I'll never tell what the data REALLY is.

Blitz Result: Warnings About Encryption (TDE or Backups) and Certificates

SQL Server 2008 introduced Transparent Data Encryption – a set-it-and-forget-it way to keep your databases protected on disk. If someone steals your backup tapes or your hard drives, they'll have a tougher time getting access to the data. Just set it up and you're done.

SQL Server 2014 introduced backup encryption as well – create a cert, specify it when backing up your databases, and your backups are encrypted.

However, if you don't back up your encryption certificate and password, you'll never be able to restore those databases!

This part of our SQL Server sp_Blitz script checks sys.databases looking for databases that have been encrypted, and also checks to make sure that the certificates have been backed up recently (in the last 30 days).

You can learn much more about both TDE and the business needs behind it at the SQL Server 2008 Compliance Portal. We highly recommend the SQL Server Compliance Guide which

explains these issues in clear, easy-to-understand terms.

Can Transparent Data Encryption Impact Performance?

After implementing TDE on any user database, be aware that tempdb is permanently encrypted. Even if you remove TDE from the user database, you'll still have the encryption overhead on tempdb. This is a great reason why all testing should be done in development environments first rather than trying it in production.

To Fix the Problem (or make sure you don't have one)

Follow both steps below to make sure you can restore your data.

If you're not sure if this has been done before, do this ASAP. The thing about TDE is that if you end up in a bad spot, it protects your data **from you**.

Return to sp_Blitz or Ask Us Questions

How to Prove You're Safe with Transparent Data Encryption

Step 1: test and verify sure you can successfully restore the encrypted databases onto another server using this guide from Microsoft.

Step 2: make sure you have the certificate and password backed up in a safe place – if you store them with your regular backups, then you're still at risk of data theft. Also think about this in case of disasters. If the whole datacenter is gone, are both the backups, the certificate, and the password all available to someone so that they can restore them (and are they also still secure)?

Step 3: Think about licensing. Transparent Data Encryption is an Enterprise Edition feature. When it's on, you can't restore the database to a Standard Edition instance– which means you can't use Standard Edition for disaster recovery.

© 2017 Brent Ozar Unlimited®. All Rights Reserved. Privacy Policy – Training Agreement