Datenbank-Monitoring mithilfe eigenständig entwickelter Tools

Jens Brill, eXirius GmbH

Die Grundlage einer optimal funktionierenden Datenbank ist eine kontinuierliche Überwachung. Oracle stellt hierfür das Diagnostik Pack bereit, bei dem es sich um eine Option der Enterprise Edition handelt. Doch was tun, wenn keine Enterprise Edition lizenziert wurde oder die Diagnostik-Pack-Option nicht erworben wurde?

Ein selbst entwickeltes Tool kann diese Aufgabe übernehmen. Eine solche Lösung ist das von eXirius IT entwickelte Tool „Database Live Monitor“ (DBLM). Das Ziel der Entwicklung eines Tools wie dem DBLM sollte es sein, eine erhöhte Verfügbarkeit zu erreichen, eine Performance-Überwachung zu gewährleisten und die Arbeitszeit der Administratoren zu optimieren. Dabei sollte das Tool die Datenbank möglichst wenig belasten.

Die Notwendigkeit einer Selbstentwicklung ergibt sich aus der täglichen Erfahrung und Arbeit der Administratoren mit Oracle-Datenbanken. Ein großer Teil dieser Arbeit besteht aus Routine-Tätigkeiten wie der Kontrolle des Backups und der Log-Dateien oder die Überwachung der Füllstände der Tablespaces. Ein eigenständig entwickeltes Tool kann einen großen Teil dieser Aufgaben übernehmen und warnen, sobald Handlungsbedarf besteht. Ziel ist es, Probleme nicht nur zu lösen, wenn sie auftreten, sondern sie proaktiv zu verhindern.

Bei der Entscheidung für eine Programmiersprache sollten verschiedene Gesichtspunkte eine Rolle spielen. Wo möchte ich das Monitoring-Tool einsetzen? Wie umfangreich sollen die Überwachungs-Funktionen sein? Welches Know-how für die Programmierung ist im Unternehmen bereits vorhanden?

Natürlich stellt sich die Frage, warum hier ausgerechnet eine als altmodisch und kryptisch geltende Programmiersprache wie Perl zum Einsatz kommt. Neben der Ausgereiftheit der bereits im Jahr 1985 in einer ersten Version implementierten Sprache spielen die freie Lizenz, die weitgehende Plattform-Unabhängigkeit und der riesige Umfang an Erweiterungs-Modulen eine wichtige Rolle. Spezielle Anforderungen müssen somit oft nicht aufwändig programmiert werden, sondern es kann einfach eine entsprechende Bibliothek („Modul“) benutzt werden.

Perl kompiliert ebenso wie Java den als „ASCII/UTF-8“-Text vorliegenden Quellcode zunächst in einen Bytecode. Dieser wird jedoch im Unterschied zu Java von der Perl-Virtuellen-Maschine ausgeführt. Dies ist einerseits sehr performant, besitzt aber andererseits die Flexibilität einer interpretierten Skript-Sprache, was unter anderem bedeutet, dass Zeichenketten zur Laufzeit als Quellcode nachkompiliert und ausgeführt werden können. Da es sich bei einem Monitoring-Tool um ein betriebskritisches Überwachungssystem handelt, sollte hier auf eine bewährte Technik zurückgegriffen werden.

Arbeitsweise und Aufbau

Der Aufbau des DBLM ist so flexibel wie möglich gestaltet. Es ist in allen Oracle-Datenbank-Versionen und auf allen Betriebssystemen einsetzbar. Die Überwachung einer Single-Instanz ist ebenso möglich wie die Überwachung von Standby-Datenbanken und Real Application Clustern (RAC). Die Anzahl der Datenbanken spielt dabei keine Rolle.

Die programmierten Überwachungs-Parameter sind in zwei Bereiche unterteilt: diejenigen, die den Betrieb der Datenbank gewährleisten, und diejenigen, die Abfragen zur Performance durchführen. Alle Parameter sind modular programmiert und können unabhängig voneinander aktiviert und deaktiviert werden. Falls notwendig, lassen sich aufgrund des modularen Aufbaus neue Parameter definieren und jederzeit einbinden. Grenzwerte werden individuell an die zu überwachenden Datenbanken angepasst.

Es sind zwei Kategorien von Parametern definiert. So gibt es Kollektoren, die einen bestimmten Zustand anzeigen. Nur die Zustände „OK“ oder „NICHT OK“ sind möglich. Der Kollektor zeigt also an, ob eine Datenbank geöffnet ist oder nicht. Die Indikatoren ermitteln einen Systemzustand, der mit vorher definierten Schwellenwerten verglichen wird. Hierbei handelt es sich etwa um Füllstände von Tablespaces.

Nicht immer ist die Datenbank für einen Stillstand verantwortlich. Daher überwacht DBLM auch wichtige Funktionen des Servers, um Fehlern an dieser Stelle vorzubeugen.

Benachrichtigung und Problemlösung

Die wichtigste Aufgabe eines Monitoring-Tools ist es, die gewonnenen Erkenntnisse dem Datenbank-Administrator in geeigneter Form bereitzustellen. DBLM versendet in seinen Grundeinstellungen die Informationen per E-Mail und gibt Handlungsanweisungen zur Problemlösung. Andere Methoden der Benachrichtigung sind integriert, etwa die später angesprochene Integration in andere Monitoring-Systeme.

Für die Ergebnisse der Abfragen ist es unumgänglich, eine Form zu wählen, in der Probleme sofort erkannt werden. Das bedeutet, wichtige von unwichtigen Informationen zu trennen und herauszufiltern. Bekommt der Datenbank-Administrator hundert E-Mails am Tag mit für ihn unwichti-

gen Informationen, tritt ein Gewöhnungseffekt ein. Eine wichtige E-Mail, bei der dringender Handlungsbedarf besteht, wird dann womöglich übersehen und als Folge kommt es zu einem Ausfall der Datenbank, der hätte verhindert werden können.

Viele Unternehmen setzen bereits fertige Überwachungs-Software ein. Oft bieten diese jedoch nicht die Möglichkeit zur Überwachung von Oracle-Datenbanken beziehungsweise die gelieferten Informationen entsprechen nicht dem geforderten Umfang. Daher ist es sinnvoll, ein selbst entwickeltes Tool in eine solche Überwachungs-Software zu integrieren.

Häufig kommt es vor, dass Oracle-Administratoren auch andere Überwachungsaufgaben übernehmen. Die Einbindung des selbst entwickelten Tools in ihrer Monitoring-Systeme stellt sicher, dass alle Informationen an einer zentralen Stelle zusammenlaufen.

Strategische Vorgaben an die IT verbieten oftmals den Betrieb weiterer Software-Komponenten auf für andere Zwecke produktiv genutzten Servern. Eine Black-Box-Lösung bietet die Alternative, das Monitoring-Tool Policy-konform zu installieren. Für DBML existiert hierfür eine Appliance-Variante, bei der alle für den Betrieb nötigen Komponenten vorinstalliert sind, sodass der Aufwand für die Inbetriebnahme in der Regel deutlich reduziert ist und sich auf die Anpassung der Konfiguration beschränkt.

Häufig steht im Unternehmen ohnehin eine Virtualisierungsplattform wie VMware, Citrix und/oder Xen zur Verfügung, auf der man dann eine DBLM-vServer-Appliance betreiben kann. Alternativ wäre sogar ein Betrieb auf alter Hardware mithilfe einer Live-CD oder eines USB-Sticks denkbar. Neben dem geringeren Aufwand für die Installation hat diese Lösung auch im laufenden Betrieb Vorteile. Bei Updates muss nur die Konfiguration übernommen werden, der dann modernere Unterbau wird einfach ausgetauscht.

Fazit

Die Entwicklung eines eigenen Monitoring Tools ist mit einem Aufwand verbunden, der nicht unterschätzt werden sollte. Je nach Anzahl der zu überwachenden Datenbanken und gewünschtem Umfang des Überwachungstools kann sich der Entwicklungsaufwand jedoch lohnen, da dadurch viele Prozesse automatisiert werden. Es ergibt sich eine enorme Zeitersparnis für die Oracle-Administratoren; das Tool hilft, Ausfallzeiten zu minimieren, und kann auf Performance-Probleme hinweisen.

Jens Brill
jens.brill@exirius.de

Oracle Database 12c: Das erste Patch-Set-Update bringt Neuerungen

Der übliche Rhythmus für das Erscheinen von Security Patch Updates (SPUs) und Patch Set Updates (PSUs) betrifft mit dem am 15. Oktober 2013 erschienen Update erstmals die neue Datenbank-Version 12c. Die Administratoren werden von einer Neuerung überrascht, denn die vor einigen Monaten erst von Critical Patch Updates (CPUs) in Security Patch Updates umbenannten Pakete werden abgeschafft — für 12c und zukünftige Versionen wird es ausschließlich Patch Set Updates geben. Das unterstützt einerseits die bei vielen Installation gängige Praxis, eben diese PSUs mehr oder weniger regelmäßig einzuspielen, beraubt Administratoren von sicherheitsrelevanten Systemen aber der Möglichkeit, exakt die geforderten (Sicherheits-)Patches einzuspielen. PSUs enthalten neben Sicherheits-Patches auch weitere Patches, die laut Oracle folgenden Bedingungen genügen:

- Die Patches werden extrem gut von Oracle kontrolliert und getestet
- Die Auslieferung als Patch-Bundle reduziert Konflikte bei der Patch-Installation
- Da API- sowie Optimizer-Änderungen etc. ausgeschlossen sind, sind nur minimale Funktionstests für die Inbetriebnahme erforderlich

Da diese Eigenschaften für die PSUs der Vergangenheit durchaus zutreffen, sind diese bei den DBAs sehr beliebt. Diejenigen, die in der Vergangenheit trotzdem lieber CPUs/SPUs eingespielt haben, sollten sich also an die neue Vorgehensweise gewöhnen. Für Oracle 11g wird es bis zum Ende der Laufzeit weiterhin SPUs geben.

Eine der zentralen Fragen bei den SPUs und PSUs ist grundsätzlich, ob diese unbedingt eingespielt werden sollen. Oft lässt sich das durch einen Blick in die Risiko-Matrix klären: Wenn bei den eingesetzten Produkten keine Schwachstellen mit hohem Risiko vorhanden sind, kann man gegebenenfalls darauf verzichten.

Diesmal ist mit CVE-2013-3826 eine Schwachstelle vorhanden, die es ermöglicht ohne Passwort über Netzwerk auf Datenbank-Inhalte lesend zuzugreifen. Betroffen sind alle aktuell unterstützten Oracle-Versionen. Daher ist ausdrücklich empfohlen, das aktuelle Update – in welcher Form auch immer – einzuspielen.

In einer Anmerkung zu dieser Schwachstelle verweist Oracle auf die Tatsache, dass die Verschlüsselung von Oracle-Net-Verbindungen nicht mehr Bestandteil der Advanced-Security-Option ist, sondern für alle Editionen kostenlos zur Verfügung steht. Dies ist wohl ein erneuter Hinweis darauf, dass Oracle den Anwendern die Verschlüsselung von Verbindungen an die Datenbank stärkstens empfiehlt.

Dierk Lenz
http://blog.hl-services.de