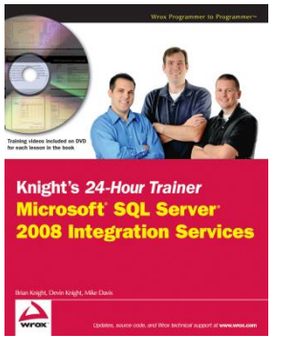
Introduction to SQL Server Security

Pragmatic Works

Pragmatic Works Company History

- Founded 2008 by MSFT MVP Brian Knight
- Focused on the MSFT SQL Server Platform
- Provides services, training and software
- MSFT/HP “go to” partner:
- Gold Certified:
  - BI
  - Data Management
  - SQL Performance
- Team led by multiple MVP’s
- Offices throughout the US with Corporate HQ in Jacksonville, FL



Microsoft GOLD CERTIFIED Partner
Business Intelligence
Data Management Solutions
SOA and Business Process
Security Solutions

Getting Started

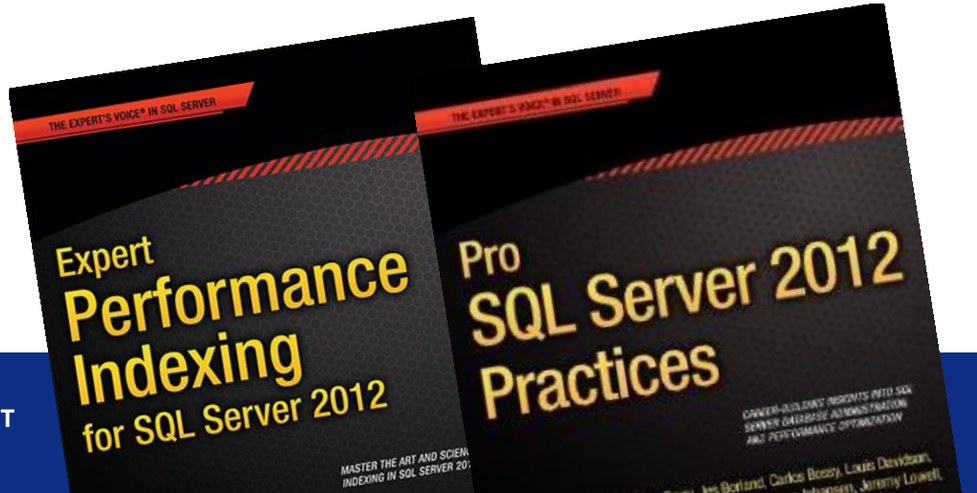
Jason Strate

e: jstrate@pragmaticworks.com

b: www.jasonstrate.com

t: StrateSQL

Microsoft CERTIFIED Master



MVP Microsoft® Most Valuable Professional

Agenda

Overview

Securing SQL Server

Accessing SQL Server

Controlling Access

Validation


Overview
Securing SQL Server
Accessing SQL Server
Controlling Access
Validation

OVERVIEW

Overview

Overview

Overview

Overview

SECURING SQL SERVER

Start With Installation

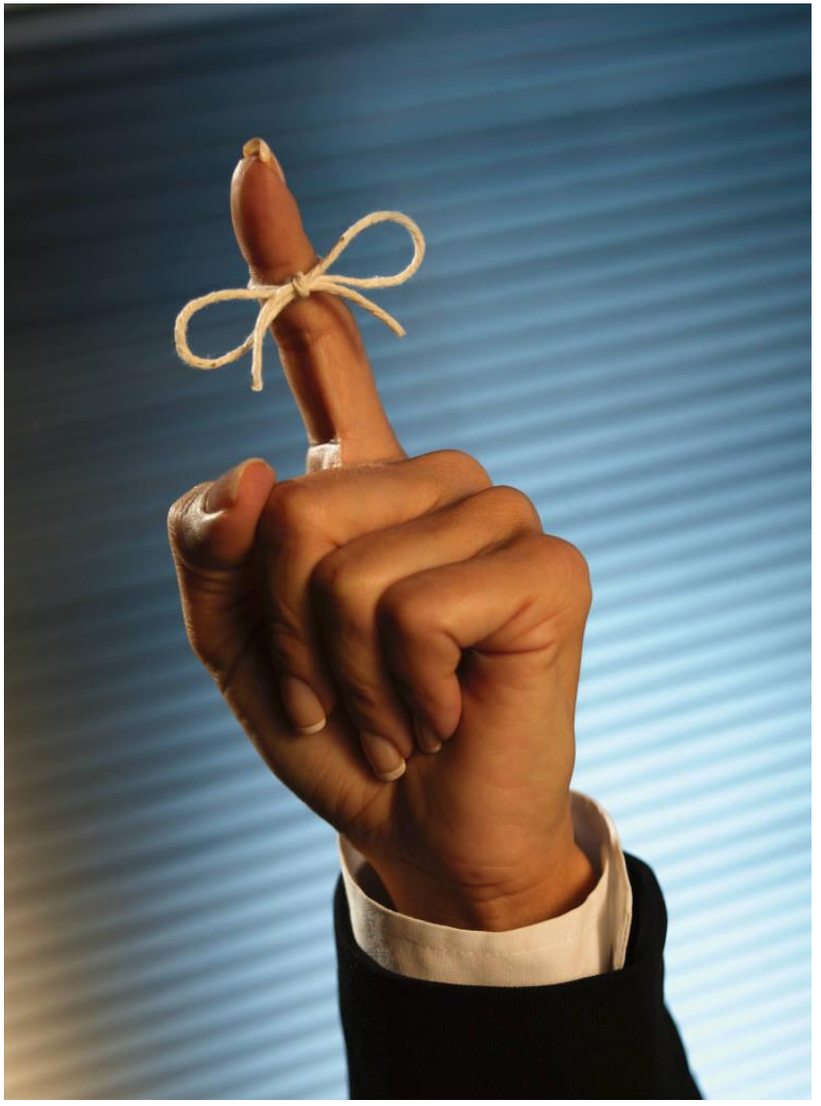
- Operating system?
- Services?
- Tools?
- Features?
- Configuration?

Service Accounts

- Virtual Service account
- Managed Service account
- Domain user
- Local user
- Network Service account
- Local System account

Security Tip

Principle of least privilege



Location, Location, Location

- Where is the server physically?
- Where is the server on the network?
- Behind the firewall?

ACCESSING SQL SERVER

Accessing the Server

- Login
  - Windows Authentication
    - Group
    - User
  - SQL Server Authentication
  - Certificate
  - Asymmetric Key

SQL Server Authentication

- Password policy
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout counter after
  - Complexity
  - Password history
- Enforce password expiration
- Change password next login

Advanced Access

Certificate

Asymmetric Key

CONTROLLING ACCESS

Security Model Basics

Securable

- Resource within SQL Server, such as a database, table, procedure, or feature.

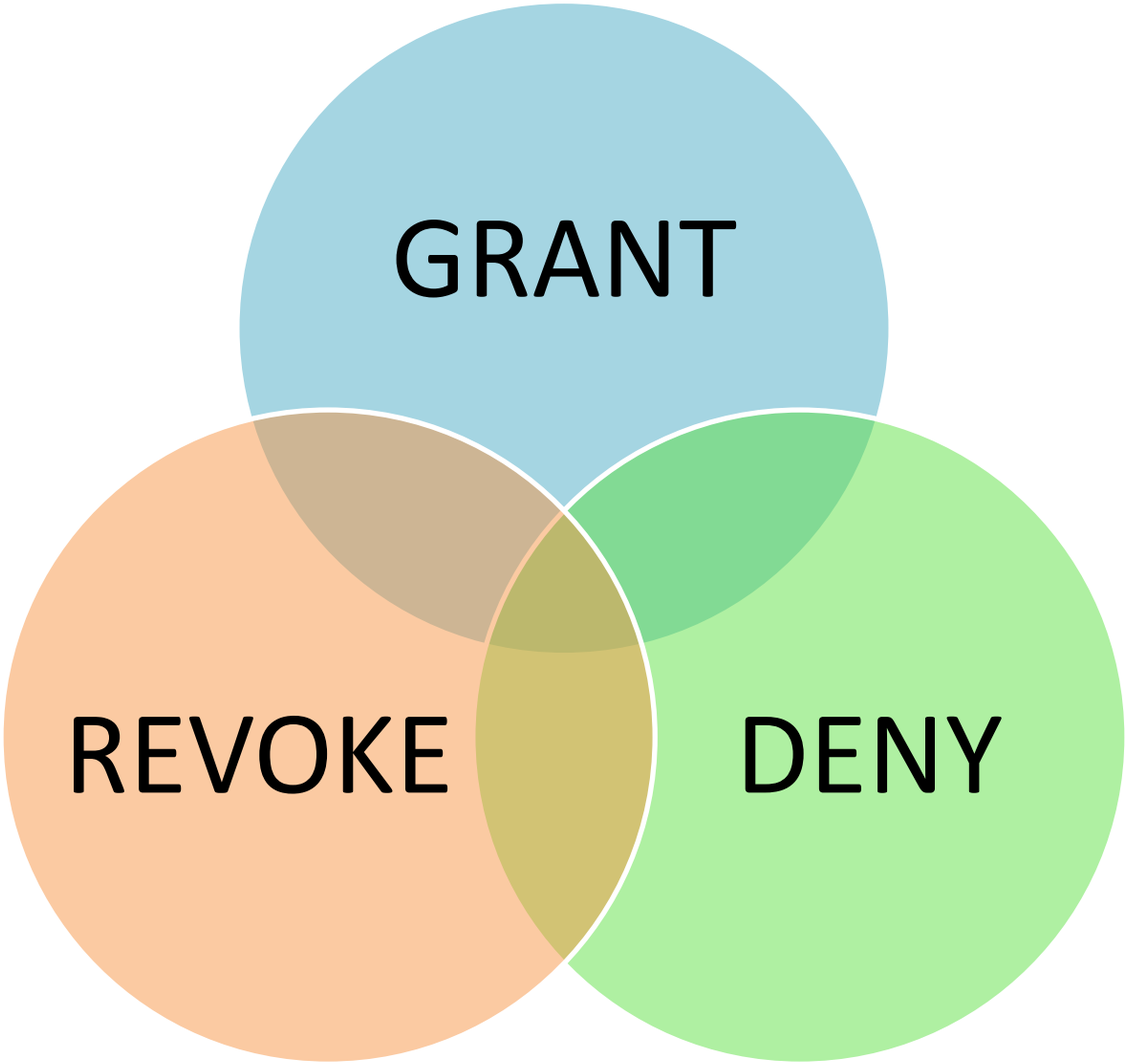
Principal

- Object to which permissions can be assigned, such as a login or certificate.

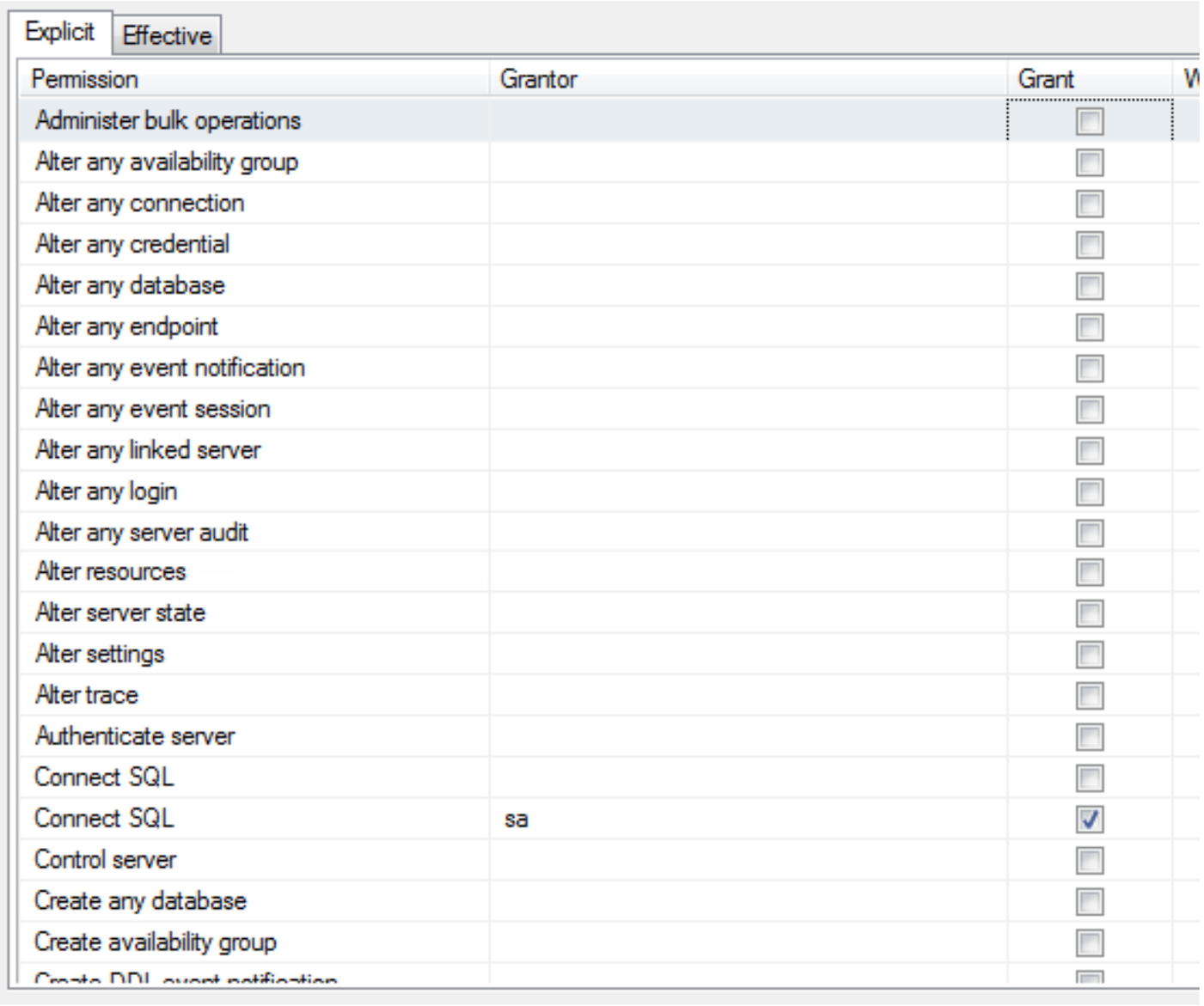
Permission

- Activity on the securable that is granted to the principal, such as read or view.

Permission Modes

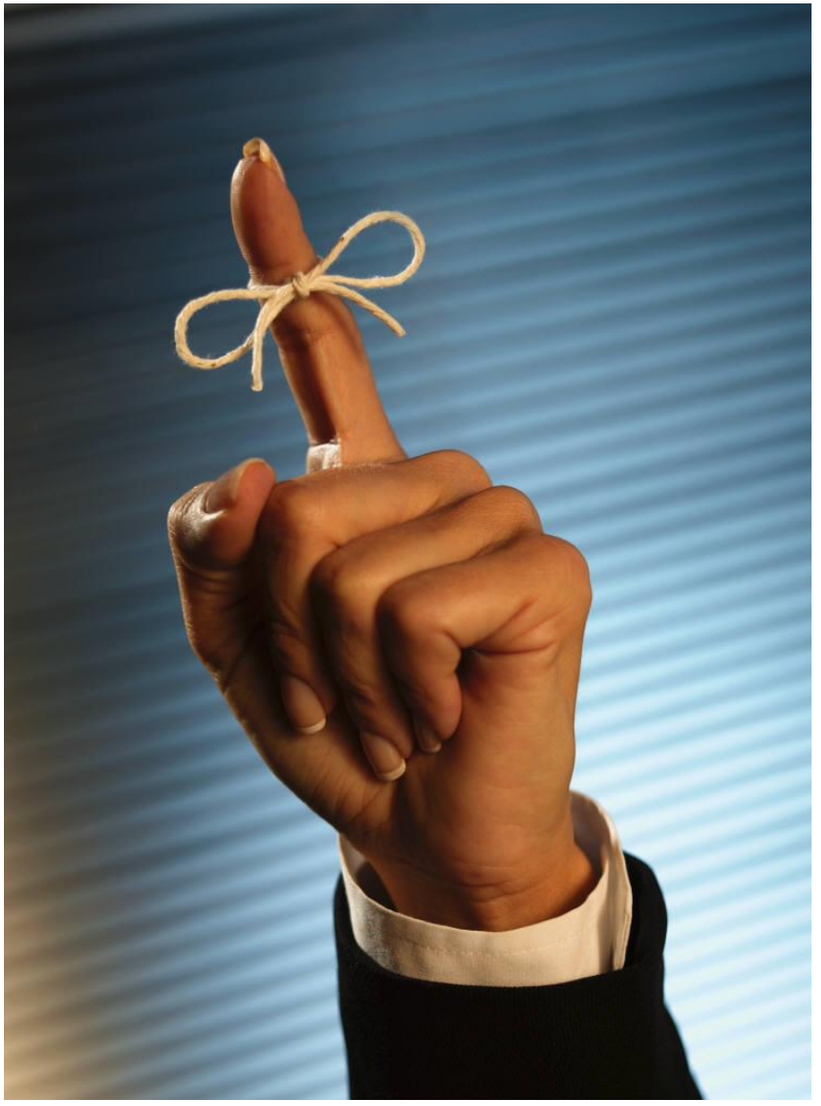


Server Securables

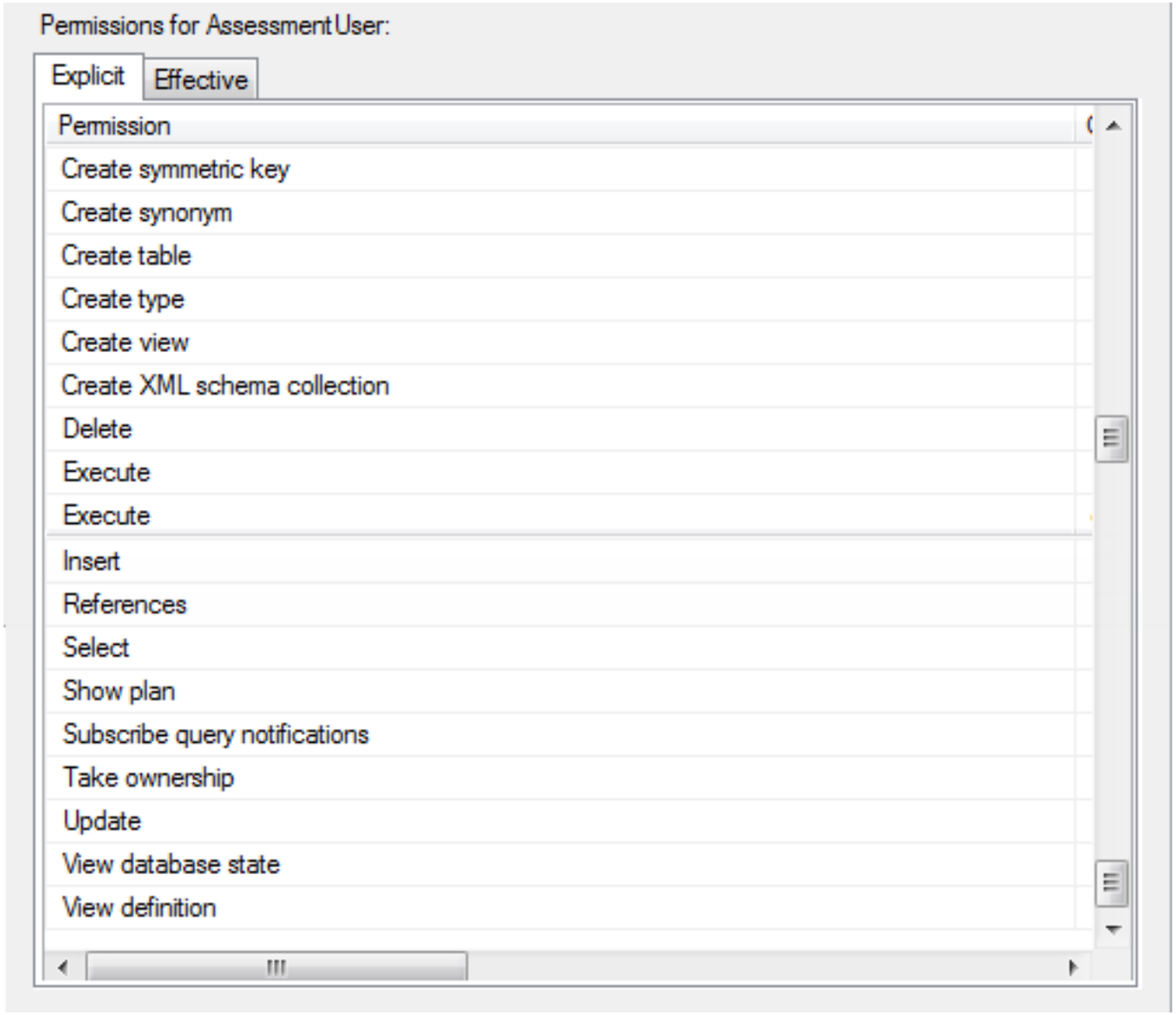


Security Tip

CONTROL SERVER is a replacement for sysadmin



Database Securables



Example 1

- GRANT VIEW SERVER STATE TO SQLCHICKEN
- GRANT CONTROL SERVER TO SQLBALLS
- GRANT SHOW PLAN TO AUNTKATHI

Example 2

- GRANT EXECUTE TO SQLCHICKEN
- DENY EXECUTE ON dbo.usp_action TO SQL CHICKEN
- GRANT SELECT ON dbo.table TO SQLBALLS
- GRANT VIEW DATABASE STATE TO AUNTKATHI

Security Roles

- Server Roles
- Custom Server Roles
- Database Roles
- Custom Database Roles

Server Roles

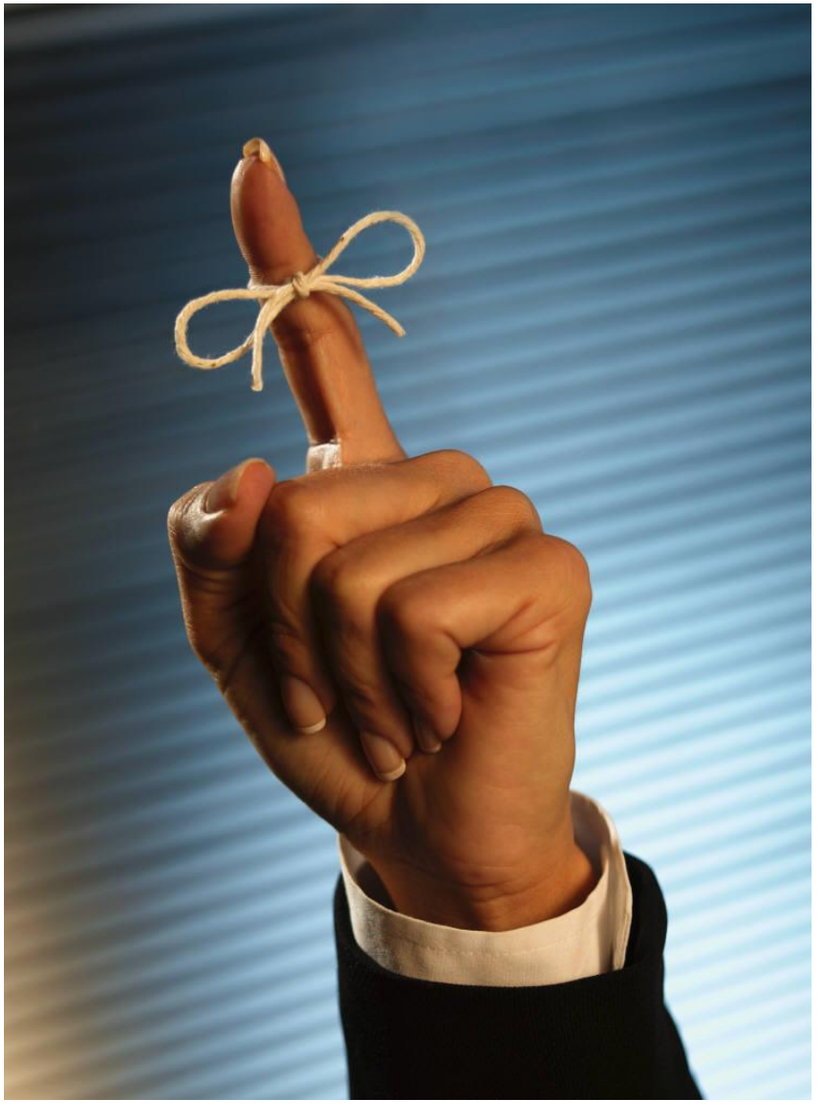
- Bulkadmin
- Dbcreator
- Diskadmin
- Processadmin
- Securityadmin
- Setupadmin
- Sysadmin

Custom Server Roles

- New for SQL Server 2012
- Create what you need
  - Junior DBA
  - Security admin
  - Monitoring

Security Tip

CONTROL SERVER is a replacement for sysadmin

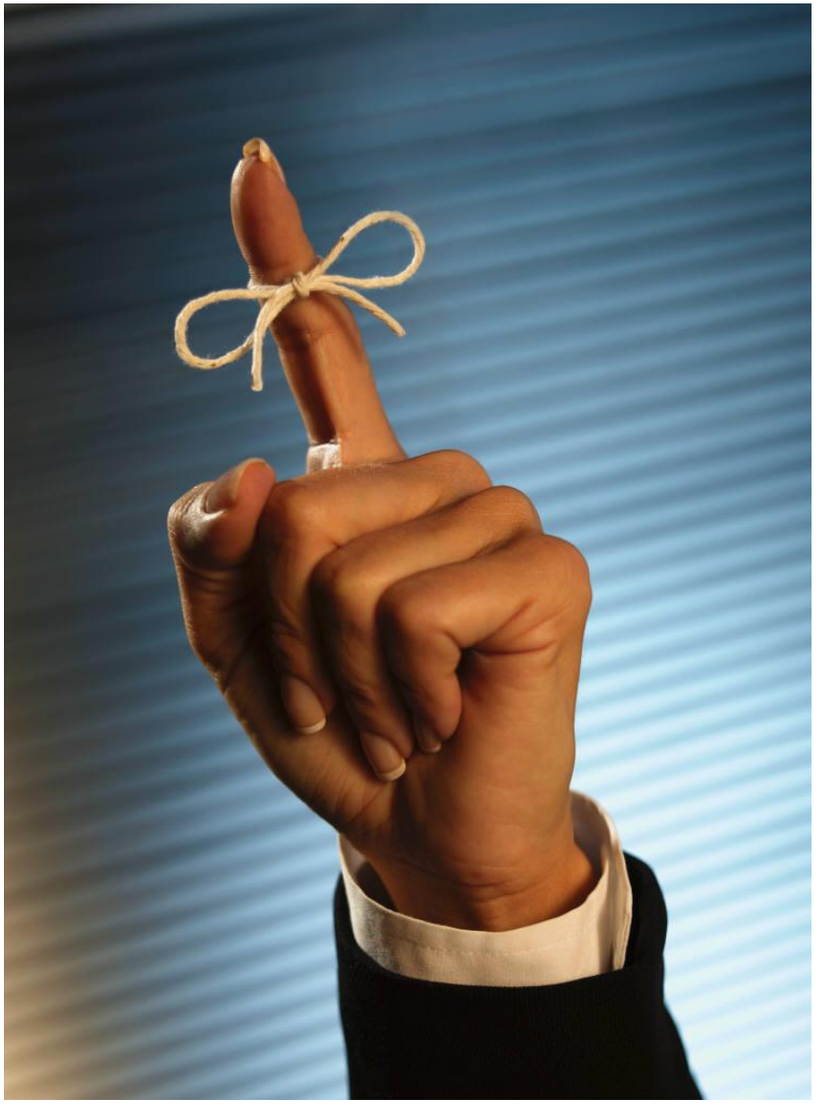


Database Roles

- Db_accessadmin
- Db_backupoperator
- Db_datareader
- Db_datawriter
- Db_ddladmin
- Db_denydatareader
- Db_denydatawriter
- Db_owner
- Db_securityadmin

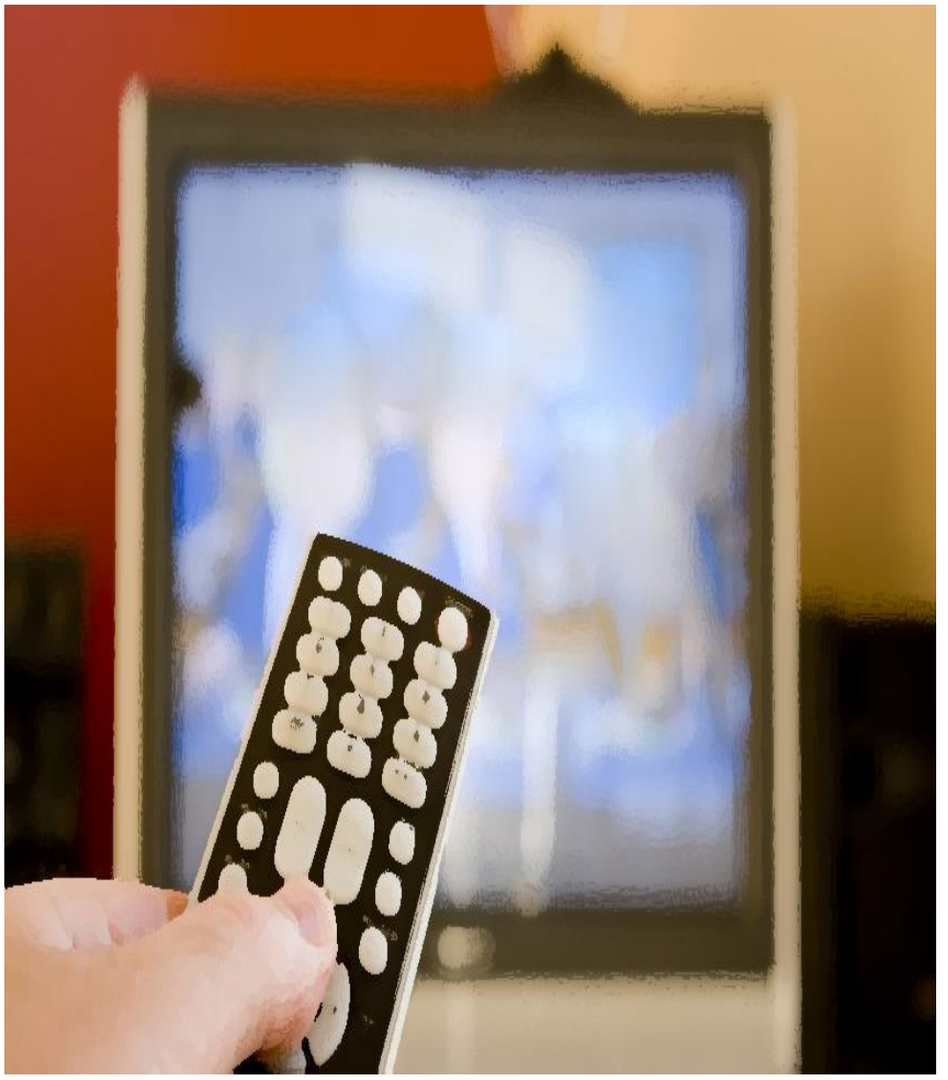
Security Tip

Beware of db_owner and RESTRICTED_USER mode



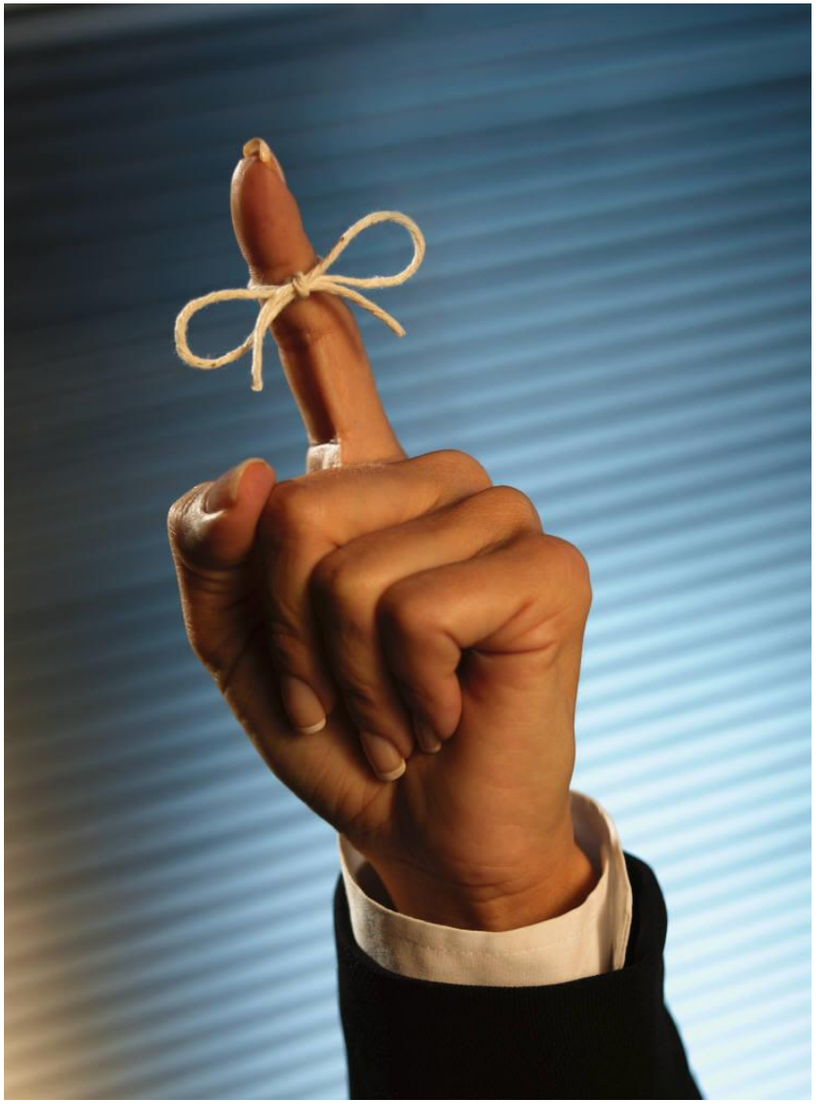
Custom Database Roles

- Been around since dirt
- Useful for
  - Setting department permissions
  - Grouping stored procedure access
  - Simplifying permission management



Security Tip

Use roles over logins for permission assignments




Overview
Securing SQL Server
Accessing SQL Server
Controlling Access
Validation

VALIDATION

Validation

- Audits
  - C2 Auditing
  - Common Criteria Control
- SQL Server Audit
- Policy Based Management

SQL Server Audit

- SQL Server 2008
  - Enterprise edition feature
- SQL Server 2012
  - Standard edition feature
  - Accessible via Extended Events

SQL Server Audit

- Server
  - Permission changes
  - DBCC events
  - Failed logins
- Database
  - DML activity
  - SELECT activity
  - Object modification

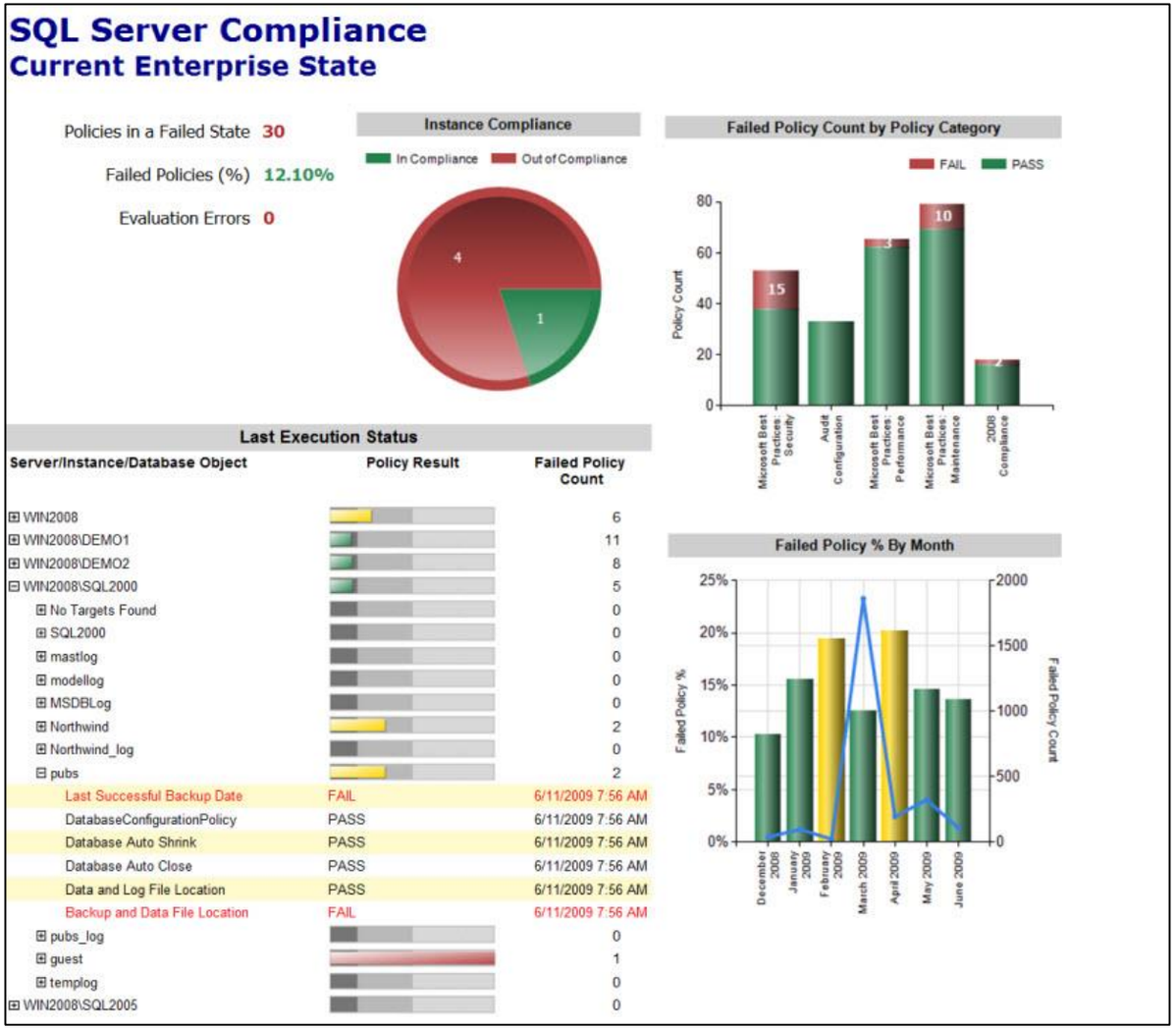
Policy Based Management

- Introduced SQL Server 2008
  - All editions
- Backwards compatibility
  - To SQL Server 2000…. Kinda
- Checks
  - DDL triggers
  - Object properties

Policy Based Management

- Add super power with…

Enterprise Policy Management Framework



Wrapping Up

Securing SQL Server

Accessing SQL Server

Controlling Access

Validation

For more **information…**

Name: Jason Strate

Email: jstrate@pragmaticworks.com

Blog: www.jasonstrate.com

Resource: jasonstrate.com/go/Security

Products

BI products to covert to a Microsoft BI platform and simplify development on the platform.

Services

Speed development through training, and rapid development services from Pragmatic Works.

Foundation

Helping those who do not have the means to get into information technology achieve their dreams.