ITPro with deep vertical Knowledge

RECENT

PRACTICAL SQL SERVER

SQL Server Database Corruption, Part IV: CHECKSUM Page Verification

overachiever | Feb 21, 2012

In previous posts within this series, we've already looked at how you can't really prevent corruption. Instead, in order to be able to better deal with corruption, you need to be able to detect it early. To that end, there are actually a number of different ways to enable early (or early-ish) detection of corruption when it happens. And, in this post, we'll look at the use of CHECKSUM Page Verification as the first of these methods.

Enabling CHECKSUM for Page Verification

When configured correctly, SQL Server can instantly spot when data that it is pulling off of disks was saved improperly – or corrupted. To enable this functionality, you just need to ensure that desired databases are configured to use the CHECKSUM option for page verification – which you can set on SQL Server 2005 and above.

To do this, simply query your server as follows, and review the names of all databases returned – as they are not configured for CHECKSUM verification:

```
USE master
GO
```

```
GO

SELECT NAME
        ,page_verify_option_desc
FROM master .sys.databases
WHERE page_verify_option_desc != 'CHECKSUM'
GO
```

Then, to enable (or toggle) these database to use CHECKSUM verification, execute the following statement per database that you wish to ‘convert’ to using CHECKSUM verification:

```
ALTER DATABASE <dbnameHere>

SET PAGE_VERIFY CHECKSUM
GO
```

Obviously, if you’ve got a lot of databases that need to be ‘toggled’, you can wire up a simple cursor, or use a poor man’s script like the following:

```
-- toggle to text output: CTRL + T SET NOCOUNT ON DECLARE @linefeed CHAR(2) SET
```

SQLKeyword">Which you can then execute – and then copy/paste the output from that query into another (or the same) query window to execute the results – as this will give you a set of ALTER statements per database as needed.

CHECKSUM – Under the Covers Once PAGE_VERIFICATION is set to CHECKSUM, SQL Server will transition to a new

> *CHECKSUM Calculates a checksum over the contents of the whole page and stores the value in the page header when a page is written to disk. When the page is read from disk, the checksum is recomputed and compared to the checksum value stored in the page header. If the values do not match, error message 824 (indicating a checksum failure) is reported to both the SQL Server error log and the Windows event log. A checksum failure indicates an I/O path problem. To determine the root cause requires investigation of the hardware, firmware drivers, BIOS, filter drivers (such as virus software), and other I/O path components.*

Of course, WHEN you switch a database over to using CHECKSUM there is NOT some magical process or operation that goes through and ‘writes’ CHECKSUMs into your EXISTING pages. If

there were, toggling this option could obviously cause some ugly problems. But, instead, since this is effectively a 'meta-data' change that instructs SQL Server to start using a new behavior (i.e., CHECKSUM functionality for writes and reads of previously CHECKSUM'd pages), you can safely toggle this change at pretty much any time without fear of bogging down your systems.

Of course, since this, in turn, means that you may have gobs of existing/older data that's been laying around without CHECKSUM configured, that data (or the data on those pages) will NOT end up getting CHECKSUM values until that data is finally pulled into SQL Server and then re-written. Consequently, if you want to 'force' CHECKSUMs into your pages, you'll need to do full-blown index rebuilds or other modifications that force all data to be pulled in and then rewritten. Happily, though, CHECKSUM is already on by default in new SQL Server 2005 and beyond databases. As such, the worries/concerns listed in this post about 'converting' a database to use CHECKSUM verification only apply to databases that were intentionally set to use a PAGE_VERIFICATION option other than CHECKSUM (which is possible but makes no sense) or for SQL Server2000 and below databases that have been migrated up to SQL Server 2005 and above – because moving older databases to new hosts/servers does NOT result in any implicit changes to PAGE_VERIFICATION settings.

The Benefits of using CHECKSUM for PAGE_VERIFICATION

As Books Online states, with CHECKSUM verification in place, SQL Server will raise error message 824 (checksum failure) whenever it now detects CHECKSUM problems. Granted, that doesn't mean that you'll catch corruption immediately as it happens (since CHECKSUMs are re-calculated for this error when data is read back in – instead of when it is written as such an operation would have enormous IO consequences) – but you will be notified of it as soon as it happens. Provided, of course, that you've got some sort of mechanism in place to alert you to instances where error message 824 is raised – which we'll address in our next post.

Part V: Storage Problem Alerts

TAGS: MICROSOFT SQL SERVER

1 COMMENT

```
SELECT STRING_AGG(CHAR(n), '')
  WITHIN GROUP (ORDER BY CHAR(n) COLLATE Latin1_General_CS_
FROM dbo.GetNums(0, 255)
WHERE CHAR(n) COLLATE Latin1_General_CS_AS LIKE '[A-Z]';


SELECT STRING_AGG(CHAR(n), '')
  WITHIN GROUP (ORDER BY CHAR(n) COLLATE Latin1_General_BIN
FROM dbo.GetNums(0, 255)
WHERE CHAR(n) COLLATE Latin1_General_BIN LIKE '[A-Z]';
```

BUSINESS INTELLIGENCE > MICROSOFT SQL SERVER

The Challenge Is on: Maintain a Custom Letter-Based Sequence

If you need to implement a custom sequence solution, and you want it to perform as well as possible, you need to ask yourself which guarantees the solution needs to provide versus which it doesn't.

Itzik Ben-Gan | Apr 01, 2018

Recently I delivered an advanced T-SQL class in Europe, and one of my students, Nicolas Barreau of Avanade France SAS, presented a nice little puzzle. The task wasn't very complex, but it was interesting and fun to work on, and I hope you will enjoy working on it, too.

The Challenge

The challenge Nicola presented was to maintain a custom, letter-based, cycling, gap-allowing, sequence, with values in the form LLL, where L is an alphabet letter in the range A through Z (26

symbols). Nicola's company uses the sequence value as a match flag for settlement, for instance, between payment and invoice. The first value produced should be AAA, and it should advance as if the letters were digits in base 26, like so:

AAA

AAB

…

AAY

READ MORE

TAGS: SOFTWARE DEVELOPMENT

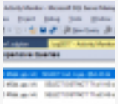
0 COMMENTS

RELATED

The Challenge Is on: Multi-Way Number Partitioning with T-SQL and SQL CLR
FEB 21, 2018

SQL Server: Avoiding a Sort with Descending Order
JAN 19, 2018

SQL Server: Avoiding a Sort with Merge Join Concatenation
DEC 18, 2017



T-SQL Puzzle Challenge: Grouping Connected Items
NOV 27, 2017

Sign up for the ITPro Update newsletter.

Email address United States SIGN UP ▸

SECURITY > ENDPOINT SECURITY

Apple Is Ready for the Tech Backlash

The only real guarantee that companies won't go overboard in invading customers' privacy is that they have large revenue streams which make it an unnecessary risk.

Bloomberg | Mar 30, 2018

(Bloomberg View) --It's easy to understand Apple CEO Tim Cook's somewhat self-righteous comments on the Facebook-Cambridge Analytica scandal: His company has never emphasized customer data monetization, and privacy has been one of its persistent selling points. Apple still collects our data — and reserves the right to share it — but the company has a much better track record than newer tech titans.

"The truth is, we could make a ton of money if we monetized our customer — if our customer was our product," Cook said on Wednesday. "We've elected not to do that." Asked what he'd do if he were in Facebook CEO Mark Zuckerberg's shoes, he replied, "I wouldn't be in this situation."

In reality, Apple collects more information about its customers than Facebook because it offers more products and services. It knows everything from an iPhone's location to its owner's taste in movies and music. It's all in the company's privacy statement, including the frank admission that Apple will share the data with "strategic partners that work with Apple to provide products and services, or that help Apple market to customers" and with law enforcement. Apple also lets applications that run on its platform (including Facebook) hoover up data. And it does have a small ad platform that allows targeted advertising.

Apple's closest equivalent in terms of data collection, sharing and "pass-through" to app developers is Google, which offers roughly the same array of services (plus search) and also owns mobile and desktop operating systems. The difference is that Apple has imposed some voluntary restrictions on itself: For example, it anonymizes location data (unless you're using the "Find My iPhone" feature) and generally employs "differential privacy" — a cryptography-based practice of obtaining usage and preference data without linking it to specific users. Google and Microsoft also use that to some degree, and a co-inventor of differential privacy, Cynthia Dwork, has even worked for Microsoft Research, but Apple was the first to market the technique as an advantage for its customers.

Cook clearly thinks of these self-restrictions as a good way of staving off external regulation. On Wednesday, he scolded Facebook for not being as far-sighted. "I think the best regulation is no regulation, is self-regulation," he said. "However, I think we're beyond that here."

As a user, however, I wouldn't put much trust in any company's ability to regulate itself. Cook has been wary of monetizing Apple's user base, but he won't be CEO forever. And people do change their mind, especially when it comes to picking up money that's there for the taking. Regulation — such as the EU's General Data Protection regulation, launching in May — is a more reliable way to ensure a level playing field. That's why Google, Apple and Microsoft all have good, convenient privacy controls which allow the user to turn off various kinds of data collection, erase data that companies already have and opt out of targeted advertising. Facebook, too, promises to put such controls in place soon.