SQL Server Security Basics

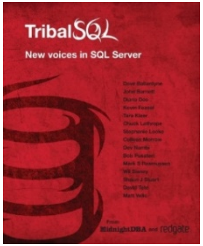
Bob Pusateri, Database Administrator,
Northwestern University

Please Support Our Sponsors

SQL Saturday is made possible with the generous support of these sponsors. You can support them by opting-in and visiting them in the sponsor area.

Microsoft
MELISSA DATA
Your Partner in Data Quality
idera
Micron
redgate
ingeniously simple
SanDisk
cisco
Profisee
pernixdata
WhereScape
DH2i
HUSH HUSH
Comunidad Windows
COZYROC
Go to the next level
PASS
serverlogic
SolidQ
Think Big. Move Fast.
SQL Soldier .com

About Me



TribalSQL

New voices in SQL Server

Dave Ballantyne
John Barnett
Diana Dee
Kevin Feasel
Tara Kizer
Chuck Lathrope
Stephanie Locke
Colleen Morrow
Dev Nambi
Bob Pusateri
Mark S Rasmussen
Wil Sisney
Shaun J Stuart
David Tate
Matt Velic

From
MidnightDBA and redgate

SSKS

www.bobpusateri.com

SQL

@SQLBob

redgate

Friend of Redgate 2015

EDW

NORTHWESTERN MEDICAL
ENTERPRISE DATA WAREHOUSE

Microsoft
CERTIFIED
Master

Why Security Basics?

Agenda

- Physical Security
- Network Security
- Instance Security
- Database Security
- Auditing

Physical Security

Physical Security

- **Everything else is pointless without it**
- Where are the servers?
- How secure are they?
- What happens if hardware gets stolen?

https://flic.kr/p/eKFTfg

https://flic.kr/p/49LQaa

Transparent Data Encryption (TDE)

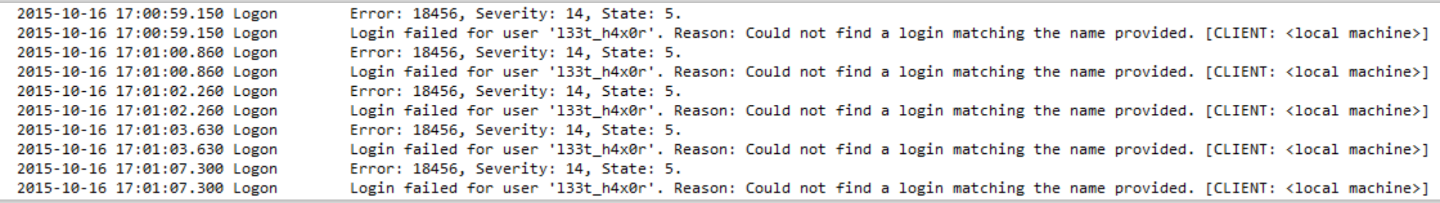
- Encrypts data when at rest (on disk)
- Backups are also encrypted
- Transparent to users
- Will increase CPU utilization
- Backup your certificates!

https://flic.kr/p/2KcaZ

Network Security

Network Security

- Is there a direct path from the internet to your DBs?
- DB attacks usually come from inside your network!
- Is network traffic monitored/logged?
- Is someone looking at those logs?



```
2015-10-16 17:00:59.150 Logon        Error: 18456, Severity: 14, State: 5.
2015-10-16 17:00:59.150 Logon        Login failed for user 'l33t_h4x0r'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]
2015-10-16 17:01:00.860 Logon        Error: 18456, Severity: 14, State: 5.
2015-10-16 17:01:00.860 Logon        Login failed for user 'l33t_h4x0r'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]
2015-10-16 17:01:02.260 Logon        Error: 18456, Severity: 14, State: 5.
2015-10-16 17:01:02.260 Logon        Login failed for user 'l33t_h4x0r'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]
2015-10-16 17:01:03.630 Logon        Error: 18456, Severity: 14, State: 5.
2015-10-16 17:01:03.630 Logon        Login failed for user 'l33t_h4x0r'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]
2015-10-16 17:01:07.300 Logon        Error: 18456, Severity: 14, State: 5.
2015-10-16 17:01:07.300 Logon        Login failed for user 'l33t_h4x0r'. Reason: Could not find a login matching the name provided. [CLIENT: <local machine>]
```

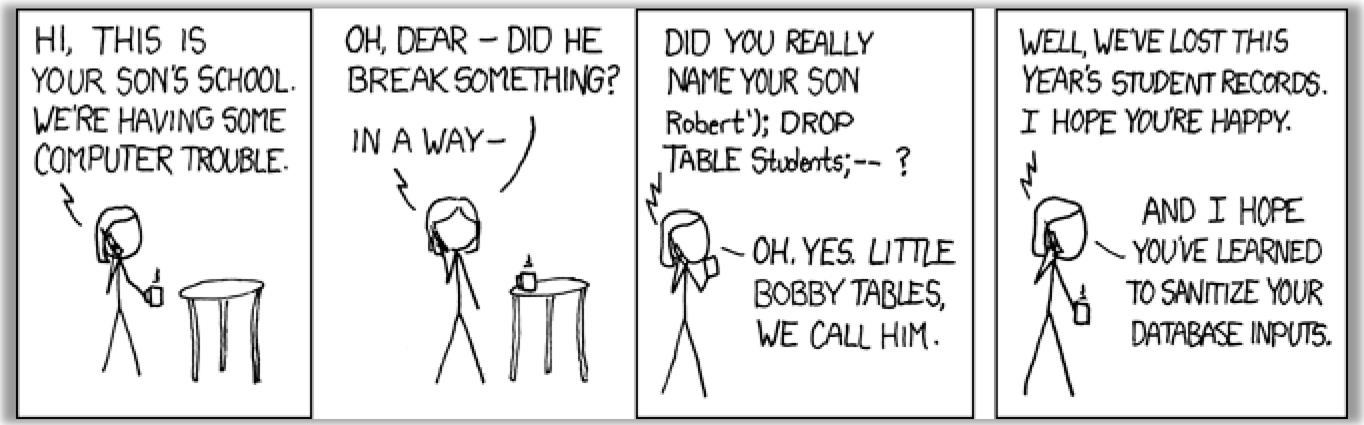
Encrypting SQL Server Connections

- Connections can be encrypted with SSL
- Protects data while travelling over the network
- Server can force connections to be encrypted
- Authentication information is always encrypted (2005+)

https://flic.kr/p/dxdmTX

SQL Injection

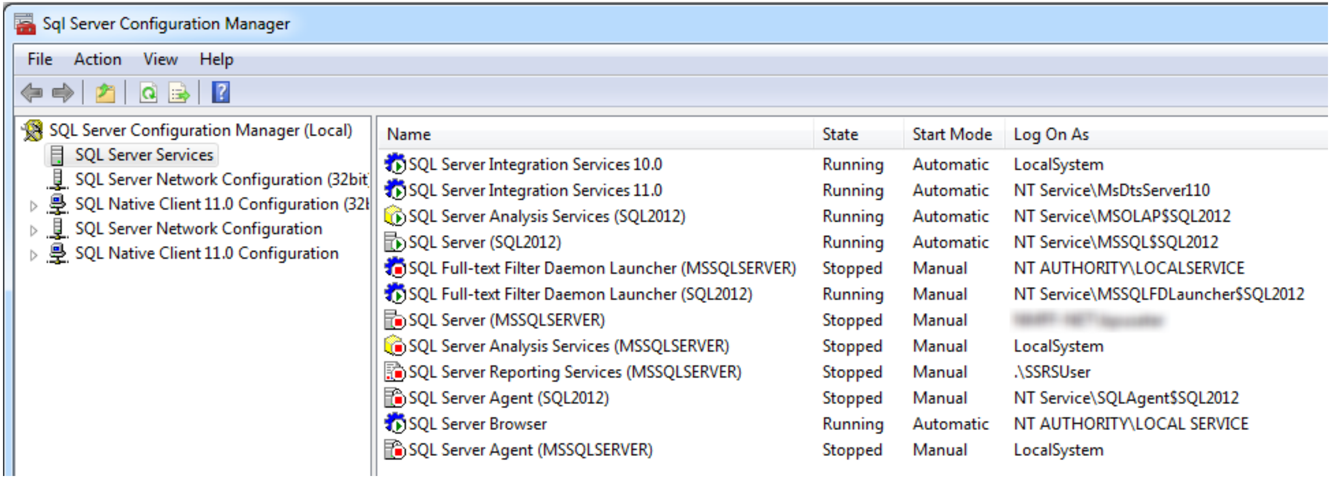
- Lock down account permissions
- Stored procedures
- Application developers also have work to do


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.

https://xkcd.com/327/

Service Accounts

- Are they also domain admins?
- Are they allowed interactive logon?
- Who has the passwords?

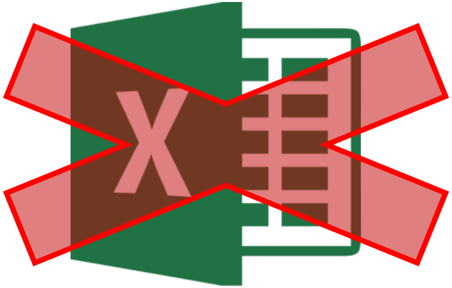


SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32l
SQL Server Network Configuration
SQL Native Client 11.0 Configuration

Name	State	Start Mode	Log On As
SQL Server Integration Services 10.0	Running	Automatic	LocalSystem
SQL Server Integration Services 11.0	Running	Automatic	NT Service\MsDtsServer110
SQL Server Analysis Services (SQL2012)	Running	Automatic	NT Service\MSOLAP$SQL2012
SQL Server (SQL2012)	Running	Automatic	NT Service\MSSQL$SQL2012
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Stopped	Manual	NT AUTHORITY\LOCALSERVICE
SQL Full-text Filter Daemon Launcher (SQL2012)	Running	Manual	NT Service\MSSQLFDLauncher$SQL2012
SQL Server (MSSQLSERVER)	Stopped	Manual	[redacted]
SQL Server Analysis Services (MSSQLSERVER)	Stopped	Manual	LocalSystem
SQL Server Reporting Services (MSSQLSERVER)	Stopped	Manual	.\SSRSUser
SQL Server Agent (SQL2012)	Stopped	Manual	NT Service\SQLAgent$SQL2012
SQL Server Browser	Running	Automatic	NT AUTHORITY\LOCAL SERVICE
SQL Server Agent (MSSQLSERVER)	Stopped	Manual	LocalSystem

Passwords

- Who has access to the passwords?
- Are they strong?
- Are they changed?
- Use a password manager!



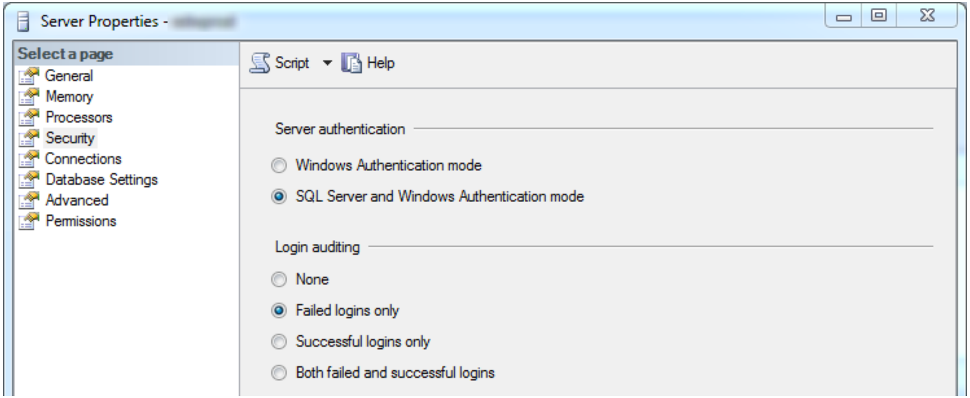
Active Directory

- Use Groups!
- Who’s being added to your groups?

Instance Security

Windows Authentication

- The ideal choice
- Get all the built-in security of AD
- Can apply policies to AD accounts
- Can use AD groups



Server authentication

○ Windows Authentication mode
● SQL Server and Windows Authentication mode

Login auditing

○ None
● Failed logins only
○ Successful logins only
○ Both failed and successful logins

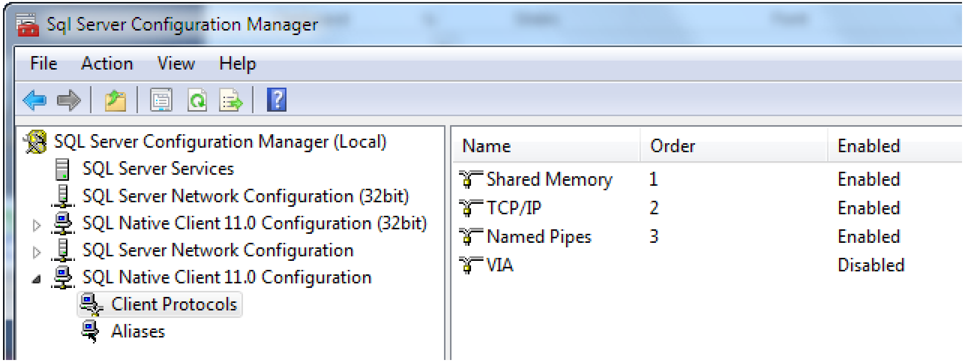
‘sa’ Account

- Can you disable it?
- Change the username?
- Create a different one?

https://flic.kr/p/dFVZx5

Connection Protocols

- Manage them in SQL Server Configuration Manager
- Disable the ones you won’t be using

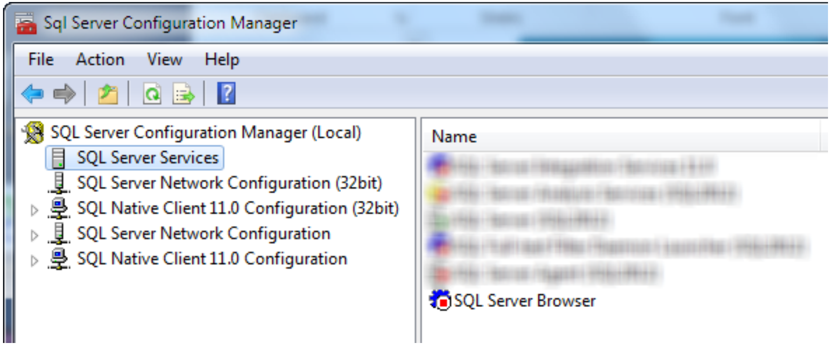


- SQL Server Configuration Manager (Local)
  - SQL Server Services
  - SQL Server Network Configuration (32bit)
  - SQL Native Client 11.0 Configuration (32bit)
  - SQL Server Network Configuration
  - SQL Native Client 11.0 Configuration
    - Client Protocols
    - Aliases

Name	Order	Enabled
Shared Memory	1	Enabled
TCP/IP	2	Enabled
Named Pipes	3	Enabled
VIA		Disabled

SQL Server Browser

- Helps "hide" your server if it's disabled
- Lowers the attack surface of your instance
- Users may need to know port numbers without it
- More difficult to connect via DAC



Sql Server Configuration Manager

SQL Server Configuration Manager (Local)
- SQL Server Services
- SQL Server Network Configuration (32bit)
- SQL Native Client 11.0 Configuration (32bit)
- SQL Server Network Configuration
- SQL Native Client 11.0 Configuration

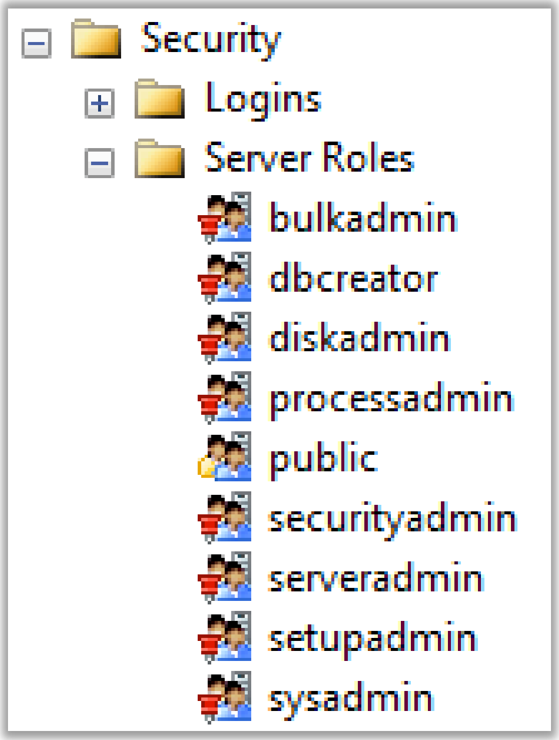
Name

[redacted]

SQL Server Browser

Fixed Server Roles

- sysadmin
- serveradmin
- securityadmin
- processadmin
- setupadmin
- bulkadmin
- diskadmin
- dbcreator
- public



Security
Logins
Server Roles
bulkadmin
dbcreator
diskadmin
processadmin
public
securityadmin
serveradmin
setupadmin
sysadmin

Securityadmin role

- Only applies to server-level permissions
- Can’t elevate its own permissions
- Can’t grant sysadmin rights to other users
- CAN create other users and grant CONTROL SERVER

User-defined Server Roles

- New in 2012
- Only applies to server-level permissions
- Pre-package your commonly-used permissions!

Database Security

Backups

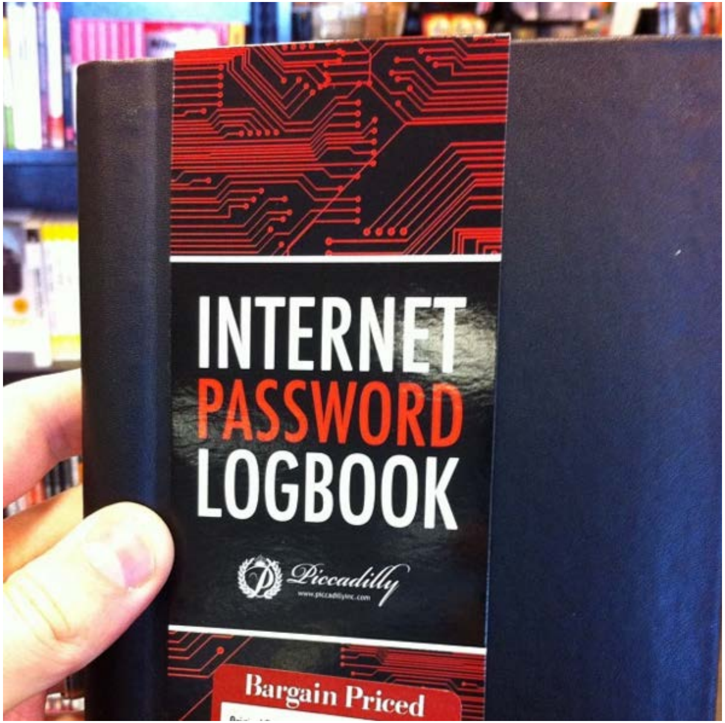
- Where are the backups stored?
- Are they being monitored?
- Who can see them?

https://flic.kr/p/2Q1fQU

Backup Passwords

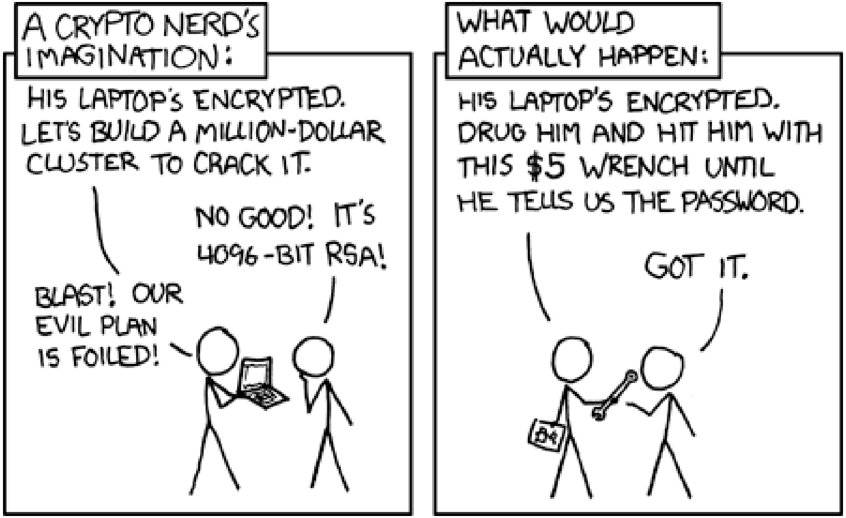
```
BACKUP DATABASE [MyTestDB]
… WITH PASSWORD = '…'
```

- Don't do this!
- Discontinued in 2012
- This is *not* encryption!



Backup Encryption

- 3rd party tools have offered this for years
- Included natively in SQL 2014
- Works in Standard Edition!


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

http://xkcd.com/538/

Backup Encryption

You Specify:

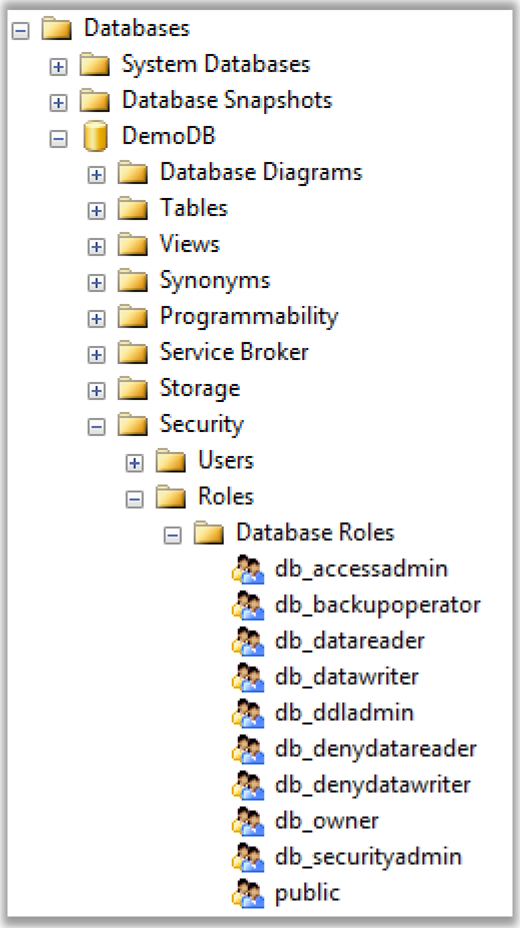
- Encryption Algorithm {AES 128, 192, 256, Triple DES}
- Encryptor {certificate, asymmetric key}
- Don’t lose your encryptor!
- Can’t be read by previous versions of SQL Server
- Can’t append to an existing backup

Backup Encryption

```
BACKUP DATABASE [MYTestDB]
TO DISK = ‘file’
WITH COMPRESSION, CHECKSUM,
ENCRYPTION (
      ALGORITHM = AES_256,
      { SERVER CERTIFICATE = certname |
        SERVER_ASYMMETRIC_KEY = keyname } );
```

Fixed Database Roles

- db_owner
- db_securityadmin
- db_accessadmin
- db_backupoperator
- db_ddladmin
- db_datawriter
- db_datareader
- db_denydatawriter
- db_denydatareader



```
⊟ Databases
    ⊞ System Databases
    ⊞ Database Snapshots
    ⊟ DemoDB
        ⊞ Database Diagrams
        ⊞ Tables
        ⊞ Views
        ⊞ Synonyms
        ⊞ Programmability
        ⊞ Service Broker
        ⊞ Storage
        ⊟ Security
            ⊞ Users
            ⊟ Roles
                ⊟ Database Roles
                      db_accessadmin
                      db_backupoperator
                      db_datareader
                      db_datawriter
                      db_ddladmin
                      db_denydatareader
                      db_denydatawriter
                      db_owner
                      db_securityadmin
                      public
```

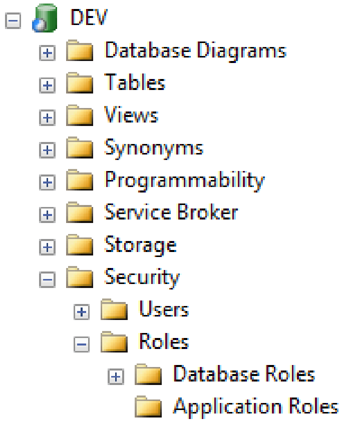
Public Database Role

- Every user in the database belongs to this role
- Rights granted to public will apply to every database user
- In the absence of other permissions, user will revert to public level

https://flic.kr/p/4RR86q/

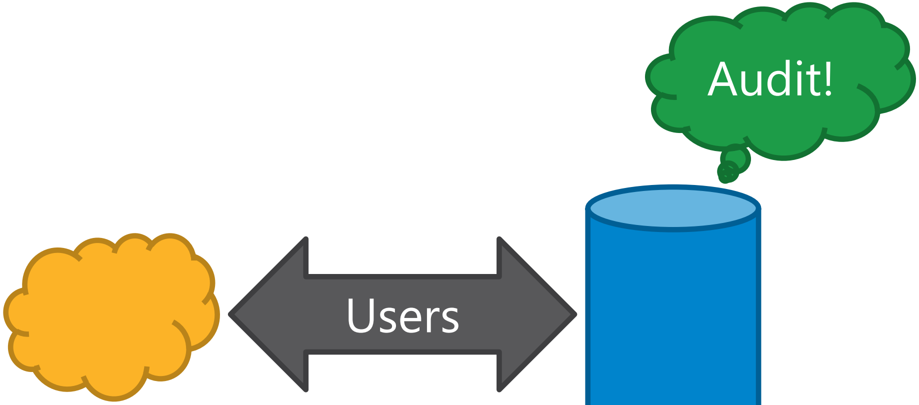
Application Roles

- Authenticate as a user without any specific rights
- Rights are granted to the application role instead
- Application activates role to obtain rights
- Application has **only** the rights of the role

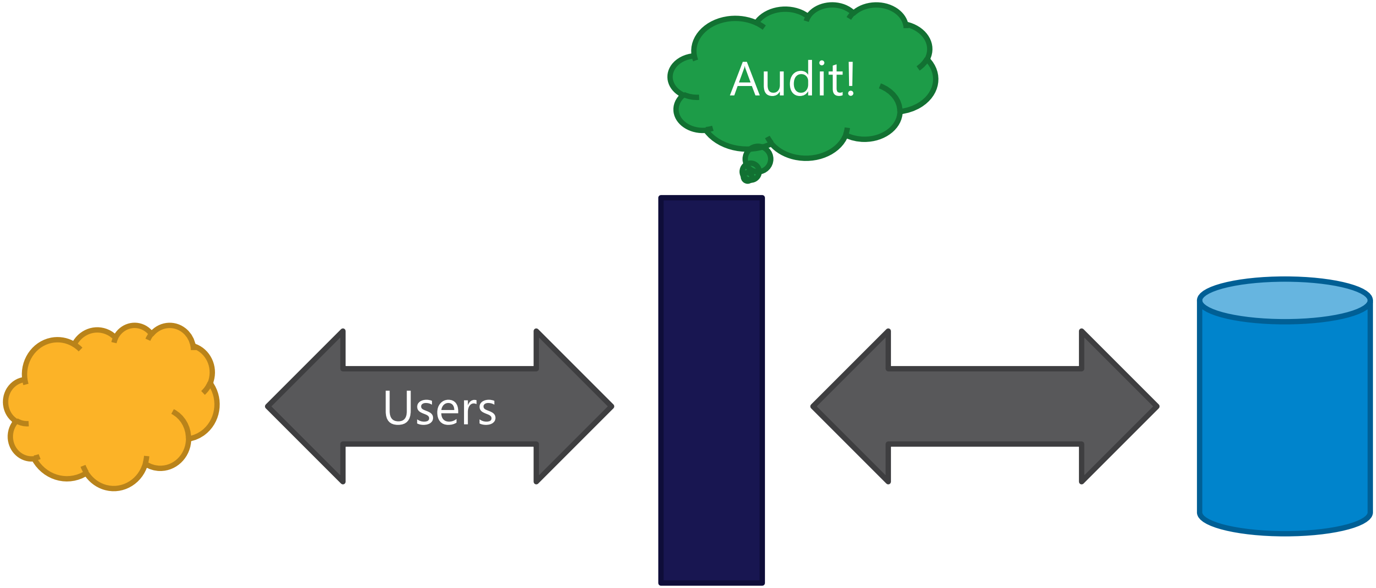


Auditing

Internal Auditing (SQL Server Audit)



External Auditing (3rd Party)



SQL Server Audit

- Introduced in 2008
- Uses Extended Events framework behind-the-scenes
- Very configurable for objects & principals
- Not configurable for data that's collected
- Decent GUI for management
- Works in Standard Edition*

*kinda

Questions?

Email: Bob@BobPusateri.com

Twitter: @SQLBob

Resources: bobpusateri.com/r/secure

I'm here to help!

Thank You!

This FREE SQL Saturday is brought to you courtesy of these sponsors, speakers and volunteers who staff this event.

Microsoft

MELISSA DATA®
Your Partner in Data Quality

idera®

Micron®

redgate
ingeniously simple

SanDisk®

cisco

Profisee®

pernixdata

WhereScape®

DH2i

HUSH HUSH

Comunidad Windows

COZYROC™
Go to the next level

PASS

serverlogic

SolidQ
Think Big. Move Fast.

SQL Soldier .com