Dynamic Data Masking (DDM)

Leonard Lobel
CTO, SLEEK TECHNOLOGIES

@lennilobel

Introducing Dynamic Data Masking (DDM)

Limit exposure to sensitive data by masking

- Full – entire column is masked
- Partial – show starting and/or ending characters of the column data, mask the rest with a custom string
- Email – show the first character of the column data, mask the rest with XXX@XXXX.com
- Random – entire column is replaced by random values

Reveals masked data to queries

- Data in the database is not changed

Enforced at the database level

- No impact at the application level

Masking Table Columns

```
CREATE TABLE Customer(
  FirstName varchar(20)
   MASKED WITH (FUNCTION='partial(1, "...", 0)'),
  LastName varchar(20),
  Phone varchar(12)
   MASKED WITH (FUNCTION='default()'),
  Email varchar(200)
   MASKED WITH (FUNCTION='email()'),
  Balance money
   MASKED WITH (FUNCTION='random(1000, 5000)'))

ALTER TABLE Customer
 ALTER COLUMN LastName
  ADD MASKED WITH (FUNCTION='default()')
```

Masking Different Data Types

Masking Function	Behavior	Strings	Numbers	Dates	Other Types
default()	Show **xxxx** mask (strings), or minimum value (other types)	Yes	Yes	Yes	Yes
partial(*a*, 'x', *b*)	Show first *a* characters, custom mask, and last *b* characters	Yes	No	No	No
email()	Show first character and **XXX@XXXX.com**	Yes	No	No	No
random(*a*, *b*)	Show random value between *a* and *b*	No	Yes	No	No

Discovering Masked Columns

sys.columns

- is_masked
- masking_function

sys.masked_columns

- Inherits from sys.columns
- Filters to show only masked columns
  - WHERE is_masked = 1

Mask Permissions

DDM is based on user permissions

Create a table with masked columns

- No special permission required

Add, replace, or remove a column mask

- Requires `ALTER ANY MASK` permission

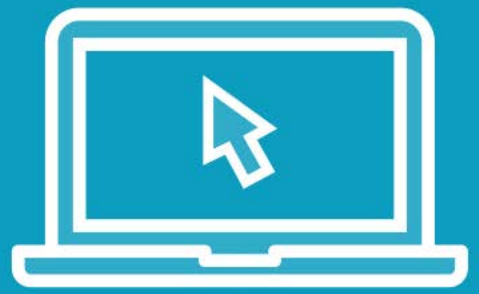
View unmasked data in masked columns

- Requires `UNMASK` permission

Updating data in a masked column

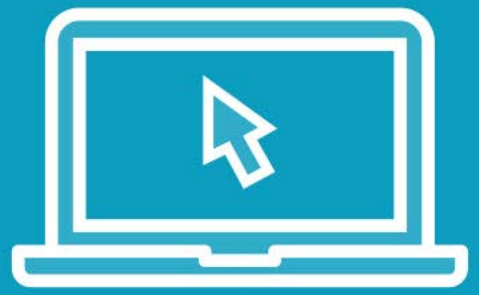
- No special permission

Demo



Getting Started with Dynamic Data Masking

Demo



Using DDM with Different Data Types

DDM Limitations and Considerations

DDM cannot be used with

- FILESTREAM columns
- COLUMN_SET, or a sparse column that's part of a COLUMN_SET
- Computed columns
  - But will return masked data if it depends on a masked column
- Key for FULLTEXT index
- Encrypted columns (Always Encrypted)

Masking is a one-way street

- Once masked, the actual data can never be obtained
- An ETL process from a source with masked columns results in an irreversible data loss when loaded into the target environment

Summary

Dynamic Data Masking

- Default, partial, email, random

Masking table columns

- Supported data types
- Discovering masked columns

Mask permissions

- ALTER ANY MASK
- UNMASK