Microsoft SQL Server Security and Auditing

Clay Risenhoover
ISACA North Texas
April 14, 2016
http://tinyurl.com/ISACAClay

RCI

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Goals

- Understand new and important security features
- Demonstrate use of some of them
- Discuss security ramifications of all of them

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Assumptions

The ideal student:

- Not a DBA
- Not freaked out by SQL
- Understand security/assurance
- Understand basic database concepts (like ACID)

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

ACID

Atomicity (all or nothing transactions)
Consistency (transactions leave DB in stable state)
Isolation (concurrency)
Durability (transactions don’t go away once committed)

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Model

Server hardening
Confidentiality
Integrity
Availability

RCI

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Server Hardening

Patch level
Authentication modes

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Patching

Determine running version

Sqlserverversions.blogspot.com

```
select @@version
select SERVERPROPERTY('productversion')
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Authentication

Determine authentication mode

```
SELECT
SERVERPROPERTY('IsIntegratedSecurityOnly')

SELECT CASE
  SERVERPROPERTY('IsIntegratedSecurityOnly')
  WHEN 1 THEN 'Windows Authentication'
  WHEN 0 THEN ‘Mixed Mode Authentication'
END as [Authentication Mode]
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Confidentiality

Encryption
Row-level security
User permissions

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Encryption Options

Transparent data encryption (TDE)
Encrypted Backups
Always encrypted

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

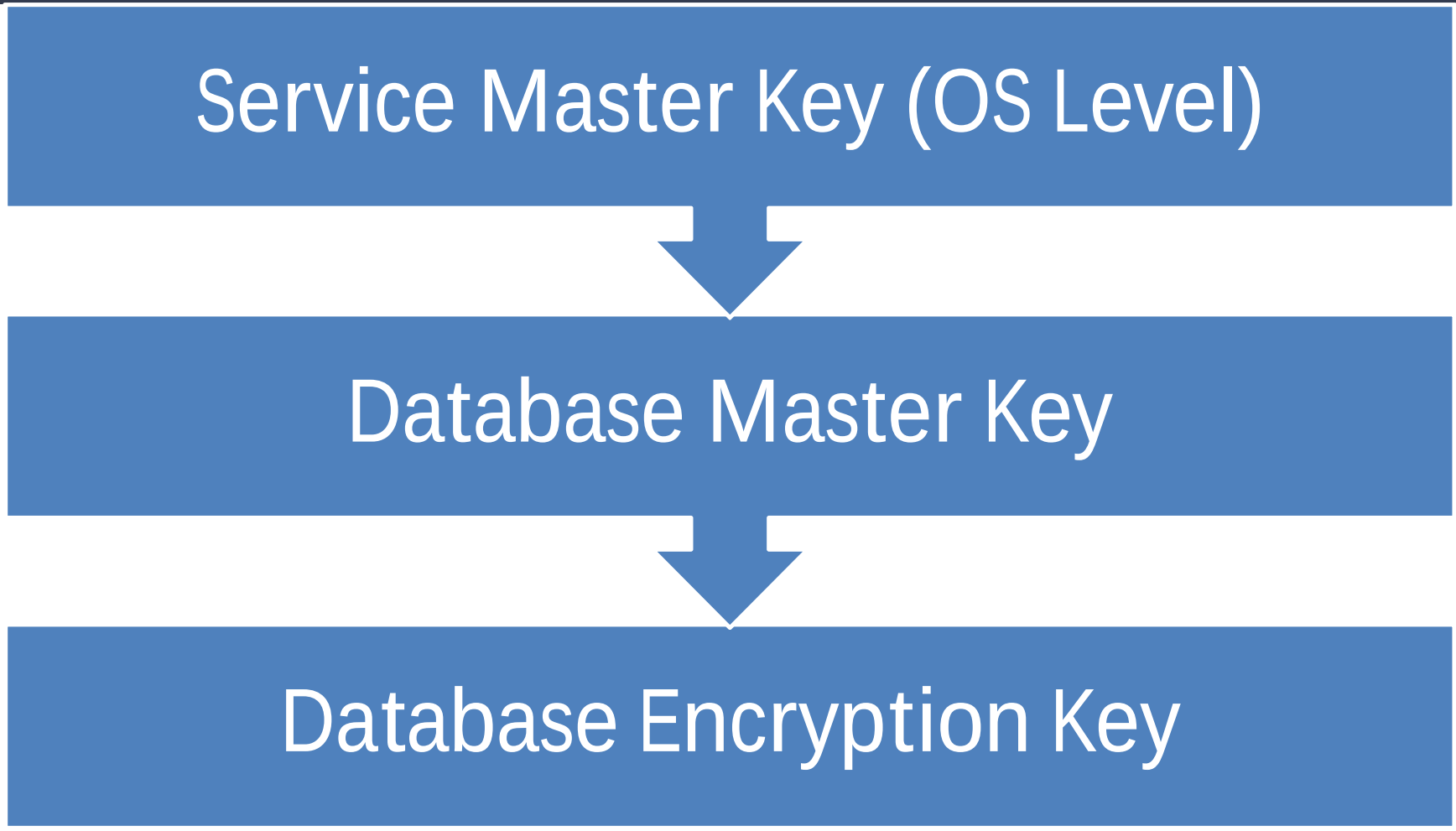
Encryption - TDE

- Introduced in SQL Server 2008 Enterprise
- Encrypts data at rest
- Uses hierarchy of keys

RCI

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

TDE Key Hierarchy



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

TDE – Key Backups

```
BACKUP MASTER KEY TO FILE =
  'path_to_file' ENCRYPTION BY
  PASSWORD = 'password‘

RESTORE MASTER KEY FROM FILE =
  'path_to_file' DECRYPTION BY
  PASSWORD = 'password' ENCRYPTION BY
  PASSWORD = 'password' [ FORCE ]
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Encryption – Encrypted Backups

Introduced in SQL Server 2014

Encrypt database backup files

Can use

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Encryption – Always Encrypted

- Introduced in SQL Server 2016
- Protects data in transit and at rest
- Columns encrypted with keys
  - stored with application, not in server

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Encryption – Final Thoughts

Backup and protect all cryptographic keys

TEST YOUR BACKUPS

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Row-Level Security

- Introduced in SQL Server 2016
- Uses functions to restrict table rows available to a user
- Older versions, had to use views and stored procedures to emulate

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Special Permissions

Server-level permissions:

- Apply to all databases, present and future

Introduced in SQL Server 2014:

CONNECT ANY DATABASE

SELECT ALL USER SECURABLES

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Integrity

- Delayed durability
- Mark transaction as committed, even if logs have not been flushed
- Makes our ACID a little less ACID-ic

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Integrity – Delayed Durability

May be set at:

- Database level
- Transaction level
- For in-memory natively compiled procedures

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Database level

```
ALTER DATABASE dbname
  SET DELAYED_DURABILITY
  = DISABLED | ALLOWED |
  FORCED;
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Transaction Level

```
COMMIT TRANSACTION WITH
 (DELAYED_DURABILITY =
 ON);
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Atomic level

For natively-compiled procedure used with in-memory OLTP:

```
BEGIN ATOMIC WITH
 (DELAYED_DURABILITY =
 ON, ...)
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

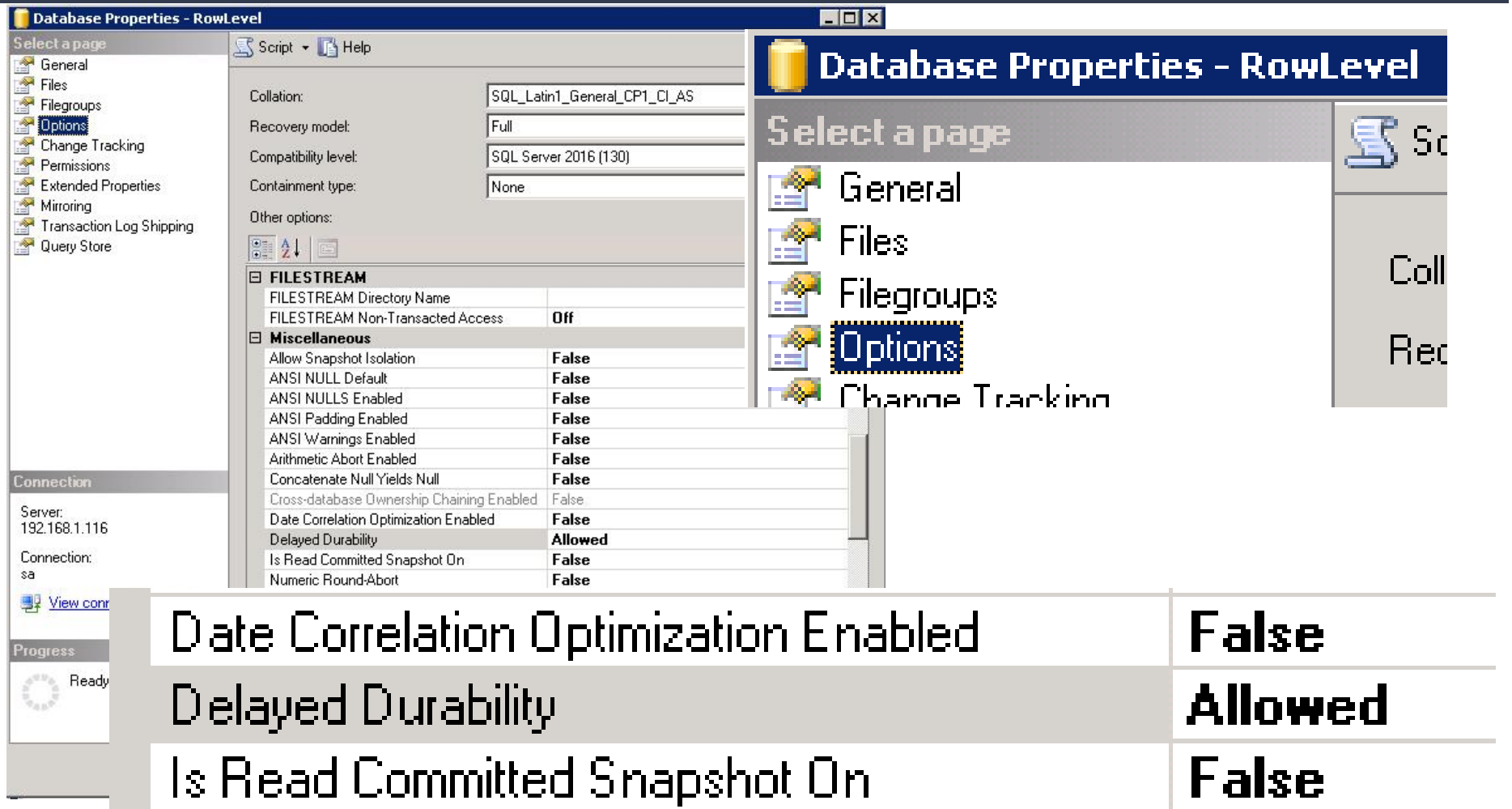
Delayed Durability Checking

Database properties dialog
  Options tab

Query

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Delayed Durability - Options



© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Delayed Durability – Query

```
SELECT name,
 DATABASEPROPERTYEX(name,
   'DelayedDurability') AS
   DelayedDurability,
 DATABASEPROPERTYEX(name,
    Status')  AS Status
FROM   master.dbo.sysdatabases
ORDER BY name
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Availability

For on-premise installations, a number of Azure availability options:

- Managed backups to Azure
- “Always on” availability groups with Azure replicas

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Managed Backup to Azure

Introduced in SQL Server 2014

Automated backup to Azure

- "blob" storage container

Similar to disk/tape backup, but

- stored in cloud

"Backup to URL"

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Backup to URL

```
BACKUP DATABASE TestDB TO URL =
  'https://<accountname>.blob.core.win
  dows.net/<containername>/TestDB.bak'
WITH CREDENTIAL =
  '<mycredentialname>' ,COMPRESSION
  ,STATS = 5;
```


© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Always-On Azure Replicas

- Always-On availability groups used for database replication
- Replicas can be hosted in Azure
- Failover to on-premise or Azure replica

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Conclusion

Brief overview of interesting features

Not exhaustive

2016 deployments a good time to re-check your DB environment

© 2016, Risenhoover Consulting, Inc. All Rights Reserved

Questions

http://tinyurl.com/ISACAClay

© 2016, Risenhoover Consulting, Inc. All Rights Reserved