb. 3: Die grundlegende Beispielarchitektur

Zur Veranschaulichung werden die Anfragen später mittels Postman [1] an den Ressource-Server gestellt. Postman bietet darüber hinaus die Möglichkeit, sich gegenüber einem OAuth-Server automatisch zu autorisieren.

Der Autorisierungsserver

Als Herzstück dieses Projektes kann der Autorisierungsserver angesehen werden. Dieser ist, wie bereits oben

beschrieben, für die Ausstellung und Validierung der JSON Web Tokens verantwortlich. Zur Konfiguration dieser Schnittstellen werden zwei Abhängigkeiten aus dem Spring-Framework verwendet (siehe Abbildung 4):

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://maven.apache.org/POM/4.0.0
http://maven.apache.org/xsd/maven-4.0.0.xsd">
…
  <dependencies>
    <dependency>
      <groupId>org.springframework.boot</groupId>
      <artifactId>spring-boot-starter-data-rest</artifactId>
    </dependency>
    <dependency>
      <groupId>org.springframework.boot</groupId>
      <artifactId>spring-boot-starter-test</artifactId>
      <scope>test</scope>
    </dependency>
    <dependency>
      <groupId>org.springframework.security</groupId>
      <artifactId>spring-security-jwt</artifactId>
      <version>1.0.7.RELEASE</version>
    </dependency>
    <dependency>
      <groupId>org.springframework.security.oauth</groupId>
      <artifactId>spring-security-oauth2</artifactId>
      <version>2.3.3.RELEASE</version>
    </dependency>
  </dependencies>
…
</project>
```

Abb. 4: Ausschnitt der Abhängigkeiten des Autorisierungsservers (pom.xml)

```
package de.ordix.news.OAuth2.autorisierungserver.config;
@Configuration
@Order(1)
public class SecurityConfig extends WebSecurityConfigurerAdap-
ter {
    @Override
    protected void configure(AuthenticationManagerBuilder
auth) throws Exception {
        auth.parentAuthenticationManager(authenticationManag
erBean())
                .inMemoryAuthentication()
                .withUser("John")
                .password(passwordEncoder().
encode("password"))
                .roles("USER");
    }
    @Bean
    @Override
    public AuthenticationManager authenticationManagerBean()
throws Exception {
        return super.authenticationManagerBean();
    }
    @Bean
    public BCryptPasswordEncoder passwordEncoder() {
        return new BCryptPasswordEncoder();
    }
}
```

Abb. 5: Security-Konfiguration (SecurityConfig.java)

- **Spring Security OAuth2 [5]**
  Dieses Paket enthält alle notwendigen Funktionalitäten zur Abwicklung von OAuth2.0-Protokollen. Es ermöglicht eine einfache Konfiguration des Autorisierungsservers.

- **Spring Security JWT**
  Mithilfe von Security JWT wird die Möglichkeit geschaffen, einen Access Token aus dem OAuth2.0-Protokoll als JSON Web Token zu übermitteln.

Neben diesen beiden Abhängigkeiten ist die Konfiguration des Autorisierungsservers denkbar einfach. Um den Server nun vollständig betriebsbereit zu machen, müssen nur noch folgende zwei Konfigurationsdateien erstellt werden:

Security-Konfiguration

Die Security-Konfiguration kann der Abbildung 5 entnommen werden. Diese Konfiguration ist grundsätzlich für die Einrichtung der Nutzer zuständig. Die Klasse **`SecurityConfig`** erbt hierbei von der Klasse **`WebSecurityConfigurerAdapter`**. Hierdurch ist es notwendig, die Methode **`configure`** zu überschreiben, welche die Konfiguration übernimmt. Der in dieser Klasse verwendete **`BcryptPasswordEncoder`** verfügt über einen Hash-Algorithmus, damit die verwendeten Passwörter nicht im Klartext in der Anwendung verwendet werden.

In diesem Fall wird eine **`InMemoryAuthentication`** verwendet. Das bedeutet, dass die Autorisierung nicht gegen eine Datenbank stattfindet, sondern zur Laufzeit der Anwendung von eben dieser bereitgestellt wird. In diesem Fall wird nur ein Nutzer mit dem Namen „John“ und dem Passwort „password“ zugelassen. Des Weiteren wird das Passwort encodiert, um zusätzliche Sicherheit zu schaffen und das Passwort nicht im Klartext abspeichern zu müssen.

Hier ist es ebenso möglich, anstelle der Methode **`InMemoryAuthentication`** eine Datenbank anzubinden oder eine andere Quelle, wie beispielsweise ein LDAP, zu verknüpfen. Um dieses Beispiel möglichst einfach zu halten, ist hier allerdings keine andere Quelle für Nutzerinformationen verknüpft.

Autorisierungsserver-Konfiguration

Mithilfe der Konfiguration des Autorisierungsservers werden die verschiedenen Schnittstellen, die auch in Abbildung 3 zu sehen sind, konfiguriert. Die vollständige Implementierung kann der Abbildung 6 entnommen werden.

Die Annotation **`@EnableAuthorizationServer`** stellt die wichtigste Zeile innerhalb dieser Konfigurationsklasse dar, da durch diese die Applikation grundsätzlich als Autorisierungs-Server verstanden wird und für das OAuth2.0-Protokoll vorbereitet wird. Das Spring-Framework benötigt nun zur Konfiguration des Autorisierungsservers nur noch die notwendigen Informationen für das Protokoll wie Client-ID, Client-Secret sowie das zu ver-

wendenden OAuth2.0-Verfahren. Diese Informationen werden in den Methoden **`configure()`** übergeben, die aus der Klasse **`AuthorizationServerConfigurer-Adapter`** überschrieben werden.

Die Methode **`configure`** hat hierbei drei Überladungen mit unterschiedlichen Eingangsparametern. Nachfolgend wird die Funktionalität der drei Methoden kurz beschrieben:

- **Configure (AuthorizationServiceSecurityConfigurer oAuthServer)**
  In dieser Methode werden die Zugriffsrechte für die zwei Endpunkte **`token`** sowie **`check_token`** definiert. Grundsätzlich sollte hier der Endpunkt **`token`** für jeden Nutzer zur Verfügung stehen, da dieser für die Anmeldung am System benötigt wird. Der Endpunkt **`check_token`** muss nur für die Nutzer zur Verfügung stehen, die bereits am System angemeldet sind. Daher wird hierbei **`isAuthenticated()`** als Berechtigungsmethode verwendet.

- **Configure (ClientDetailsServiceConfigurer clients)**
  Hierdurch werden die notwendigen Client-Informationen bereitgestellt, d. h., dass die OAuth2.0-Protokolle für verschiedene Clients konfiguriert werden. In diesem Beispiel wird nur ein Client mit der ID: **`OrdixSampleID`** und dem Secret: **`ordixSecret`** verwendet. Diesem Client wird der Grant_Type **`password`** mitgegeben, was dem gleichnamigen Flow von OAuth2.0 entspricht.

- **Configure (AuthorizationServerEndpointsConfigurer endpoints)**
  Diese Methode dient zum Koppeln der standardmäßig von Spring zur Verfügung gestellten Endpunkte für OAuth2.0 mit den Implementierungen unserer Applikation. Da es sich in diesem Beispiel um ein JSON Web Token als Access-Token handelt, wird hier der dazugehörige **`JwtTokenStore`** mit dem Endpunkt verknüpft. Des Weiteren wird hier der **`AuthentcationManager`** mitgegeben, der zuvor in der Security-Konfiguration mit Nutzerinformationen versorgt wurde.

Sind alle Konfigurationen soweit getätigt, lässt sich die Applikation über das Kommando **`mvn spring-boot:run`** in der Kommandozeile starten.

Der Ressourcen-Server

Der Ressourcen-Server stellt Ressourcen (REST-Schnittstellen) zur Verfügung, die durch den Autorisierungsserver abgesichert sein sollen. Als Beispiel wird hierbei ein einzelner Endpunkt zur Verfügung stehen, der unter **`api/hello`** erreichbar ist. Dieser Endpunkt wird daraufhin den angemeldeten Nutzer begrüßen. Somit kann sichergestellt werden, dass die Anbindung am Autorisierungsserver funktioniert.

Die Maven-Abhängigkeiten für diese Applikation können der Abbildung 8 entnommen werden. Zum Starten der Anwendung werden für einen Ressourcenserver verschiedene Konfigurationen zum Start der Anwendung erwartet, die in der Abbildung 7 zu finden sind.

Diese Konfigurationen werden von der Annotation **`@EnableResourceServer`** in der Konfigurationsklasse **`ResourceServerConfig`** erwartet. Diese Klasse stellt alle

```
package de.ordix.news.OAuth2.autorisierungserver.config;
@Configuration
@EnableAuthorizationServer
public class AuthServerConfig extends AuthorizationServerConfi-
gurerAdapter {
    @Autowired
    private PasswordEncoder passwordEncoder;
    @Autowired
    private AuthenticationManager authenticationManager;
    @Override
    public void configure(final AuthorizationServerSecurityCon-
figurer oauthServer) throws Exception {
        oauthServer.tokenKeyAccess("permitAll()")
                .checkTokenAccess("isAuthenticated()");
    }
    @Override
    public void configure(final ClientDetailsServiceConfigurer
clients) throws Exception {
        clients.inMemory()
                .withClient("OrdixSampleID")
                .secret(passwordEncoder.
encode("ordixSecret"))
                .authorizedGrantTypes("password")
                .scopes("user_info")
                .autoApprove(true);
    }
    @Override
    public void configure(final AuthorizationServerEndpoint-
sConfigurer endpoints) throws Exception {
        endpoints
                .tokenStore(tokenStore())
                .accessTokenConverter(accessTokenConverter())
                .authenticationManager(authenticationManag
er);
    }
    @Bean
    public TokenStore tokenStore() {
        return new JwtTokenStore(accessTokenConverter());
    }
    @Bean
    public JwtAccessTokenConverter accessTokenConverter() {
        JwtAccessTokenConverter converter = new JwtAccessTo-
kenConverter();
        converter.setSigningKey("dein-signing-key");
        return converter;
    }
}
```

Abb. 6: Konfiguration des Autorisierungsservers (AuthServerConfig.java).

```
security:
  oauth2:
   client:
    clientId: OrdixSampleID
    clientSecret: ordixSecret
    accessTokenUri: http://localhost:8081/oauth/token
    userAuthorizationUri: http://localhost:8081/oauth/authorize
    resource:
     token-info-uri: http://localhost:8081/oauth/check_token
```

Abb. 7: Applikations Einstellungen Ressourcenservers (application.yml)

```
<dependencies>
     <dependency>
       <groupId>org.springframework.boot</groupId>
       <artifactId>spring-boot-starter-data-rest</artifactId>
     </dependency>
     <dependency>
       <groupId>org.springframework.boot</groupId>
       <artifactId>spring-boot-starter-test</artifactId>
       <scope>test</scope>
     </dependency>
     <dependency>
       <groupId>org.springframework.security.oauth</groupId>
       <artifactId>spring-security-oauth2</artifactId>
       <version>2.3.3.RELEASE</version>
     </dependency>
     <dependency>
       <groupId>org.springframework.security.oauth.boot
       </groupId>
       <artifactId>spring-security-oauth2-autoconfigure
       </artifactId>
          <version>2.0.0.RELEASE</version>
     </dependency>
</dependencies>Aciis iam nostabe mendum quit.
```

Abb. 8: Ausschnitt der Abhängigkeiten des Ressourcenservers (pom.xml)

```
package de.ordix.news.OAuth2.ressourceserver.config;
@Configuration
@EnableResourceServer
@Order(1)
public class ResourceServerConfig extends ResourceServerConfi-
gurerAdapter {
    @Value("${security.oauth2.client.clientId}")
    private String clientId;
    @Value("${security.oauth2.client.clientSecret}")
    private String clientSecret;
    @Value("${security.oauth2.resource.token-info-uri}")
    private String tokenEndpoint;
    @Override
    public void configure(final HttpSecurity httpSecurity)
throws Exception {
        httpSecurity.requestMatchers()
              .antMatchers("/api/**")
              .and()
              .authorizeRequests()
              .anyRequest()
              .authenticated().antMatchers("/").permitAll();
    }
    @Primary
    @Bean
    public RemoteTokenServices tokenServices() {
     RemoteTokenServices tokenService = new RemoteTokenServices();
      tokenService.setCheckTokenEndpointUrl(tokenEndpoint);
      tokenService.setClientId(clientId);
      tokenService.setClientSecret(clientSecret);
      return tokenService;
    }
}
```

Abb. 9: Resource-Server-Konfiguration (ResourceServerConfig.java)

```
package de.ordix.news.OAuth2.ressourceserver.controller;
@RestController
@RequestMapping("/api/hello")
public class HelloController {
    @GetMapping()
    public String hello(Principal principal) {
        return "Hallo " + principal.getName();
    }
}
```

Abb. 10: Principal aus dem Request erhalten (HelloController.java)

relevanten Informationen zur Verfügung, um die Anbindung an den Autorisierungsserver bereitzustellen (siehe Abbildung 9). Die Vererbung findet von der Klasse **`ResourceServerConfigurerAdapter`** statt. Diese benötigt zur Verbindung zum Autorisierungsserver einen Token-Service, welcher durch die notwendigen Verbindungsdaten (Client-ID, Client-Secret sowie die URL des Autorisierungsservers) initialisiert wird.

Des Weiteren ist es notwendig zu definieren, welche Endpunkte durch diese Autorisierung abgesichert werden sollen. Dies wird in der Methode **`configure()`** definiert. In diesem Beispiel werden alle Endpunkte abgesichert, die mit **`api/`** beginnen. Alle weiteren Endpunkte sind ohne Autorisierung erreichbar.

Nun wird nur noch der Endpunkt **`api/hello`** benötigt. Hierfür wird eine Klasse **`HelloController.java`** angelegt, der diesen bereitstellt (siehe Abbildung 10). Über das Objekt **`Principal`** lässt sich der aktuell eingeloggte Benutzer des eingehenden Requests ermitteln. In diesem Beispiel wird über den Aufruf **`principal.getName()`** der Name zurückgegeben.

Sind alle Konfigurationen abgeschlossen, lässt sich die Applikation über das Kommando **`mvn spring-boot:run`** in der Kommandozeile starten.

Ein kleiner Test

Will man nun die Schnittstelle **`api/hello`** vom Ressourcenserver aufrufen, so muss zuerst ein Access-Token vom Autorisierungsserver abgerufen werden.

Über den Button **`Get New Access Token`** kann dies im Postman geschehen, wenn die Autorisierung auf OAuth 2.0 gestellt wird. Im nachfolgenden Dialog müssen, dann die Daten für den Autorisierungsserver eingegeben werden (siehe Abbildung 11). Durch einen Klick auf **`Request Token`** wird der Autorisierungsserver mittels HTTP-POST nach einem Access-Token gefragt. Dieser kann dann im weiteren Verlauf verwendet werden.

Mittels **`HTTP-GET`** kann dann eine Anfrage an den Ressource-Server gestellt werden (siehe Abbildung 12). Hat alles funktioniert, so sollte als Antwort „Hallo John“ zurückgesendet werden.

Beendet man nun den Autorisierungs-Server innerhalb der Kommandozeile (STRG + C), so sollte bei einem wiederholten Aufruf an den Ressourcenserver ein Fehler zurückgegeben werden, dass der mitgelieferte Token nicht validiert werden konnte.

Fazit

Dieser Artikel zeigt anschaulich, wie REST-Schnittstellen innerhalb einer Spring-Applikationen abgesichert werden können. Mittels einfacher Konfigurationsklassen kann so in

kürzester Zeit eine zentrale Komponente zur Autorisierung von Nutzern aufgebaut werden.

Ein zentraler Autorisierungsserver kann in einer Microservice-Landschaft für mehrere Applikationen gleichzeitig verwendet werden und die Komplexität von Security-Anforderungen an einer Stelle bündeln.

Unter Zunahme weiterer Security-Aspekte wie der Rollenverwaltung lassen sich so verschiedene Schnittstellen für unterschiedliche Nutzergruppen absichern.

Der gesamte Source-Code der Anwendung kann online heruntergeladen werden. [8]

Phillipp Kürsten
(info@ordix.de)

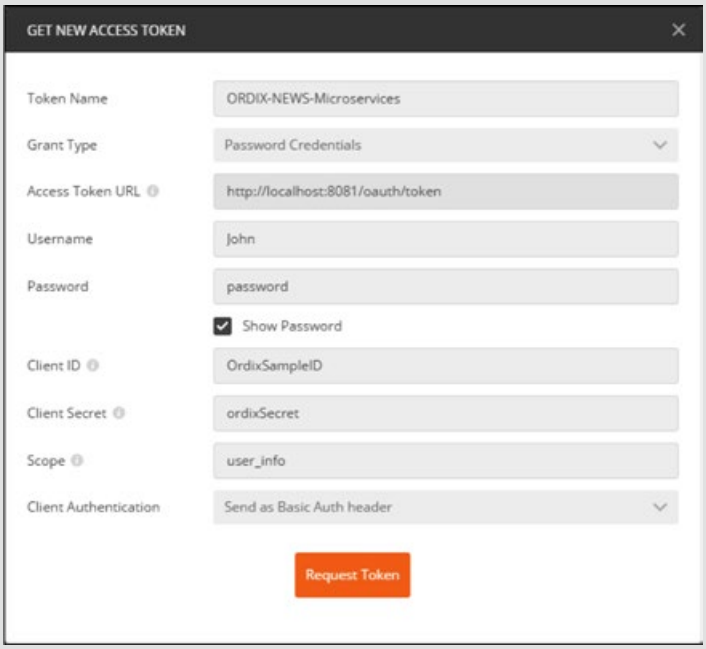


Abb. 11: Access Token anfordern mittels Postman

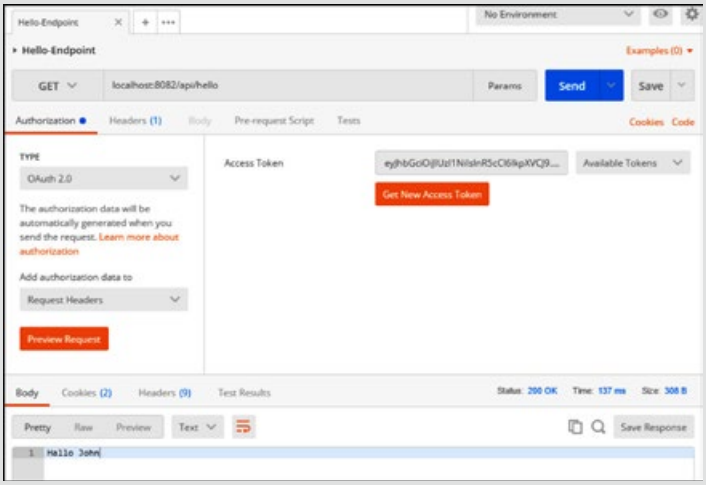


Abb. 12: Schnittstelle Aufruf mit Access-Token

Links/Quellen

[1] OAuth 2.0: https://oauth.net/2/

[2] JSON Web Token - Standard: https://tools.ietf.org/html/rfc7519#

[3] JSON Web Token - Encoder: https://jwt.io/

[4] Java - Spring: https://spring.io/

[5] Spring Security OAuth 2:
https://projects.spring.io/spring-security-oauth/docs/oauth2.html

[6] Postman – API Development:
https://www.getpostman.com/

[7] OAuth 2.0 – Password Flow:
https://developer.okta.com/blog/2018/06/29/what-is-the-oauth2-password-grant

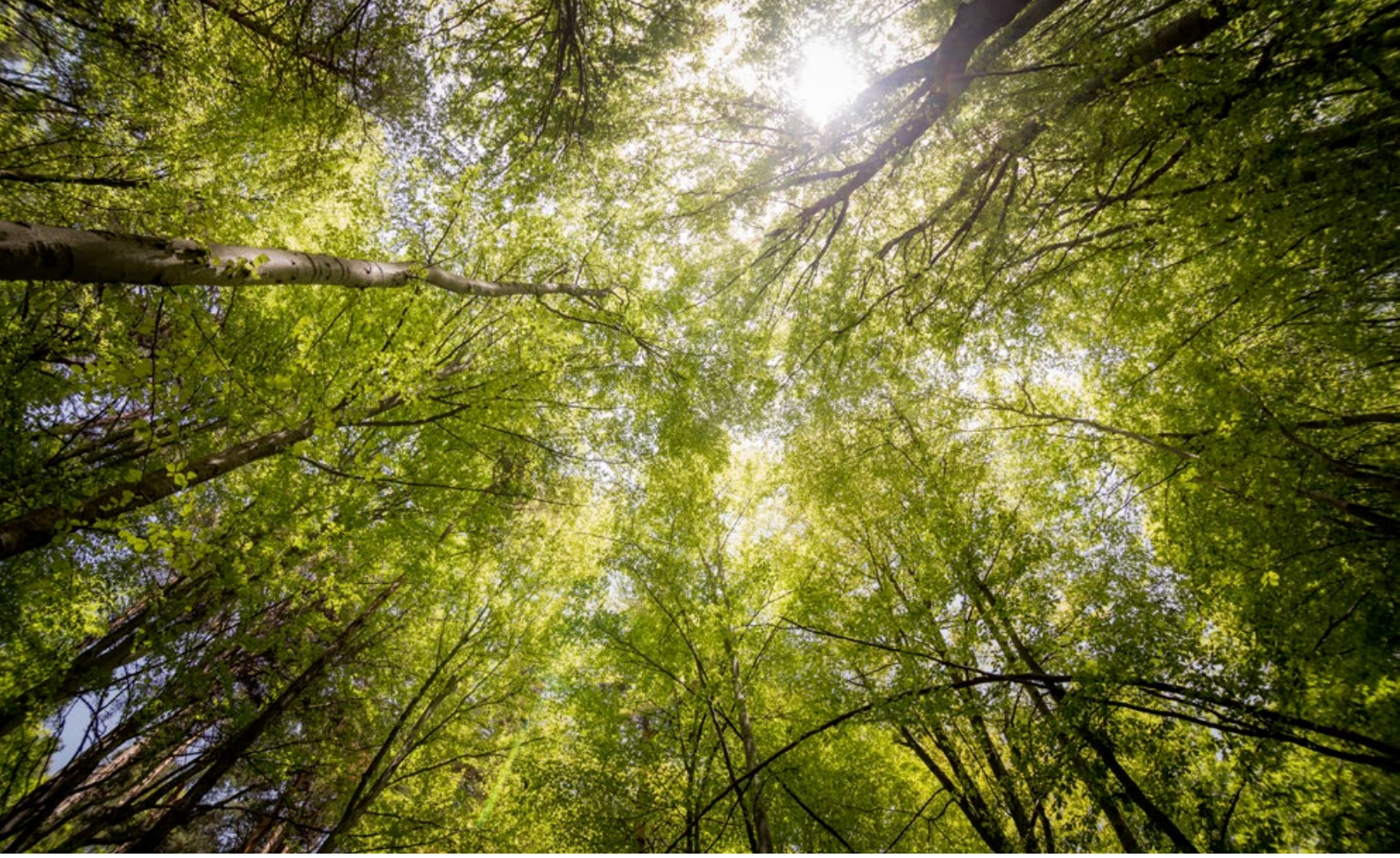
[8] GitHub – Beispiel-Projekt:
https://github.com/PhilKuer/spring-jwt-oauth2-sample

[Q1] IT-Security – ORDIX Blog:
https://blog.ordix.de/component/easyblog/tags/it-security

[Q2] Spring Power Workshop – ORDIX Seminare:
https://seminare.ordix.de/seminare/entwicklung/java-ee/spring-power-workshop.html

[Q3] Microservices Workshop mit Spring Boot – ORDIX Seminare:
https://seminare.ordix.de/seminare/entwicklung/java-ee/microservices-workshop-mit-spring-boot.html

Bildnachweis



Wie nachhaltig sind IT-Dienstleistungen?

Nachhaltig handeln – aber wie?

Bei einem IT-Dienstleister denkt man nicht sofort an Industrie, Abfälle oder Umweltbelastung. Aber auch wir tragen die Verantwortung für unsere Umwelt. Im Großen und Ganzen sind unsere Dienstleistungen sauber – dennoch gibt es bei uns auch noch Verbesserungsbedarf, den wir nach und nach in Angriff nehmen wollen. Bei über 150 Beratern, von denen ein Großteil zwischen ihrem Zuhause, der Geschäftsstelle und ihrem Kunden pendelt, kommen einige Kilometer zusammen. Was tun wir, um unsere Umweltbilanz zu verbessern?

A wie Autos

Die Diesel-Diskussion und auch die daraus resultierenden Fahrverbote machten 2018 eine Menge Schlagzeilen. Doch bevor die große Diskussion ausgelöst wurde, wurden bei ORDIX bereits die richtigen Weichen gestellt.

Die Anforderungen für neue Autos im Unternehmen wurden auf die neue Euro 6d-TEMP-Norm angepasst. Somit haben wir bereits ab Anfang 2018 einen Großteil unserer Fahrzeugflotte auf den neuen Standard umgestellt. Der Rest folgt im ersten Halbjahr 2019.

Fahrverbote werden unsere Consultants und unsere Kunden deshalb nicht bzw. kaum treffen und wir verringern zudem den Ausstoß von Stickoxiden und Feinstaub.

Zudem komplettieren seit November 2018 zwei Elektro-Autos die Flotte (siehe auch E wie Elektrizität).

C wie Computer

Wir achten seit einigen Jahren beim Einkauf unserer Hardware (Handy und Telefon) auf die Nachhaltigkeit. Neben einer Nutzungsdauer von mindestens vier Jahren achten wir auf stromsparende Geräte. Eine umweltgerechte Entsorgung (Recycling-Einrichtungen) der Geräte ist für uns selbstverständlich.

E wie Elektrizität

Im Seminarzentrum Wiesbaden gibt es seit dem letzten Jahr zwei Elektro-Tankstellen für unsere Seminarteilnehmer und die ORDIX-Mitarbeiter mit Elektro-Fahrzeugen. Im November des letzten Jahres wurden die ersten zwei Elektroautos in den Fuhrpark der ORDIX AG aufgenommen. Einer der beiden Renault ZOE wurde bereits nach

Wiesbaden überführt. Der zweite folgt in ca. zwei Monaten, wenn das dritte Elektro-Fahrzeug in Paderborn stationiert wird.

Die Elektro-Betankung in Paderborn erfolgt über Ökostrom und ist somit CO_2-neutral. Die Elektromobile werden in der ORDIX-Flotte für Städtefahrten, Kundenbesuche im näheren Umfeld und Besorgungen genutzt.

M wie Mülltrennung

Wir sensibilisieren unsere Mitarbeiter im Bereich der Mülltrennung. Neben den Behältern für Altpapier stehen in unseren Bistro-Bereichen auch entsprechende Behälter für die Trennung von Kunststoffabfall, Bio- und Restmüll zur Verfügung.

P wie Publikationen

Wir achten darauf, keine Papier-Ressourcen zu verschwenden. Die Umstellung unserer ORDIX news und des Seminarprogramms auf einen Online-Bezug haben die Menge der Print-Produkte schon sehr reduziert. Dennoch wird es auch weiterhin eine Auflage dieser beiden Print-Publikationen geben, diese wird CO_2-neutral produziert. Zudem wird beim Versand der Publikationen darauf geachtet, dass die Polyetylenfolie zu 100% recyclingfähig ist. Dank der Rückmeldungen von Ihnen zu nicht aktuellen Adressdaten wird die Verteiler-Liste ständig aktualisiert und somit sparen wir zusätzlich.

S wie Seminarunterlagen

Intern gehen wir mit gutem Beispiel voran und drucken nur wirklich wichtige Dokumente aus. Auch im Seminarbereich haben wir durch die Einführung unserer Cloud-Umgebung eine erhebliche Einsparung im Papierbereich erreicht. Seit diesem Jahr kann der Seminarteilnehmer entscheiden, ob er eine Print- oder eine digitale Ausgabe des Unterrichtsstoffes haben möchte.

T wie Taschen

Infomaterial erhalten unsere Seminarteilnehmer seit zwei Jahren in PVC-freien Taschen der Marke Halfar. Diese schonen bei der Produktion und beim Recycling die Natur.

W wie Wasser

Neben den Mehrweg-Flaschen für Mitarbeiter und Seminarteilnehmer in unserem Seminarzentrum haben wir in der Geschäftsstelle Paderborn seit dem Umzug im Jahr 2016 auf ein Wasserspender-System (Fa. Welltec) umgestellt, welches an das städtische Wassernetz angeschlossen ist. Im Hinblick auf ökologische Gesichtspunkte erzeugen wir hierdurch keinen Müll, sparen die Transportkosten der Pfandflaschen und sparen eine Menge Energie für die Reinigung, Herstellung und Befüllung von Flaschen.

Z wie Ziele

Mit dem Wissen, dass noch einige Dinge mehr möglich sind, werden wir zukünftig noch genauer darauf achten, Rohstoffe und Energieressourcen schonend einzusetzen.

Zwei Elektro-Autos sind bereits im Einsatz, ein weiteres folgt.

Wasser aus dem Wasserhahn – ohne Pfand oder weitere Kosten

Bildnachweis

© pexels.com
© welltec.de | https://www.welltec-wasser.de/de/

Wie sicher ist Oracle's Webentwicklungstool?

Oracle Application Express auf dem Security-Prüfstand

In Zeiten der fortschreitenden Digitalisierung bekommen Daten einen immer größer werdenden Wert für Unternehmen. Somit gilt es, diese Daten immer besser zu schützen. Oracle Application Express bietet die Möglichkeit, Webapplikationen zu erstellen, die äußerst effizient und detailliert Daten auswerten und darstellen können.

Doch welche Möglichkeiten bietet eine solche Applikation für Hacker und Wirtschaftsspione, sich an Ihren Daten zu bereichern? Wer genauer hinschaut sieht, dass oft schon die einfachsten Werkzeuge reichen, um eine Applikation zu knacken.

Im Großen und Ganzen sicher, aber...

Oracle APEX ist von Hause aus sicher konfiguriert und entwickelt worden. Sofern man diese Konfigurationen beibehält und in manchen Punkten (wie beispielsweise Autorisierungsschemata) gegebenenfalls noch etwas nachjustiert, bringt Oracle APEX keine Bedrohungen für Ihre Daten mit sich.

Doch sobald Applikationen über den Standard hinausgehen und die Entwickler die vorgefertigten Wege von Oracle APEX verlassen, sind sie selbst gefragt, dieses Sicherheitsniveau beizubehalten.

Arbeiten die Entwickler hier nicht gewissenhaft, kommt es schnell zu Schwachstellen, die ein großes Schadenspotenzial bieten und mittels einfachster Werkzeuge auszunutzen sind. Hierbei handelt es sich um zwei Schwachstellen, die in der Webentwicklung bereits lange bekannt sind. Dennoch treten sie durch nachlässige Entwicklung leider immer wieder auf. Die Rede ist von SQL-Injection und Cross-Site-Scripting.

In diesem Artikel möchte ich diese Schwachstellen kurz vorstellen und exemplarisch zeigen, was für ein Schadens-

potenzial sie mit sich bringen. Anschließend möchte ich erläutern, welche Fehler man bei der Entwicklung von APEX-Applikationen begehen kann, durch die diese Schwachstellen auftreten. Zudem wird erläutert, wie man sich vor diesen Schwachstellen schützen kann.

SQL-Injection

Bei der SQL-Injection kann von einem Nutzer Code an ein SQL-Statement oder eine Abfrage angehängt werden. Somit können nicht vorgesehene Kommandos ausgeführt werden oder es kann unautorisiert auf Daten zugegriffen werden.

In Webapplikationen treten SQL-Injection-Schwachstellen in verschiedenen Konstellationen auf. Alternative 1 ist, dass sie durch die Verwendung von Substitutionsvariablen in SQL-Statements eintreten.

So kann beispielsweise bei dem folgenden Statement, das hinter der Suche für eine Sucheingabe steht:

```
SELECT *
FROM ABTEILUNGEN
WHERE ABTEILUNGSNR='&Abteilungsnummer.' AND AB-
TEILUNGSNR!=1
;
```

durch die Eingabe von:

```
' OR 1=1 --
```

das Statement so manipuliert werden, dass alle Datensätze der Tabelle Abteilungen – einschließlich der Datensätze mit der Abteilungsnummer 1 – angezeigt werden. Und das, obwohl nur die Datensätze einer Abteilung angezeigt und die Datensätze mit der Abteilungsnummer 1 niemals ausgegeben werden sollten.

Um dieses Verhalten beim Ausführen des Statements zu veranschaulichen, wird die Substitutionsvariable durch die Eingabe ersetzt.

```
SELECT *
FROM   ABTEILUNGEN
WHERE  ABTEILUNGSNR='' OR 1=1 -- ' AND ABTEILUNGSNR!=1
;
```

Nun ist zu sehen, dass nach einer leeren Abteilungsnummer oder nach allen Zeilen (1 = 1) gesucht wird. Somit werden alle Zeilen selektiert. Zudem ist zu erkennen, dass die folgende Bedingung, dass nur Zeilen ausgegeben werden sollen, in denen die Abteilungsnummer nicht gleich 1 ist, auskommentiert wurde.

Um Variablen in SQL-Statements verwenden zu können, ohne die Gefahr von SQL-Injection eingehen zu müssen, sollten Bind-Variablen genutzt werden.

Der Inhalt einer Bind-Variable wird automatisch vom JDBC-Driver maskiert, sodass dieser automatisch als Nutzereingabe erkannt wird. Zudem wird der Inhalt von Bind-Variablen erst nach dem Parsen des SQL-Statements ausgelesen. Eine Bind-Variable definiert sich durch das Anführen mittels eines Doppelpunktes wie in dem folgenden SQL-Statement zu sehen:

```
SELECT *
FROM ABTEILUNGEN
WHERE ABTEILUNGSNR=:Abteilungsnummer AND AB-
TEILUNGSNR!=1
;
```

Bei Alternative 2 können SQL-Injection-Schwachstellen durch dynamische SQL-Statements entstehen, in denen aus verschiedenen Gründen keine Bind-Variablen genutzt werden.

In diesem Fall sollten alle Nutzereingaben mittels des PL/SQL-Paketes **`dbms_assert`** geprüft werden, um sich vor SQL-Injection-Angriffen zu schützen.

In Oracle-APEX-Applikationen ist die Gefahr von SQL-Injection-Schwachstellen sehr hoch, da diese, sobald sie über den normalen Standard hinausgehen, auf sehr viel SQL- und PL/SQL-Code zurückgreifen, der von den Entwicklern stammt.

Zudem ist es sehr schwer, Applikationen auf SQL-Injection-Schwachstellen zu prüfen, da Oracle APEX an vielen verschiedenen Stellen die Möglichkeit bietet, SQL- und PL/SQL-Code zu implementieren. Daher müssen die Entwickler hier sehr gewissenhaft arbeiten.

Cross-Site-Scripting

Cross-Site-Scripting ist eine Angriffsmethode, bei der ein Nutzer die Möglichkeit hat, eigenen Quelltext in eine Webseite zu injizieren, sodass er vom eigenen Browser und von den Browsern anderer Nutzer ausgeführt wird. Möglichkeiten, dieses zu tun, gibt es viele. So kann ein Nutzer beispielsweise ein Gästebuch oder die Kommentarfunktionen nutzen, um Quelltext dauerhaft in einer Webseite unterzubringen. Werden die Nutzereingaben nicht maskiert, so wird der vom Angreifer eingegebene Schad-Code vom Browser interpretiert und nicht als Text angezeigt.

Dieses Vorgehen wird häufig genutzt, um Nutzer von Webseiten anzugreifen. Dabei sind beispielsweise Session- oder Anmelde-Informationen das Ziel der Angreifer. Es bietet aber auch die Möglichkeit, Inhalte und Funktionen freizuschalten, die für den Angreifer und andere Nutzer nicht vorgesehen sind.

Eine weitere Möglichkeit, einen solchen Angriff umzusetzen, ist beispielsweise das Manipulieren von URLs, sodass der injizierte Quelltext nur lokal bei dem Angreifer ausgeführt wird. So hat der Angreifer beispielsweise die Möglichkeit, sich Inhalte oder Funktionalitäten freizuschalten, die nicht für ihn vorgesehen sind.

Letztere Möglichkeit bietet sich in Oracle APEX allerdings nicht so einfach an, da die URLs von Oracle APEX Applikationen standardmäßig mit einer Checksumme versehen sind (Session State Protection). Diese verhindert

zudem URL-Tampering-Angriffe sowie Cross-Site-Request-Forgery-Angriffe.

In Oracle Application Express bietet sich der Angriffsvektor wie folgt: Ein Angreifer kann Schad-Code über Eingabemasken in der Datenbank speichern, der später von einer Oracle-APEX-Applikation ausgelesen wird und beispielsweise in Reports dargestellt wird.

Die Option **`Escape Special Characters`** in Oracle APEX schützt davor, dass ein solcher Code ausgeführt wird. Diese ist standardmäßig auf YES gesetzt (siehe Abbildung 1).

In der Praxis kommt es jedoch häufig vor, dass diese Funktion deaktiviert wird. Das passiert meist durch das berühmte „..nur einmal kurz etwas ausprobieren..“ und anschließend wird die Funktion nicht mehr aktiviert.

Ein weiteres Beispiel für das Ausschalten der Funktion **`Escape Special Characters`** aus der Praxis ist das „Aufhübschen“ der Datenausgabe im SQL durch die Verwendung von HTML. Das folgende Statement stammt in abgewandelter Form aus einem Oracle-APEX-Sicherheitscheck und soll dieses Beispiel veranschaulichen.

```
SELECT   adresse || '<br/>'  || plz || '' || ort
FROM     kunden
WHERE    id=:kunden_nr
;
```

Anfällig für solche Angriffe sind nicht nur Reports, sondern ALLE Elemente, die Daten der Datenbank in HTML anzeigen.

Da Oracle APEX eine breite Masse solcher Elemente anbietet, ist eine nachträgliche manuelle Kontrolle einer Applikation je nach Größe der Applikation sehr komplex und somit sehr fehleranfällig. Daher sollte darauf geachtet werden, dass diese Funktion niemals geändert wird, um eine solche Schwachstelle auszuschließen.

Die Einstellung der Funktion **`Escape Special Characters`** wird im Data-Dictionary zu den einzelnen Elementen, die in Oracle APEX genutzt werden können, gespeichert.

Dieses bietet die Möglichkeit, mittels eines SQL-Statements alle Elemente der Applikation auszugeben, bei denen die Einstellung dieser Funktion auf „NO“ steht. Somit können alle Cross-Site-Scripting-Schwachstellen in einer Applikation gefunden werden.

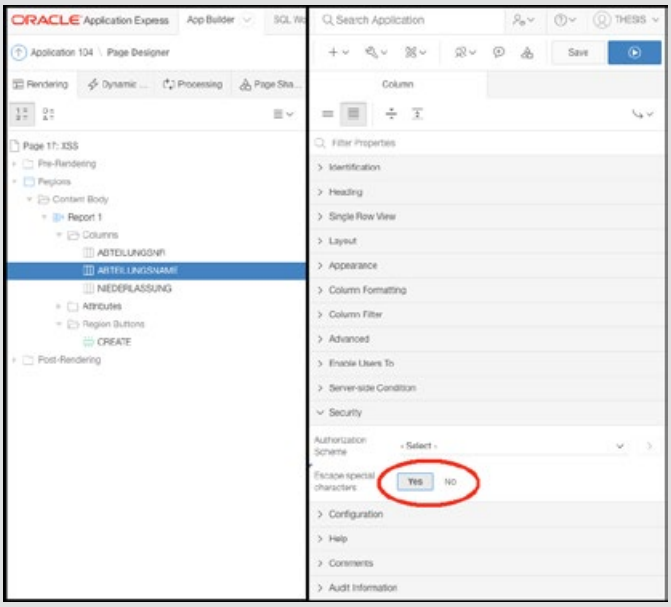


Abb. 1: Oracle APEX Escape Special Characters

Fazit

Um SQL-Injection-Schwachstellen zu vermeiden, muss der Entwickler bei der Entwicklung von SQL-Statements und PL/SQL-Funktionalitäten sehr gewissenhaft arbeiten.

Hier muss der Entwickler darauf achten, dass Nutzereingaben ausschließlich mit Bind-Variablen in SQL und PL/SQL Code eingebaut werden. Sollte die Verwendung von Bind-Variablen nicht möglich sein, so müssen Nutzereingaben mittels des PL/SQL-Paketes „dbms_assert“ geprüft werden.

Cross-Site-Scripting Schwachstellen sind durch die APEX-Standardkonfiguration vorerst nicht möglich. Um eine solche Schwachstelle in einer APEX-Applikation zu verursachen, muss der Entwickler die Funktion **`Escape Special Characters`** auf „NO“ setzen. Daher ist zu raten, dieses niemals zu tun.

Links

[1] Bundesamt für Sicherheit in der Informationstechnik:
G 5.170 - Cross-Site Scripting (XSS)
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05170.html

[2] Bundesamt für Sicherheit in der Informationstechnik:
G 5.131 - SQL-Injection
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05131.html

Tobias Flüter
(info@ordix.de)

Microservices mit Java EE

Mit Eclipse MicroProfile zu leichtgewichtigen verteilten Java EE Microservices

Mit Eclipse MicroProfile steht ein Quasistandard zur Verfügung, der die Implementierung von Microservices erheblich vereinfacht, ohne den bewährten Java-EE-Standard aufzugeben.

JEE-Monolithen

Java-EE-Anwendungen lassen sich in der Regel deswegen als Monolithen (siehe Abbildung 1) bezeichnen, weil sie komplexe und umfangreiche fachliche Logik implementieren und diese in einer Deployment-Unit ausliefern. Der Aufwand, derartige Anwendungen zu erweitern und zu warten, wächst erfahrungsgemäß mit zunehmendem Alter. Das liegt einerseits daran, dass die Anwendung an die sich verändernden fachlichen Anforderungen angepasst werden muss.

Nicht selten passt das Software-Design dann nicht mehr zu den Anforderungen. Sponsoren für eine Refaktorierung finden sich selten. Andererseits altert Software dadurch, dass im Zuge der Wartung das Design vernachlässigt wird, was wiederum die Komplexität erhöht und die Wartung erschwert. Nicht zuletzt ist der Aufwand für ein neues Release schon aufgrund der umfangreichen Systemtests erheblich. Eine derartige Software wird nicht als agil wahrgenommen.

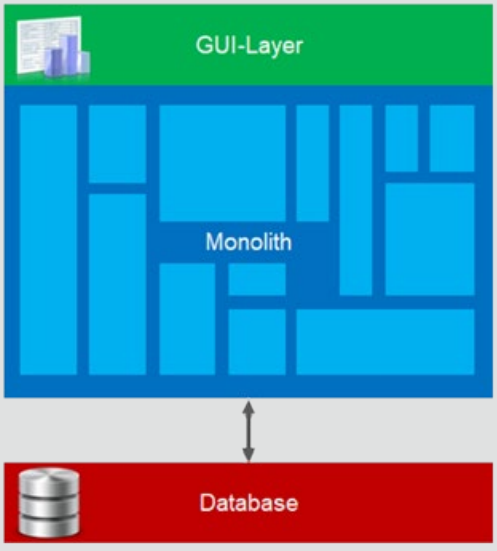


Abb. 1: Monolith

Microservice

Demgegenüber steht die lose Kopplung von Microservices (siehe Abbildung 2). Sie wird dadurch erreicht, dass Microservices oft aus fachlicher Sicht geschnitten werden und im Idealfall nur durch Kommunikation über das Netzwerk miteinander verbunden sind. Ein Microservice übernimmt nur eine Aufgabe. Die Microservices sollen unabhängig voneinander entwickelbar, deploybar und testbar sein. Die Idee zur Microservice-Architektur ist im Jahre 2011 entstanden.

Microservices können, im Gegensatz zu Monolithen, kurzfristig an fachliche Anforderungen angepasst werden. Sie kommen überall dort zum Einsatz, wo die Agilität von großer Bedeutung ist. Vorreiter sind Internetanbieter für Video-on-Demand oder Internet-Shops. Derartige Vorbilder zeigen, dass auch in einer komplexen IT kurzfristige Anpassungen vorgenommen werden können.

Spring-Microservice-Architektur wurde immer beliebter

Dieser neue Ansatz der losen Kopplung wurde von den Application-Server-Herstellern anfangs nicht wahrgenommen. Als Spring-Microservices immer beliebter wurden, haben einzelne Application-Server-Hersteller angefangen, eigene Lösungen zu entwickeln, um die Microservice-Architektur in ihrem Application Server umsetzen zu können. Der Nachteil der eigenen Bemühungen war, dass sie nicht in das bisher auf Standards setzende Java EE passten. Dieses Problem wurde dadurch gelöst, dass sich mehrere Hersteller unter dem Eclipse-MicroProfile-Projekt

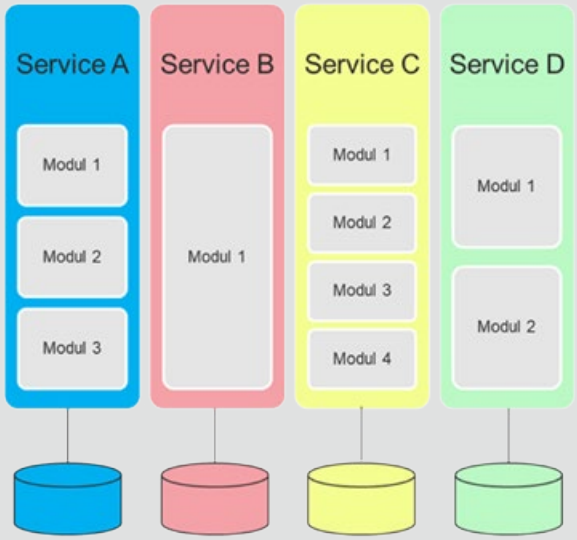


Abb. 2: Microservice

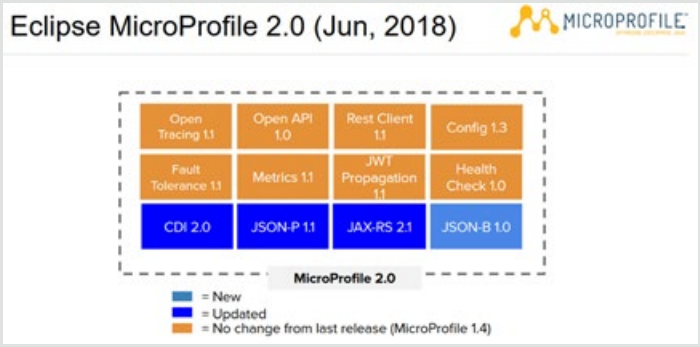


Abb. 3: Eclipse MicroProfile 2.0 – Quelle: https://microprofile.io

(https://microprofile.io) zusammengeschlossen haben, um die Entwicklung aufeinander abgestimmt voranzutreiben und somit einen Quasistandard einzuführen.

Microservice-Architektur im Java-EE-Umfeld

Um monolithische Strukturen zu vermeiden, ist es naheliegend, die Themen fachlich passend zu schneiden und auf einzelne Self-Contained-Systems- Microservices (SCS-Microservices) zu verteilen. Mit Domain-Driven-Design (DDD) gelingt dies. DDD bietet mit Bounded Context ein Konzept, um Fachdomänen voneinander abzugrenzen. Hinzu kommt, dass die Entwickler und die Fachabteilungen intensiver zusammenarbeiten (müssen), um die Microservices passend schneiden zu können. Die Fachlichkeit rückt in den Vordergrund und die Technik eher in den Hintergrund. Ein Microservice soll so klein sein, dass bei Änderung der Fachlichkeit dieser kann durch eine Neuimplementierung ausgetauscht werden kann ohne zeitaufwendige Test- und Refactoring-Runden.

Um die Abhängigkeit der Microservices zu minimieren, wird jeder Microservice auf einem eigenen Application Server betrieben. Die Kommunikation der Services untereinander wird über das Netzwerk betrieben.

Dieses Vorgehen hat aber den Nachteil, dass der Overhead (ein kompletter Application Server) pro Service sehr groß ist, da nicht jeder Service alle Komponenten aus dem Application Server benötigt. Es entsteht außerdem ein hoher Aufwand für Systemkonfiguration, Deployment und Management der einzelnen Services. Hinzu kommt der Aufwand für das Monitoring der vielen Server/Services. Da jeder Service auf einem eigenen Application Server läuft, braucht jeder Service/Application Server eine eigene Konfiguration, u.a. Netzwerkeinstellungen (IP und Port für den eigenen Service und IPs und Ports für die Services, mit dem er kommuniziert), ein eigenes Deployment und seine eigenen Logging- und Monitoring-Einstellungen.

Um all diese Herausforderungen zu meistern, wurde das Eclipse MicroProfile gegründet. Die Idee dahinter ist, einen abgespeckten Application Server (ohne Overhead) betreiben zu können und APIs bereitzustellen, die die Herausforderungen der Pflege und Überwachung der verteilten Server/Services vereinfachen.

Eclipse MicroProfile APIs

Im Java-EE-Umfeld gibt es schon viele erprobte Konzepte, um Software modular zu gestalten, wie beispielsweise CDI. Allerdings fehlen Konzepte, die speziell auf verteilte Systeme und ihre Anforderungen zugeschnitten sind. Hierfür wurden die Eclipse MicroProfile APIs entwickelt (siehe Abbildung 3).

Durch den Einsatz von JAX-RS und JSON-P kann die Kommunikation zwischen den einzelnen Services über REST-Schnittstellen im JSON-Format umgesetzt werden.

Um die einzelnen Services an die jeweilige Umgebung (Dev, Test, Prod) von außen anpassen zu können, wurde die Config-API eingeführt.

Die Konfiguration der einzelnen Services wird durch den Einsatz der Config-API erleichtert. So können Konfigurationen auf unterschiedlichen Ebenen eingesetzt werden.

Die Reihenfolge ist wie folgt:

- `System.getProperties()`
- `System.getenv()`
- META-INF (`microprofile-config.properties`-Dateien, die im ClassPath liegen)

Ein Überblick über die Systemgesundheit aller verteilt laufenden Services kann durch den Einsatz von Health Checks und Metrics APIs erstellt werden. Mit der Health Check API kann von außen festgestellt werden, ob ein Service noch so läuft, wie geplant. Die API stellt einfache Health-End-

points zur Verfügung, die bei einem Aufruf mit einer Statusmeldung "`UP`" oder "`DOWN`" oder mit einem Netzwerkfehler antworten.

Die Informationen aus den Health-Endpoints können benutzt werden, um Services über Tools wie beispielsweise Kubernetes (https://kubernetes.io) automatisch neu zu starten.

Die Metrics API liefert Detailinformationen über einen einfachen Health-Check hinaus. So lassen sich durch Langzeitmessungen Tendenzen des Speicherverbrauchs vorhersagen. Außerdem kann man durch das permanente Auswerten von Antwortzeiten schleichende Verschlechterungen frühzeitig erkennen.

Um auf Fehlersituationen in verteilten Systemen besser reagieren zu können, wurde die Fault Tolerance API hinzugefügt. Sie enthält unter anderem Hystrix (https://github.com/Netflix/Hystrix). Hystrix wird darüber hinaus oft in Spring Microservices eingesetzt und enthält Entwurfsmuster, um die Ausfallsicherheit zu erhöhen.

Um Security einerseits zwischen den einzelnen Services und andererseits zwischen Client und Services umsetzen zu können, wird JWT Propagation eingesetzt. JWT Propagation vereinfacht die Umsetzung von OAuth2, OpenID Connect (OIDC) und JSON Web Tokens (JWT).

Die nächsten Themen

Somit haben wir schon einige Hilfsmittel, um Microservices mit Java EE umsetzen zu können. Allerdings sind noch nicht alle Lücken zum Vorreiter Spring geschlossen. So fehlt noch eine Möglichkeit der Service-Discovery. Die Service-Discovery kann mithilfe von Consul (https://www.consul.io/discovery.html) übernommen werden, Consul ist aber nicht im Microprofile aufgenommen.

Die Weiterentwicklung folgender Themen wird aktuell diskutiert:

- Long Running Actions
- Reactive Streams
- Reactive Events
- Data Access
- Event Data

Fazit

Die Architektur von kleinen selbstständigen Services lässt sich dank MicroProfile auch mit Java EE umsetzen.

Die Vorteile der Umsetzung von Microservices mit Java EE sind:

1. Java EE ist ein Standard, Komponenten können von mehreren Herstellern eingesetzt werden. Die Abhängigkeit zu einem Hersteller wird vermieden.
2. Der Standard ist gut dokumentiert.
3. Es gibt viele Entwickler, die Erfahrung in der Verwendung dieses Standards haben.
4. Der Standard ist stabil – Abwärtskompatibilität ist gewährleistet. Release-Zyklen sind in der Regel größer als ein Jahr, Ausnahme: kürzere Release-Zyklen für Eclipse MicroProfile.
5. Java-EE-Lösungen sind schon lange am Markt (> 15 Jahre).

Christian Rädisch
(info@ordix.de)

Glossar

Domain-Driven-Design (DDD)
DDD wurde 2003 von Eric Evans in seinem gleichnamigen Buch geprägt. Dabei wird die Modellierung von Software im Wesentlichen von den umzusetzenden Fachlichkeiten der Anwendungsdomäne beeinflusst.

Enterprise Application Archive (EAR)
EAR ist ein Dateiformat, welches alle Programm- und Konfigurationsdateien enthält, um eine Applikation auf einem Applikationsserver betreiben zu können.

Java Enterprise Edition (Java EE)
Java EE ist eine Sammlung von Spezifikationen, um Anwendungen auf herstellerunabhängigen Applikationsservern betreiben zu können.

Monolithen
Von einer monolithischen Software Architektur (Monolith) ist die Rede, wenn die funktionalen Elemente in einem einzigen, untrennbaren sowie homogenen Gebilde miteinander verbunden sind.

Links/Quellen

[1] Seminarempfehlung: Softwarearchitekturen - https://seminare.ordix.de/seminare/entwicklung/allgemeines/softwarearchitekturen.html

[2] Produktseite Eclipse-Microprofile-Projekt - https://microprofile.io

[3] Hystrix-Bilbliothek - https://github.com/Netflix/Hystrix

[4] Kubernetes Produktseite - https://kubernetes.io/

[5] Produktseite Consul Software - https://www.consul.io/discovery.html

Oracle Directory Services (Teil II)

Datenbanken & Verzeichnisdienst – ein Bund für's Leben

Kann man ein technisch komplexes Konzept mit dem sozialen Modell einer Ehe vergleichen? Entscheiden Sie am Ende selbst. Es ist nicht leicht, den Überblick und die Kontrolle über etwas zu behalten, was auf viele Orte verteilt ist. Datenbankbenutzer bilden da keine Ausnahme. Das weckt den Wunsch nach einem Weg, alles an einem Ort zu bündeln. Die Nutzung eines Verzeichnisdienstes ermöglicht das. Ein Verzeichnisdienst bildet nur die Plattform, die erforderlichen Strukturen hingegen liefert die Enterprise User Security (EUS). Die Oracle-Verzeichnisdienste haben wir im Teil I vorgestellt. Der vorliegende Teil beschreibt den Weg, wie Oracle-Datenbanken und Verzeichnisdienst auf der Basis von EUS einen Bund eingehen.

Das große Ganze

Beim Anlegen von Datenbankbenutzern ist der Standard die lokale Datenbanksicht, bei der sich ein lokaler Benutzer mit einem Passwort anmelden muss und lokal seine Rechte vergeben bekommt. EUS schaut aus Sicht des Unternehmens (engl. enterprise) auf die Mitarbeiter, die Datenbanken und die Rechtevergabe. Man spricht daher von Enterprise Usern, die Zugriff auf Datenbanken in Enterprise Domains erhalten und denen Rechte über Enterprise-Rollen zugewiesen werden.

Abbildung 1 veranschaulicht die Verbindung von Datenbank und EUS. Unten ist der Verzeichnisdienst dargestellt mit der Gruppe CTO und dem Benutzer Larry, der ebenfalls Mitglied der Gruppe CTO ist. Daneben das Enterprise-User-Security-Schema mit dem Enterprise-Domain-Objekt, welchem Datenbanken und Enterprise-Rolle zugeordnet sind. Enterprise-Rollen bündeln Rechte, die sie durch die Verknüpfung mit globalen Rollen erhalten.

Es lassen sich nur globale Rollen aus Datenbanken verknüpfen, die sich mit der Enterprise-Rolle in der gleichen Enterprise Domain befinden. Dem Enterprise User Larry kann eine Enterprise-Rolle direkt zugewiesen werden. Die Enterprise-Rolle kann aber auch der Gruppe CTO zugewiesen werden und steht damit allen Mitgliedern der Gruppe zur Verfügung. Ähnlich verhält es sich mit der Zuordnung eines Globalen Users, bei dem eine Verknüpfung zu dem Enterprise User Larry, aber auch zur Gruppe CTO hergestellt werden kann. Alle Anwender werden nur im zentralen Verzeichnisdienst verwaltet.

Globaler User, globale Rolle

Mit der Option **`IDENTIFIED GLOBALLY AS`** … wird ein Benutzer als globaler User definiert (siehe Abbildung 5). Globale User und lokale User können nebeneinander in der Datenbank existieren. Eine direkte Anmeldung als globaler User ist nicht möglich. Sie bilden den „Dummy-User" unter dem ein Enterprise User in der Datenbank agiert. Globalen Usern werden keine Rechte direkt vergeben, außer evtl. dem Recht sich anzumelden. Sie können von beliebig vielen Enterprise Usern für unterschiedliche Aufgaben gleichzeitig in einer Datenbank benutzt werden. Deshalb haben sie keine eigenen Objekte in der Datenbank. Enterprise User erhalten alle Rechte ausschließlich über Enterprise-Rollen.

Mit der Option **`IDENTIFIED GLOBALLY`** (Abbildung 5) wird auch eine globale Rolle definiert. Globale Rollen können nicht einem Benutzer oder einer anderen Rolle direkt zugewiesen werden, sondern ausschließlich einer oder mehreren Enterprise-Rollen.

Enterprise Domain

Die Enterprise Domain hilft, Datenbanken zu gruppieren. Eine Datenbank sollte nur einer Domain angehören. In einer Enterprise Domain werden Enterprise-Rollen definiert und es können administrative Rechte an Benutzer vergeben werden. Denkbar ist, z. B., alle Datenbanken einer Anwendung oder eines Entwicklerteams in einer Enterprise Domain zusammenzufassen. Die Unterteilung in Entwicklungs-, Test-, QS- und Produktionsdatenbanken lässt sich ebenfalls in Enterprise Domains abbil-

den. Zum EUS-Schema gehört die Enterprise Domain **`OracleDefaultDomain`**, der alle Datenbanken bei der Registrierung im OUD automatisch zugewiesen werden.

Der EUS-Realm

Verzeichnisdienste sind in Baumstrukturen organisiert. Der EUS-Realm definiert den Einstiegspunkt, ab dem alle Daten in der Baumstruktur abgelegt werden, zum Beispiel **`dc=ordix`**,**`dc=de`**. In einem OUD können mehrere EUS-Realms parallel bestehen. Der EUS-Realm wird in anderen Tools auch **`base_DN`**, für Basis Distinguished Name, bezeichnet. Mit seinem Distinguished Name wird jedes Objekt im Verzeichnisbaum eindeutig beschrieben (siehe Abbildung 3). Das EUS-Schema beginnt im Verzeichnisbaum mit dem Zweig OracleContext direkt unterhalb des EUS-Realms und darf ausschließlich im EUS-Kontext verwendet werden.

Der Anmeldevorgang

Wie ein vollständiger Anmeldevorgang unter Verwendung von EUS abläuft, verdeutlicht Abbildung 3.

Der Client schickt die Verbindungsdaten zur Datenbank (1). Wenn der Benutzer nicht in der Datenbank existiert, fragt die Datenbank beim Verzeichnisdienst nach (2). Ist der Benutzer im OUD bekannt und einem globalen User in der Datenbank zugeordnet, wird der Name des globalen Users zurückgegeben (3). Nun erfragt die Datenbank die Rechte (4) und erhält die Namen der zugeteilten globalen Rollen zurück (5).

Man nehme ...

Schauen wir uns nach dem Überblick die Umsetzung an. Im Teil I der Reihe wurden die Oracle-Verzeichnisdienste und Fusion-Middleware-Komponenten bereits vorgestellt, daher folgt nur eine kurze Zusammenfassung. Die Verzeichnisdienste gehören zum Identity-Management-Paket der Fusion-Middleware. Ich bevorzuge die Lösung mit dem Oracle Unified Directory (OUD), weil es seine eigene schlanke Datenbank enthält. Über ein Web Interface zur Verwaltung von OUD-Instanzen, genannt Oracle Unified Directory Services Manager (OUDSM), lassen sich fast alle administrativen Tätigkeiten bequem ausführen. Anwender sind mit ihrem Passwort wahrscheinlich schon in einem Verzeichnisdienst eingetragen, der als Datenbasis integriert werden kann. Für die Synchronisation zwischen den Verzeichnisdiensten dient die Komponente Directory Integration Platform (DIP). DIP benötigt einen Repository Katalog, der in der Fusion-Middleware-Version 11g in der OUD-Datenbank installiert wurde. Mit der Version 12c muss eine eigene Datenbank, bevorzugt Oracle Server, vorhanden sein.

Wurden alle Komponenten erfolgreich installiert, können sie zusammenwirken. Die Kommunikation mit anderen Verzeichnisdiensten, wie z.B. einem zentralen Active Directory, wird in einem späteren Teil betrachtet. Dieser Teil beschränkt sich auf die Kommunikation zwischen Datenbank und OUD-Instanz.

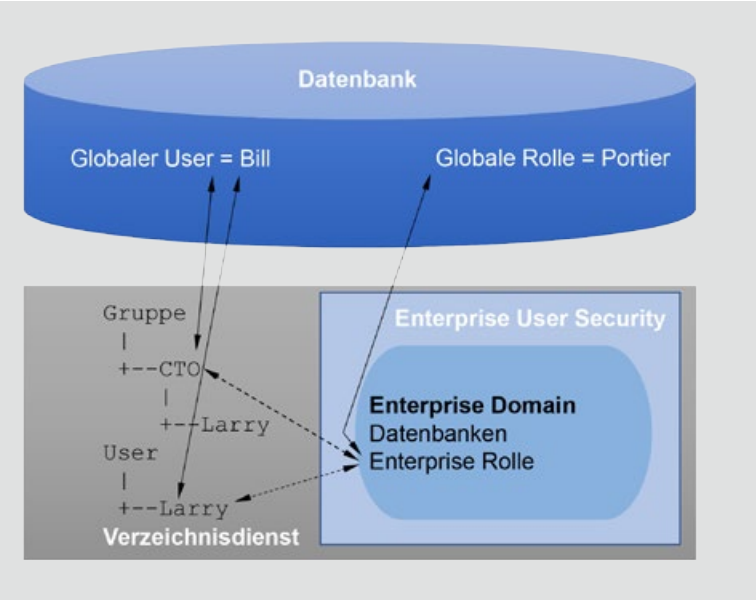


Abb. 1: Verbindung von Datenbank und EUS

```
(root)
   +-- de
      +-- ordix
          +-- OracleContext ( Beginn des EUS-Schemas )
          +-- User
              +-- Trakle  (DN: cn=Thomas,cn=User,dc=ordix,dc=de)
```

Abb. 2: Beispiel-Baumstruktur

Ziehen wir zum Vergleich das Modell der Ehe heran.

Die Planungsphase. Wir müssen reden ...

Das Interesse ist geweckt. Man hat sich entschlossen, es miteinander zu versuchen. Alles ist möglich, die Brille rosarot, das Ziel ist das Optimum. Je mehr Gemeinsamkeiten jetzt entwickelt werden, umso besser. Für die Datenbank bedeutet dies die Umstellung auf globale Benutzer und globale Rollen. Das Ziel: Möglichst viele Enterprise User teilen sich einen globalen User – einen Shared-Global-User.

Regeln für Shared-Global-User:

- keine eigenen Objekte
- keine eigenen Rechte, evtl. **`CREATE SESSION`**

Im Verzeichnisdienst sehen wir, welche globale Rolle einer Enterprise-Rolle zugeordnet ist, aber nicht, welche Rechte die globale Rolle in der Datenbank hat. Es sei denn, in allen Datenbanken haben globale Rollen mit gleichem

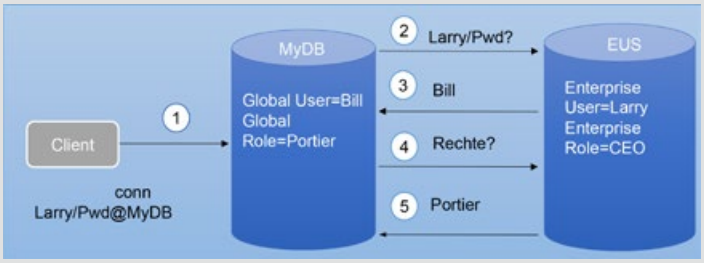


Abb. 3: Anmeldevorgang

Komponente	Software
Oracle Unified Directory	fmw_12.2.1.3.0_oud_Disk1_1of1.zip
OUDSM / EM Console / WebLogic Server	fmw_12.2.1.3.0_idm_Disk1_1of1.zip
Directory Integration Platform	fmw_12.2.1.3.0_oid_linux64_Disk1_1of1.zip
Oracle-Datenbank	Oracle Server Enterprise Edition

Abb. 4: Software-Übersicht

```
create user tt identified globally as
'cn=eu1,cn=users,cn=…';
create user guest identified globally as '';

create role GR_READ identified globally;
grant select on v_$instance to gr_read;
```

Abb. 5: Globalen User und globale Rolle erstellen.

Namen auch exakt gleiche Rechte. Disziplin und klare Regeln sind gefragt.

Applikations-User können keine Shared-Global-User sein. Enterprise User mit eigenen Objekten und/oder direkt zugewiesenen Rechten werden einem eigenen globalen User zugeordnet. Diese Zuordnung sollte aber nicht in der Datenbank definiert werden, wie in Abbildung 5 (obere Zeile) dargestellt. Wird eine Verbindung durch die Angabe des Distinguished Name (DN) eines Enterprise Users in der Datenbank definiert, dann ist diese Verbindung im Verzeichnisdienst nicht bekannt.

Im OUD muss jede Datenbank mit dem Database-Configuration-Assistant (DBCA) registriert werden. Eine Fleißarbeit, die aber gut per Skript ausgeführt werden kann. Hier muss lediglich zwischen einer Container-Datenbank und einer Pluggable-Datenbank unterschieden werden. Die Verbindungsinformation zum OUD liest der DBCA aus der Datei **`ldap.ora`**.

Kniffeliger kann es da sein, die günstigste Gruppierung der Datenbanken in Enterprise Domains zu ermitteln. Je mehr Informationen man über die Anwender, die Anwendungen und die Anforderungen hat, umso besser. Ziehen Sie Anwendungsverantwortliche rechtzeitig in die Planung mit ein, auch bei der Planung der globalen Rollen. In der Enterprise Domain wird auch die Enterprise-Rolle angelegt. Selbst wenn in den Datenbanken einer Enterprise Domain alle globalen Rollen die gleichen Namen haben, muss dennoch jede globale Rolle einzeln den Enterprise-Rollen zugeordnet werden. An diesem Punkt kann einiges an Aktionen zusammenkommen. Im Falle einer nachträglichen Umorganisation müssen Zuordnungen erst einzeln getrennt und anschließend neu angelegt werden.

Anwender dagegen sind im Active Directory in der Regel schon Mitglieder in unterschiedlichen AD-Gruppen. Es gibt damit einen Rahmen, den man übernehmen oder zumindest als Richtlinie verwenden kann. Gelingt es im optimalen Fall, sowohl Shared-Global-User als auch Enterprise-Rollen ausschließlich mit Enterprise-Gruppen zu verbinden, ist der Gewinn am größten. Mitarbeiter, die zum Unternehmen hinzukommen, im Unternehmen eine andere Tätigkeit wahrnehmen oder das Unternehmen verlassen, müssen nur ihren Gruppen zugewiesen, bzw. aus ihren Gruppen entfernt werden. Über die Gruppenzugehörigkeit ergeben sich dann alle Optionen zur Nutzung der Datenbanken.

Mit den Anwendern verschiebt sich auch das Thema Sicherheit ins OUD. Die Verschlüsselungsmethode der Passwörter, die Komplexität der Passwörter, ihre Lebensdauer, ihr Sperrverhalten, die Lebensdauer einer Session – alles das wird jetzt im OUD verwaltet. Das Oracle Unified Directory steht der Datenbank an Möglichkeiten darin nicht nach.

Zusammen starten

Am Ende der Planungszeit sind die Bedenken aus dem Weg geräumt und die Entscheidung gefestigt, es miteinander zu versuchen. Das neue Zuhause wird eingerichtet und der Umzugstermin festgelegt. Eine Zeit, in der neue Freunde an Bedeutung gewinnen. Zu diesen Freunden werden sicherlich **`dsconfig`**, **`eusm`**, **`ldapmodify`** und **`ldapsearch`** gehören. Alle drei sind CLI-Tools und nach der Installation bereits vorhanden.

Da ist zuerst das Tool dsconfig. Mit diesem Tool kann die OUD-Instanz konfiguriert werden. Die Verwaltung von Portkonfigurationen, Passwortsicherheit, Verschlüsselung und Benutzerprofilen sind nur einige Einsatzgebiete. Es ist ein sehr mächtiges Tool und Bestandteil der OUD-Software.

Die Tools ldapmodify und ldapsearch sind auch Teil der OUD-Installation und dienen dem Hinzufügen, Ändern, Löschen und Lesen von Einträgen im Verzeichnisbaum. Arbeitsanweisungen werden im LDIF-Format an das OUD übergeben. ldapmodify ist z. B. das Tool, mit dem Benutzer im OUD angelegt, geändert und entfernt werden können. Datenbanken einer bestimmten Enterprise Domain zuzuweisen, kann ebenfalls mit dem Tool **`ldapmodify`** ausgeführt werden.

Das Tool eusm gehört zur Oracle-Datenbank-Software-Installation. Sein Einsatzgebiet sind die Strukturen im EUS-Schema. Mit diesem Tool können Enterprise Domains und Enterprise-Rollen erstellt, verwaltet und entfernt werden. Es unterstützt die Verknüpfung von globalen Rollen mit Enterprise-Rollen, oder von globalen Benutzern mit Enterprise-Gruppen/-Benutzern und der Verknüpfung von Enterprise-Rollen mit Enterprise-Gruppen/-Benutzern. Darüber hinaus können mit diesem Tool alle Informationen über die oben genannten Komponenten im EUS-Schema abgefragt werden. Mit dem eusm-Tool können alle Aktionen ausgeführt werden, die in der Oracle-Dokumentation mit dem Enterprise Manager GUI beschrieben sind.

Ist der Umzug dann abgeschlossen, kommt der Alltag. Man wird Dinge finden, die „früher“ besser waren. In einer Multitenant-Datenbank kann man als Common User nicht mehr mit dem Kommando `ALTER SESSION SET CONTAINER` in die CDB oder eine andere PDB wechseln. Gerade Administratoren werden Stellen finden, an denen sie PL/SQL-Code nicht verwenden können, weil das direkt zugewiesene Recht fehlt. Hat ein Anwender seinen Account gesperrt, dann hat er auf keine Datenbank mehr Zugriff, weil der Account im OUD gesperrt ist.

Diese Mankos rücken jedoch in den Hintergrund, betrachtet man die Vorteile, die der Umzug mit sich bringt: Mit EUS hat ein Anwender nur noch ein Passwort für alle Datenbanken, es wird daher eher weniger Sperrungen geben. Hat man das OUD gut mit dem zentralen AD verknüpft, dann wird ein neuer Anwender automatisch in das OUD übernommen und erhält sofort alle nötigen Rechte für die Nutzung der Datenbank. Das ist der Idealfall und es wird immer wieder Punkte geben, an denen Kompromisse erforderlich sind, die zur Abweichung führen. Aber gerade bei Kompromissen stärkt die Einhaltung der Regeln, die ein gutes Miteinander von Datenbank und EUS sichern, die eigene Position. Man ist widerstandsfähiger gegen „Können Sie mal eben“-Aktionen, die am Ende zu ewig lebenden Kurzzeitlösung führen. Der größte Vorteil liegt im Bereich Security. Sicherheitsanforderungen können mit EUS deutlich klarer um- und durchgesetzt werden. Durch gemeinsam genutzte Datenbank-Accounts war es vorher nur mit Auditing möglich, zu ermitteln, welche Anwender sich mit einer Datenbank verbinden. Nun kann es zentral im OUD abgefragt werden. Die genaue Anzahl der Datenbanknutzer kann für die Oracle-Lizenzbetrachtung leichter bestimmt werden. Bei Wartungsarbeiten oder Ausfällen können betroffene Anwender leichter ermittelt werden. Ein Nebeneffekt: Hat man einmal alle Datenbanken im OUD registriert, stehen sie für die TNS-Namensauflösung zur Verfügung. Die Pflege einzelner TNSNames.ora-Dateien kann entfallen.

Fazit

Rechtfertigt der Aufwand den Nutzen? Muss man mit EUS nicht Probleme lösen, die man alleine nicht hat? Berechtigte Fragen, die jeder für sich im Vorfeld klären muss. Nicht jeder eignet sich für eine Ehe und nicht jede Datenbank-Umgebung braucht eine zentrale Benutzerverwaltung. Manche heiraten, um für ein Kind geregelte Strukturen zu schaffen. In der IT kann das „Kind“, das nach geregelten Strukturen verlangt, Datenschutzgrundverordnung heißen. Mein persönliches Fazit ist: Ja, solange nicht Einschränkungen durch Anwendungen Grenzen setzen, lohnt sich der Aufwand. Aber er verlangt auch einiges an Struktur und Disziplin. Krummgedrückte Zahnpastatuben und rumliegende Socken sind hier ein gern genutztes Bild für Kleinigkeiten, die zu Sand im Getriebe führen. Auf der anderen Seite gewinnt man auch. Mit Sorgfalt behandelt und gut gepflegt wird die Verbindung von Datenbank und EUS ein Bund für’s Leben.

Thomas Trackle
(info@ordix.de)

Quellen

[Q1] Oracle Online Dokumentation Datenbank 12cR2
https://docs.oracle.com/en/database/oracle/oracle-database/12.2/dbimi/enterprise-user-security-administrators-guide.pdf

[Q2] Oracle Online Dokumentation Fusion Middleware / Oracle Unified Directory 12.2.1.3.0
https://docs.oracle.com/en/middleware/idm/unified-directory/12.2.1.3/

[Q3] My Oracle Support | Doc ID 1085065.1
EUSM, Command Line Tool For EUS Administration and Some EUS Good to Knows

CISSP – Certified Information Systems Security Professional

ORDIX AG baut Portfolio im Bereich IT-Security aus

In der Vielfalt der am Markt verfügbaren Zertifizierungen von IT-Profis für Sicherheit in Informationssystemen hat sich in den letzten Jahren der CISSP als besonders anerkannt erwiesen. Die Zertifizierung wurde vom International Information Systems Security Certification Consortium (ISC)² entwickelt und ist eine anspruchsvolle Form, um ein breites Spektrum an theoretischen und praktischen Kenntnissen in Informationssicherheit nachzuweisen. Durch unsere vier Mitarbeiter, die die CISSP-Prüfung bestanden haben, kann die ORDIX AG ihren Kunden gegenüber eine hohe Expertise in IT-Sicherheit anbieten.

Die Prüfung zum CISSP deckt eine Vielzahl von technischen und organisatorischen Aspekten ab, die der Sicherstellung der Triade aus Vertraulichkeit, Verfügbarkeit und Integrität von Daten dienen. Insofern dokumentiert der CISSP ein breitgefächertes Wissen auf technologischer Ebene sowie auf der Management-Ebene, um grundlegende Zusammenhänge zu begreifen, ohne jedoch zu tief in die jeweilige Produktebene abzutauchen. In Deutschland gibt es übrigens nur ca. 2.000 Zertifikatshalter.

Die Bewertung der Kompetenz des IT-Profis durch die Zertifizierung ist durch den unabhängigen Prüfungsmodus objektiv und durch ANSI als ISO-Standard 17024:2003 im Bereich Informationssicherheit offiziell akkreditiert und weltweit anerkannt.

Die Prüfung

Um das Zertifikat zu erlangen, ist es notwendig, eine theoretische Prüfung über die acht Domains des „Common Body of Knowledge" abzulegen.

Die acht Domains umfassen:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Dabei kann die Prüfung in englischer Sprache (ca. 100-150 Fragen in drei Stunden) oder in deutscher Sprache (ca. 250 Fragen in sechs Stunden) abgelegt werden. Mindestens 70% der Fragen müssen dabei korrekt sein. Die englische Prüfung stellt darüber hinaus auch sicher, dass die Mindestanzahl richtiger Antworten in jeder einzelnen Domain gegeben wurde. Zur Prüfungsvorbereitung dienen ein Seminar, ein 1000-seitiger Study Guide und viele Hundert Prüfungsfragen. Zu den Kernpunkten der theoretischen Ausbildung gehören:

- Verschlüsselungstechnologien und deren Anwendung
- Softwareentwicklung unter Sicherheitsgesichtspunkten
- Risikomanagement
- Disaster Recovery Strategien
- Erkennung und Abwehr von Angriffen
- sicheres Identitätsmanagement
- Authentisierungsmethoden
- Absicherung von Cloud-Technologien
- sichere IT- und Netzwerkarchitekturen
- und vieles mehr

CISSP-Status

Zu Erlangung des CISSP-Status ist neben der bestandenen Prüfung auch der Nachweis von mindestens fünf Jahren Berufserfahrung im IT-Sicherheitsumfeld erforderlich. Des Weiteren ist die Unterzeichnung und Befolgung des (ISC)² „Code of Ethics" verpflichtend:

"Beschütze die Gesellschaft, das Gemeinwesen und die Infrastruktur; handle ehrenwert, ehrlich, gerecht, verantwortungsvoll und den Gesetzen entsprechend; arbeite gewissenhaft und kompetent; fördere und beschütze den Berufsstand."

Zudem erklärt sich der Zertifikatshalter dazu bereit, sich nachweislich jährlich im Thema fortzubilden, um CISSP zu bleiben. Die ORDIX AG kann Sie nun mit unseren CISSP-zertifizierten Mitarbeitern noch fachkundiger bei Projekten unterstützen, bei denen Sie

- Best Practices im Umfeld von Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten für erforderlich erachten,
- Unterstützung im Dickicht nationaler und europäischer Regularien (BSI, DSVGO, PCI-DSS) benötigen,
- Security-Konzepte für Ihre IT erstellen oder testen,
- moderne technische wie organisatorische Standards zur Sicherung Ihrer IT-Werte einführen möchten.

Neuigkeiten im Überblick

Apache Hadoop 3

Die Features der Hadoop Version 3 sind bereits seit Ende 2017 verfügbar, wurden aber erst Mitte 2018 von den großen kommerziellen Distributionen adaptiert. Es gibt zu beachtende Änderungen, wie zum Beispiel die Neubelegung der Service Ports, aber auch neue Features, wie den Support für Erasure Coding innerhalb des HDFS. Die Plattformen Hortonworks HDP 3 und Cloudera CDH 6 enthalten Hadoop 3, es werden jedoch nicht zwingend alle Features unterstützt. Wir geben einen Überblick über die Neuerungen und beleuchten die wichtigen Features der neuen Hadoop-Version.

Was bringt Hadoop 3?

Obwohl Hadoop 3 schon länger verfügbar ist, basieren viele produktive Deployments noch auf Hadoop 2. Dies liegt vor allem daran, dass die kommerziellen Distributionen die neuen Open-Source-Versionen mit einem zeitlichen Versatz adaptieren. Im Folgenden werden wir die wichtigsten neuen Features beleuchten, um einen Überblick über die Änderungen zu geben.

Speicherplatz einsparen mit Erasure Coding

Mit Hadoop 3 kommt ein mächtiges Feature, das eine starke Reduzierung des Brutto-Datenverbrauchs durch das HDFS ermöglicht. Bisher war es üblich, die Datenblöcke dreifach zu replizieren, was einen Speicher-Overhead von 200% mit sich bringt. Mit Erasure Coding lässt sich der Overhead auf bis zu 40% reduzieren.

Bei Erasure Coding werden die Daten meist in 1024-KB-Blöcke aufgeteilt und zu einer konfigurierbaren Anzahl an Datenblöcken Paritätsblöcke generiert. Zur Widerherstellung von verlorenen Datenblöcken (z.B. Ausfall eines `DataNodes`), werden die Paritätsblöcke zur Berechnung genutzt. Als theoretische Grundlage dienen unter anderem Reed-Solomon-Codes, welche bereits in anderen Bereichen praktisch angewendet werden (z.B. bei optischen Datenträgern oder im Festplattenverbund RAID 6).

Ein großer Vorteil in bestehenden Clustern ist die Möglichkeit, Replikation und Erasure Coding gleichzeitig betreiben zu können. So lassen sich verschiedene Policies für Erasure Coding auf einzelne Verzeichnisse im HDFS gleichzeitig aktivieren. Eine Migration erfolgt dann über einfaches Kopieren im HDFS.

Für den Produktivbetrieb empfiehlt es sich, die Intel ISA-L Library einzubinden, um die Berechnungen für Erasure Coding nativ ausführen zu lassen. Weil der Datendurchsatz groß genug ist, wird der mögliche Bottleneck auf Netzwerkhardware und Festsplatten verlagert [Q1].

Darüber hinaus ist zu beachten, dass der Vorteil des geringeren Speicherverbrauchs bei besonders vielen kleinen Dateien zunichte gemacht wird. Eine Datei, die kleiner als 1024 Kibibyte ist, verbraucht bei drei Datenblöcken und zwei Paritätsblöcken trotzdem 300% Speicher.

Wie funktioniert Schreiben, Lesen und Verarbeiten mit Erasure Coding?

Beim Schreiben teilt der HDFS Client die Daten in Blöcke auf, die meist 1024 KB groß sind. Je nach Einstellung (Coding Policy) werden jeweils für eine feste Anzahl an Blöcken Paritätsblöcke generiert (siehe Abbildung 1). Die Blöcke werden dann über die `DataNodes` verteilt (siehe Abbildung 2). Dabei muss die Anzahl der `DataNodes` mindestens der Anzahl der Daten- und Paritätsblöcken entsprechen. Bei der Coding Policy RS-6-3-1024k würde man mindestens neun `DataNodes` benötigen, um sechs Daten- und drei Paritätsblöcke verteilen zu können.

Beim Lesevorgang werden zunächst nur die `DataNodes` vom Client angesprochen, die Datenblöcke enthalten. Nur falls ein `DataNode` mit dem angeforderten Datenblock ausfällt, werden die Paritätsblöcke angefordert und Berechnungen zur Widerherstellung durchgeführt.

Im Gegensatz zur Dreifachreplikation, ist bei Erasure Coding keine Data Locality gegeben, wenn Berechnungen (z.B. Spark oder Mapreduce) auf Daten ausgeführt werden. Die Blöcke werden streifenweise (Striped Layout) abgelegt. Vor einer Verarbeitung wird dadurch mehr Netzwerklast erzeugt, da logisch zusammenhängende Daten zunächst zusammengefasst werden müssen.

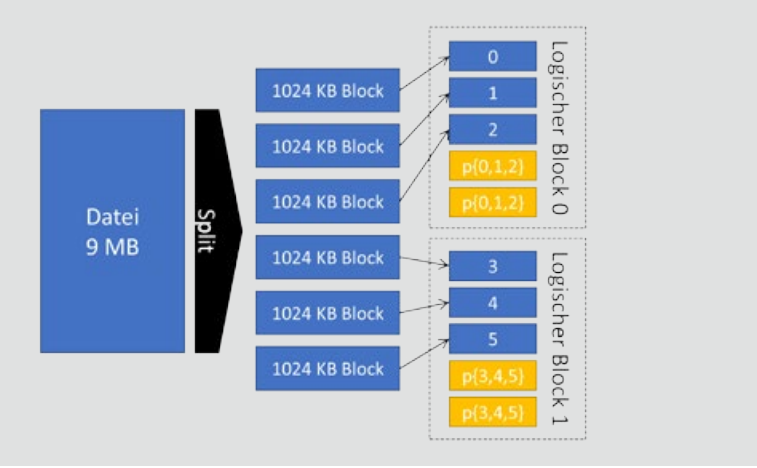


Abb. 1: Aufteilung einer Datei in Blöcke & Berechnung der Paritätsblöcke

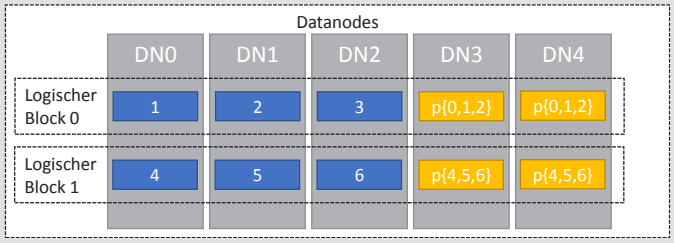


Abbildung 2: Verteilung der Daten- und Paritätsblöcke

Welche Coding Policies gibt es?

Hadoop 3 erlaubt die Verwendung verschiedener Konfigurationen für Erasure Coding als Policies. Die Policy XOR-2-1-1024K ist kein Reed-Solomon-Code, sondern basiert auf der bitweisen Verknüpfung XOR (Exklusives-Oder).

Die Policies bieten für verschieden Cluster-Konfigurationen Vor- und Nachteile. Für eine größere Anzahl an Daten- und Paritätsblöcken, wird ein entsprechend großer Cluster vorausgesetzt. Eine geringere Anzahl an Blöcken verringert die Ausfalltoleranz.

Die Datenblöcke enthalten die Nutzdaten und die Paritätsblöcke sichern gegen Ausfälle und Datenverlust. Zum Beispiel bietet der Code RS-3-2-1024k eine Verlusttoleranz von bis zu zwei Blöcken bei fünf Blöcken insgesamt.

Policy	Datenblöcke	Paritätsblöcke	Blockgröße
RS-3-2-1024k	3	2	1024 KiB
RS-6-3-1024k	6	3	1024 KiB
RS-10-4-1024k	10	4	1024 KiB
RS-LEGACY-6-3-1024k	6	3	1024 KiB
XOR-2-1-1024k	2	1	1024 KiB

Wie werden Erasure-Codes aktiviert?

Die Policies zur Verwendung der Erasure Codes müssen zunächst für den Cluster über die Shell aktiviert werden:

```
$ hdfs ec -enablePolicy -policy <Policy>
```

Beispiel:

```
$ hdfs ec -enablePolicy -policy RS-3-2-1024k
```

Anschließend wird für ein Verzeichnis und dessen Unterverzeichnisse rekursiv die Policy gesetzt:

```
$ hdfs ec -setPolicy -path <Pfad> -policy <Policy>
```

Beispiel:

```
$ hdfs ec -setPolicy -path /folder/subfolder -policy
RS-3-2-1024k
```

Alle Daten, die sich in diesem Pfad befinden werden nun mit Erasure Coding im HDFS verteilt. Für die Migration dreifach replizierter Daten nach Erasure Coding, reicht ein Verschieben oder Kopieren aus:

```
$ hadoop fs -mv /replicated_data /ec_data
```

Unterstützung von mehr als drei HDFS NameNodes

Bisher erlaubte Hadoop 2 nur ein Deployment mit bis zu zwei **NameNodes**. Hadoop 3 hebt diese Grenze auf und erlaubt mehr **NameNodes** gleichzeitig. Zu einem Zeitpunkt darf weiterhin nur ein **NameNode** aktiv sein (Active-Passive) und in die Edit-Logs der **JournalNodes** schreiben. Die **JournalNodes** dienen der Synchronisation der **NameNodes**. Das automatische Failover kann mit dem Zookeeper Failover Controller (ZKFC) in Verbindung mit einem Zookeeper-Cluster realisiert werden.

Wie wird ein Split-Brain-Szenario verhindert?

Um bei einem möglichen Split-Brain-Szenario, zum Beispiel bei einer Netzwerktrennung, ein gleichzeitiges Schreiben in die Edit-Logs durch unterschiedliche **NameNodes** zu vermeiden, wird der Quorum Journal Manager (QJM) verwendet.

Jeder **NameNode** handelt mit den **JournalNodes** eine zentrale Epoch-Zahl aus. Bei mehreren aktiven **NameNodes** wird der zuerst anfragende **NameNode** gewinnen – sofern die Mehrheit der **JournalNodes** die neue Epoch-Zahl bestätigt.

Alle anderen **NameNodes**, die danach versuchen, eine Epoch-Zahl festzulegen, scheitern und fahren sich selbst herunter. Der tatsächlich aktive **NameNode** sendet nun mit jeder Schreibanfrage die Epoch-Zahl mit, welche durch die **JournalNodes** mit der zentralen zur Autorisierung verglichen wird.

Konfiguration mehrerer HDFS NameNodes

Die Konfiguration mehrerer NameNodes erfolgt über die core-site.xml und **`hdfs-site.xml`**. Folgende Properties müssen gesetzt werden:

`core-site.xml`	
fs.defaultFS	Name-Service für den HDFS Cluster Beispiel: hdfs://democluster
ha.zookeeper.quorum	Für automatisches Failover: **`Zookeeper-Nodes`** mit Portangabe Beispiel: zk1.demo.net:2181,zk2.demo.net:2181, zk3.demo.net:2181

hdfs-site.xml	
dfs.ha.automatic-failover	Automatisches Failover mit ZKFC mit „true“ aktivieren. Für manuelles Failover auf „false“ setzen.
dfs.namenservices	Name-Service des HDFS Cluster (fs.defaultFS, ohne „hdfs://“) Beispiel: democluster
dfs.ha.namenodes.<hdfs-alias>	Liste an Aliase für **`NameNodes`** Beispiel: nn1, nn2, nn3
dfs.namenode.rpc-address.<hdfs-alias>.<namenode-alias>	RPC-Adresse und -Port des jeweiligen **`NameNodes`** pro **`NameNode`**-Alias Beispiel: namenode1.ordix.de:9820
dfs.namenode.http-address.<hdfs-alias>.<namenode-alias>	HTTP-Adresse und -Port des jeweiligen **`NameNodes`** pro **`NameNode`**-Alias Beispiel: namenode1.ordix.de:9870
dfs.namenode.shared.edits.dir	Edit-Verzeichnis und **`JournalNode`**-Quorum Beispiel: qjournal://journalnode1.ordix.de:port, journalnode2.ordix.de:port,.../democluster
dfs.journalnode.edits.dir	Verzeichnispfad für Edit-Logs der **`JournalNodes`** Beispiel: /hadoop/journalnode/edits

Inbetriebnahme mehrerer HDFS NameNodes

Werden Cloudera CDH oder Hortonworks HDP verwendet, übernehmen die jeweiligen Cluster Manager den korrekten Start der jeweiligen Komponenten. In diesem Abschnitt wird der Start im Detail beschrieben, wie er mit der Open-Source-Version durchgeführt werden kann.

Vor dem Start der **`NameNodes`** werden die JournalNodes gestartet, um ein Quorum **`JournalNodes`** zu ermöglichen. Ein **`NameNode`** wird dann genutzt, um das HDFS zu formatieren. Wie gehabt wird dabei der Befehl **`hdfs namenode -format`** verwendet. Anschließend kann dieser NameNode gestartet werden.

Die weiteren **`NameNodes`** beziehen den Dateiindex (fsimage) über den als Erstes gestarteten **`NameNode`**. Dazu werden die weiteren **`NameNodes`** vor dem Start mit folgendem Befehl **`bootstrapped`**: **`hdfs namenode -bootstrapStandby`** aufgegrufen. Danach werden die **`NameNodes`** normal gestartet.

Die Reihenfolge zusammengefasst:

1. Start aller JournalNodes
2. Formatierung des HDFS durch den ersten NameNode
3. Starten des ersten NameNodes
4. Bootstrap der weiteren NameNodes
5. Start der weiteren NameNodes
6. Bei automatischem Failover: Start der ZKFCs

Festplatten mit Intra DataNode Diskbalancer gleichmäßig auslasten

Pro **`DataNode`** werden die HDFS-Nutzdaten auf mehreren Festplatten verteilt. Bisher gab es jedoch keine Möglichkeit, eine Imbalance, beispielsweise durch den Austausch einer Festplatte, zu begradigen. Ungleichmäßig ausgelastete Festplatten (auch Skew genannt) verringern die Lebensdauer einzelner Festplatten und bremsen die Schreib- und Leseperformance.

Hadoop 3 schafft hier Abhilfe durch den **`Intra DataNode Diskbalancer`**, der es ermöglicht, die Datenblöcke über die Festplatten wieder gleichmäßig zu verteilen. Die Neuverteilung kann zunächst durch einen Plan erstellt, aber zu einem späteren Zeitpunkt ausgeführt werden.

Vor der Verwendung muss in der **`hdfs-site.xml`** der **`Intra DataNode Balancer`** aktiviert werden, in dem die Property **`dfs.disk.balancer.enabled`** auf **`true`** gesetzt wird.

Der Intra DataNode Balancer im Praxisbeispiel

Wir zeigen ein Praxisbeispiel für das pro **`DataNode`** drei sehr kleine virtuelle Festplatten über zwei Mountpoints eingebunden werden. In der HDFS Konfiguration sind zunächst aber nur zwei der drei Festplatten eingebunden. Zusätzlich wird die HDFS-Blockgröße mit 32 MB besonders klein gewählt.

hdfs-site.xml

```
<configuration>
[...]
    <property>
        <name>dfs.datanode.data.dir</name>
        <value>/hadoop/disk1,/hadoop/disk2</value>
    </property>
    <property>
        <name>dfs.disk.balancer.enabled</name>
        <value>true</value>
    </property>
    <property>
        <name>dfs.blocksize</name>
       <value>33554432</value> <!-- 32 MB blocksize -->
    </property>
[...]
</configuration>
```

Abbildung 3: Ungerade Verteilung der Daten über die Festplatten einer DataNode

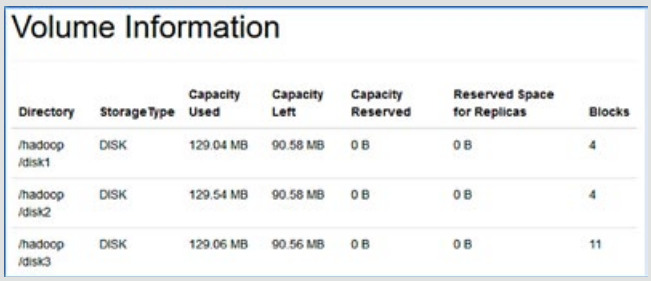


Abbildung 4: Begradigte Verteilung der Daten über die Festplatten einer DataNode

Glossar

Cloudera
Cloudera ist ein Hadoop Distributor. Neben einer kostenlosen Version bietet Cloudera auch Support und zusätzliche Funktionalitäten als Teil von kostenpflichtigen Distributionen an.

Hortonworks
Hortonworks ist ein Hadoop Distributor. Als Managment-Interface wird Apache Ambari eingesetzt.

HDFS
Das Hadoop Distributed File System ist ein verteiltes Dateisystem zur Speicherung sehr großer Datenmengen.

YARN
Acronym für Yet Another Resource Negotiator - Service zur Allokation und Verwaltung der Clusterressourcen (CPU/RAM) sowie Ablaufplaung der Applikationen im Cluster

Größenangaben
Die Größenangaben in diesem Artikel verwenden Binärpräfixe:
1 TB = 1024 GB = 10242 MB = 10243 KB = 10244 Byte

Intel ISA-L
Abkürzung für Intelligent Storage Acceleration Library. Bibliothek für diverse Storage-Anwendungen. Unterstützt die Berechnungen für Erasure Coding bei guter Prozessorauslastung. https://software.intel.com/en-us/storage/ISA-L

Quorum
Bei einer Abstimmung notwendige Stimmenanzahl für ein gültiges Ergebnis. In verteilten Systemen muss eine Mehrheit der Knoten einheitlich abstimmen, um einen gültigen Zustand zu erreichen.

Die ersten beiden Festplatten werden nun mit HDFS-Nutzdaten ausgelastet. Die dritte Festplatte hat derzeit noch keine Verwendung.

```
[hadoop@datanode1 hadoop]$ df -h
Filesystem      Size  Used Avail  Use% Mounted on
[...]
/dev/loop0              239M  196M   27M  89%
/hadoop/disk1
/dev/loop1              239M  196M   27M  89%
/hadoop/disk2
/dev/loop2              239M  2.1M  220M   1%
/hadoop/disk3
```

Nun wird die dritte Festplatte eingebunden. Die Datenblöcke sind nun über alle drei Festplatten ungleichmäßig verteilt.

```
[...]
  <property>
      <name>dfs.datanode.data.dir</name>
   <value>/hadoop/disk1,/hadoop/disk2,/hadoop/disk3
   </value>
  </property>
[...]
```

Die Sektion **`Volume Information`** der **`DataNode`**-Webseite gibt uns Informationen über die eingebundenen Festplatten und die Datenblock-Verteilung (siehe Abbildung 3). Zu erkennen ist, dass die dritte Festplatte über keine Datenblöcke verfügt.

Vom **`NameNode`** aus wird nun ein Plan zum Verteilen der Daten erstellt. Dies kann aber auch auf dem **`DataNode`** direkt geschehen. Der Plan wird als JSON-Datei im HDFS abgelegt. Das Erstellen des Plans verbraucht noch keine Cluster-Ressourcen und kann von der tatsächlichen Ausführung unabhängig ausgeführt werden.

Weil die Umverteilung größerer Datenmengen mehr Zeit in Anspruch nimmt, kann mit der Option **`-query`** der Zustand der Umverteilung abgefragt werden.

```
[hadoop@namenode ~]$ hdfs diskbalancer -plan
datanode1
[...]

Writing plan to:
/system/diskbalancer/2018-Sep-30-10-09-38/data-
node1.plan.json
[hadoop@namenode ~]$ hdfs diskbalancer -execute
/system/diskbalancer/2018-Sep-30-10-09-38/data-
node1.plan.json
2018-09-30 10:09:59,179 INFO command.Command:
Executing "execute plan" command

[hadoop@namenode ~]$ hdfs diskbalancer -query da-
tanode1
2018-09-30 10:10:14,129 INFO command.Command:
Executing "query plan" command.
Plan File: /system/diskbalancer/2018-Sep-30-10-09-38/
datanode1.plan.json
Plan ID: aaa963209fec294013ff28e2922e24cdd5f22b49
Result: PLAN_DONE
```

Nach erfolgreicher Ausführung des Balancierens ist nun auf der Webseite des `DataNode` zu erkennen, dass die Daten gleichmäßig über alle Festplatten verteilt sind (siehe Abbildung 4).

Der Diskbalancer bietet darüber hinaus noch weitere Optionen:

- Versatz-Toleranz: Wie viel % darf die Festplattenauslastung vom Durchschnitt abweichen, bevor ein Plan zur Ausbalancierung erstellt werden muss?
- Fehlertoleranz: Wie viele Fehler werden bei der Ausführung des Plans toleriert, bevor er abgebrochen werden muss?
- Bandbreiten-Begrenzung: Wie hoch darf die Datentransferrate maximal sein (MB pro Sekunde)?
- Mit dem `Intra DataNode Diskbalancer` und dem bereits vorhandenen HDFS Balancer, wird nun mehr Flexibilität bei der horizontalen, aber auch vertikalen Speicherskalierung angeboten. Das Ausbalancieren lässt sich dabei im Voraus planen und zu günstigen Zeitpunkten ausführen.

Verbesserte Clusterauslastung durch Yarn Opportunistic Containers

Um die Effizienz eines Hadoop Clusters zu erhöhen, muss die Ressourcenauslastung (Prozessor, Hauptspeicher) über einen Zeitraum möglichst gleich verteilt sein. Mit Opportunistic Containers bietet Hadoop 3 eine Möglichkeit an, dies zu erreichen.

Mit einem neuen Feature soll die Ressourcenauslastung (Prozessor, Hauptspeicher) über Yarn verbessert werden. Die Opportunistic Containers ermöglichen den Start einer Applikation mit garantierten Containern und opportunistischen Containern. Für Erstere müssen zum Startzeitpunkt ausreichend Ressourcen verfügbar sein – für Letztere können Ressourcen zusätzlich allokiert werden, sofern welche zur Verfügung stehen. Opportunistic Containers können gestoppt (Preemption) werden, falls auf einem NodeManager ein anderer Container mit Ausführungsgarantie eintrifft.

Was ändert sich noch mit Hadoop 3?

- **Yarn Timeline Service v2**
  Mapreduce Native Optimierungen - Um die Performance des Mapreduce-Frameworks zu steigern, wurden Teile der Implementation auf nativer Ebene verlagert und optimiert.
- **Migration auf Java 8**
  Die Unterstützung für Java 7 (öffentliche Updates) ist bereits April 2015 abgelaufen. Mit der Migration zu Java 8 geht die Hadoop Community den logischen Schritt, um Updates bis Januar 2019 zu gewährleisten.
- **Shellscript Rewrite**
  Für Hadoop 3 wurden die Shell-Skripte zum Administrieren von Hadoop neu geschrieben, um Fehler zu beheben und die Benutzung zu optimieren.

  Die Hadoop Daemons werden nun über die Option `--daemon` gestartet. Zusätzlich ermöglicht die Option `--debug` eine einfachere Fehlerbehebung der Shell-Skripte.
- **Shaded Client Jars**
  Bisher konnte es bei der Entwicklung von Hadoop-Clients zu Versionskonflikten zwischen eigenen und Hadoop-spezifischen, transitiv eingebundenen, Abhängigkeiten kommen. Mit Hadoop 3 werden die transitiven Abhängigkeiten der Hadoop Client Libraries versteckt (shaded).

Links/Quellen

[Q1] Einführung in Erasure Coding (Cloudera Blog)
http://blog.cloudera.com/blog/2015/09/introduction-to-hdfs-erasure-coding-in-apache-hadoop/

[Q2] Portbelegung Cloudera CDH 6
https://www.cloudera.com/documentation/enterprise/6/6.0/topics/cdh_ports.html

[Q3] HDFS Intra DataNode Disk Balancer (Cloudera Blog)
http://blog.cloudera.com/blog/2016/10/how-to-use-the-new-hdfs-intra-datanode-disk-balancer-in-apache-hadoop/

[Q4] Hortonworks HDP Platform 3 Datasheet
https://de.hortonworks.com/datasheet/hortonworks-data-platform-3-0-datasheet/

[Q5] Apache Hadoop Releases
https://hadoop.apache.org/releases.html

[Q6] Apache Hadoop 3 Dokumentation
https://hadoop.apache.org/docs/r3.0.0/index.html

[Q7] Cloudera Unsupported Features
https://www.cloudera.com/documentation/enterprise/6/release-notes/topics/rg_cdh_600_unsupported_features.html#hdfs_600_unsupported

[Q8] Portänderungen (Apache Software Foundation JIRA)
https://issues.apache.org/jira/browse/HDFS-9427
https://issues.apache.org/jira/browse/HADOOP-12811

[Q9] Mapreduce Native Optimization (Apache Software Foundation JIRA)https://issues.apache.org/jira/browse/MAPREDUCE-2841

[Q10] Migration auf Java 8 (Apache Software Foundation JIRA)
https://issues.apache.org/jira/browse/HADOOP-9902

[Q11] Shellscript Rewrite (Apache Software Foundation JIRA)
https://issues.apache.org/jira/browse/HADOOP-11656

Portbelegungen

Weil die Portbelegungen von Hadoop 2 gegen die Empfehlungen der IANA für temporäre Ports verstoßen, wurden die Belegungen in Hadoop 3 angepasst. Die Ports im Bereich zwischen 49152 und 65535 sind für dynamische, temporäre Zuweisungen vorgesehen.

In Hadoop 3 wird daher auf Ports im Bereich zwischen 9600 und 9871 ausgewichen. Zusätzlich wurde für KMS der Standard-Port geändert, um Konflikten mit dem Apache HBase Master Service vorzubeugen.

Service	Hadoop 2	Hadoop 3
HDFS NameNode	50470	9871
	50070	9870
	8020	9820
HDFS Secondary NameNode	50091	9869
	50090	9868
HDFS DataNode	50020	9867
	50010	9866
	50475	9865
	50075	9864
KMS Service	16000	9600

Fazit

Hadoop 3 bietet neue Features, die vor allem Vorteile für den Produktiveinsatz bringen. Mit Erasure Coding kann der Datenverbrauch durch das HDFS reduziert werden, was Kosteneinsparungen bei der Hardware mit sich bringt, ohne dabei auf Verlusttoleranz verzichten zu müssen. Die Erweiterung oder der Austausch von Festplattenspeicher wird mit dem Intra DataNode Diskbalancer nun erheblich vereinfacht. Der Einsatz mehrerer NameNodes bietet noch mehr Ausfallsicherheit im Betrieb. Und die Ressourcenauslastung wird durch die Yarn Opportunistic Containers zusätzlich erhöht. Zu beachten sind die Änderungen der Service-Ports, die mögliche Rekonfiguration der Firewall-Einstellungen mit sich bringen. Die Migration auf Java 8 ist der logische Schritt, um eine Langlebigkeit zu gewährleisten.

Aron Tigor Möllers
(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

NEUGIERIG?

ORDIX® seminare
einfach. gut. geschult

WETTBEWERBSVORTEILE SCHON GESICHERT?

UNSER SEMINARPROGRAMM 2019 BIETET VIELE MÖGLICHKEITEN

Neben der Digitalisierung, geänderten Geschäftsprozessen und vielen tiefgreifenden Veränderungen, die damit verbunden sind, ist eine stetige Weiterbildung Pflicht.

Wissen sichert Unternehmern und Mitarbeitern gleichermaßen Wettbewerbsvorteile. Deshalb wird die kontinuierliche Weiterbildung der Mitarbeiter in Zukunft immer stärker über den wirtschaftlichen Erfolg von Unternehmen entscheiden.

VIRTUELLE KLASSENRÄUME ab 2019

Lernen verändert sich. Wir geben Ihnen mit virtuellen Klassenräumen die Möglichkeit, Ihre Mitarbeiter kosten- und zeitsparend weiterzuentwickeln.

Seminarteilnehmer verschiedener Standorte kommen im virtuellen Klassenraum als Lerngruppe zusammen und haben die Gelegenheit, zeitgleich wie in einem richtigen Seminarraum zu lernen und miteinander in Echtzeit zu kommunizieren.

SICHERN SIE SICH IHR WISSEN UNTER: **SEMINARE.ORDIX.DE**