

Fortgeschrittene Nutzung von Big-Data-Clustern: Hadoop Security und hochparallele Datenbank-Engines

Viele Unternehmen haben bereits erste Proofs of Concepts (PoCs) mit Big-Data-Clustern durchgeführt, sehr oft mit Hadoop. Erste Erfolge beim Laden und Analysieren von Daten stellen sich schnell ein. Die Transition von einem PoC-Status zu einer sicheren Enterprise-Architektur, die unterschiedliche Workloads für parallel laufende Projekte hochverfügbar unterstützt, ist dann oft noch ein weiter Weg, und die Zahl der zur Verfügung stehenden Datenbanken (on premise und besonders in der Cloud) nimmt ständig zu.

Auf dem Roundtable am 26.04.2018 in München haben wir einige Aspekte aus diesem Themenkomplex betrachtet:

Dr. Henrik Behrens, Data Reply GmbH, hielt einen Überblicksvortrag über das Thema „Hadoop Security“ und erklärte dabei sowohl Grundlagen („Wie funktioniert eine Authentifizierung mit Kerberos, ohne dass das Passwort über das Netzwerk geschickt werden muss?“), aber stellte auch praktische Fragen wie verschiedene Deployment-Alternativen des Kerberos Key Distribution Center im Zusammenspiel mit einem Active Directory-Server vor und verglich sie. Weitere Themen waren die Autorisierung von Zugriffen auf den Ebenen Applikation, Tabelle und Datei, der sichere Zugriff auf den Cluster durch BI-Tools über eine JDBC-Verbindung und einige Aspekte von TLS-Verschlüsselung. Abschließend wurden verschiedene Möglichkeiten der Datensicherung betrachtet (Knoten-Replikation, Mirror-Cluster und Snapshots) und gezeigt, dass Snapshots den besten Schutz gegen versehentliches oder böswilliges Löschen oder Überschreiben von Daten bieten.

Es folgte eine Diskussionsrunde über praktische Erfahrungen bei der Absicherung von Hadoop-basierten Architekturen. Obwohl die ursprünglich vorgesehenen Experten (Francesco Sbaraglia und Artyom Topchyan von Data Reply) kurzfristig absagen mussten, wurden mit Gavin Perrie und Yunus Yünel zwei ebenso versierte Exper-



Foto©: Dr. Henrik Behrens

ten (aus dem gleichen Hause) gefunden, die auf spannende Weise von ihren Erfahrungen im Kontext Hadoop Security berichteten. Daraus ergab sich eine spannende und rege Diskussion mit den Teilnehmern, von der wir die folgenden Ergebnisse festgehalten haben:

Beim Aufsetzen von Big-Data-Clustern sollte das Thema „Security“ möglichst von Anfang an in der Konzeption berücksichtigt werden, denn ein nachträgliches Ergänzen der Security (Kerberos etc.) kann für ein bereits in Produktion befindliches System eine Herausforderung sein, da alle betroffenen Projekte miteinander koordiniert werden müssen.

Das Kerberos Key Distribution Center (KDC) sollte hochverfügbar ausgelegt werden, weil ein Ausfall des Kerberos-Systems den Cluster unbenutzbar macht.

Minimalanforderung für eine Cluster-Absicherung ist eine TLS-Verschlüsselung der Verbindungen von außen zum Cluster (z.B. für JDBC-Zugriffe durch BI-Tools).

- Backups sind nur notwendig für Daten, die man nicht so leicht aus den Quellsystemen neu extrahieren kann. Ein reines Replikat der Quellsysteme mit davon direkt abgeleiteten Tabellen oder Views benötigt nicht unbedingt ein Backup.

- Eine Verschlüsselung der gespeicherten Daten („encryption of data at rest“) sollte aufgrund des Performance Impacts mit Vorsicht betrachtet werden – ein möglicher Weg ist die Verwendung von „encryption zones“, um nur Daten zu verschlüsseln, bei denen es notwendig ist (z.B. personenbezogene Daten).
- Ein vorhandenes Active Directory kann die Rolle des KDC übernehmen, so dass keine Installation eines lokalen KDC erforderlich ist. Die Nachteile dieses Ansatzes sind, dass zahlreiche technische User (Prinzipale) manuell angelegt werden müssen, weil die Admins des zentralen AD der Clusterverwaltungs-Software (z.B. Cloudera Manager) meist nicht das Recht einräumen, automatisiert AD-User zu erzeugen. Außerdem kann selbst ein kleiner Hadoop-Cluster viele tausend Authentisierungsanfragen pro Sekunde generieren, mit der Gefahr einer Überlastung des zentralen AD-Systems. Die Alternative ist in diesem Fall die Installation eines lokalen KDC auf separater Hardware für die Verwaltung der technischen User – die persönlichen User können weiterhin auf dem zentralen AD-Server gepflegt werden („cross realm trust“).
- Interessant war auch eine Diskussion über den richtigen Einsatz von Data Lakes: Während in der Vergangenheit oft die Devise vorherrschte, stets alle verfügbaren Daten in den Data Lake zu laden, hat Gavin Perrie berichtet, dass inzwischen der Trend eher dahin geht, doch nur die Daten zu laden, die für einen konkreten Use Case benötigt werden. Ansonsten bestehe die Gefahr eines „Data Swamp“.
- Yunus Yünel berichtete von seinen Erfahrungen bei der Automatisierung der Installation von Hadoop-Clustern: Bei seinen Kunden hat er die vollständige Basis-Installation und Teile der Security-Konfiguration über Ansible automatisiert, so dass die Installation von mehrerer Cluster inklusiv der vollständigen Security-Konfiguration mit jeweils Dutzenden von Knoten beim gleichen Kunden in kurzer Zeit ausgeführt werden konnte.

Im zweiten Teil des Roundtables ging es um hoch performante Datenbanken, konkret um die Anforderung, Data Warehouse-typische Abfragen auf einem Datenmodell von zwei Terabyte (bis 5 Mrd. Datensätze pro

Tabelle) innerhalb von 3 Sekunden zu beantworten. Hierzu hat Sadik Bakiu, Data Reply, folgende Datenbanken getestet und die Ergebnisse vorgetragen:

- AWS Redshift, die Warehouse-Datenbank von Amazon Webservices
- MapD, eine GPU-beschleunigte In-Memory-Datenbank
- Kinetica, ebenfalls eine GPU-beschleunigte In-Memory-Datenbank (im Test mit 5 Nodes)
- Ignite, eine Technologie zur Verteilten Ausführung von Queries über verschiedene austauschbare Storage-Systeme
- Cloudera Impala mit dem Hadoop Distributed File System (HDFS)
- Impala mit Kudu, einer neuen Technologie zur Abdeckung von analytischen und Einzeldatensatz-basierten Workloads auf der Hadoop-Plattform (Batch und Realtime)
- Presto, der von Facebook entwickelten Datenbank-engine für Hadoop

Abgesehen von Cloudera Impala mit HDFS wurden alle Tests in der AWS Cloud durchgeführt, unter Beachtung der Sizing-Empfehlungen der Hersteller. Die einzige Datenbank, die die Performanzvorgaben ansatzweise erfüllen konnte (Kinetica), war aufgrund der hohen Hardware-Anforderungen zugleich auch mit Abstand die teuerste und damit nur bei wirklich hohen Performanceanforderungen zu empfehlen. Manche Datenbanken sind aber schon aufgrund von Schwierigkeiten bei der Data Ingestion (Ignite) oder beim unterstützten Datenvolumen (MapD) aus dem Rennen ausgeschieden.

Der Roundtable fand erstmals im Veranstaltungssaal des Stadtteilkultur 2411 e.V. statt. Dieser Ort hat sich sehr bewährt, einziger Mangel war die Anzahl der verfügbaren Parkplätze in der Nähe, so dass eine Anreise mit der U-Bahn vorzuziehen war. Die Diskussionen beim anschließenden Networking waren so rege, dass wir gegen 22 Uhr die weiteren Diskussionen nach Austausch von Visitenkarten auf später verschieben mussten. **Der nächste Roundtable befindet sich noch in Planung.**

Dr. Henrik Behrens