Auditing Data Access

Module Overview

- Auditing Data Access in SQL Server
- Implementing SQL Server Audit
- Encrypting Databases

Lesson 1: Auditing Data Access in SQL Server

- Discussion: Auditing Data Access
- Common Criteria Auditing
- SQL Trace
- DML Triggers
- Demonstration: Using DML Triggers for Auditing
- SQL Server Audit

Discussion: Auditing Data Access

- Why is auditing required?
- What methods have you used for auditing?
- What are the limitations of the methods you have used?
- Which standards that require auditing does your organization need to comply with?

SQL Trace

- SQL Server Profiler is used to trace commands sent to the server and errors returned:
  - Can be heavy on resources
  - Is run interactively
  - Can trace command executions

- SQL Trace:
  - A set of system stored procedures that enable you to create traces
  - Can be used from within applications
  - Relatively lightweight when well-filtered

DML Triggers

- Triggers can provide part of an auditing solution:
  - DML triggers for data modification
  - Logon triggers for tracking logons

- Limitations:
  - Performance impact
  - Ability to disable triggers
  - Lack of SELECT triggers
  - Trigger nesting issues
  - Complexities around trigger firing order

Demonstration: Using DML Triggers for Auditing

In this demonstration, you will see how to:

- Create a DML trigger for auditing

SQL Server Audit

- Event tracking and logging system based on Extended Events

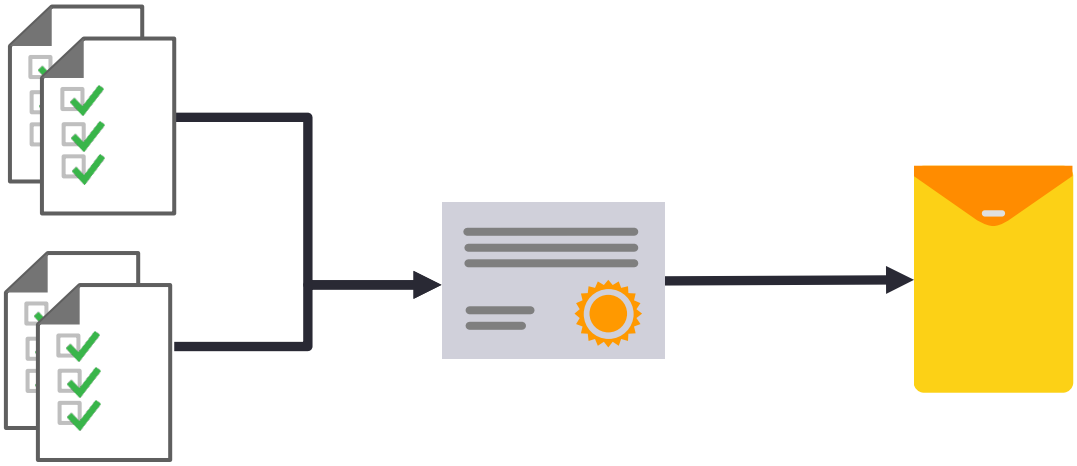
- Comprised of:
  - Audits
  - Audit specifications
  - Actions and action groups
  - Targets

Lesson 2: Implementing SQL Server Audit

- SQL Server Audit Overview
- Creating an Audit
- Creating a Server Audit Specification
- Creating Database Audit Specifications
- User-Defined Audit Actions
- Reading Audited Events
- Managing SQL Server Audit
- Demonstration: Using SQL Server Audit

SQL Server Audit Overview

- **Audit**: Where and how events are logged
- **Audit Specification**: A set of events to be logged in an audit
- **Actions** and **Action Groups**: Events that can be included in an audit specification



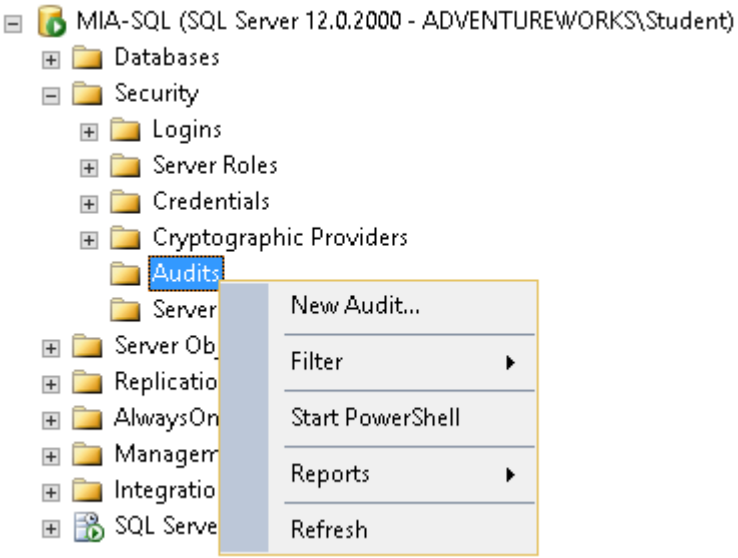
Action Groups / Actions

Audit Specification

Audit

Creating an Audit

- Specify:
  - Target
  - Queue delay
  - Action on failure
- Set STATE = ON to enable

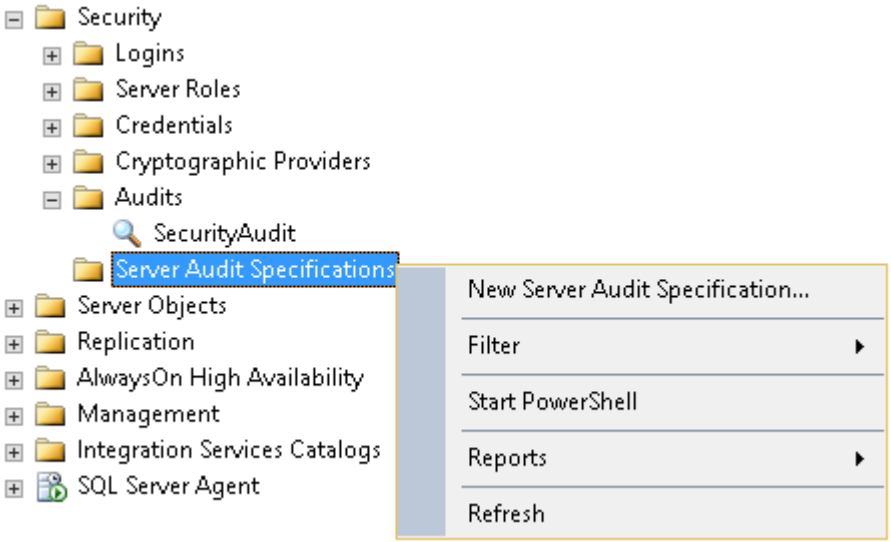



```
CREATE SERVER AUDIT SecurityAudit
TO FILE
(FILEPATH = '\\MIA-SQL\AuditFiles\' ,MAXSIZE = 0 MB
 ,MAX_ROLLOVER_FILES = 2147483647 ,RESERVE_DISK_SPACE = OFF)
WITH
(QUEUE_DELAY = 1000 ,ON_FAILURE = FAIL_OPERATION);
GO

ALTER SERVER AUDIT SecurityAudit
WITH (STATE = ON);
```

Creating a Server Audit Specification

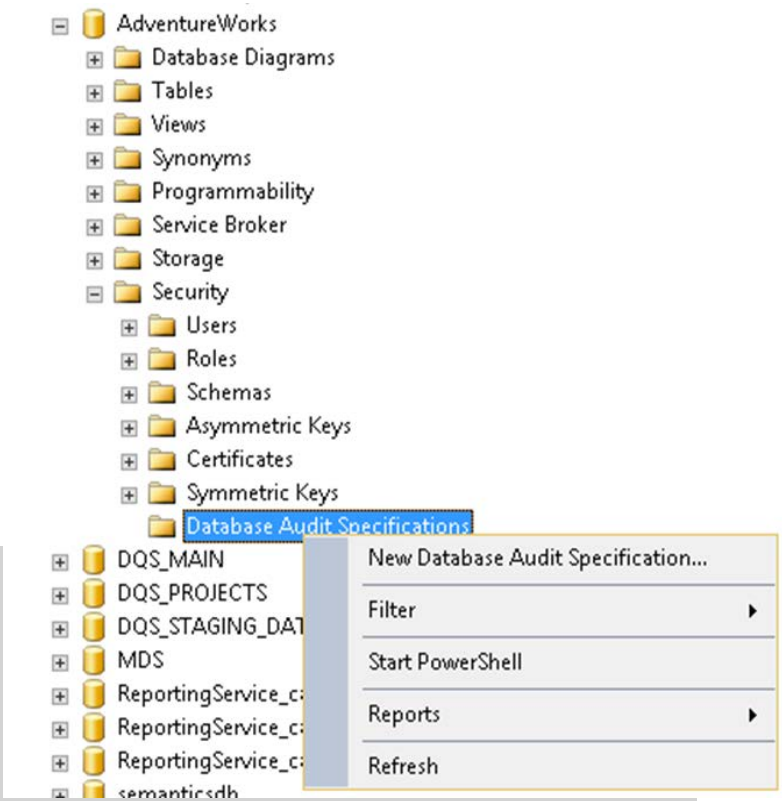
- Specify:
  - Audit
  - Action groups to be included
  - State




```
CREATE SERVER AUDIT SPECIFICATION AuditLogins
FOR SERVER AUDIT SecurityAudit
ADD (FAILED_LOGIN_GROUP),
ADD (SUCCESSFUL_LOGIN_GROUP)
WITH (STATE = ON);
```

Creating Database Audit Specifications

- Specify:
  - Audit
  - Action Groups
  - Actions on specific securable by specific principals
  - State




```
USE AdventureWorks;

CREATE DATABASE AUDIT SPECIFICATION
AdventureWorks_DBSecurity
FOR SERVER AUDIT SecurityAudit
ADD
(DATABASE_PRINCIPAL_CHANGE_GROUP),
ADD
(SELECT ON SCHEMA::HumanResources BY db_datareader)
WITH (STATE = ON);
```

User-Defined Audit Actions

- Enable you to audit custom events:
  - Add USER_DEFINED_AUDIT_GROUP to an audit specification

```
CREATE TRIGGER HR.BonusChecker ON HR.EmployeeBonus
AFTER INSERT
AS
DECLARE @bonus money, @empid integer, @msg nvarchar(4000)

select @bonus = i.Bonus, @empid = i.EmployeeID
from inserted i

IF @bonus > 1000
BEGIN
   SET @msg = 'Employee '+ CAST(@empid as varchar(50))
         +' bonus is over $1000'
   EXEC sp_audit_write @user_defined_event_id = 12,
         @succeeded = 1, @user_defined_information = @msg;
END
```

Reading Audited Events

- Use Event Viewer to view Windows event logs
- Retrieve file-based audits by using the **sys.fn_get_audit_file** function

```
SELECT event_time, object_id, server_principal_name,
   database_name, schema_name, object_name, statement
FROM
   sys.fn_get_audit_file('\\MIA-SQL\AuditFiles\*', default, default);
```

Managing SQL Server Audit

- Enable or disable audits by setting STATE
- View audit configuration details in DMVs
- Audit considerations include:
  - Restoring or attaching a database may result in a mismatched GUID
  - Attaching a database to a different edition of SQL Server may result in the audit not running
  - Mirrored servers may result in mismatched GUIDs
  - Auditing a large number of events can cause performance issues
  - Failure during audit can cause SQL Server to fail to start

Demonstration: Using SQL Server Audit

In this demonstration, you will see how to:

- Create an audit
- Create a server audit specification
- Create a database audit specification
- View audited events