NoSQL MEANS No SECURITY?

Philipp Krenn @xeraaa
<table>
<thead>
<tr>
<th>Rank</th>
<th>DBMS</th>
<th>Database Model</th>
<th>Score Feb 2018</th>
<th>Score Jan 2018</th>
<th>Score Feb 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Oracle</td>
<td>Relational DBMS</td>
<td>1303.28</td>
<td>-38.66</td>
<td>-100.55</td>
</tr>
<tr>
<td>2</td>
<td>MySQL</td>
<td>Relational DBMS</td>
<td>1252.47</td>
<td>-47.24</td>
<td>-127.83</td>
</tr>
<tr>
<td>3</td>
<td>Microsoft SQL Server</td>
<td>Relational DBMS</td>
<td>1122.04</td>
<td>-26.03</td>
<td>-81.42</td>
</tr>
<tr>
<td>4</td>
<td>PostgreSQL</td>
<td>Relational DBMS</td>
<td>388.38</td>
<td>+2.19</td>
<td>+34.70</td>
</tr>
<tr>
<td>5</td>
<td>MongoDB</td>
<td>Document store</td>
<td>336.42</td>
<td>+5.47</td>
<td>+0.92</td>
</tr>
<tr>
<td>6</td>
<td>SQL Server</td>
<td>Relational DBMS</td>
<td>1286.97</td>
<td>+8.63</td>
<td>+2.07</td>
</tr>
<tr>
<td>7</td>
<td>Microsoft Access</td>
<td>Relational DBMS</td>
<td>1024.67</td>
<td>+13.83</td>
<td>-3.32</td>
</tr>
<tr>
<td>8</td>
<td>Redis</td>
<td>Key-value store</td>
<td>127.02</td>
<td>+3.88</td>
<td>+12.98</td>
</tr>
<tr>
<td>9</td>
<td>Elasticsearch</td>
<td>Search engine</td>
<td>125.32</td>
<td>+2.76</td>
<td>+17.01</td>
</tr>
<tr>
<td>10</td>
<td>Cassandra</td>
<td>Wide column store</td>
<td>122.78</td>
<td>-1.10</td>
<td>-11.60</td>
</tr>
<tr>
<td>11</td>
<td>SQLite</td>
<td>Relational DBMS</td>
<td>117.27</td>
<td>+3.02</td>
<td>+1.96</td>
</tr>
<tr>
<td>12</td>
<td>Teradata</td>
<td>Relational DBMS</td>
<td>72.99</td>
<td>+0.36</td>
<td>-2.60</td>
</tr>
<tr>
<td>13</td>
<td>Splunk</td>
<td>Search engine</td>
<td>67.27</td>
<td>+3.27</td>
<td>+11.24</td>
</tr>
<tr>
<td>14</td>
<td>Solr</td>
<td>Search engine</td>
<td>63.87</td>
<td>-0.50</td>
<td>-3.81</td>
</tr>
<tr>
<td>15</td>
<td>SAP Adaptive Server</td>
<td>Relational DBMS</td>
<td>63.49</td>
<td>-1.98</td>
<td>-8.25</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
<td>----------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>1.</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Oracle +</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>2.</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>MySQL +</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>3.</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>Microsoft SQL Server +</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>4.</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>PostgreSQL +</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>5.</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>MongoDB +</td>
<td>Document store</td>
</tr>
<tr>
<td>6.</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>DB2 +</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>7.</td>
<td>7</td>
<td>8</td>
<td>7</td>
<td>Microsoft Access</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>8.</td>
<td>9</td>
<td>10</td>
<td>9</td>
<td>Redis +</td>
<td>Key-value store</td>
</tr>
<tr>
<td>9.</td>
<td>10</td>
<td>11</td>
<td>10</td>
<td>Elasticsearch +</td>
<td>Search engine</td>
</tr>
<tr>
<td>10.</td>
<td>8</td>
<td>7</td>
<td>8</td>
<td>Cassandra +</td>
<td>Wide column store</td>
</tr>
<tr>
<td>11.</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>SQLite +</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>12.</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>Teradata</td>
<td>Relational DBMS</td>
</tr>
<tr>
<td>13.</td>
<td>15</td>
<td>16</td>
<td>13</td>
<td>Splunk</td>
<td>Search engine</td>
</tr>
<tr>
<td>14.</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>Solr</td>
<td>Search engine</td>
</tr>
<tr>
<td>15.</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>SAP Adaptive Server +</td>
<td>Relational DBMS</td>
</tr>
</tbody>
</table>

341 systems in ranking, February 2018
Hi, this is your son's school. We're having some computer trouble.

Oh, dear - did he break something? In a way-

Did you really name your son Robert? Drop table students;--?

Oh, yes. Little Bobby Tables, we call him.

Well, we've lost this year's student records. I hope you're happy.

And I hope you've learned to sanitize your database inputs.
Best argument for NoSQL: You can't have SQL injection attacks if you don't have SQL.
MongoDB IPO? Now you can lose your data AND your money!

2:49 AM - 22 Sep 2017

18 Retweets  15 Likes
Injections
def self.search(query)
  Person.all('$where' => "function() {
    return this.diaspora_handle.match(/#{query}/i) ||
    this.profile.first_name.match(/#{query}/i) ||
    this.profile.last_name.match(/#{query}/i);
  }")
end
$where

db.eval()

db.runCommand( { mapReduce:

  db.collection.group()
Solution JS Evaluation

DEACTIVATE: --noscripting OR security.javascriptEnabled: false

ESCAPE: CodeWScope
Saarbrücker Cybersicherheits-Studenten entdecken bis zu 40.000 ungesicherte Datenbanken im Internet

– http://www.uni-saarland.de/nc/aktuelles/artikel/nr/12173.html, Feb 2015
Massive ransomware attack takes out 27,000 MongoDB servers

Bound to all interfaces by default?
MongoDB 3.6 comes hardened against database ransomware by default

by MATTHEW HUGHES — 28 days ago in SECURITY
Authentication enabled by default?
Authentication & Authorization
Enable auth=true
<3.0
MONGODB CHALLENGE RESPONSE
(MONGODB-CR)
IETF RFC 5802 (SCRAM-SHA-1) \( \geq 3.0 \)
SCRAM-SHA-1

CONFIGURABLE iterationCount

SALT PER USER INSTEAD OF SERVER

SHA-1 INSTEAD OF MD5

SERVER AUTHENTICATES AGAINST THE CLIENT AS WELL
Predefined Roles

read/readAnyDatabase
readWrite/readWriteAnyDatabase
dbAdmin/dbAdminAnyDatabase
userAdmin/userAdminAnyDatabase
dbOwner

BACKUP, RESTORE, CLUSTER MANAGEMENT,...
\[ \geq 3.0 \]

SSL INCLUDED

(ALMOST) EVERYWHERE
Bound to all interfaces by default?
Protected Mode
>=3.2.0

ANSWER LOCAL QUERIES
RESPOND WITH AN ERROR FOR REMOTE
Authentication & Authorization
a tiny layer of authentication

– http://redis.io/topics/security
AUTH <password> COMMAND

PLAIN-TEXT PASSWORD IN Redis.conf

NO (BUILT-IN) SSL OR RATE LIMITS
Hiding Commands
SET IN `REDIS.CONF`

RESET AFTER RESTART
rename-command CONFIG mysecretconfigname
rename-command CONFIG ""
PS: Don't Pass in Random Lua Scripts
Bound to all interfaces by default?
Broadcasting on the local subnet?
Running as root?
Cockroaches claims that disappear for a while when proved wrong, but just keep on coming back.
Scripting
ELASTICSEARCH

HTTPS://WWW.ELASTIC.CO/COMMUNITY/SECURITY

CVE-2014-3120 (6.8): Dynamic scripting
CVE-2014-6439 (4.3): CORS misconfiguration
CVE-2015-1427 (6.8): Groovy sandbox escape
CVE-2015-3337 (4.3): Directory traversal
CVE-2015-4165 (3.3): File modifications
CVE-2015-5377 (5.1): RCE related to Groovy
CVE-2015-5531 (5.0): Directory traversal
CVE-2014-3120 (6.8): Dynamic scripting
CVE-2014-6439 (4.3): CORS misconfiguration
CVE-2015-1427 (6.8): Groovy sandbox escape
CVE-2015-3337 (4.3): Directory traversal
CVE-2015-4165 (3.3): File modifications
CVE-2015-5377 (5.1): RCE related to Groovy
CVE-2015-5531 (5.0): Directory traversal
Painless
HIRED DEVELOPER

1 YEAR DEVELOPMENT
Why build a brand new language when there are already so many to choose from?

– https://www.elastic.co/blog/painless-a-new-scripting-language
Goal
SECURE & PERFORMANT
POST posts/doc/1/_update
{
    "script": {
        "lang": "painless",
        "source": "if(ctx._source.details.containsKey("plus_ones")) {
            ctx._source.details.plus_ones++;
        } else {
            ctx._source.details.plus_ones = 1;
        }"
    }
}
Painless DEFAULT

GROOVY, PYTHON, JAVASCRIPT DEPRECATED
Authentication & Authorization
<table>
<thead>
<tr>
<th>Index</th>
<th>Status</th>
<th>Version</th>
<th>Docs</th>
<th>Bytes</th>
<th>Size</th>
<th>Docstore Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>yellow open goal12</td>
<td>5</td>
<td>1</td>
<td>9397</td>
<td>0</td>
<td>27mb</td>
<td>27mb</td>
</tr>
<tr>
<td>yellow open please_read</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4.9kb</td>
<td>4.9kb</td>
</tr>
<tr>
<td>yellow open un-webhose</td>
<td>5</td>
<td>1</td>
<td>2294</td>
<td>1</td>
<td>25.4mb</td>
<td>25.4mb</td>
</tr>
<tr>
<td>yellow open goal11</td>
<td>5</td>
<td>1</td>
<td>4828</td>
<td>0</td>
<td>13.3mb</td>
<td>13.3mb</td>
</tr>
</tbody>
</table>
{
  "took": 1,
  "timed_out": false,
  "_shards": {
    "total": 5,
    "successful": 5,
    "failed": 0
  },
  "hits": {
    "total": 1,
    "max_score": 1.0,
    "hits": [{
      "_index": "please_read",
      "_type": "info",
      "_id": "AVm3qmXeus_FduwRD54v",
      "_score": 1.0,
      "_source": {
        "Info": "Your DB is Backed up at our servers, to restore send 0.5 BTC to the Bitcoin Address then send an email with your server ip",
        "Bitcoin Address": "12JNfaS2Gzic2vqzGMvDEo38MQSX1kDQrx",
        "Email": "elasticsearch@mail2tor.com"
      }
    }]
  }
}
1 Bitcoin equals
8588.10 US Dollar
On 03 Feb 14:12, reports@reports.cert-bund.de wrote:

Dear Sir or Madam,

Elasticsearch is a popular search engine based on Apache Lucene, often used with web applications.

If an Elasticsearch server is openly accessible from the Internet and not protected by any forms of authentification, anyone who can connect to the server has unrestricted access to the data stored with it. This allows attackers to modify or delete any data or potentially steal sensitive information. In addition, prior to versions 1.2.x an attacker can use dynamic scripting to perform arbitrary code execution on the machine that Elasticsearch is hosted on.

Affected systems on your network:

Format: ASN | IP | Timestamp (UTC) | Elasticsearch version | Instance name
24940 | 10.10.16.176 | 2018-02-02 04:14:47 | 6.2.0 | docker-test-node-1
Conclusion
Injections Are Still a Thing
Enable Security by Default
Be Creative — Or Not
Custom Scripting Can Make Sense
Security Takes Time
Thanks!

Questions?

Philipp Krenn

@xeraa