

OFFIZIELLES MICROSOFT LEARNING-PRODUKT

# 21764C

Verwalten einer  
SQL-Datenbankinfrastruktur

Die in diesen Unterlagen enthaltenen Angaben und Daten, einschließlich URLs und anderer Verweise auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen sowie E-Mail-Adressen und Logos sind frei erfunden, soweit nichts anderes angegeben ist. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, Personen, Orten, Ereignissen, E-Mail-Adressen und Logos ist rein zufällig. Die Benutzer sind für das Einhalten aller geltenden Urheberrechtsgesetze verantwortlich. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Microsoft besitzt möglicherweise Patente, Patentanmeldungen, Handelsmarken, Urheberrechte oder andere geistige Eigentumsrechte für die in diesem Dokument behandelten Inhalte. Sofern nicht anderweitig in einer schriftlichen Lizenzvereinbarung von Microsoft ausdrücklich angegeben, wird mit der Bereitstellung dieses Dokuments keinerlei Recht auf diese Patente, Handelsmarken, Urheberrechte oder andere geistige Eigentumsrechte erteilt.

Die Namen von Herstellern, Produkten und URLs dienen nur zu Informationszwecken, und Microsoft schließt für diese Hersteller bzw. die Verwendung der Produkte mit Microsoft-Technologien jegliche ausdrückliche, konkludente oder gesetzliche Zusicherung und Gewährleistung aus. Die Nennung eines Herstellers oder Produkts impliziert nicht, dass Microsoft den Hersteller oder das Produkt unterstützt. Das Dokument enthält Links zu Websites Dritter. Diese Websites stehen nicht unter der Verwaltung von Microsoft. Microsoft ist nicht verantwortlich für den Inhalt von Websites, die durch Hyperlinks verbunden sind, für Hyperlinks auf diesen Websites oder für die Änderungen bzw. Aktualisierungen solcher Websites. Microsoft ist nicht für Webcasting oder andere Übertragungsformen verantwortlich, die von anderen durch Hyperlinks verbundenen Websites empfangen werden. Die Tatsache, dass Microsoft Hyperlinks von anderen Websites einschließt, impliziert nicht, dass Microsoft den Inhalt dieser Websites oder die Produkte unterstützt. Microsoft stellt Ihnen diese Links vielmehr nur als Service zur Verfügung.

© 2018 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft und die unter <https://www.microsoft.com/en-us/legal/intellectualproperty/trademarks/en-us.aspx> aufgeführten Marken sind Marken der Microsoft-Unternehmensgruppe. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Produktnummer: 21764C

Artikelnummer (falls zutreffend): X21-75630

Freigegeben: 06/2018

# Unterrichtseinheit 1

## SQL Server-Sicherheit

### Inhalt:

<b>Lektion 1:</b> Authentifizieren von Verbindungen mit SQL Server	2
<b>Lektion 2:</b> Autorisieren von Anmeldungen zum Herstellen von Verbindungen mit Datenbanken	6
<b>Lektion 3:</b> Serverübergreifende Autorisierung	8
<b>Lektion 4:</b> Teilweise eigenständige Datenbanken	10
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	13
Fragen und Antworten zur Zusammenfassung der Übungseinheit	14

## Lektion 1

# Authentifizieren von Verbindungen mit SQL Server

### Inhalt:

Fragen und Antworten	3
Ressourcen	3
Vorführung: Authentifizieren von Anmeldungen	4

## Fragen und Antworten

**Frage:** Welche dieser Aussagen ist falsch?

- Azure-Firewall-Regeln werden auf zwei Ebenen konfiguriert: Server- und Datenbankebene
- Sie können Kennwörter nur mithilfe der Transact-SQL-Anweisung ALTER LOGIN zurücksetzen.
- Das vertrauenswürdige Anwendungsmodell wird häufig in größeren Unternehmensanwendungen, Websites und Internetdiensten verwendet.
- In einer Windows-basierten Umgebung können Administratoren Richtlinien für Windows-Benutzer aktivieren, durch die eine Kennwortkomplexität und ein Kennwortablauf erzwungen wird. SQL Server kann ähnliche Beschränkungen für SQL Server-Anmeldungen erzwingen.
- Um eine Verbindung zu SQL Server herstellen zu können, muss der Prinzipal Informationen angeben, die mit den in SQL Server gespeicherten Anmeldeinformationen übereinstimmen.

**Antwort:**

- Azure-Firewall-Regeln werden auf zwei Ebenen konfiguriert: Server- und Datenbankebene
- Sie können Kennwörter nur mithilfe der Transact-SQL-Anweisung ALTER LOGIN zurücksetzen.
- Das vertrauenswürdige Anwendungsmodell wird häufig in größeren Unternehmensanwendungen, Websites und Internetdiensten verwendet.
- In einer Windows-basierten Umgebung können Administratoren Richtlinien für Windows-Benutzer aktivieren, durch die eine Kennwortkomplexität und ein Kennwortablauf erzwungen wird. SQL Server kann ähnliche Beschränkungen für SQL Server-Anmeldungen erzwingen.
- Um eine Verbindung zu SQL Server herstellen zu können, muss der Prinzipal Informationen angeben, die mit den in SQL Server gespeicherten Anmeldeinformationen übereinstimmen.

**Frage:** Richtig oder falsch? Damit eine Verbindung zur Azure-Datenbank hergestellt werden kann, muss TCP-Port **1344** in Ihren lokalen Firewallregeln offen sein.

- Richtig
- Falsch

**Antwort:**

- Richtig
- Falsch

## Ressourcen

### Überblick über SQL Server-Sicherheit



**Bewährte Methoden:** Erwägen Sie bei der Planung einer Sicherheitslösung folgende bewährte Methoden:

- Stellen Sie den Prinzipalen nur die Berechtigungen zur Verfügung, die sie tatsächlich benötigen.
- Verwenden Sie die sicherungsfähige Vererbung, um die Anzahl impliziter Berechtigungen zu verringern, die festgelegt werden, damit die erforderliche Zugriffsstufe aktiviert wird.

- Verwenden Sie Prinzipalcontainer, wie z. B. Gruppen oder Rollen, um eine Abstraktionsebene zwischen Prinzipalen und Berechtigungen für den Zugriff auf sicherungsfähige Elemente zu schaffen. Sie können anschließend die Mitgliedschaft dieser Gruppen für die Steuerung des Zugriffs auf Ressourcen über die Berechtigungen verwenden, die Sie definiert haben. Aufgrund von Veränderungen im Personal sollten keine Änderungen an Berechtigungen erforderlich sein.

## SQL Server-Authentifizierung



**Bewährte Methoden:** Nach Möglichkeit sollte die Windows-Authentifizierung verwendet werden.

## Azure SQL-Datenbank-Firewall



**Bewährte Methoden:** Microsoft empfiehlt die Verwendung von Firewallregeln auf Datenbankebene. Sie sollten in Erwägung ziehen, Serverregeln zu verwenden, wenn Sie über viele Datenbanken mit den gleichen Zugriffsanforderungen verfügen.

## Vorführung: Authentifizieren von Anmeldungen

### Vorführungsschritte

Einstellen des Authentifizierungsmodus

1. Vergewissern Sie sich, dass die virtuellen Computer **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie im Ordner **D:\Demofiles\Mod01** die Datei **Setup.cmd** als Administrator aus.
3. Klicken Sie bei der Aufforderung auf **Ja**, in der Sie dazu aufgefordert werden, zu bestätigen, dass Sie die Befehlsdatei ausführen möchten und warten Sie anschließend, bis das Skript beendet wurde.
4. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine **MIA-SQL** her.
5. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf die **MIA-SQL**-Instanz, und klicken Sie dann auf **Eigenschaften**.
6. Überprüfen Sie im Dialogfeld **Servereigenschaften - MIA-SQL** auf der Seite **Sicherheit**, ob **SQL Server- und Windows-Authentifizierungsmodus** ausgewählt ist, und klicken Sie dann auf **Abbrechen**.

Erstellen von Anmeldungen

1. Erweitern Sie im Objekt-Explorer **Sicherheit** und **Anmeldungen**, um die Anmeldungen anzuzeigen, die aktuell für diese Serverinstanz definiert sind.
2. Klicken Sie mit der rechten Maustaste auf **Anmeldungen** und dann auf **Neue Anmeldung**.
3. Klicken Sie im Dialogfeld **Anmeldung - Neu** neben dem Namensfeld **Anmeldung** auf **Suchen**.
4. Klicken Sie im Dialogfeld **Benutzer, Dienstkonto oder -gruppe auswählen** auf **Objekttypen**.
5. Vergewissern Sie sich im Dialogfeld **Objekttypen**, dass nur **Benutzer** und **Gruppen** ausgewählt sind, und klicken Sie dann auf **OK**.
6. Klicken Sie im Dialogfeld **Benutzer, Dienstkonto oder -gruppe auswählen** auf **Speicherorte**.
7. Erweitern Sie im Dialogfeld **Speicherorte Gesamtes Verzeichnis**, klicken Sie auf **adventureworks.msft** und dann auf **OK**.

8. Klicken Sie im Dialogfeld **Benutzer, Dienstkonto oder -gruppe auswählen** auf **Erweitert**.
9. Klicken Sie im Dialogfeld **Benutzer, Dienstkonto oder -gruppe auswählen** auf **Suchen**. Dadurch wird eine Liste aller Benutzer und Gruppen in der Active Directory-Domäne generiert.
10. Klicken Sie in der Liste der Domänenobjekte auf **HumanResources\_Users** (hierbei handelt es sich um eine lokale Gruppe der Domäne, die mehrere globale Gruppen enthält, die wiederum Benutzer enthalten), und klicken Sie dann auf **OK**.
11. Vergewissern Sie sich im Dialogfeld **Benutzer, Dienstkonto oder -gruppe auswählen**, dass **HumanResources\_Users** aufgeführt ist, und klicken Sie dann auf **OK**.
12. Klicken Sie im Dialogfeld **Anmeldung - Neu** in der Liste **Standarddatenbank** auf **AdventureWorks** und dann auf **OK**.
13. Vergewissern Sie sich im Objekt-Explorer im Ordner **Anmeldungen**, dass die Anmeldung **ADVENTUREWORKS\HumanResources\_Users** hinzugefügt wurde.
14. Klicken Sie mit der rechten Maustaste auf **Anmeldungen** und dann auf **Neue Anmeldung**.
15. Geben Sie im Dialogfeld **Anmeldung - Neu** in das Feld **Anmeldename** **Payroll\_Application** ein, und klicken Sie dann auf **SQL Server-Authentifizierung**.
16. Geben Sie das Kennwort **Pa55w.rd** ein, und bestätigen Sie es. Deaktivieren Sie anschließend das Kontrollkästchen **Kennwortablauf erzwingen** (dadurch wird das Kontrollkästchen **Benutzer muss das Kennwort bei der nächsten Anmeldung ändern** automatisch deaktiviert).
17. Klicken Sie in der Liste **Standarddatenbank** auf **AdventureWorks**, und klicken Sie dann auf **OK**.
18. Vergewissern Sie sich im Objekt-Explorer im Ordner **Anmeldungen**, dass die Anmeldung **Payroll\_Application** hinzugefügt wurde.
19. Öffnen Sie die Skriptdatei **CreateLogins.sql** im Ordner **D:\Demofiles\Mod01**, und prüfen Sie den darin enthaltenen Code. Dadurch wird eine Windows-Anmeldung für den Benutzer **ADVENTUREWORKS\AnthonyFrizzell**, die lokale Gruppe **ADVENTUREWORKS\Database\_Managers** und eine SQL Server-Anmeldung mit der Bezeichnung **Web\_Application** erstellt.
20. Klicken Sie auf **Ausführen**, und aktualisieren Sie nach erfolgreichem Beenden des Skripts im Objekt-Explorer den Ordner **Anmeldungen**, vergewissern Sie sich anschließend, dass die Anmeldungen erstellt wurden.
21. Klicken Sie im Menü **Datei** auf **Schließen**.
22. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Autorisieren von Anmeldungen zum Herstellen von Verbindungen mit Datenbanken

### Inhalt:

Fragen und Antworten	7
Vorführung: Autorisieren von Anmeldungen und Benutzertoken	7

## Fragen und Antworten

**Frage:** Richtig oder falsch? Sie können Sicherheitstokens mithilfe der Systemansichten **sys.login\_token** und **sys.user\_token** anzeigen.

- Richtig  
 Falsch

**Antwort:**

- Richtig  
 Falsch

## Vorführung: Autorisieren von Anmeldungen und Benutzertoken

### Vorführungsschritte

1. Öffnen Sie in SQL Server Management Studio die Skriptdatei **Security Tokens Demo.sql** im Ordner **D:\Demofiles\Mod01**. Beachten Sie, dass Sie in einigen Fällen im Objekt-Explorer mit der rechten Maustaste auf den Objekte enthaltenden Knoten klicken und anschließend auf **Aktualisieren** klicken, damit die Objekte aktualisiert und die Ergebnisse in SQL Server Management Studio angezeigt werden.
2. Markieren Sie den Code unter **Schritt A**, und klicken Sie dann auf **Ausführen**.
3. Markieren Sie den Code unter **Schritt B**, und klicken Sie dann auf **Ausführen**.
4. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** unter **Sicherheit** die Option **Serverrollen**, um die neuen Serverrollen anzuzeigen.
5. Markieren Sie den Code unter **Schritt C**, und klicken Sie dann auf **Ausführen**.
6. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** unter **Sicherheit**, die Option **Anmeldungen**, um die neue Anmeldung anzuzeigen.
7. Markieren Sie den Code unter **Schritt D**, und klicken Sie dann auf **Ausführen**.
8. Markieren Sie den Code unter **Schritt E**, und klicken Sie dann auf **Ausführen**.
9. Erweitern Sie im Objekt-Explorer unter **MIA-SQL Datenbanken, AdventureWorks, , Sicherheit** und **Rollen**, und erweitern Sie dann **Datenbankrollen**, um die neuen Datenbankrollen anzuzeigen.
10. Markieren Sie den Code unter **Schritt F**, und klicken Sie dann auf **Ausführen**.
11. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** unter **Datenbanken, AdventureWorks**, und **Sicherheit Benutzer**, um den neuen Benutzer anzuzeigen.
12. Markieren Sie den Code unter **Schritt G**, und klicken Sie dann auf **Ausführen**.
13. Markieren Sie den Code unter **Schritt H**, und klicken Sie dann auf **Ausführen**, um die aktuellen Benutzer- und Anmeldetokens anzuzeigen. Der Code wird im Sicherheitskontext der Anmeldung ausgeführt, die für diese Vorführung erstellt wurde. Beachten Sie, dass Tokens mit Bezug zum Datenbankbenutzer, die beiden Datenbankrollen **MyExtDatabaseRole** und **MyDatabaseRole** und die **öffentliche** Datenbankrolle mit dem Benutzer verknüpft sind.
14. Markieren Sie den Code unter **Schritt I**, und klicken Sie dann auf **Ausführen**, um alle Änderungen zu entfernen.
15. Klicken Sie im Menü **Datei** auf **Schließen**.
16. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Serverübergreifende Autorisierung

### Inhalt:

Fragen und Antworten	9
Vorführung: Arbeiten mit nicht übereinstimmenden Sicherheits-IDs	9

## Fragen und Antworten

**Frage:** Richtig oder falsch? Sie können die Tabelle „sys.missing\_sids“ abfragen, um verwaiste Benutzer in einer Datenbank zu ermitteln.

- Richtig
- Falsch

**Antwort:**

- Richtig
- Falsch

## Vorführung: Arbeiten mit nicht übereinstimmenden Sicherheits-IDs

### Vorführungsschritte

1. Öffnen Sie in SQL Server Management Studio die Skriptdatei **MismatchedIDs.sql** im Ordner **D:\Demofiles\Mod01**.
2. Markieren Sie den Code unter **Schritt A**, und klicken Sie dann auf **Ausführen**, um den Bericht zu verwaisten Benutzern in der **TSQL**-Datenbank auszuführen. Es sollten zwei Benutzer zurückgegeben werden. Beachten Sie die SID für den Benutzer **appuser1**.
3. Markieren Sie den Code unter **Schritt B**, und klicken Sie dann auf **Ausführen**, um aufzuzeigen, dass eine **appuser**-Anmeldung vorhanden ist, sie jedoch über eine andere SID verfügt als die SID, auf die der Benutzer **appuser1** verweist.
4. Markieren Sie den Code unter **Schritt C**, und klicken Sie dann auf **Ausführen**, um den Benutzer **appuser1** durch Verknüpfen mit der **appuser**-Anmeldung zu reparieren.
5. Markieren Sie den Code unter **Schritt D**, und klicken Sie dann auf **Ausführen**, um aufzuzeigen, dass der Benutzer **appuser1** nicht mehr verwaist ist. Beachten Sie die SID für den Benutzer **reportuser1**.
6. Markieren Sie den Code unter **Schritt E**, und klicken Sie dann auf **Ausführen**, um die **reportuser**-Anmeldung mit einem definierten SID-Wert zu erstellen. Die SID stimmt mit der SID überein, die in dem Bericht zu verwaisten Benutzern für **reportuser1** zurückgegeben wird.
7. Markieren Sie den Code unter **Schritt F**, und klicken Sie dann auf **Ausführen**, um aufzuzeigen, dass keine verwaisten Benutzer mehr übrig sind.
8. Klicken Sie im Menü **Datei** auf **Schließen**.
9. Lassen Sie SQL Server Management Studio geöffnet.

## Lektion 4

# Teilweise eigenständige Datenbanken

### Inhalt:

Fragen und Antworten	11
Vorführung: Erstellen einer teilweise eigenständigen Datenbank	11

## Fragen und Antworten

### Frage:

Richtig oder falsch? Mithilfe des folgenden Codes kann **SalesMan1** zur **Masterdatenbank** hinzugefügt werden:

```
USE master
```

```
GO
```

```
CREATE USER SalesMan1 WITH PASSWORD = 'Pa55w.rd'
```

```
GO
```

Richtig

Falsch

### Antwort:

Richtig

Falsch

**Frage:** Welche Option gilt nicht für teilweise eigenständige Datenbanken?

Sie können die ALTER-Anweisung verwenden, um eine nicht eigenständige Datenbank in eine teilweise eigenständige Datenbank zu konvertieren.

CDC und CT werden in teilweise eigenständigen Datenbanken nicht unterstützt.

Nummerierte und temporäre Prozeduren werden in teilweise eigenständigen Datenbanken unterstützt.

Die Replikation wird in teilweise eigenständigen Datenbanken nicht unterstützt.

### Antwort:

Sie können die ALTER-Anweisung verwenden, um eine nicht eigenständige Datenbank in eine teilweise eigenständige Datenbank zu konvertieren.

CDC und CT werden in teilweise eigenständigen Datenbanken nicht unterstützt.

Nummerierte und temporäre Prozeduren werden in teilweise eigenständigen Datenbanken unterstützt.

Die Replikation wird in teilweise eigenständigen Datenbanken nicht unterstützt.

## Vorführung: Erstellen einer teilweise eigenständigen Datenbank

### Vorführungsschritte

Anzeigen des Einschlusswerts

1. Öffnen Sie in SQL Server Management Studio die Skriptdatei **ContainedDatabase.sql** im Ordner **D:\Demofiles\Mod01**.
2. Markieren Sie den Code unter **Schritt A**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass der zurückgegebene Wert „1“ lautet, da der Einschluss aktiviert sein sollte.
3. Markieren Sie den Code unter **Schritt B**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass der Wert für **value\_in\_use** „0“ lautet (Einschluss ist deaktiviert). So bestätigen Sie dies:
  - a. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **MIA-SQL**, und klicken Sie auf **Eigenschaften**.

- b. Beachten Sie, dass das Attribut **Eigenständige Datenbanken aktivieren** auf der Seite **Erweitert** im Dialogfeld **Servereigenschaften - MIA-SQL False** lautet, und klicken Sie dann auf **Abbrechen**.
4. Markieren Sie den Code unter **Schritt C**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass der Wert für **value\_in\_use** wieder auf „**1**“ gesetzt wird. So bestätigen Sie dies:
  - a. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **MIA-SQL**, und klicken Sie auf **Eigenschaften**.
  - b. Beachten Sie, dass das Attribut **Eigenständige Datenbanken aktivieren** auf der Seite **Erweitert** im Dialogfeld **Servereigenschaften - MIA-SQL True** lautet, und klicken Sie dann auf **Abbrechen**.
5. Markieren Sie den Code unter **Schritt D**, und klicken Sie dann auf **Ausführen**.
6. Klicken Sie im Objekt-Explorer unter **MIA-SQL** mit der rechten Maustaste auf **Datenbanken**, und klicken Sie dann auf **Aktualisieren**, um eine Liste der Datenbanken anzuzeigen, einschließlich der neuen teilweise eigenständigen Datenbank.
7. Markieren Sie den Code unter **Schritt E**, und klicken Sie dann auf **Ausführen**. Über die SELECT-Anweisung werden die neuen Benutzer zurückgegeben.
8. Erweitern Sie im Objekt-Explorer unter **MIA-SQL**, **Datenbanken**, **PClientData**, **Ansichten**, und erweitern Sie **Systemansichten**, klicken Sie mit der rechten Maustaste auf **sys.database\_principals**, und klicken Sie dann auf **Oberste 1.000 Zeilen auswählen**. Bestätigen Sie, dass die neuen Benutzer in der Liste der eigenständigen Benutzer erstellt wurden.
9. Markieren Sie auf der Registerkarte **ContainedDatabase.sql** den Code unter **Schritt F**, und klicken Sie dann auf **Ausführen**.
10. Schließen Sie SQL Server Management Studio, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Fragen zur Lernzielkontrolle

**Frage:** Was geschieht, wenn eine Anmeldung keinen Zugriff auf ihre Standarddatenbank hat und verwendet wird, um eine Verbindung mit einer SQL Server-Instanz herzustellen?

- Die Anmeldung kann sich mit SQL Server verbinden, aber eine Fehlermeldung wird angezeigt.
- Die Anmeldung kann sich nicht mit SQL Server verbinden.
- Die Anmeldung wird automatisch deaktiviert.
- Die Anmeldung erhält automatisch Zugriff auf ihre Standarddatenbank.

**Antwort:**

- Die Anmeldung kann sich mit SQL Server verbinden, aber eine Fehlermeldung wird angezeigt.
- Die Anmeldung kann sich nicht mit SQL Server verbinden.
- Die Anmeldung wird automatisch deaktiviert.
- Die Anmeldung erhält automatisch Zugriff auf ihre Standarddatenbank.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Authentifizieren von Benutzern

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Warum wurde der Benutzer **ADVENTUREWORKS\WebApplicationSvc** in der letzten Übungseinheit nicht als verwaister Benutzer gemeldet?

**Antwort:** Weil der Benutzer mit einer Anmeldung verknüpft ist, die auf einem Windows-Benutzerkonto basiert.

# Unterrichtseinheit 2

## Zuweisen von Server- und Datenbankrollen

### Inhalt:

Lektion 1: Arbeiten mit Serverrollen	2
Lektion 2: Arbeiten mit festen Datenbankrollen	5
Lektion 3: Benutzerdefinierte Datenbankrollen	8
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	11
Fragen und Antworten zur Zusammenfassung der Übungseinheit	12

## Lektion 1

# Arbeiten mit Serverrollen

### Inhalt:

Fragen und Antworten	3
Ressourcen	3
Vorführung: Zuweisen fester und benutzerdefinierter Serverrollen	3

## Fragen und Antworten

**Frage:** Welche feste Serverrolle sollte aufgrund ihrer Fähigkeit zum Zuweisen von Serverprinzipalen für Serverrollen als vergleichbar mit **sysadmin** betrachtet werden?

- serveradmin
- securityadmin
- processadmin
- setupadmin
- bulkadmin

**Antwort:**

- serveradmin
- securityadmin
- processadmin
- setupadmin
- bulkadmin

## Ressourcen

### public-Serverrolle

 **Bewährte Methoden:** Die Zugriffssteuerung sicherungsfähiger Serverobjekte durch das Gewähren zusätzlicher Berechtigungen für die Rolle **public** wird nicht empfohlen, da für die einzelnen Anmeldungen versehentlich ein umfassenderer Zugriff als vorgesehen gewährt werden könnte. Aus dem gleichen Grund sollten Sie regelmäßig die Berechtigungen überprüfen, die der Rolle **public** gewährt werden.

### Arbeiten mit benutzerdefinierten Serverrollen

 **Bewährte Methoden:** Es wird nicht empfohlen, benutzerdefinierte Serverrollen zu Mitgliedern fester Serverrollen zu machen. Dadurch hätten die Mitglieder der benutzerdefinierten Serverrolle Kontrolle über die Mitgliedschaft der festen Serverrolle, das wiederum könnte zu einer versehentlichen Erhöhung von Berechtigungen führen.

## Vorführung: Zuweisen fester und benutzerdefinierter Serverrollen

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie die **Setup.cmd** im Ordner **D:\Demofiles\Mod02** als Administrator aus. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
3. Starten Sie SQL Server Management Studio, und verbinden Sie sich unter Verwendung der Windows®-Authentifizierung mit der Datenbank-Engine-Instanz **MIA-SQL**.
4. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie auf **Projekt/Projektmappe**.

5. Navigieren Sie im Dialogfeld **Projekt öffnen** zu **D:\Demofiles\Mod02\Project**, klicken Sie auf **Project.ssmssl**, und klicken Sie dann auf **Öffnen**.
6. Erweitern Sie im Projektmappen-Explorer **Abfragen**, und doppelklicken Sie dann auf **Demo 1 - server roles.sql**.
7. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um die Berechtigungshierarchie anzuzeigen.
8. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um zwei Anmeldungen zu erstellen.
9. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um zu veranschaulichen, dass eine neue Anmeldung Mitglied von **public** ist.
10. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um die Berechtigung einer neuen Anmeldung zu veranschaulichen.
11. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um eine Anmeldung zur Rolle **diskadmin** hinzuzufügen.
12. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die im vorherigen Schritt erstellte Mitgliedschaft zu bestätigen.
13. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um eine benutzerdefinierte Serverrolle zu erstellen.
14. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um der neuen Rolle Berechtigungen zu gewähren.
15. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um aus einer Anmeldung ein Mitglied der neuen Rolle zu machen.
16. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um die im vorherigen Schritt erstellte Mitgliedschaft zu bestätigen.
17. Führen Sie den Code unter der Überschrift für **Schritt 11** aus, um die Anmeldungsberechtigungen anzuzeigen.
18. Führen Sie den Code unter der Überschrift für **Schritt 12** aus, um die Anmeldungen und die Rolle zu entfernen.
19. Klicken Sie im Menü **Datei** auf **Schließen**.
20. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Arbeiten mit festen Datenbankrollen

### Inhalt:

Fragen und Antworten	6
Vorführung: Verwalten von Datenbankrollen und -benutzern	6

## Fragen und Antworten

**Frage:** Welche der folgenden Aussagen trifft nicht zu? (eine auswählen)

- ( ) dbo und db\_owner sind Begriffe, die sich auf dasselbe beziehen.
- ( ) dbo ist ein Datenbankbenutzer, der ein Alias für die Anmeldung ist, die Besitzer der Datenbank ist.
- ( ) db\_owner ist eine feste Datenbankrolle mit vollständigen, administrativen Berechtigungen für eine Datenbank.
- ( ) Die Rolle „db\_owner“ kann mehr als ein Mitglied umfassen.
- ( ) Standardmäßig ist „dbo“ ein Mitglied der Rolle „db\_owner“.

**Antwort:**

- (v) dbo und db\_owner sind Begriffe, die sich auf dasselbe beziehen.
- ( ) dbo ist ein Datenbankbenutzer, der ein Alias für die Anmeldung ist, die Besitzer der Datenbank ist.
- ( ) db\_owner ist eine feste Datenbankrolle mit vollständigen, administrativen Berechtigungen für eine Datenbank.
- ( ) Die Rolle „db\_owner“ kann mehr als ein Mitglied umfassen.
- ( ) Standardmäßig ist „dbo“ ein Mitglied der Rolle „db\_owner“.

## Vorführung: Verwalten von Datenbankrollen und -benutzern

### Vorführungsschritte

1. Klicken Sie in SQL Server Management Studio im Objekt-Explorer auf **Verbinden**, und klicken Sie dann auf **Datenbankmodul**.
2. Geben Sie im Dialogfeld **Verbindung mit Server herstellen** im Feld **Servername** den Namen Ihrer Azure-Instanz an, die die **AdventureWorksLT**-Datenbank ausführt, z. B. **<Servername>.database.windows.net**.
3. Klicken Sie in der Liste **Authentifizierung** auf **SQL Server-Authentifizierung**, geben Sie dann in das Feld **Anmeldung Student** und in das Feld **Kennwort Pa55w.rd** ein, und klicken Sie dann auf **Verbinden**.
4. Doppelklicken Sie im Projektmappen-Explorer auf **Demo 2 - database roles.sql**.
5. Zeigen Sie im Menü **Abfrage** auf **Verbindung**, und klicken Sie auf **Verbindung ändern**.
6. Klicken Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** in der Liste **Servername** auf **<Servername>.database.windows.net**, geben Sie in das Feld **Kennwort Pa55w.rd** ein, und klicken Sie dann auf **Verbinden**.
7. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine neue Anmeldung zu erstellen.
8. Klicken Sie auf der Symbolleiste in der Liste **Verfügbare Datenbanken** auf **AdventureWorksLT**.
9. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um einen neuen Benutzer zu erstellen.
10. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um die Datenbankberechtigungs-hierarchie anzuzeigen.
11. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um zu veranschaulichen, dass der Benutzer standardmäßig Mitglied der **public**-Datenbankrolle ist.
12. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um den Benutzer zu zwei festen Datenbankrollen hinzuzufügen.

13. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Benutzerrollen-Mitgliedschaften zu bestätigen.
14. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um die Vorführungsobjekte zu entfernen.
15. Zeigen Sie im Menü **Abfrage** auf **Verbindung**, und klicken Sie auf **Verbindung ändern**.
16. Klicken Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** in der Liste **Servername** auf **<Servername>.database.windows.net**, geben Sie in das Feld **Kennwort Pa55w.rd** ein, und klicken Sie dann auf **Verbinden**.
17. Führen Sie den Code unter der Überschrift für **Schritt 8** aus.
18. Klicken Sie im Menü **Datei** auf **Schließen**.
19. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Benutzerdefinierte Datenbankrollen

### Inhalt:

Fragen und Antworten	9
Vorführung: Benutzerdefinierte Datenbankrollen	9
Vorführung: Anwendungsrollen	10

## Fragen und Antworten

Nummerieren Sie jeden der folgenden Schritte, um die richtige Reihenfolge anzugeben, in der die Aktionen einer Anwendung beim Verwenden einer Anwendungsrolle durchgeführt werden.

	Schritte
	Ein Administrator macht den Benutzer zu einem Mitglied der Datenbankrolle „public“.
	Der Benutzer startet eine Anwendung, die mithilfe der Anmeldeinformationen des Benutzers eine Verbindung zur Datenbank herstellt.
	Die Anwendung aktiviert eine Anwendungsrolle mithilfe des Kennworts, das in der Konfigurationsdatei der Anwendung gespeichert ist.
	Der Benutzer arbeitet mit dem Sicherheitskontext der Anwendungsrolle in der Anwendung.
	Der Benutzer schließt die Anwendung.

**Antwort:**

	Schritte
1	Ein Administrator macht den Benutzer zu einem Mitglied der Datenbankrolle „public“.
2	Der Benutzer startet eine Anwendung, die mithilfe der Anmeldeinformationen des Benutzers eine Verbindung zur Datenbank herstellt.
3	Die Anwendung aktiviert eine Anwendungsrolle mithilfe des Kennworts, das in der Konfigurationsdatei der Anwendung gespeichert ist.
4	Der Benutzer arbeitet mit dem Sicherheitskontext der Anwendungsrolle in der Anwendung.
5	Der Benutzer schließt die Anwendung.

## Vorführung: Benutzerdefinierte Datenbankrollen

### Vorführungsschritte

1. Doppelklicken Sie in SQL Server Management Studio im Projektmappen-Explorer auf **Demo 3 - user database roles.sql**.
2. Zeigen Sie im Menü **Abfrage** auf **Verbindung**, und klicken Sie auf **Verbindung ändern**.

3. Klicken Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** in der Liste **Servername** auf **MIA-SQL**, klicken Sie im Feld **Authentifizierung** auf **Windows-Authentifizierung**, und klicken Sie dann auf **Verbinden**.
4. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine benutzerdefinierte Datenbankrolle zu erstellen.
5. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um der Rolle SELECT-Berechtigungen im **HumanResources**-Schema zu gewähren.
6. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um die Rollenberechtigungen zu überprüfen.
7. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um zwei Benutzer zu der Rolle hinzuzufügen.
8. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um die Rollenmitgliedschaft zu überprüfen.
9. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Vorführungsrolle zu entfernen.
10. Klicken Sie im Menü **Datei** auf **Schließen**.
11. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Anwendungsrollen

### Vorführungsschritte

1. Doppelklicken Sie in SQL Server Management Studio im Projektmappen-Explorer auf **Demo 4 - application roles.sql**.
2. Zeigen Sie im Menü **Abfrage** auf **Verbindung**, und klicken Sie auf **Verbindung ändern**.
3. Klicken Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** in der Liste **Servername** auf **MIA-SQL**, klicken Sie in der Liste **Authentifizierung** auf **Windows-Authentifizierung**, und klicken Sie dann auf **Verbinden**.
4. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine Anwendungsrolle zu erstellen.
5. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um der Rolle Berechtigungen zu gewähren.
6. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um das Verhalten aufzuzeigen, bevor die Anwendungsrolle aktiviert wird.
7. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um die Anwendungsrolle zu aktivieren.
8. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um aufzuzeigen, dass die Anwendungsrolle angewendet wird.
9. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um aufzuzeigen, wie die Identität des Benutzers dargestellt wird.
10. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um aufzuzeigen, dass der datenbankübergreifende Zugriff eingeschränkt ist.
11. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um die Anwendungsrolle zu beenden.
12. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um aufzuzeigen, wie die Identität des Benutzers dargestellt wird.
13. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um die Anwendungsrolle zu entfernen.
14. Klicken Sie im Menü **Datei** auf **Schließen**.
15. Schließen Sie SSMS, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

Berücksichtigen Sie beim Implementieren der rollenbasierten Sicherheit in SQL Server folgende bewährte Methoden:

Verwenden Sie Windows-Gruppenanmeldungen, die mit Rollen verknüpft sind, um die laufende Verwaltung soweit wie möglich zu vereinfachen.

Zielen Sie darauf ab, die minimal mögliche Anzahl von expliziten Berechtigungen zu gewähren, damit die Sicherheitsanforderungen erfüllt werden und verwenden Sie die Rollenmitgliedschaft und Vererbung, um sicherzustellen, dass die korrekten Berechtigungen aktiviert sind.

Vergewissern Sie sich, dass die Datenbankbenutzer nur über die Berechtigung verfügen, die sie tatsächlich benötigen.

## Fragen zur Lernzielkontrolle

**Frage:** Richtig oder falsch? Wenn `sp_setapprole` über den `@encrypt = 'odbc'`-Parameter aufgerufen wird, wird das Anwendungsrollenkennwort mit einer starken Verschlüsselung verschlüsselt.

Richtig

Falsch

**Antwort:**

Richtig

Falsch

**Frage:** Welche Berechtigung ist zum Anzeigen des Inhalts des Abfrageplancaches für eine lokale SQL Server-Instanz erforderlich?

SHOWPLAN (Datenbankebene)

SHOWPLAN (Serverebene)

VIEW SERVER STATE (Serverebene)

VIEW SERVER STATE (Datenbankebene)

**Antwort:**

SHOWPLAN (Datenbankebene)

SHOWPLAN (Serverebene)

VIEW SERVER STATE (Serverebene)

VIEW SERVER STATE (Datenbankebene)

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Zuweisen von Server- und Datenbankrollen

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:**

Ihr Unternehmen möchte den Datenzugriff anhand einzelner Windows-Benutzer nachverfolgen. Heißt das, Anmeldungen dürfen nicht aus Windows-Gruppen stammen?

**Antwort:** Nein. SQL Server kann mithilfe der SUSER\_NAME-Funktion auf einzelne Windows-Identitäten zugreifen, selbst wenn die für den Zugriff auf SQL Server verwendete Anmeldung auf einer Windows-Gruppe basiert. Die in SQL Server integrierte Überwachungsfunktion (wird im weiteren Kursverlauf behandelt) profitiert davon, ebenso wie Überwachungen aller Aktionen auf Ebene des einzelnen Benutzers.

# Unterrichtseinheit 3

## **Autorisieren von Benutzern für den Zugriff auf Ressourcen**

### **Inhalt:**

<b>Lektion 1:</b> Autorisieren des Benutzerzugriffs auf Objekte	2
<b>Lektion 2:</b> Autorisieren von Benutzern zum Ausführen von Code	4
<b>Lektion 3:</b> Konfigurieren von Berechtigungen auf Schemaebene	6
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	8
Fragen und Antworten zur Zusammenfassung der Übungseinheit	9

## Lektion 1

# Autorisieren des Benutzerzugriffs auf Objekte

### Inhalt:

Fragen und Antworten	3
Vorführung: Autorisieren des Benutzerzugriffs auf Objekte	3

## Fragen und Antworten

**Frage:** Wozu dient die REFERENCES-Berechtigung?

**Antwort:** Die REFERENCES-Berechtigung wird verwendet, bevor eine Fremdschlüsselbeziehung das Objekt als Ziel angeben kann, und sie ist nur erforderlich, wenn es keine anderen Berechtigungen zu dem Objekt gibt, auf das verwiesen wird.

## Vorführung: Autorisieren des Benutzerzugriffs auf Objekte

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie die **Setup.cmd** im Ordner **D:\Demofiles\Mod03** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Klicken Sie auf der Taskleiste auf **Microsoft SQL Server Management Studio**.
5. Klicken Sie im Dialogfeld **Verbindung mit Server herstellen** auf **Verbinden**.
6. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie dann auf **Datei**.
7. Navigieren Sie im Dialogfeld **Datei öffnen** zu **D:\Demofiles\Mod03**, klicken Sie auf **AuthorizingUserAccessToObjects.sql**, und klicken Sie dann auf **Öffnen**.
8. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um einen Benutzer für die Vorführung zu erstellen.
9. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um die Liste der Serverprinzipale abzufragen. Beachten Sie **Mod03Login** am Ende der Liste.
10. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um die Liste der Datenbankprinzipale abzufragen. Beachten Sie erneut den Eintrag **Mod03Login** in der Liste.
11. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um **Mod03Login** die SELECT-Berechtigungen für die Tabelle **Product** zu gewähren.
12. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um den Ausführungskontext zu ändern.
13. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Berechtigungen zu testen. Beachten Sie, dass Sie in der Tabelle **Product**, für die Ihnen Berechtigungen gewährt wurden, eine Auswahl treffen können, jedoch nicht in der Tabelle **ProductInventory**.
14. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um den Ausführungskontext zurückzusetzen.
15. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um **Mod03Login** die SELECT-Berechtigungen für bestimmte Spalten in der Tabelle **ProductInventory** zu gewähren.
16. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um den Ausführungskontext zu ändern.
17. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um die Berechtigungen zu testen. Beachten Sie, dass die erste Abfrage zum Auswählen der beiden bestimmten Spalten ausgeführt wird, Sie können jedoch nicht alle Spalten aus der Tabelle **ProductInventory** auswählen.
18. Führen Sie den Code unter der Überschrift für **Schritt 11** aus, um den Ausführungskontext zurückzusetzen.
19. Klicken Sie im Menü **Datei** auf **Schließen**.
20. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Autorisieren von Benutzern zum Ausführen von Code

### Inhalt:

Fragen und Antworten	5
Vorführung: Autorisieren von Benutzern zum Ausführen von Code	5

## Fragen und Antworten

**Frage:** Mit welcher Berechtigung kann ein Benutzer die Definition einer gespeicherten Prozedur ändern?

- CHANGE
- CHANGE DEFINITION
- ALTER
- ALTER DEFINITION
- 

**Antwort:**

- CHANGE
- CHANGE DEFINITION
- ALTER
- ALTER DEFINITION
- 

## Vorführung: Autorisieren von Benutzern zum Ausführen von Code

### Vorführungsschritte

1. Zeigen Sie in SQL Server Management Studio im Menü **Datei** auf **Öffnen**, und klicken Sie dann auf **Datei**.
2. Navigieren Sie im Dialogfeld **Datei öffnen** zu **D:\Demofiles\Mod03**, klicken Sie auf **AuthorizingUsersToExecuteCode.sql**, und klicken Sie dann auf **Öffnen**.
3. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um den Datenbankkontext zu ändern.
4. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um den Ausführungskontext zu ändern.
5. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um zu versuchen, die gespeicherte Prozedur **uspGetManagerEmployees** auszuführen. Beachten Sie, dass die Berechtigung verweigert wird.
6. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um den Ausführungskontext zurückzusetzen.
7. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um EXECUTE-Berechtigungen für die gespeicherte Prozedur zu gewähren.
8. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um den Ausführungskontext zu ändern.
9. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um zu versuchen, die gespeicherte Prozedur **uspGetManagerEmployees** erneut auszuführen. Beachten Sie, dass der Code dieses Mal ausgeführt wird.
10. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um zu versuchen, die **ufnGetStock**-Funktion auszuführen. Beachten Sie, dass die Berechtigung verweigert wird.
11. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um den Ausführungskontext zurückzusetzen.
12. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um der Funktion EXECUTE-Berechtigungen zu gewähren.
13. Führen Sie den Code unter der Überschrift für **Schritt 11** aus, um den Ausführungskontext zu ändern und die neue Berechtigung zu testen. Beachten Sie, dass die Funktion nun erwartungsgemäß funktioniert.
14. Klicken Sie im Menü **Datei** auf **Schließen**.
15. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Konfigurieren von Berechtigungen auf Schemaebene

### Inhalt:

Fragen und Antworten	7
Vorführung: Konfigurieren von Berechtigungen auf Schemaebene	7

## Fragen und Antworten

**Frage:** Richtig oder falsch? Wenn ein Benutzer nicht über ein Standardschema verfügt, übernimmt SQL Server das **Gast**-Schema.

- ( ) Richtig
- ( ) Falsch

**Antwort:**

- ( ) Richtig
- (√) Falsch

## Vorführung: Konfigurieren von Berechtigungen auf Schemaebene

### Vorführungsschritte

1. Zeigen Sie in SQL Server Management Studio im Menü **Datei** auf **Öffnen**, und klicken Sie dann auf **Datei**.
2. Navigieren Sie im Dialogfeld **Datei öffnen** zu **D:\Demofiles\Mod03**, klicken Sie auf **ConfiguringPermissionsAtSchemaLevel.sql**, und klicken Sie dann auf **Öffnen**.
3. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um den Datenbankkontext zu ändern.
4. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um die Berechtigung zur gespeicherten Prozedur **uspGetManagerEmployees** zu widerrufen.
5. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um zu bestätigen, dass die Berechtigung widerrufen wurde.
6. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um EXECUTE-Berechtigungen für das **dbo**-Schema zu gewähren.
7. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um zu versuchen, zu bestätigen, dass die Berechtigung zu dem Schema und der darin gespeicherten Prozedur gewährt wurde.
8. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Berechtigung zum Ausführen der gespeicherten Prozedur zu verweigern.
9. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um zu bestätigen, dass die Berechtigung verweigert wurde.
10. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um den Datenbankkontext zu ändern.
11. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um eine neue Funktion zu erstellen.
12. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um festzustellen, welche Berechtigungen die Option für die Auswahl aus einem Schema implizieren.
13. Führen Sie den Code unter der Überschrift für **Schritt 11** aus, um festzustellen, welche Berechtigungen die Option zum Anzeigen der Definition eines Objekts implizieren.
14. Führen Sie den Code unter der Überschrift für **Schritt 12** aus, um festzustellen, welche Berechtigungen die Option für die Auswahl aus einem Objekt implizieren.
15. Führen Sie den Code unter der Überschrift für **Schritt 13** aus, um den Benutzer und die Anmeldung zu verwerfen.
16. Klicken Sie im Menü **Datei** auf **Schließen**.
17. Schließen Sie SQL Server Management Studio.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

Das Zuweisen von Berechtigungen auf Schemaebene kann Ihre Sicherheitsarchitektur vereinfachen.

## Fragen zur Lernzielkontrolle

**Frage:** Wie unterscheidet SQL Server im Hinblick auf Berechtigungen zwischen ANSI und SQL?

**Antwort:** Folglich stellt ANSI SQL keine DENY-Anweisung bereit.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Autorisieren von Benutzern für den Zugriff auf Ressourcen

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Ihr Unternehmen muss den Datenzugriff anhand einzelner Windows-Benutzer nachverfolgen. Heißt das, Anmeldungen dürfen nicht aus Windows-Gruppen stammen?

**Antwort:** Nein. SQL Server kann mithilfe der `SUSER_NAME`-Funktion auf einzelne Windows-Identitäten zugreifen, selbst wenn die für den Zugriff auf SQL Server verwendete Anmeldung auf einer Windows-Gruppe basiert.

# Unterrichtseinheit 4

## Schützen von Daten durch Verschlüsselung und Überwachung

### Inhalt:

Lektion 1: Optionen zum Überwachen des Datenzugriffs in SQL Server	2
Lektion 2: Implementieren von SQL Server Audit	5
Lektion 3: Verwalten von SQL Server Audit	8
Lektion 4: Schützen von Daten durch Verschlüsselung	10
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	14
Fragen und Antworten zur Zusammenfassung der Übungseinheit	15

## Lektion 1

# Optionen zum Überwachen des Datenzugriffs in SQL Server

### Inhalt:

Fragen und Antworten	3
Vorführung: Überwachung mit temporalen Tabellen	4

## Fragen und Antworten

Kategorisieren Sie die Überwachungsmethoden in der entsprechenden Kategorie. Geben Sie Ihre Antwort an, indem Sie rechts neben jedem Element die Kategoriennummer notieren.

Elemente	
1	Trigger
2	SQL Server Profiler
3	Temporale Tabellen

Kategorie 1	Kategorie 2
Erfasst Änderungen an Daten- oder Datenbankobjekten	Erfasst DML-Anweisungen oder DDL-Anweisungen

**Antwort:**

Kategorie 1	Kategorie 2
Erfasst Änderungen an Daten- oder Datenbankobjekten	Erfasst DML-Anweisungen oder DDL-Anweisungen
Trigger Temporale Tabellen	SQL Server Profiler

## Vorführung: Überwachung mit temporalen Tabellen

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Starten Sie SQL Server Management Studio, und stellen Sie mithilfe der SQL Server-Authentifizierung eine Verbindung mit Ihrer Azure-Instanz her, in der die **AdventureWorksLT**-Datenbank ausgeführt wird. Geben Sie in das Feld **Anmeldung Student** ein, geben Sie in das Feld **Kennwort Pa55w.rd** ein, und klicken Sie dann auf **Verbinden**.
3. Öffnen Sie die Projektmappe **Demo.ssmssl** im Ordner **D:\Demofiles\Mod04\Demo**.
4. Öffnen Sie die Abfrage **Demo 01 - temporal table audit.sql**, und stellen Sie eine Verbindung zur **AdventureWorksLT**-Datenbank her.
5. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine temporäre Tabelle mit Systemversionsverwaltung zu erstellen.
6. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um einige Beispieldaten einzufügen.
7. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um eine Zeile zu aktivieren.
8. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um die aktuelle und Verlaufstabelle zu untersuchen, aus denen die temporale Tabelle besteht.
9. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um das Verhalten der FOR SYSTEM TIME ALL-Unterklausel aufzuzeigen.
10. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um das Verhalten der FOR SYSTEM TIME AS OF-Unterklausel aufzuzeigen.
11. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um aufzuzeigen, dass die Verlaufstabelle nicht bearbeitet werden kann. Beide Befehle generieren einen Fehler.
12. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um aufzuzeigen, dass ein Benutzer mit der Berechtigung zum direkten Aktualisieren der Tabelle irreführende Informationen einfügen kann.
13. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um die temporale Tabelle nach der Aktualisierung erneut zu untersuchen.
14. Führen Sie nach Abschluss der Vorführung den Code unter der Überschrift für **Schritt 11** aus, um die Vorführungsobjekte zu entfernen.
15. Schließen Sie SQL Server Management Studio, ohne die Änderungen zu speichern.

## Lektion 2

# Implementieren von SQL Server Audit

### Inhalt:

Fragen und Antworten	6
Ressourcen	6
Vorführung: Verwenden von SQL Server Audit	6
Vorführung: Verwenden von benutzerdefinierten Überwachungsereignissen	7

## Fragen und Antworten

**Frage:** Welcher der folgenden Komponenten gehört nicht zur SQL Server Audit-Architektur?

- Ziel
- Zielgruppe
- Serverüberwachung
- Spezifikation der Datenbanküberwachung
- Spezifikation der Serverüberwachung

**Antwort:**

- Ziel
- Zielgruppe
- Serverüberwachung
- Spezifikation der Datenbanküberwachung
- Spezifikation der Serverüberwachung

## Ressourcen

### Einführung in erweiterte Ereignisse

 **Weitere Informationen:** Da erweiterte Ereignisse die Basis für SQL Server Audit sind, können Sie sich dazu entscheiden, Ihr eigenes Überwachungssystem auf Grundlage von erweiterten Ereignissen zu schreiben. Weitere Informationen zum Arbeiten mit erweiterten Ereignissen finden Sie in Unterrichtseinheit 12 dieses Kurses unter *Verfolgen des Zugriffs auf SQL Server mit erweiterten Ereignissen*.

## Vorführung: Verwenden von SQL Server Audit

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie **Setup.cmd** im Ordner **D:\Demofiles\Mod04** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**, und warten Sie, bis das Skript beendet wurde.
4. Starten SQL Server Management Studio und stellen Sie über die Windows-Authentifizierung einer Verbindung zu **MIA-SQL** her.
5. Öffnen Sie die Projektmappe **Demo.ssmssl** im Ordner **D:\Demofiles\Mod04\Demo**.
6. Öffnen Sie die Abfrage **Demo 02 - audit.sql**.
7. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine neue Überwachung zu erstellen.
8. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine neue Überwachung zu aktivieren.
9. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um eine Spezifikation für die Serverüberwachung zur neuen Überwachung hinzuzufügen.

10. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um eine Spezifikation für die Datenbanküberwachung zur neuen Überwachung hinzuzufügen.
11. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um die Spezifikation für die Datenbanküberwachung durch Hinzufügen einer weiteren Aktionsgruppe zu ändern.
12. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Überwachungsmetadaten zu überprüfen.
13. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um die Metadaten der Spezifikation für die Serverüberwachung zu überprüfen.
14. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um die Metadaten der Spezifikation für die Datenbanküberwachung zu überprüfen.
15. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um die für diese Vorführung erstellte Überwachung und die Spezifikationen zu entfernen.
16. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Verwenden von benutzerdefinierten Überwachungsereignissen

### Vorführungsschritte

1. Öffnen Sie im Projektmappen-Explorer die Abfrage **Demo 03 - custom audit.sql**.
2. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine neue Überwachung zu erstellen.
3. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine Spezifikation für die Serverüberwachung einschließlich der USER\_DEFINED\_AUDIT\_GROUP-Aktionsgruppe zu erstellen.
4. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um **sp\_audit\_write** direkt aufzurufen.
5. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um aufzuzeigen, wie das benutzerdefinierte Ereignis in der Überwachungsprotokolldatei dargestellt wird.
6. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um eine gespeicherte Prozedur zu erstellen, die **sp\_audit\_write** verwendet. Die gespeicherte Prozedur protokolliert ein benutzerdefiniertes Überwachungsereignis, wenn der auf eine Zeile der Tabelle **Sales.OrderDetails** angewendete Rabatt mehr als 30 Prozent beträgt.
7. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die neue gespeicherte Prozedur zwei Mal aufzurufen. Nach dem zweiten Aufruf sollte ein benutzerdefiniertes Überwachungsereignis protokolliert werden, da der angewendete Rabatt 45 Prozent beträgt.
8. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um zu überprüfen, wie das benutzerdefinierte Ereignis in der Überwachungsprotokolldatei erfasst wurde.
9. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um die Überwachungsobjekte der Vorführung zu verwerfen.
10. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Verwalten von SQL Server Audit

### Inhalt:

Fragen und Antworten	9
Vorführung: Anzeigen der Ausgabe von SQL Server Audit	9

## Fragen und Antworten

**Frage:** Welches der folgenden Ziele dient nicht für SQL Server Audit?

- Datei
- Windows-Anwendungsprotokoll
- Windows-Sicherheitsprotokoll
- Ringpuffer

**Antwort:**

- Datei
- Windows-Anwendungsprotokoll
- Windows-Sicherheitsprotokoll
- Ringpuffer

## Vorführung: Anzeigen der Ausgabe von SQL Server Audit

### Vorführungsschritte

1. Öffnen Sie im Projektmappen-Explorer die Abfrage **Demo 04 - audit output.sql**.
2. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine Überwachung mit einer Zieldatei zu erstellen.
3. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine Überwachung mit einem Windows-Anwendungsprotokollziel zu erstellen.
4. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um zu jeder Überwachung eine Spezifikation hinzuzufügen, die SELECT-Anweisungen erfasst, die für das **salesapp1.Sales**-Schema ausgeführt werden.
5. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um eine ausgewählte Anweisung auszuführen, die überwacht wird.
6. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um die Inhalte der Überwachungszieldatei zu überprüfen. Stellen Sie die nützlichsten Felder heraus.
7. Klicken Sie mit der rechten Maustaste auf die Schaltfläche **Start**, und klicken Sie dann auf **Ereignisanzeige**.
8. Erweitern Sie in der Ereignisanzeige den Knoten **Windows-Protokolle**, klicken Sie anschließend auf **Anwendung**. Bei dem Überwachungseintrag handelt es sich um den aktuellsten im Anwendungsbereich mit dem Quellwert MSSQLSERVER. Veranschaulichen Sie den Eintrag und schließen Sie dann die Ereignisanzeige.
9. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um die Überwachungsobjekte der Vorführung zu entfernen.
10. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 4

# Schützen von Daten durch Verschlüsselung

### Inhalt:

Fragen und Antworten	11
Ressourcen	12
Vorführung: Verwenden der dynamischen Datenmaskierung	12

## Fragen und Antworten

Kategorisieren Sie die einzelnen Elemente mithilfe des entsprechenden SQL Server-Features. Geben Sie Ihre Antwort an, indem Sie rechts neben jedem Element die Kategorienummer notieren.

Elemente	
1	Verschlüsselte, gespeicherte Daten
2	Verschlüsselte, gespeicherte Daten und während Übertragungen verschlüsselte Daten
3	Verschleierte Datenwerte
4	Verschlüsselung und Entschlüsselung wird von SQL Server durchgeführt
5	Verschlüsselung und Entschlüsselung finden in der Clientanwendung statt
6	In Klartext gespeicherte Daten
7	Agiert auf Datenbankebene
8	Agiert auf Spaltenebene

Kategorie 1	Kategorie 2	Kategorie 3
Transparente Datenverschlüsselung	Always Encrypted	Dynamische Datenmaskierung

**Antwort:**

Kategorie 1	Kategorie 2	Kategorie 3
Transparente Datenverschlüsselung	Always Encrypted	Dynamische Datenmaskierung
Verschlüsselte, gespeicherte Daten Verschlüsselung und Entschlüsselung wird von SQL Server durchgeführt Agiert auf Datenbankebene	Verschlüsselte, gespeicherte Daten und während Übertragungen verschlüsselte Daten Verschlüsselung und Entschlüsselung finden in der Clientanwendung statt Agiert auf Spaltenebene	Verschleierte Datenwerte In Klartext gespeicherte Daten

**Ressourcen****Transparente Datenverschlüsselung**

 **Weitere Informationen:** Die transparente Datenverschlüsselung ist in Azure SQL-Datenbank verfügbar. Weitere Informationen dazu finden Sie unter *Verschlüsselung mit Azure SQL-Datenbank* zu einem späteren Zeitpunkt dieser Lektion.

**Vorführung: Verwenden der dynamischen Datenmaskierung****Vorführungsschritte**

1. Öffnen Sie im Projektmappen-Explorer die Abfrage **Demo 05 - masking.sql**.
2. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um eine neue Tabelle mit maskierten Daten zu erstellen, gewähren Sie einem Testbenutzer die Berechtigung und fügen Sie die Testdaten ein.
3. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um aufzuzeigen, dass ein Administrator nicht maskierte Daten anzeigen kann.
4. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um aufzuzeigen, dass ein Benutzer, der nur über die SELECT-Berechtigung verfügt, die maskierten Daten anzeigen kann. Nehmen Sie sich etwas Zeit, um die maskierte Ausgabe mit den Tabellendefinitionen zu vergleichen.
5. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um eine Maske zur **home\_phone\_number**-Spalte hinzuzufügen.
6. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um die neue Maske aufzuzeigen.
7. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Maske aus der **salary**-Spalte zu entfernen.
8. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um aufzuzeigen, dass die Maske zu „salary“ nicht mehr vorhanden ist.

9. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um dem Testbenutzer die UNMASK-Berechtigung zu gewähren. Beachten Sie, dass es sich hierbei um eine Berechtigung auf Datenbankebene handelt.
10. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um die Auswirkung der UNMASK-Berechtigung zu veranschaulichen.
11. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um die Vorführungstabelle zu verwerfen.
12. Schließen Sie SQL Server Management Studio, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

Erwägen Sie bei der Planung einer Überwachungsimplementierung folgende bewährte Methoden:

- Wählen Sie die Option zum Herunterfahren von SQL Server bei einem Überwachungsfehler. Es macht normalerweise keinen Sinn, eine Überwachung einzurichten und anschließend Situationen vorzufinden, in denen Ereignisse auftreten, jedoch nicht überwacht werden können. Dieser Aspekt ist besonders wichtig in Umgebungen mit hohen Sicherheitsanforderungen.
- Stellen Sie sicher, dass Dateiüberwachungen auf Laufwerken mit großen Mengen an freiem Speicherplatz abgelegt sind und vergewissern Sie sich, dass der verfügbare Speicherplatz regelmäßig überwacht wird.

## Bewährte Methoden

Erwägen Sie bei der Planung der Implementierung einer Datenbankverschlüsselung folgende bewährte Methoden:

- Verwenden Sie zum Schutz des Datenbank Hauptschlüssels für die Masterdatenbank ein komplexes Kennwort.
- Sorgen Sie dafür, die zum Implementieren der transparenten Datenverschlüsselung verwendeten Zertifikate und privaten Schlüssel zu sichern und speichern Sie die Sicherungsdateien an einem sicheren Speicherort.
- Wenn Sie die Datenverschlüsselung in einem großen Unternehmen auf mehreren Servern implementieren, erwägen Sie, zum Verwalten der Verschlüsselungsschlüssel eine Lösung für die erweiterbare Schlüsselverwaltung zu verwenden.
- Wenn Sie Always Encrypted verwenden möchten, müssen Sie planen, wie Sie die Spaltenhauptschlüssel speichern, damit Anwendungen darauf zugreifen können, die Daten verschlüsseln und entschlüsseln müssen.

## Fragen zur Lernzielkontrolle

**Frage:** Sie möchten möglicherweise Aktionen durch einen Datenbankadministrator überwachen lassen. Woran könnten Sie beim Durchführen verborgener Aktionen erkennen, dass der Datenbankadministrator die Überwachung gestoppt hat?

**Antwort:** Änderungen am Überwachungsstatus werden protokolliert.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Verwenden der Überwachung und Verschlüsselung

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Welcher Typ der Always Encrypted-Verschlüsselung verschlüsselt konsistent den gleichen Klartextwert mit dem gleichen Zifferntext (vorausgesetzt, derselbe Verschlüsselungsschlüssel wird verwendet)?

- Deterministische Verschlüsselung
- Verschlüsselung nach dem Zufallsprinzip
- Keine der genannten Antworten

**Antwort:**

- Deterministische Verschlüsselung
- Verschlüsselung nach dem Zufallsprinzip
- Keine der genannten Antworten

# Unterrichtseinheit 5

## Wiederherstellungsmodelle und Sicherungsstrategien

### Inhalt:

Lektion 1: Grundlegendes zu Sicherungsstrategien	2
Lektion 2: SQL Server-Transaktionsprotokolle	5
Lektion 3: Planen von Sicherungsstrategien	7
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	9

## Lektion 1

# Grundlegendes zu Sicherungsstrategien

### Inhalt:

Fragen und Antworten	3
Vorführung: Sichern einer lokalen Datenbank in Microsoft Azure	3

## Fragen und Antworten

**Frage:** Welche Vorteile bietet die Verwendung der SQL Server-Sicherung mit Azure Blob Storage?

**Antwort:** Die SQL Server-Sicherung mit Azure Blob Storage bietet viele Vorteile, z. B.:

- Unbegrenzte Speicherkapazität
- Kein Kauf und keine Wartung von Hardware erforderlich
- Offsitesicherung, ohne dass Bänder transportiert werden müssen

## Vorführung: Sichern einer lokalen Datenbank in Microsoft Azure

### Vorführungsschritte

Installieren des Azure PowerShell-Moduls

1. Geben Sie im Startmenü **Windows PowerShell** ein. Klicken Sie dann mit der rechten Maustaste auf **Windows PowerShell™**, und klicken Sie auf **ISE als Administrator ausführen**.
2. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
3. Geben Sie an der Eingabeaufforderung **Install-Module AzureRM -AllowClobber** ein, und drücken Sie dann die EINGABETASTE.
4. Wenn die Meldung **Der NuGet-Anbieter ist erforderlich, um den Vorgang fortzusetzen** angezeigt wird, geben Sie **J** ein, und drücken Sie dann die **EINGABETASTE**.
5. Wenn die Meldung **Nicht vertrauenswürdiges Repository** angezeigt wird, geben Sie **A** ein, und drücken Sie dann die **EINGABETASTE**.
6. Warten Sie, bis die Installation abgeschlossen ist, und schließen Sie dann das PowerShell-Fenster.

Erstellen eines Speicherkontos

1. Führen Sie **Setup.cmd** im Ordner **D:\Demofiles\Mod05** als Administrator aus. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
2. Klicken Sie auf der Taskleiste auf **Internet Explorer**, und wechseln Sie zu **portal.azure.com**.
3. Melden Sie sich bei Ihrem Azure-Konto an, und klicken Sie im linken Blatt auf **Speicherkonten**.
4. Klicken Sie auf dem Blatt **Speicherkonten** auf **Hinzufügen**.
5. Geben Sie auf dem Blatt **Speicherkonto erstellen** die folgenden Details ein, und klicken Sie anschließend auf **Erstellen**:
  - a. **Name:** 21764+ihreinitialen+HeutigesDatum, z. B. 21764jhd20160421
  - b. **Bereitstellungsmodell:** Resource Manager
  - c. **Kontoart:** Speicher (allgemein, Version 1)
  - d. **Leistung:** Standard
  - e. **Replikation:** Zonenredundanter Speicher
  - f. **Abonnement:** Azure Pass
  - g. **Ressourcengruppe:** 21764C
  - h. **Standort:** Ihr nächstgelegener Standort
6. Das Speicherkonto wird erstellt. Minimieren Sie Internet Explorer.

Erstellen eines Speichercontainers und eines SAS-Tokens

1. Klicken Sie auf der Taskleiste mit der rechten Maustaste auf das Symbol **Windows PowerShell**, und klicken Sie dann auf **Windows PowerShell ISE**.
2. Klicken Sie im Menü **Datei** auf **Öffnen**.
3. Navigieren Sie im Dialogfeld **Öffnen** zu **D:\Demofiles\Mod05**, klicken Sie auf **ContainerSAS.ps1** und dann auf **Öffnen**.
4. Ändern Sie **\$accountName** in das Microsoft-Konto, das Ihrem Azure Pass zugeordnet ist.
5. Ändern Sie **\$storageAccountName** in den Namen des Speicherkontos, das Sie in der vorherigen Aufgabe erstellt haben.
6. Klicken Sie auf der Symbolleiste auf **Skript ausführen**.
7. Klicken Sie im Dialogfeld **Windows PowerShell ISE** auf **OK**.
8. Geben Sie im Dialogfeld **Bei Ihrem Konto anmelden** den Benutzernamen und das Kennwort Ihres Microsoft Azure-Kontos ein, und klicken Sie dann auf **Anmelden**.
9. Klicken Sie im Dialogfeld **Bestätigen** auf **Ja**, um das Konto zu löschen (keine Angst, das Konto wird nicht wirklich gelöscht).

**Hinweis:** Lassen Sie das Fenster geöffnet, da Sie die angezeigten Informationen in der nächsten Aufgabe benötigen.

#### Sichern einer Datenbank mit Azure Blob Storage

1. Starten Sie SQL Server Management Studio, und stellen Sie eine Verbindung mit der Instanz **MIA-SQL** her.
2. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie dann auf **Datei**.
3. Navigieren Sie im Dialogfeld **Datei öffnen** zu **D:\Demofiles\Mod05**, klicken Sie auf **AzureBackup.sql** und dann auf **Öffnen**.
4. Ersetzen Sie die zwei Instanzen des Eintrags **https://xxx.blob.core.windows.net/aw2018** in den Zeilen 2 und 11 durch den Namen der **URL des Cloud Blob-Containers** im PowerShell-Fenster.
5. Ersetzen Sie den Eintrag **sv=enter key here** durch die **Shared Access Signature** im PowerShell-Fenster.
6. Markieren Sie in SQL Server Management Studio die Anweisung unter dem Kommentar **Create credential**, und klicken Sie dann auf **Ausführen**.
7. Markieren Sie die Anweisungen unter dem Kommentar **Backup the database**, klicken Sie auf **Ausführen**, und warten Sie, bis der Sicherungsvorgang erfolgreich abgeschlossen wurde.
8. Klicken Sie in Internet Explorer auf dem Blatt **Alle Ressourcen** auf **Aktualisieren**, und klicken Sie dann auf den Namen von Ihrem **Speicherkonto (klassisch)**.
9. Klicken Sie auf dem Blatt Ihres Kontos unter **BLOB-DIENST** auf **Container** und dann auf **aw2016**.
10. Vergewissern Sie sich, dass die Sicherungsdatei **logtest.bak** erstellt wurde.
11. Schließen Sie Internet Explorer und Windows PowerShell.
12. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Lektion 2

# SQL Server-Transaktionsprotokolle

### Inhalt:

Fragen und Antworten	6
Vorführung: Protokolle und vollständige Wiederherstellung	6

## Fragen und Antworten

**Frage:** Was sind die spezifischen Merkmale von Transaktionsprotokoll-Wiederherstellungen?

**Antwort:** Zeitpunktwiederherstellung und die Möglichkeit, bis zur Fehlerquelle wiederherzustellen, wenn nur Datendateien beschädigt sind.

## Vorführung: Protokolle und vollständige Wiederherstellung

### Vorführungsschritte

1. Erweitern Sie im Objekt-Explorer von SQL Server Management Studio den Eintrag **Datenbanken**, klicken Sie mit der rechten Maustaste auf **LogTest**, und klicken Sie dann auf **Eigenschaften**.
2. Vergewissern Sie sich im Dialogfeld **Datenbankeigenschaften - LogTest** auf der Seite **Optionen**, dass das **Wiederherstellungsmodell** auf **Vollständig** festgelegt ist, und klicken Sie dann auf **Abbrechen**.
3. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie dann auf **Datei**.
4. Navigieren Sie im Dialogfeld **Datei öffnen** zu **D:\Demofiles\Mod05**, klicken Sie auf **LogComparisonTest.sql** und dann auf **Öffnen**.
5. Markieren Sie den Code unter dem Kommentar **Perform a full database backup**, und klicken Sie dann auf **Ausführen**.
6. Markieren Sie den Code unter dem Kommentar **View log file space**, und klicken Sie dann auf **Ausführen**. Nehmen Sie die Protokollgröße und den im Protokoll **LogTest** verwendeten Speicherplatz zur Kenntnis.
7. Markieren Sie den Code unter dem Kommentar **Insert data**, und klicken Sie dann auf **Ausführen**, um 10.000 Zeilen einzufügen.
8. Markieren Sie den Code unter dem Kommentar **View log file space**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass die Protokollgröße und der in der Protokolldatei **LogTest** verwendete Speicherplatz zugenommen haben.
9. Markieren Sie den Code unter dem Kommentar **Issue checkpoint**, und klicken Sie dann auf **Ausführen**, um SQL Server zu zwingen, einen Prüfpunkt auszuführen und die geänderten Seiten auf Datenträger zu leeren.
10. Markieren Sie den Code unter dem Kommentar **View log file space**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass der in der Protokolldatei **LogTest** verwendete Speicherplatz nicht abgenommen hat.
11. Markieren Sie den Code unter dem Kommentar **Check log status**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass SQL Server auf eine Protokollsicherung wartet, bevor die Protokolldatei gekürzt werden kann.
12. Markieren Sie den Code unter dem Kommentar **Perform a log backup**, und klicken Sie dann auf **Ausführen**.
13. Markieren Sie den Code unter dem Kommentar **Verify log file truncation**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass der in der Protokolldatei **LogTest** verwendete Speicherplatz abgenommen hat, da das Protokoll gekürzt wurde.
14. Schließen Sie SSMS, ohne die Änderungen zu speichern.

## Lektion 3

# Planen von Sicherungsstrategien

### **Inhalt:**

Fragen und Antworten

8

## Fragen und Antworten

**Frage:** Welche Art von Datenbank eignet sich gut für eine Strategie auf Basis vollständiger Sicherungen?

**Antwort:** Eine kleine Datenbank, die schnell gesichert werden kann.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

- Planen Sie Ihre Sicherungsstrategie sorgfältig.
- Planen Sie die Sicherungsstrategie in Verbindung mit den Geschäftsanforderungen.
- Wählen Sie das geeignete Datenbank-Wiederherstellungsmodell.
- Planen Sie die Größe des Transaktionsprotokolls basierend auf der Häufigkeit der Transaktionsprotokollsicherung.
- Ziehen Sie die Nutzung von differenziellen Sicherungen sowie Teil- und Dateigruppensicherungen in Erwägung, um die Wiederherstellung zu beschleunigen.

## Fragen zur Lernzielkontrolle

**Frage:** Wann kann eine Strategie auf Basis vollständiger Datenbanksicherungen geeignet sein?

**Antwort:** Wenn es in einem Notfall ausreichend ist, die Datenbank bis zu den Punkten vollständiger Datenbanksicherungen wiederherzustellen.

# Unterrichtseinheit 6

## Sichern von SQL Server-Datenbanken

### Inhalt:

<b>Lektion 1:</b> Sichern von Datenbanken und Transaktionsprotokollen	2
<b>Lektion 2:</b> Verwalten von Datenbanksicherungen	5
<b>Lektion 3:</b> Erweiterte Datenbankoptionen	7
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	10

## Lektion 1

# Sichern von Datenbanken und Transaktionsprotokollen

### **Inhalt:**

Vorführung: Durchführen von Sicherungen

3

## Vorführung: Durchführen von Sicherungen

### Vorführungsschritte

Durchführen einer vollständigen Datenbanksicherung

1. Vergewissern Sie sich, dass die virtuellen Computer **21764C-MIA-DC** und **21764C-MIA-SQL** gestartet wurden, und melden Sie sich dann als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie im Ordner **D:\Demofiles\Mod06** die Datei **Setup.cmd** als Administrator aus. Warten Sie auf den Abschluss des Skripts, und drücken Sie dann die EINGABETASTE.
3. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine **MIA-SQL** her.
4. Erweitern Sie im Objekt-Explorer den Eintrag **Datenbanken**, klicken Sie mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, und klicken Sie auf **Sichern**.
5. Vergewissern Sie sich im Dialogfeld **Datenbank sichern - AdventureWorks**, dass **Sicherungstyp** auf **Vollständig** festgelegt ist.
6. Wählen Sie im Abschnitt **Ziel** jeden vorhandenen Dateipfad aus, klicken Sie auf **Entfernen**, und klicken Sie dann auf **Hinzufügen**.
7. Geben Sie im Dialogfeld **Sicherungsziel auswählen** im Feld **Dateiname** den Namen **D:\Demofiles\Mod06\Demo\AW.bak** ein, und klicken Sie auf **OK**.
8. Im Dialogfeld **Datenbank sichern - AdventureWorks** ist auf der Seite **Medienoptionen** standardmäßig die Option zum Anfügen an einen vorhandenen Mediensatz ausgewählt. In diesem Fall ist noch kein Mediensatz vorhanden, daher wird ein neuer erstellt. Auch Sicherungssätze sind keine zum Überschreiben vorhanden.
9. Im Dialogfeld **Datenbank sichern - AdventureWorks** sind auf der Seite **Sicherungsoptionen** Standardeinstellungen für Sicherungsname und Ablauf festgelegt.
10. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Dropdownliste **Skript** auf **Skript für Aktion in Fenster 'Neue Abfrage' schreiben**, und klicken Sie dann auf **OK**.
11. Wenn die Sicherung erfolgreich abgeschlossen wurde, klicken Sie auf **OK**.
12. Sehen Sie sich im Abfragebereich die Transact-SQL-Anweisung **BACKUP** an, die zum Sichern der Datenbank verwendet wurde.
13. Sehen Sie sich den Ordner **D:\Demofiles\Mod06\Demo** an, und beachten Sie die Größe der Datei **AW.bak**.

Durchführen einer differenziellen Sicherung

1. Öffnen Sie in SQL Server Management Studio die Skriptdatei **UpdatePrices.sql** im Ordner **D:\Demofiles\Mod06\Demo**, und klicken Sie auf **Ausführen**. Dieses Skript aktualisiert die Tabelle **Production.Product** in der **AdventureWorks**-Datenbank.
2. Klicken Sie im Objekt-Explorer unter **Datenbanken** mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, und klicken Sie auf **Sichern**.
3. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Liste **Sicherungstyp** auf **Differenziell**.
4. Vergewissern Sie sich, dass im Abschnitt **Ziel** die Datei **D:\Demofiles\Mod06\Demo\AW.bak** als einziges Sicherungsmedium aufgeführt wird.

- Überprüfen Sie, ob im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Medienoptionen** die Option zum Anfügen an den vorhandenen Mediensatz ausgewählt ist.
- Ändern Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Sicherungsoptionen** den Eintrag im Feld **Name** in **AdventureWorks-Diff Database Backup**.
- Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Dropdownliste **Skript** auf **Skript für Aktion in Fenster 'Neue Abfrage' schreiben**, und klicken Sie dann auf **OK**.
- Wenn die Sicherung erfolgreich abgeschlossen wurde, klicken Sie auf **OK**.
- Sehen Sie sich im Abfragebereich die Transact-SQL-Anweisung BACKUP an, die zum Sichern der Datenbank verwendet wurde. Beachten Sie, dass sie die Option WITH DIFFERENTIAL enthält.
- Sehen Sie sich den Ordner **D:\Demofiles\Mod06\Demo** an. Die Datei **AW.bak** ist größer geworden, allerdings nicht viel, da die zweite Sicherung nur die Erweiterungen mit Seiten umfasst, die seit der vollständigen Sicherung geändert wurden.

#### Durchführen einer Transaktionsprotokollsicherung

- Wechseln Sie in SQL Server Management Studio zum Skript **UpdatePrices.sql**, das Sie bereits zuvor geöffnet haben, und klicken Sie auf **Ausführen**, um die Tabelle **Production.Product** in der **AdventureWorks**-Datenbank erneut zu aktualisieren.
- Klicken Sie im Objekt-Explorer unter **Datenbanken** mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, und klicken Sie auf **Sichern**.
- Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Liste **Sicherungstyp** auf **Transaktionsprotokoll**.
- Vergewissern Sie sich, dass im Abschnitt **Ziel** die Datei **D:\Demofiles\Mod06\Demo\AW.bak** als einziges Sicherungsmedium aufgeführt wird.
- Überprüfen Sie, ob im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Medienoptionen** die Option zum Anfügen an den vorhandenen Mediensatz ausgewählt ist. Überprüfen Sie außerdem, ob die Option zum Kürzen des Transaktionsprotokolls ausgewählt ist.
- Ändern Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Sicherungsoptionen** den Eintrag im Feld **Name** in **AdventureWorks-Transaction Log Backup**.
- Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Dropdownliste **Skript** auf **Skript für Aktion in Fenster 'Neue Abfrage' schreiben**, und klicken Sie dann auf **OK**.
- Wenn die Sicherung erfolgreich abgeschlossen wurde, klicken Sie auf **OK**.
- Sehen Sie sich im Abfragebereich die Transact-SQL-Anweisung BACKUP an, die zum Sichern der Datenbank verwendet wurde. Beachten Sie, dass die Anweisung dieses Mal BACKUP LOG lautet.
- Sehen Sie sich den Ordner **D:\Demofiles\Mod06** an. Die Datei **AW.bak** ist größer geworden, allerdings nicht viel, da die dritte Sicherung nur die Transaktionsprotokolleinträge für Datenänderungen seit der vollständigen Sicherung enthält.
- Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Verwalten von Datenbanksicherungen

### **Inhalt:**

Vorführung: Überprüfen von Sicherungen

6

## Vorführung: Überprüfen von Sicherungen

### Vorführungsschritte

Anzeigen des Berichts über Sicherungs- und Wiederherstellungsereignisse

1. Klicken Sie in SQL Server Management Studio im Objekt-Explorer unter **Datenbanken** mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Berichte**, zeigen Sie auf **Standardberichte**, und klicken Sie dann auf **Sicherungs- und Wiederherstellungsereignisse**.
2. Erweitern Sie im Bericht **Sicherungs- und Wiederherstellungsereignisse [AdventureWorks]** den Eintrag **Erfolgreiche Sicherungsvorgänge**, und sehen Sie sich die Sicherungsvorgänge an, die für diese Datenbank ausgeführt wurden.
3. Erweitern Sie in der Spalte **Medientyp** jeden der Einträge **Festplatte (temporär)**, um Details der Sicherungsmediensatzdateien anzuzeigen.

Abfragen der Sicherungsverlaufstabellen

1. Öffnen Sie in SQL Server Management Studio die Skriptdatei **VerifyingBackups.sql** im Ordner **D:\Demofiles\Mod06\Demo**.
2. Markieren Sie den Code unter dem Kommentar **View backup history**, und klicken Sie dann auf **Ausführen**.
3. Sehen Sie sich die Abfrageergebnisse an. Diese zeigen die Sicherungen, die für die **AdventureWorks**-Datenbank ausgeführt wurden.
4. Beachten Sie, dass Zeile 21 des Codes den derzeit festgelegten Abrufzeitraum auf 30 Tage beschränkt. Diese Beschränkung kann durch Ändern der Zahl 30 oder durch Entfernen dieser Zeile geändert werden.

Überprüfen der Sicherungsmedien

1. Markieren Sie den Code unter dem Kommentar **Use RESTORE HEADERONLY**, und klicken Sie dann auf **Ausführen**.
2. Sehen Sie sich die Abfrageergebnisse an. Diese zeigen die Sicherungen im Sicherungsmedium **AW.bak** an.
3. Markieren Sie den Code unter dem Kommentar **Use RESTORE FILELISTONLY**, und klicken Sie dann auf **Ausführen**.
4. Sehen Sie sich die Abfrageergebnisse an. Diese zeigen die in den Sicherungen enthaltenen Datenbankdateien an.
5. Markieren Sie den Code unter dem Kommentar **Use RESTORE VERIFYONLY**, und klicken Sie dann auf **Ausführen**.
6. Sehen Sie sich die zurückgegebene Meldung an. Diese sollte anzeigen, dass die Sicherung gültig ist.

## Lektion 3

# Erweiterte Datenbankoptionen

### Inhalt:

Vorführung: Verwenden der Sicherungskomprimierung	8
Vorführung: Verwenden der Sicherungsverschlüsselung	8

## Vorführung: Verwenden der Sicherungskomprimierung

### Vorführungsschritte

Verwenden der Sicherungskomprimierung

1. Klicken Sie im Objekt-Explorer von SQL Server Management Studio unter **Datenbanken** mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, und klicken Sie auf **Sichern**.
2. Vergewissern Sie sich im Dialogfeld **Datenbank sichern - AdventureWorks**, dass **Sicherungstyp** auf **Vollständig** festgelegt ist.
3. Wählen Sie im Abschnitt **Ziel** den vorhandenen Dateipfad aus, klicken Sie auf **Entfernen**, und klicken Sie dann auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Sicherungsziel auswählen** im Feld **Dateiname** den Namen **D:\Demofiles\Mod06\Demo\AW\_Comp.bak** ein, und klicken Sie auf **OK**.
5. Im Dialogfeld **Datenbank sichern - AdventureWorks** ist auf der Seite **Medienoptionen** standardmäßig die Option zum Anfügen an einen vorhandenen Mediensatz ausgewählt. In diesem Fall ist noch kein Mediensatz vorhanden, daher wird ein neuer erstellt. Auch Sicherungssätze sind keine zum Überschreiben vorhanden.
6. Ändern Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Sicherungsoptionen** den Eintrag im Feld **Name** in **AdventureWorks-Compressed Backup**.
7. Klicken Sie in der Liste **Sicherungskomprimierung festlegen** auf **Sicherung komprimieren**.
8. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Dropdownliste **Skript** auf **Skript für Aktion in Fenster 'Neue Abfrage' schreiben**, und klicken Sie dann auf **OK**.
9. Wenn die Sicherung erfolgreich abgeschlossen wurde, klicken Sie auf **OK**.
10. Sehen Sie sich im Abfragebereich die Transact-SQL-Anweisung BACKUP an, die zum Sichern der Datenbank verwendet wurde. Beachten Sie, dass die Option COMPRESSION angegeben wurde.
11. Sehen Sie sich den Ordner **D:\Demofiles\Mod06\Demo** an, und beachten Sie die Größe der Datei **AW\_Comp.bak**. Diese Datei sollte erheblich kleiner sein als die Datei **AW.bak** nach der vollständigen Datenbanksicherung in der vorherigen Vorführung.
12. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Verwenden der Sicherungsverschlüsselung

### Vorführungsschritte

Erstellen eines Datenbank-Hauptschlüssels

1. Erstellen Sie mit dem Datei-Explorer einen Ordner namens **D:\Backups**.
2. Öffnen Sie in SQL Server Management Studio die Skriptdatei **EncyptionKeys.sql** im Ordner **D:\Demofiles\Mod06\Setupfiles**.
3. Markieren Sie den Code unter dem Kommentar **Create a database master key**, und klicken Sie dann auf **Ausführen**.
4. Markieren Sie den Code unter dem Kommentar **Back up the database master key**, und klicken Sie dann auf **Ausführen**.

Erstellen eines Zertifikats

1. Markieren Sie den Code unter dem Kommentar **Create a certificate**, und klicken Sie dann auf **Ausführen**.

2. Markieren Sie den Code unter dem Kommentar **Back up the certificate and its private key**, und klicken Sie dann auf **Ausführen**.

Verschlüsseln einer Datenbanksicherung

1. Klicken Sie im Objekt-Explorer unter **Datenbanken** mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, und klicken Sie dann auf **Sichern**.
2. Vergewissern Sie sich im Dialogfeld **Datenbank sichern - AdventureWorks**, dass **Sicherungstyp** auf **Vollständig** festgelegt ist.
3. Wählen Sie im Abschnitt **Ziel** den vorhandenen Dateipfad aus, klicken Sie auf **Entfernen**, und klicken Sie dann auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Sicherungsziel auswählen** im Feld **Dateiname** den Namen **D:\Backups\AW\_Encrypt.bak** ein, und klicken Sie dann auf **OK**.
5. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Medienoptionen** auf **Auf neuen Mediensatz sichern und alle vorhandenen Sicherungssätze löschen**.
6. Geben Sie im Feld **Name für neuen Mediensatz** den Namen **Encrypted Backup** ein.
7. Ändern Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Seite **Sicherungsoptionen** den Eintrag im Feld **Name** in **AdventureWorks-Encrypted Backup**.
8. Klicken Sie in der Liste **Sicherungskomprimierung festlegen** auf **Sicherung komprimieren**.
9. Aktivieren Sie im Abschnitt **Verschlüsselung** das Kontrollkästchen **Sicherung verschlüsseln**, vergewissern Sie sich, dass der Algorithmus **AES 256** ausgewählt ist, und wählen Sie das zuvor erstellte **AdventureWorks**-Zertifikat aus.
10. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** in der Dropdownliste **Skript** auf **Skript für Aktion in Fenster 'Neue Abfrage' schreiben**, und klicken Sie dann auf **OK**.
11. Wenn die Sicherung erfolgreich abgeschlossen wurde, klicken Sie auf **OK**.
12. Sehen Sie sich im Abfragebereich die Transact-SQL-Anweisung **BACKUP** an, die zum Sichern der Datenbank verwendet wurde. Beachten Sie, dass die Option **ENCRYPTION** angegeben wurde.
13. Schließen Sie SSMS, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

- Planen Sie Ihre Sicherungsstrategie sorgfältig.
- Planen Sie die Sicherungsstrategie in Verbindung mit den Geschäftsanforderungen.
- Wählen Sie das geeignete Datenbank-Wiederherstellungsmodell.
- Planen Sie die Größe des Transaktionsprotokolls basierend auf der Häufigkeit der Transaktionsprotokollsicherung.
- Erwägen Sie die Nutzung von differenziellen Sicherungen, um die Wiederherstellung zu beschleunigen.
- Erwägen Sie die Komprimierung von Sicherungen, um den Speicherbedarf und die Sicherungszeit zu verringern.

## Fragen zur Lernzielkontrolle

**Frage:** Was sind die spezifischen Merkmale von Transaktionsprotokoll-Wiederherstellungen?

**Antwort:** Die spezifischen Merkmale von Transaktionsprotokoll-Wiederherstellungen sind Zeitpunktwiederherstellung und die Möglichkeit, bis zur Fehlerquelle wiederherzustellen, wenn nur Datendateien beschädigt sind.

**Frage:** Wann kann eine Strategie auf Basis vollständiger Datenbanksicherungen geeignet sein?

**Antwort:** Eine Strategie auf Basis vollständiger Datenbanksicherungen kann geeignet sein, wenn es ausreichend ist, die Datenbank bis zu den Punkten vollständiger Datenbanksicherungen wiederherzustellen.

# Unterrichtseinheit 7

## Wiederherstellen von SQL Server-Datenbanken

### Inhalt:

Lektion 1: Wiederherstellen von Datenbanken	2
Lektion 2: Erweiterte Wiederherstellungsszenarios	4
Lektion 3: Zeitpunktwiederherstellung	6
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	8

## Lektion 1

# Wiederherstellen von Datenbanken

### **Inhalt:**

Vorführung: Wiederherstellen von Datenbanken

3

## Vorführung: Wiederherstellen von Datenbanken

### Vorführungsschritte

Erstellen einer Sicherung des Protokollfragments

1. Vergewissern Sie sich, dass die virtuellen Computer **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie im Ordner **D:\Demofiles\Mod07** die Datei **Setup.cmd** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**, und warten Sie, bis das Skript beendet wurde.
4. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine **MIA-SQL** her.
5. Klicken Sie auf **Neue Abfrage**, und geben Sie den folgenden Transact-SQL-Code ein, um eine Sicherung des Protokollfragments durchzuführen:

```
BACKUP LOG AdventureWorks TO DISK = 'D:\Demofiles\Mod07\BackupDemo.bak'  
WITH NO_TRUNCATE;
```

6. Klicken Sie auf **Ausführen**, und überprüfen Sie anhand der resultierenden Meldung, ob die Sicherung erfolgreich war.

Wiederherstellen einer Datenbank

1. Erweitern Sie im Objekt-Explorer den Eintrag **Datenbanken**, klicken Sie mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, zeigen Sie auf **Wiederherstellen**, und klicken Sie dann auf **Datenbank**.
2. Im Dialogfeld **Datenbank wiederherstellen - AdventureWorks** wird angezeigt, dass mit dem Wiederherstellungsvorgang sowohl die vollständige Sicherung als auch das kürzlich gesicherte Transaktionsprotokoll wiederhergestellt werden. Klicken Sie auf **OK**.
3. Im Dialogfeld **Microsoft SQL Server Management Studio** wird angezeigt, dass der Wiederherstellungsvorgang erfolgreich war. Klicken Sie auf **OK**.
4. Überprüfen Sie im Objekt-Explorer, ob die **AdventureWorks**-Datenbank betriebsbereit ist.
5. Schließen Sie SQL Server Management Studio, ohne die Dateien zu speichern.

## Lektion 2

# Erweiterte Wiederherstellungsszenarios

### **Inhalt:**

Vorführung: Wiederherstellen einer verschlüsselten Sicherung

5

## Vorführung: Wiederherstellen einer verschlüsselten Sicherung

### Vorführungsschritte

Wiederherstellen einer verschlüsselten Sicherung

1. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine **MIA-SQL\SQL2** her.
2. Erweitern Sie im Objekt-Explorer den Eintrag **Datenbanken**, und sehen Sie sich die auf dieser Instanz vorhandenen Datenbanken an.
3. Öffnen Sie die Skriptdatei **Restore Encrypted Backup.sql** im Ordner **D:\Demofiles\Mod07**.
4. Markieren Sie den Code unter dem Kommentar **Try to restore an encrypted backup**, und klicken Sie auf **Ausführen**. Beachten Sie, dass dieser Vorgang nicht ausgeführt werden kann, weil das benötigte Zertifikat fehlt.
5. Markieren Sie den Code unter dem Kommentar **Create a database master key for master**, und klicken Sie auf **Ausführen**. Hierdurch wird ein Datenbank-Hauptschlüssel für die Masterdatenbank auf **MIA-SQL\SQL2** erstellt.
6. Markieren Sie den Code unter dem Kommentar **Import the backed up certificate**, und klicken Sie dann auf **Ausführen**. Hierdurch wird ein Zertifikat aus Sicherungen von öffentlichen und privaten Schlüsseln erstellt, die auf der Instanz **MIA-SQL** durchgeführt wurden.
7. Markieren Sie den Code unter dem Kommentar **Restore the encrypted database**, und klicken Sie dann auf **Ausführen**. Beachten Sie, dass der Wiederherstellungsvorgang dieses Mal erfolgreich ist.
8. Aktualisieren Sie den Ordner **Datenbanken** im Objekt-Explorer, und überprüfen Sie, ob die **AdventureWorks**-Datenbank wiederhergestellt wurde.
9. Schließen Sie SQL Server Management Studio, ohne die Änderungen zu speichern.

## Lektion 3

# Zeitpunkt wiederherstellung

### **Inhalt:**

Vorführung: Durchführen einer Zeitpunkt wiederherstellung

7

## Vorführung: Durchführen einer Zeitpunktwiederherstellung

### Vorführungsschritte

Durchführen einer Zeitpunktwiederherstellung

1. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine **MIA-SQL** her.
2. Öffnen Sie in SQL Server Management Studio die Skriptdatei **Point-in-Time Restore.sql** im Ordner **D:\Demofiles\Mod07**.
3. Markieren Sie den Code unter dem Kommentar **Create a database and back it up**, und führen Sie ihn aus. Hierdurch wird eine Datenbank mit einer einzelnen Tabelle erstellt. Außerdem wird eine vollständige Sicherung durchgeführt.
4. Markieren Sie den Code unter dem Kommentar **Enter some data**, und führen Sie ihn aus. Hierdurch wird ein Datensatz in die Tabelle **Customers** eingefügt.
5. Markieren Sie den Code unter dem Kommentar **Get the current time**, und führen Sie ihn aus. Das aktuelle Datum und die aktuelle Uhrzeit werden angezeigt. Notieren Sie sich die aktuelle Uhrzeit.
6. Warten Sie, bis eine Minute verstrichen ist. Markieren Sie dann erneut den Code unter dem Kommentar **Get the current time**, und führen Sie ihn aus, um zu überprüfen, ob mindestens eine Minute vergangen ist, seit Sie die Zeit notiert haben.
7. Markieren Sie den Code unter dem Kommentar **Enter some more data**, und führen Sie ihn aus. Hierdurch wird ein zweiter Datensatz in die Tabelle **Customers** eingefügt.
8. Markieren Sie den Code unter dem Kommentar **Backup the transaction log**, und führen Sie ihn aus. Hierdurch wird eine Transaktionsprotokollsicherung der Datenbank durchgeführt.
9. Schließen Sie das Abfragefenster.
10. Erweitern Sie im Objekt-Explorer den Eintrag **Datenbanken**, und vergewissern Sie sich, dass **BackupDemo** aufgeführt wird (klicken Sie andernfalls mit der rechten Maustaste auf den Ordner **Datenbanken**, und klicken Sie auf **Aktualisieren**).
11. Klicken Sie mit der rechten Maustaste auf die Datenbank **BackupDemo**, zeigen Sie auf **Tasks**, zeigen Sie auf **Wiederherstellen**, und klicken Sie dann auf **Datenbank**.
12. Klicken Sie im Dialogfeld **Datenbank wiederherstellen - BackupDemo** auf **Zeitachse**.
13. Wählen Sie im Dialogfeld **Sicherungszeitachse: BackupDemo** die Option **Bestimmtes Datum und bestimmte Uhrzeit** aus, legen Sie den Wert im Feld **Uhrzeit** auf die zuvor notierte Zeit fest (bevor Daten eingefügt wurden), und klicken Sie dann auf **OK**.
14. Klicken Sie im Dialogfeld **Datenbank wiederherstellen - BackupDemo** auf **OK**.
15. Wenn die Benachrichtigung angezeigt wird, dass die Datenbank erfolgreich wiederhergestellt wurde, klicken Sie auf **OK**.
16. Erweitern Sie im Objekt-Explorer die Datenbank **BackupDemo**, erweitern Sie den Ordner **Tables**, klicken Sie mit der rechten Maustaste auf **dbo.Customers**, und klicken Sie dann auf **Oberste 1.000 Zeilen auswählen**. Wenn die Ergebnisse angezeigt werden, vergewissern Sie sich, dass die Datenbank bis zum Zeitpunkt vor dem Einfügen von Daten wiederhergestellt wurde.
17. Schließen Sie SQL Server Management Studio, ohne die Dateien zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

- Vergessen Sie nicht, eine Sicherung des Protokollfragments durchzuführen, bevor Sie eine Wiederherstellungssequenz starten.
- Sofern verfügbar, verwenden Sie eine differenzielle Wiederherstellung, um den Wiederherstellungsprozess zu beschleunigen.
- Verwenden Sie die Wiederherstellung auf Dateiebene, um Wiederherstellungen zu beschleunigen, wenn nicht alle Datenbankdateien beschädigt sind.
- Führen Sie regelmäßige Sicherungen der folgenden Systemdatenbanken durch: **Masterdatenbank**, **Modelldatenbank** und **msdb**-Datenbank.
- Erstellen Sie einen Notfallwiederherstellungsplan für Ihren SQL Server, und denken Sie daran, die Wiederherstellung von Datenbanken regelmäßig zu testen.

## Fragen zur Lernzielkontrolle

**Frage:** Aus welchen drei Phasen besteht der Wiederherstellungsprozess?

**Antwort:** Die drei Phasen einer Wiederherstellung sind Datenkopierphase, Rollforwardphase und Rollbackphase. In der Datenkopierphase werden alle Daten-, Protokoll- und Indexseiten vom Sicherungsmedium kopiert. In der Rollforwardphase werden die Transaktionen auf die aus der Sicherung kopierten Daten angewendet, für die ein Rollforward bis zum Wiederherstellungspunkt ausgeführt werden soll. In der Rollbackphase werden alle nicht committeten Transaktionen rückgängig und die Datenbank für Benutzer verfügbar gemacht. Nach der Rollbackphase können keine nachfolgenden Sicherungen mehr wiederhergestellt werden.

# Unterrichtseinheit 8

## **Automatisieren der SQL Server-Verwaltung**

### **Inhalt:**

<b>Lektion 1:</b> Automatisieren der SQL Server-Verwaltung	2
<b>Lektion 2:</b> Arbeiten mit dem SQL Server-Agent	6
<b>Lektion 3:</b> Verwalten von Aufträgen des SQL Server-Agents	9
<b>Lektion 4:</b> Verwalten mehrerer Server	13
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	16

## Lektion 1

# Automatisieren der SQL Server-Verwaltung

### Inhalt:

Fragen und Antworten	3
Vorführung: SQL Server-Agent	4

## Fragen und Antworten

Welche vier wichtigen Objekttypen verwendet der SQL Server-Agent?

Elemente	
1	Aufträge
2	Wartungspläne
3	Zeitpläne
4	Sicherungsaufgaben
5	Warnungen
6	Protokolle
7	Operatoren
8	SCOM-Berichterstellung

Kategorie 1		Kategorie 2
Vom SQL Server-Agent bereitgestellt		Nicht vom SQL Server-Agent bereitgestellt

**Antwort:**

Kategorie 1	Kategorie 2
Vom SQL Server-Agent bereitgestellt	Nicht vom SQL Server-Agent bereitgestellt
Aufträge Zeitpläne Warnungen Operatoren	Wartungspläne Sicherungsaufgaben Protokolle SCOM-Berichterstellung

**Vorführung: SQL Server-Agent****Vorführungsschritte**

Erstellen eines Auftrags

1. Vergewissern Sie sich, dass die virtuellen Computer **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich dann als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Navigieren Sie im Datei-Explorer zu **D:\Demofiles\Mod08**, klicken Sie mit der rechten Maustaste auf **Setup.cmd**, und klicken Sie auf **Als Administrator ausführen**.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Klicken Sie auf der Taskleiste auf **Microsoft SQL Server Management Studio**.
5. Geben Sie im Dialogfeld **Verbindung mit Server herstellen** im Feld **Servername** den Wert **MIA-SQL** ein, und klicken Sie auf **Verbinden**.
6. Erweitern Sie im Objekt-Explorer nacheinander die Einträge **SQL Server-Agent** und **Aufträge**.
7. Beachten Sie die vorhandenen Aufträge auf dem Server.
8. Klicken Sie mit der rechten Maustaste auf den Ordner **Aufträge**, und klicken Sie auf **Neuer Auftrag**.
9. Geben Sie im Dialogfeld **Neuer Auftrag** im Feld **Name** den Wert **Manuelle AdventureWorks-Sicherung** ein, und klicken Sie in der Liste **Kategorie** auf **Datenbankwartung**.
10. Klicken Sie auf der Seite **Schritte** auf **Neu**.
11. Geben Sie im Dialogfeld **Neuer Auftragschritt** im Feld **Schrittname** den Wert **AdventureWorks sichern** ein, und klicken Sie in der Liste **Datenbank** auf **AdventureWorks**.
12. Geben Sie im Feld **Befehl** Folgendes ein, und klicken Sie auf **OK**:

```
BACKUP DATABASE [AdventureWorks] TO DISK =
N'D:\Demofiles\Mod08\Backups\AdventureWorksAgentBackup.bak' WITH NOFORMAT, INIT,
NAME = N'AdventureWorks-Full Database Backup', COMPRESSION, STATS = 10
GO
```

13. Klicken Sie im Dialogfeld **Neuer Auftrag** auf **OK**.
14. Der neue Auftrag **Manuelle AdventureWorks-Sicherung** wird jetzt im Objekt-Explorer unter **Aufträge** angezeigt.

Ausführen eines Auftrags und Überprüfen der Ausgabe

1. Klicken Sie im Objekt-Explorer unter **Aufträge** mit der rechten Maustaste auf **Manuelle AdventureWorks-Sicherung**, und klicken Sie auf **Auftrag starten bei Schritt**.
2. Beachten Sie, wie der Status der einzelnen Schritte im Dialogfeld **Aufträge starten - MIA-SQL** nach Abschluss zu **Erfolg** wechselt, und klicken Sie auf **Schließen**.
3. Doppelklicken Sie im Objekt-Explorer unter **SQL Server-Agent** auf **Auftragsaktivitätsmonitor**.
4. Überprüfen Sie im Fenster **Auftragsaktivitätsmonitor - MIA-SQL** die angezeigten Informationen für SQL Server-Agent-Aufträge.
5. Überprüfen Sie die Informationen in der Zeile **Manuelle AdventureWorks-Sicherung** in der Tabelle **Agentauftragsaktivität**, und klicken Sie auf **Schließen**.
6. Navigieren Sie im Datei-Explorer zu **D:\Demofiles\Mod08\Backups**, und vergewissern Sie sich, dass die Datei **AdventureWorksAgentBackup.bak** erstellt wurde.
7. Klicken Sie in SSMS im Fenster **Auftragsaktivitätsmonitor - MIA-SQL** auf **Schließen**.
8. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Lektion 2

# Arbeiten mit dem SQL Server-Agent

### Inhalt:

Fragen und Antworten	7
Vorführung: Skripten von Aufträgen	7

## Fragen und Antworten

Legen Sie die erforderliche Reihenfolge der folgenden SQL Server-Agent-Schritte für die Erstellung eines Auftrags fest, indem Sie die Schritte korrekt durchnummerieren.

	Schritte
	Erstellen eines Auftrags.
	Kategorisieren des Auftrags.
	Erstellen eines oder mehrerer Schritte.
	Erstellen eines oder mehrerer Zeitpläne.
	Erstellen oder Auswählen eines Operators für Benachrichtigungen.
	Planen der Ausführung des Auftrags.

**Antwort:**

	Schritte
1	Erstellen eines Auftrags.
2	Kategorisieren des Auftrags.
3	Erstellen eines oder mehrerer Schritte.
4	Erstellen eines oder mehrerer Zeitpläne.
5	Erstellen oder Auswählen eines Operators für Benachrichtigungen.
6	Planen der Ausführung des Auftrags.

## Vorführung: Skripten von Aufträgen

### Vorführungsschritte

Skriptgesteuertes Hinzufügen einer Aufgabe zu einem Auftrag

1. Erweitern Sie im Objekt-Explorer von SSMS den Eintrag **Datenbanken**, klicken Sie mit der rechten Maustaste auf **AdventureWorks**, zeigen Sie auf **Tasks**, und klicken Sie auf **Sichern**.
2. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** im Abschnitt **Ziel** auf das vorhandene Sicherungsziel, klicken Sie auf **Entfernen** und dann auf **Hinzufügen**.

3. Geben Sie im Dialogfeld **Sicherungsziel auswählen** im Feld **Dateiname** den Wert **D:\Demofiles\Mod08\Backups\AdventureWorksScript.bak** ein, und klicken Sie auf **OK**.
4. Wählen Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf der Symbolleiste in der Dropdownliste **Skript** die Option **Skript für Aktion in Auftrag schreiben** aus.
5. Beachten Sie im Dialogfeld **Neuer Auftrag** auf der Seite **Allgemein** den Standardnamen für den Auftrag (Datenbank sichern - AdventureWorks).
6. Beachten Sie auf der Seite **Schritte**, dass der Auftrag einen **Transact-SQL-Schritt** namens **1** enthält.
7. Klicken Sie auf der Seite **Zeitpläne** auf **Neu**.
8. Geben Sie im Dialogfeld **Neuer Auftragszeitplan** im Feld **Name** den Wert **Wochentage** ein.
9. Wählen Sie unter **Häufigkeit** die Kontrollkästchen **Montag**, **Dienstag**, **Mittwoch**, **Donnerstag** und **Freitag** aus, deaktivieren Sie das Kontrollkästchen **Sonntag**, und klicken Sie auf **OK**.
10. Klicken Sie im Dialogfeld **Neuer Auftrag** auf **OK**.
11. Klicken Sie im Dialogfeld **Datenbank sichern - AdventureWorks** auf **Abbrechen**, um den Auftrag zu speichern, jedoch nicht auszuführen.
12. Vergewissern Sie sich im Objekt-Explorer, dass der Auftrag **Datenbank sichern - AdventureWorks** im Ordner **Aufträge** angezeigt wird.

#### Generieren von Skripts für vorhandene Aufträge

1. Klicken Sie im Objekt-Explorer unter **Aufträge** mit der rechten Maustaste auf **AdventureWorks DB überprüfen**, zeigen Sie auf **Skript für Auftrag als**, zeigen Sie auf **ERSTELLEN nach**, und klicken Sie auf **Neues Abfrage-Editor-Fenster**. Daraufhin wird der notwendige Transact-SQL-Code für den Auftrag generiert.
2. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Datenbank sichern - AdventureWorks**, zeigen Sie auf **Skript für Auftrag als**, zeigen Sie auf **ERSTELLEN nach**, und klicken Sie auf **Zwischenablage**.
3. Platzieren Sie die Einfügemarke an das Ende des Transact-SQL-Codes im Abfrage-Editor-Fenster, und klicken Sie im Menü **Bearbeiten** auf **Einfügen**.
4. Speichern Sie das Transact-SQL-Skript unter dem Namen **Create Jobs.sql** im Ordner **D:\Demofiles\Mod08**.
5. Diese Methode ist hilfreich, um Skripteraufgaben zu generieren und diese anschließend wiederherstellen zu können, falls sie versehentlich gelöscht oder auf einem anderen Server benötigt werden.
6. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Verwalten von Aufträgen des SQL Server-Agents

### Inhalt:

Fragen und Antworten	10
Vorführung: Anzeigen des Auftragsverlaufs und Beheben von fehlgeschlagenen Aufträgen	11

## Fragen und Antworten

Welche vier Schritte können unternommen werden, wenn ein Fehler bei einem Auftrag auftritt?

Elemente	
1	Überprüfen des SQL Server-Agent-Status
2	Starten und Beenden von SQL Server
3	Überprüfen des Auftragsverlaufs
4	Überprüfen des freien Speicherplatzes
5	Überprüfen der Auftragsausführung
6	Überprüfen des Aktivitätsmonitors
7	Überprüfen des Zugriffs auf Abhängigkeiten

Kategorie 1	Kategorie 2
Schritt zur Problembehebung	Sonstige Datenbankaktivität

**Antwort:**

Kategorie 1	Kategorie 2
Schritt zur Problembehebung	Sonstige Datenbankaktivität
Überprüfen des SQL Server-Agent-Status Überprüfen des Auftragsverlaufs Überprüfen der Auftragsausführung Überprüfen des Zugriffs auf Abhängigkeiten	Starten und Beenden von SQL Server Überprüfen des freien Speicherplatzes Überprüfen des Aktivitätsmonitors

## Vorführung: Anzeigen des Auftragsverlaufs und Beheben von fehlgeschlagenen Aufträgen

### Vorführungsschritte

Ausführen von Aufträgen

1. Klicken Sie in SQL Server Management Studio im Objekt-Explorer mit der rechten Maustaste auf **Datenbank sichern - AdventureWorks**, und klicken Sie auf **Auftrag starten bei Schritt**.
2. Warten Sie, bis der Auftrag erfolgreich abgeschlossen wurde, und klicken Sie auf **Schließen**.
3. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **AdventureWorks-DB überprüfen**, und klicken Sie auf **Auftrag starten bei Schritt**.
4. Beachten Sie, dass dieser Auftrag nicht automatisch gestartet wird, da der mehr als einen Auftragsschritt enthält.
5. Klicken Sie im Dialogfeld **Auftrag starten auf 'MIA-SQL'** in der Tabelle **Ausführung starten bei Schritt** auf **1**, und klicken Sie auf **Starten**. Beachten Sie, dass der Auftrag fehlschlägt, und klicken Sie auf **Schließen**.

Problembehandlung für Aufträge

1. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Datenbank sichern - AdventureWorks**, und klicken Sie auf **Verlauf anzeigen**.
2. Erweitern Sie im Dialogfeld **Protokolldateianzeige - MIA-SQL** das Datum der neuesten Instanz des Auftrags, beachten Sie, dass alle Schritte erfolgreich ausgeführt wurden, und klicken Sie auf **Schließen**.
3. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **AdventureWorks-DB überprüfen**, und klicken Sie auf **Verlauf anzeigen**.
4. Erweitern Sie im Dialogfeld **Protokolldateianzeige - MIA-SQL** das Datum der neuesten fehlgeschlagenen Instanz des Auftrags, und beachten Sie, dass Schritt **3** fehlgeschlagen ist.
5. Wählen Sie den fehlerhaften Schritt aus, und beachten Sie die zurückgegebene Nachricht am unteren Rand des Dialogfelds. Möglicherweise müssen Sie einen Bildlauf nach unten durchführen. Klicken Sie anschließend auf **Schließen**.
6. Doppelklicken Sie im Objekt-Explorer auf **AdventureWorks-DB überprüfen**.
7. Klicken Sie im Dialogfeld **Auftragseigenschaften - AdventureWorks-DB überprüfen** auf der Seite **Schritte** in der Tabelle **Auftragungsschrittliste** auf Schritt **3**, und dann auf **Bearbeiten**.
8. Klicken Sie im Dialogfeld **Auftragungsschritt-Eigenschaften - DB überprüfen** auf **Analysieren**.
9. Beachten Sie, dass im Dialogfeld **Befehlstext analysieren** dieselbe Fehlermeldung wie im Auftragsverlauf angezeigt wird, und klicken Sie auf **OK**.
10. Ändern Sie im Dialogfeld **Auftragungsschritt-Eigenschaften - DB überprüfen** den Text im Feld **Befehl** wie folgt, und klicken Sie auf **OK**:

```
DBCC CHECKDB ('AdventureWorks');
```

11. Klicken Sie im Dialogfeld **Auftragseigenschaften - AdventureWorks-DB überprüfen** auf **OK**.
12. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **AdventureWorks-DB überprüfen**, und klicken Sie auf **Auftrag starten bei Schritt**.
13. Klicken Sie im Dialogfeld **Auftrag starten auf 'MIA-SQL'** in der Tabelle **Ausführung starten bei Schritt** auf **1**, und klicken Sie auf **Starten**.

14. Warten Sie, bis die Schritte erfolgreich abgeschlossen wurden, und klicken Sie auf **Schließen**.
15. Doppelklicken Sie im **Objekt-Explorer** unter **Auftrag** auf **Aktivitätsmonitor**.
16. Beachten Sie im Dialogfeld **Auftragsaktivitätsmonitor - MIA-SQL** in der Tabelle **Agentenauftragsaktivität** den Status des Auftrags **AdventureWorks-DB überprüfen**, und klicken Sie auf **Schließen**.
17. Sehen Sie sich im Ordner **D:\Demofiles\Mod08\AdventureWorks** die Dateien an, die der Auftrag generiert hat.
18. Vergewissern Sie sich im Ordner **D:\Demofiles\Mod08\Backups**, dass der Auftrag **Datenbank sichern - AdventureWorks** eine Sicherungsdatei erstellt hat.
19. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 4

# Verwalten mehrerer Server

### Inhalt:

Fragen und Antworten	14
Vorführung: Konfigurieren von Master- und Zielserversn	14

## Fragen und Antworten

**Frage:** Welche der folgenden Aussagen trifft nicht zu?

- Ein Masterserver kann mehrere Zielserver haben.
- Eine große Anzahl von Zielservern wirkt sich nicht negativ auf die Leistung eines Masterservers mit hoher Last aus.
- Jeder Zielserver kann sich nur mit einem einzigen Masterserver verbinden.
- Wenn der Name eines Zielservers geändert wird, muss der Server erneut beim Masterserver registriert werden.

**Antwort:**

- Ein Masterserver kann mehrere Zielserver haben.
- Eine große Anzahl von Zielservern wirkt sich nicht negativ auf die Leistung eines Masterservers mit hoher Last aus.
- Jeder Zielserver kann sich nur mit einem einzigen Masterserver verbinden.
- Wenn der Name eines Zielservers geändert wird, muss der Server erneut beim Masterserver registriert werden.

## Vorführung: Konfigurieren von Master- und Zielservern

### Vorführungsschritte

Verwenden des Masterserver-Assistenten

1. Klicken Sie in SQL Server Management Studio im Objekt-Explorer unter **MIA-SQL** mit der rechten Maustaste auf **SQL Server-Agent**, zeigen Sie auf **Multiserververwaltung**, und klicken Sie auf **Diesen Server als Master festlegen**.
2. Klicken Sie im Dialogfeld **Masterserver-Assistent - MIA-SQL** auf der Seite **Willkommen beim Masterserver-Assistenten** auf **Weiter**.
3. Geben Sie auf der Seite **Masterserveroperator** im Feld **E-Mail-Adresse** den Wert **student@adventureworks.com** ein, und klicken Sie auf **Weiter**.
4. Erweitern Sie auf der Seite **Zielserver** nacheinander die Einträge **Datenbankmodul** und **Lokale Servergruppen**, klicken Sie auf **mia-sql\sql2**, klicken Sie auf **>** und anschließend auf **Weiter**.
5. Klicken Sie im Dialogfeld **Serverkompatibilität wird überprüft** auf **Schließen**.
6. Klicken Sie auf der Seite **Masterserver-Anmeldeinformationen** auf **Weiter**.
7. Klicken Sie auf der Seite **Assistenten abschließen** auf **Fertig stellen**.
8. Klicken Sie nach Abschluss der Konfiguration auf **Schließen**.

Verwenden von Transact-SQL zum Registrieren eines Zielservers

1. Klicken Sie im Objekt-Explorer auf der Symbolleiste auf **Verbinden**, und klicken Sie auf **Datenbankmodul**.
2. Wählen Sie im Dialogfeld **Verbindung mit Server herstellen** in der Liste **Servername** den Eintrag **MIA-SQL\SQL3** aus, und klicken Sie auf **Verbinden**.
3. Erweitern Sie im Objekt-Explorer unter **MIA-SQL\SQL3** nacheinander die Einträge **Datenbanken** und **Systemdatenbanken**, klicken Sie mit der rechten Maustaste auf **msdb**, und klicken Sie auf **Neue Abfrage**.

4. Geben Sie im neu geöffneten Abfragefenster den folgenden Befehl ein, und klicken Sie auf **Ausführen**:

```
EXEC dbo.sp_msx_enlist N'MIA-SQL';
```

5. Klicken Sie im Objekt-Explorer unter **MIA-SQL** mit der rechten Maustaste auf **SQL Server-Agent (MSX)**, zeigen Sie auf **Multiserververwaltung**, und klicken Sie auf **Zielsever verwalten**.
6. Beachten Sie, dass im Dialogfeld **Zielseverstatus - MIA-SQL** die Server **MIA-SQL\SQL2** und **MIA-SQL\SQL3** beide als Zielsever aufgelistet werden.
7. Klicken Sie im Dialogfeld **Zielseverstatus - MIA-SQL** auf **Schließen**.
8. Schließen Sie SSMS, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## **Bewährte Methoden**

Falls Sie eine große Anzahl an Zielservern betreiben, sollten Sie es nach Möglichkeit vermeiden, einen Produktionsserver als Masterserver zu verwenden, da der Datenverkehr der Zielserver die Leistung des Produktionsservers beeinträchtigen kann.

# Unterrichtseinheit 9

## Konfigurieren der Sicherheit für den SQL Server-Agent

### Inhalt:

Lektion 1: Grundlegendes zu den Sicherheitskonzepten des SQL Server-Agents	2
Lektion 2: Konfigurieren von Anmeldeinformationen	5
Lektion 3: Konfigurieren von Proxykonten	8
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	10
Fragen und Antworten zur Zusammenfassung der Übungseinheit	11

## Lektion 1

# Grundlegendes zu den Sicherheitskonzepten des SQL Server-Agents

### Inhalt:

Fragen und Antworten	3
Vorführung: Zuweisen eines Sicherheitskontexts zu einem Auftragschritt	3

## Fragen und Antworten

Nummerieren Sie die folgenden festen Rollen in der richtigen Reihenfolge von den niedrigsten zu den höchsten Berechtigungen.

Schritte
SQLAgentUserRole
SQLAgentReaderRole
SQLAgentOperatorRole
sysadmin

**Antwort:**

Schritte
1 SQLAgentUserRole
2 SQLAgentReaderRole
3 SQLAgentOperatorRole
4 sysadmin

## Vorführung: Zuweisen eines Sicherheitskontexts zu einem Auftragschritt

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Klicken Sie im Ordner **D:\Demofiles\Mod09** mit der rechten Maustaste auf **Setup.cmd**, und klicken Sie dann auf **Als Administrator ausführen**.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Starten Sie Microsoft SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine-Instanz **MIA-SQL** her.
5. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie auf **Projekt/Projektmappe**.
6. Öffnen Sie die Lösung **Demo.ssmssl** im Ordner **D:\Demofiles\Mod09\Demo**.
7. Doppelklicken Sie auf die Skriptdatei **Demo 1 - security context.sql**.
8. Erweitern Sie im Objekt-Explorer nacheinander die Einträge **SQL Server-Agent** und **Aufträge**, klicken Sie mit der rechten Maustaste auf **Ausführungsidentität aufzeichnen**, und klicken Sie auf **Auftrag starten bei Schritt**.
9. Vergewissern Sie sich im Dialogfeld **Aufträge starten - MIA-SQL**, dass der Auftrag erfolgreich ausgeführt wurde, und klicken Sie auf **Schließen**.

Der Auftrag ruft die gespeicherte Prozedur **dbo.RecordIdentity** in der Datenbank **AdminDB** auf. Diese Prozedur erfasst die Identität der aufrufenden Person nach **dbo.IdentityLog**.

10. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Ausführungsidentität aufzeichnen**, und klicken Sie auf **Verlauf anzeigen**.

- Erweitern Sie die angezeigten ausgeführten Aufträge im Fenster **Protokolldateianzeige - MIA-SQL**, indem Sie auf das Pluszeichen im rechten Bereich der Zeile klicken und einen Bildlauf nach rechts durchführen, bis die Spalte **Nachricht** angezeigt wird.

Laut der ersten Zeile wurde der Auftrag von **ADVENTUREWORKS\Student**, aufgerufen, aber in der Zeile des Auftrags schritt sehen Sie, dass er als **ADVENTUREWORKS\ServiceAcct** ausgeführt wurde. Wenn ein **sysadmin**-Benutzer einen Auftrag besitzt, werden die Auftrags schritte standardmäßig im Kontext des SQL Server-Agent-Dienstkontos ausgeführt.

Schließen Sie das Fenster **Protokolldateianzeige - MIA-SQL**.

- Führen Sie im Abfragebereich **Demo 1 - security context.sql** die Abfrage unter dem Kommentar aus, der mit **Task 1** beginnt, um den Inhalt der Tabelle **AdminDB.dbo.IdentityLog** anzuzeigen. Beachten Sie, dass die Identität des Dienstkontos erfasst wurde.
- Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Ausführungsidentität aufzeichnen**, und klicken Sie auf **Eigenschaften**.
- Löschen Sie im Fenster **Auftragseigenschaften - Ausführungsidentität aufzeichnen** auf der Seite **Allgemein** den Inhalt des Felds **Besitzer**, geben Sie **ITSupportLogin** ein, und klicken Sie auf **OK**.
- Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Ausführungsidentität aufzeichnen**, und klicken Sie auf **Auftrag starten bei Schritt**.
- Beobachten Sie im Dialogfeld **ITSupportLogin**, wie der Auftrag fehlschlägt, und klicken Sie auf **Schließen**.
- Um den Auftragsverlauf anzuzeigen und die Fehlerursache herauszufinden, klicken Sie mit der rechten Maustaste auf **Ausführungsidentität aufzeichnen**, und klicken Sie auf **Verlauf anzeigen**.
- Erweitern Sie den fehlgeschlagenen Auftrag im Fenster **Protokolldateianzeige - MIA-SQL**, indem Sie auf das Pluszeichen neben dem Fehlersymbol klicken, und einen Bildlauf nach rechts durchführen, bis die Spalte **Nachricht** angezeigt wird. Notieren Sie die Fehlerursache. Die Fehlerursache sollte wie folgt angezeigt werden:

```
Ausgeführt als Benutzer: ITSupportLogin. Die EXECUTE-Berechtigung wurde für das Objekt „RecordIdentity“, Datenbank „AdminDB“, Schema „dbo“ verweigert. [SQLSTATE 42000] (Fehler 229). Fehler bei Schritt.
```

Schließen Sie das Fenster **Protokolldateianzeige - MIA-SQL**.

Der Auftrag wurde mit der Anmeldung **ITSupportLogin** ausgeführt, die zum Benutzer **ITSupport** in der Datenbank **AdminDB** zugeordnet ist. Dieser Benutzer hat keine Berechtigungen zum Ausführen der gespeicherten Prozedur, daher ist der Auftrags schritt fehlgeschlagen.

- Führen Sie im Abfragebereich **Demo 1 - security context.sql** die Abfrage unter dem Kommentar aus, der mit **Task 2** beginnt, um die erforderliche Berechtigung für die Ausführung des Auftrags zu erteilen.
- Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Ausführungsidentität aufzeichnen**, und klicken Sie auf **Auftrag starten bei Schritt**.
- Vergewissern Sie sich im Dialogfeld **Aufträge starten - MIA-SQL**, dass der Auftrag erfolgreich ausgeführt wurde, und klicken Sie auf **Schließen**.
- Führen Sie im Abfragebereich **Demo 1 - security context.sql** die Abfrage unter dem Kommentar aus, der mit **Task 1** beginnt, um den Inhalt der Tabelle **AdminDB.dbo.IdentityLog** anzuzeigen.
- Klicken Sie im Menü **Datei** auf **Schließen**.
- Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Konfigurieren von Anmeldeinformationen

### **Inhalt:**

Fragen und Antworten	6
Vorführung: Konfigurieren von Anmeldeinformationen	6

## Fragen und Antworten

**Frage:** Was geschieht mit den Anmeldeinformationen, wenn das Kennwort des verknüpften Windows-Benutzers geändert wird?

- Die Anmeldeinformationen werden automatisch gelöscht.
- Die Anmeldeinformationen werden deaktiviert.
- Die Anmeldeinformationen können erst wieder verwendet werden, nachdem das Kennwort aktualisiert wurde.
- Die Anmeldeinformationen funktionieren weiterhin normal.

**Antwort:**

- Die Anmeldeinformationen werden automatisch gelöscht.
- Die Anmeldeinformationen werden deaktiviert.
- Die Anmeldeinformationen können erst wieder verwendet werden, nachdem das Kennwort aktualisiert wurde.
- Die Anmeldeinformationen funktionieren weiterhin normal.

## Vorführung: Konfigurieren von Anmeldeinformationen

### Vorführungsschritte

1. Klicken Sie in SQL Server Management Studio im Objekt-Explorer unter **MIA-SQL** unter **SQL Server-Agent** mit der rechten Maustaste auf **Aufträge**, und klicken Sie auf **Neuer Auftrag**.
2. Geben Sie im Fenster **Neuer Auftrag** auf der Seite **Allgemein** im Feld **Name** den Wert **Exportdatei kopieren** ein.
3. Klicken Sie auf der Seite **Schritte** auf **Neu**.
4. Geben Sie im Fenster **Neuer Auftragschritt** auf der Seite **Allgemein** im Feld **Schrittname** den Wert **Datei kopieren** ein.
5. Klicken Sie in der Liste **Typ** auf **Betriebssystem (CmdExec)**.
6. Geben Sie im Fenster **Befehl** Folgendes ein:

```
copy d:\demoFiles\Mod09\ExportData\export.txt  
d:\demoFiles\Mod09\ImportData\import.txt /Y
```

Beachten Sie, dass der Auftrag für die Ausführung im Sicherheitskontext des SQL Server-Agent-Dienstkontos konfiguriert ist.

7. Klicken Sie auf der Seite **Erweitert** im Feld **Aktion bei Erfolg** auf **Beenden des Auftrags mit Erfolgsmeldung**, und klicken Sie auf **OK**.
8. Klicken Sie im Fenster **Neuer Auftrag** auf **OK**, um den Auftrag zu erstellen.
9. Klicken Sie im Objekt-Explorer unter **Aufträge** mit der rechten Maustaste auf **Exportdatei kopieren**, und klicken Sie auf **Auftrag starten bei Schritt**.
10. Vergewissern Sie sich im Dialogfeld **Aufträge starten - MIA-SQL**, dass der Auftrag fehlschlägt, und klicken Sie auf **Schließen**.
11. Um den Auftragsverlauf anzuzeigen und die Fehlerursache herauszufinden, klicken Sie mit der rechten Maustaste auf **Exportdatei kopieren**, und klicken Sie auf **Verlauf anzeigen**.

12. Erweitern Sie den fehlgeschlagenen Auftrag im Fenster **Protokolldateianzeige - MIA-SQL**, indem Sie auf das Pluszeichen neben dem Fehlersymbol klicken, und einen Bildlauf nach rechts durchführen, bis die Spalte **Nachricht** angezeigt wird. Notieren Sie die Fehlerursache. Die Fehlerursache sollte wie folgt angezeigt werden:

```
Ausgeführt als Benutzer: ADVENTUREWORKS\ServiceAcct. Zugriff wurde verweigert.  
Prozessexitcode 1. Fehler bei Schritt.
```

- Schließen Sie das Fenster „Protokolldateianzeige - MIA-SQL“. Der Auftragschritt ist fehlgeschlagen, weil das Dienstkonto keine Zugriffsberechtigungen für die Quell- und Zielordner im Dateisystem hat. (Als mögliche Lösung könnten Sie dem Dienstkonto Zugriff auf die Ordner erteilen. Stattdessen werden Sie in der nächsten Vorführung jedoch Anmeldeinformationen erstellen und mit einem Proxykonto verknüpfen.)
13. Doppelklicken Sie im Projektmappen-Explorer auf die Skriptdatei **Demo 2 - credential.sql**.
  14. Führen Sie den Code unter dem Kommentar aus, der mit **Task 1** beginnt, um Anmeldeinformationen mit dem Namen **FileOperation** zu erstellen, die mit dem Domänenbenutzer **ADVENTUREWORKS\FileOps** mit dem geheimen Schlüssel **Pa55w.rd** verknüpft sind.
  15. Führen Sie den Code unter dem Kommentar aus, der mit **Task 2** beginnt, um den Inhalt der Katalogsicht **sys.credentials** anzuzeigen. Daraufhin sollte eine Zeile für die soeben erstellten Anmeldeinformationen zurückgegeben werden.
  16. Klicken Sie im Menü **Datei** auf **Schließen**.
  17. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Konfigurieren von Proxykonten

### **Inhalt:**

Fragen und Antworten	9
Vorführung: Konfigurieren von Proxykonten	9

## Fragen und Antworten

**Frage:** Warum werden Anmeldeinformationen in der **master**-Systemdatenbank und Proxykonten in der **msdb**-Systemdatenbank gespeichert?

**Antwort:** Anmeldeinformationen werden im SQL Server-Agent nicht nur zu Sicherheitszwecken verwendet.

Proxykonten werden ausschließlich für SQL Server-Agent-Auftragungsschritte verwendet und daher wie alle anderen SQL Server-Agent-Konfigurationen in **msdb** gespeichert. Anmeldeinformationen sind ein Allzweck-Sicherheitstool mit zahlreichen Anwendungen und werden daher in **master** gespeichert.

## Vorführung: Konfigurieren von Proxykonten

### Vorführungsschritte

1. Doppelklicken Sie in SQL Server Management Studio im Projektmappen-Explorer auf die Skriptdatei **Demo 3 - proxy.sql**.
2. Führen Sie den Code unter dem Kommentar aus, der mit **Task 1**, um ein neues Proxykonto zu erstellen, das mit den Anmeldeinformationen **FileOperation** aus der letzten Vorführung verknüpft ist.
3. Führen Sie den Code unter dem Kommentar aus, der mit **Task 2** beginnt, um die Katalogsicht **dbo.sysproxies** anzuzeigen.
4. Führen Sie den Code unter dem Kommentar aus, der mit **Task 3** beginnt, um den Inhalt der Systemansicht **dbo.syssubsystems** anzuzeigen. Beachten Sie, dass die **subsystem\_id** des Subsystems **CmdExec** den Wert **3** hat.
5. Führen Sie den Code unter dem Kommentar aus, der mit **Task 4** beginnt, um das Proxykonto **FileOp** mit dem Subsystem **CmdExec** (**@subsystem\_id = 3**) zu verknüpfen.
6. Klicken Sie im Objekt-Explorer unter **Aufträge** mit der rechten Maustaste auf **Exportdatei kopieren**, und klicken Sie auf **Eigenschaften**.
7. Klicken Sie im Fenster **Auftragseigenschaften - Exportdatei kopieren** auf der Seite **Schritte** auf **Bearbeiten**.
8. Klicken Sie im Fenster **Auftragungsschritt-Eigenschaften - Datei kopieren** in der Liste **Typ** auf **Betriebssystem (CmdExec)**.
9. Klicken Sie in der Liste **Ausführen als** auf **FileOp**, und klicken Sie auf **OK**.
10. Klicken Sie im Fenster **Auftragseigenschaften - Exportdatei kopieren** auf **OK**.
11. Navigieren Sie im Datei-Explorer zu **D:\Demofiles\Mod09\ImportData**, um zu zeigen, dass der Ordner leer ist.
12. Klicken Sie in SQL Server Management Studio im Objekt-Explorer unter **Aufträge** mit der rechten Maustaste auf **Exportdatei kopieren**, und klicken Sie auf **Auftrag starten bei Schritt**.
13. Vergewissern Sie sich im Dialogfeld **Aufträge starten - MIA-SQL**, dass der Auftrag erfolgreich ausgeführt wurde, und klicken Sie auf **Schließen**.
14. Zeigen Sie im Datei-Explorer, dass der Ordner jetzt eine Kopie der Datei aus dem Ordner **ExportData** enthält, und schließen Sie den Datei-Explorer.
15. Schließen Sie SQL Server Management Studio, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

- Verwenden Sie einen Windows-Domänenbenutzer als SQL Server-Agent-Dienstkonto.
- Verwenden Sie ein Konto mit minimalen Berechtigungen.
- Erstellen Sie Proxykonten mit minimalen Berechtigungen für die Auftragsausführung.

## Fragen zur Lernzielkontrolle

**Frage:** Warum sollten Proxykonten normalerweise nicht zum Zugriff auf alle Subsysteme von Auftragschritten berechtigt sein?

**Antwort:** Auf Grundlage des Prinzips der „geringsten Rechte“.

Proxykonten sollten immer die minimal erforderlichen Berechtigungen zum Erfüllen von Aufgaben im jeweiligen Sicherheitskontext haben. Entfernen Sie nicht benötigte Berechtigungen, um das Risiko von versehentlichen oder böswilligen Fehlkonfigurationen zu vermeiden, die das System beschädigen könnten.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Konfigurieren der Sicherheit für den SQL Server-Agent

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Das SQL Server Integration Services-Paket in dieser Übungseinheit verwendet SQL Server-Authentifizierung, um sich für die Extraktion der Daten mit der Instanz MIA-SQL zu verbinden. Unter welchem Sicherheitskontext wird die Verbindung hergestellt, wenn der Auftrag **Generate Sales Log** von **ADVENTUREWORKS\Administrator** ausgeführt und das SQL Server Integration Services-Paket für die Verwendung der Windows-Authentifizierung für die Datenbankverbindung konfiguriert ist?

Gehen Sie bei der Auswahl Ihrer Antwort davon aus, dass die Übung erfolgreich abgeschlossen wurde.

- ADVENTUREWORKS\Administrator
- PromoteApp
- ADVENTUREWORKS\Student
- SQL Server-Agent-Dienstkonto

**Antwort:**

- ADVENTUREWORKS\Administrator
- PromoteApp
- ADVENTUREWORKS\Student
- SQL Server-Agent-Dienstkonto

# Unterrichtseinheit 10

## Überwachen von SQL Server mithilfe von Warnungen und Benachrichtigungen

### Inhalt:

Lektion 1: Überwachen von SQL Server-Fehlern	2
Lektion 2: Konfigurieren von Datenbank-E-Mail	5
Lektion 3: Operatoren, Warnungen und Benachrichtigungen	8
Lektion 4: Warnungen in Azure SQL-Datenbank	12
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	15
Fragen und Antworten zur Zusammenfassung der Übungseinheit	16

## Lektion 1

# Überwachen von SQL Server-Fehlern

### Inhalt:

Fragen und Antworten	3
Vorführung: Arbeiten mit dem Fehlerprotokoll der Datenbank-Engine	3

## Fragen und Antworten

**Frage:** Welche der folgenden Bereiche von Schweregraden werden für reine Informationsmeldungen verwendet?

- 0 bis 10
- 11 bis 16
- 17 bis 19
- 20 bis 24

**Antwort:**

- 0 bis 10
- 11 bis 16
- 17 bis 19
- 20 bis 24

## Vorführung: Arbeiten mit dem Fehlerprotokoll der Datenbank-Engine

### Vorführungsschritte

Anzeigen des SQL Server-Fehlerprotokolls

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55.wrd** bei **21764C-MIA-SQL** an.
2. Führen Sie im Ordner **D:\Demofiles\Mod10** die Datei **Setup.cmd** als Administrator aus.
3. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine-Instanz **MIA-SQL** her.
4. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** nacheinander die Einträge **Verwaltung** und **SQL Server-Protokolle**.
5. Klicken Sie mit der rechten Maustaste auf **Aktuell**, und klicken Sie auf **SQL Server-Protokoll anzeigen**.
6. Beachten Sie die Protokolleinträge im Fenster **Protokolldateianzeige - MIA-SQL**. Wenn Sie einen Protokolleintrag auswählen, werden die entsprechenden Details im unteren Bereich angezeigt.
7. Erweitern Sie im Bereich **Protokolle auswählen** den Eintrag **SQL Server-Agent**, und wählen Sie **Aktuell** aus.
8. Führen Sie im Hauptbereich der Protokolleinträge einen Bildlauf nach rechts durch, bis die Spalte **Protokolltyp** angezeigt wird, und führen Sie anschließend einen Bildlauf nach unten durch, bis Sie einen Eintrag mit dem Protokolltyp **SQL Server-Agent** sehen.
9. Sehen Sie sich die Protokolleinträge an, und klicken Sie anschließend auf **Schließen**.
10. Navigieren Sie im Datei-Explorer zum Ordner **C:\Programme\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Log**.
11. Falls das Dialogfeld **Protokoll** angezeigt wird, klicken Sie auf **Weiter**.
12. Falls das Dialogfeld **Benutzerkontensteuerung** angezeigt wird, klicken Sie auf **Ja**.
13. Beachten Sie, dass das aktuelle SQL Server-Protokoll in der Datei mit dem Namen **ERRORLOG** gespeichert ist, und das aktuelle SQL Server-Agent-Protokoll als **SQLAGENT.1**. Die restlichen Protokolldateien enthalten Einträge für andere SQL Server-Komponenten und -Dienste.

### Rotieren der Protokolldatei

1. Klicken Sie in SSMS auf **Neue Abfrage**.
2. Geben Sie den folgenden Code im Abfragefenster ein, und klicken Sie auf **Ausführen**:

```
EXEC sys.sp_cycle_errorlog;
```

3. Klicken Sie im Objekt-Explorer unter SQL Server-Protokolle mit der rechten Maustaste auf **Aktuell**, und klicken Sie auf **SQL Server-Protokoll anzeigen**.
4. Vergewissern Sie sich im Fenster **Protokolldateianzeige - MIA-SQL**, dass das Protokoll neu initialisiert wurde, und klicken Sie auf **Schließen**.
5. Schließen Sie das Abfragefenster, ohne Ihre Änderungen zu speichern, aber lassen Sie SSMS für die nächste Vorführung geöffnet.

## Lektion 2

# Konfigurieren von Datenbank-E-Mail

### **Inhalt:**

Fragen und Antworten	6
Vorführung: Konfigurieren von Datenbank-E-Mail	6

## Fragen und Antworten

**Frage:** Sie behandeln ein Problem in Datenbank-E-Mail. Sie möchten eine je Liste der E-Mail-Nachrichten anzeigen, die erfolgreich verschickt wurden und die nicht verschickt werden konnten. Wo finden Sie diese Informationen?

**Antwort:** Abfragen der Ansichten **dbo.sysmail\_sentitems** und **dbo.sysmail\_faileditems** in der **msdb**-Datenbank.

Die von Datenbank-E-Mail verschickten Nachrichten werden in der Ansicht **msdb.dbo.sysmail\_sentitems** angezeigt. Nachrichten, bei deren Versand ein Fehler aufgetreten ist, werden in der Ansicht **msdb.dbo.sysmail\_faileditems** angezeigt.

## Vorführung: Konfigurieren von Datenbank-E-Mail

### Vorführungsschritte

Erstellen eines Datenbank-E-Mail-Profiles

1. Klicken Sie im Objekt-Explorer unter **MIA-SQL** unter **Verwaltung** mit der rechten Maustaste auf **Datenbank-E-Mail**, und klicken Sie auf **Datenbank-E-Mail konfigurieren**.
2. Klicken Sie auf der Seite **Willkommen beim Konfigurations-Assistent für Datenbank-E-Mail** auf **Weiter**.
3. Klicken Sie auf der Seite **Konfigurationsaufgabe auswählen** auf **Datenbank-E-Mail durch Ausführen der folgenden Aufgaben einrichten**, und klicken Sie auf **Weiter**.
4. Geben Sie auf der Seite **Neues Profil** im Feld **Profilname** den Wert **SQL Server-Agent-Profil** ein, und klicken Sie auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Konto zu Profil „SQL Server-Agent-Profil“ hinzufügen** auf **Neues Konto**.
6. Geben Sie die folgenden Details im Dialogfeld **Neues Konto für Datenbank-E-Mail** ein, und klicken Sie auf **OK**:
  - **Kontoname:** AdventureWorks-Administrator
  - **E-Mail-Adresse:** administrator@adventureworks.msft
  - **Anzeigename:** Administrator (AdventureWorks)
  - **Antwort-E-Mail:** administrator@adventureworks.msft
  - **Servername:** mia-sql.adventureworks.msft
7. Klicken Sie auf der Seite **Neues Profil** auf **Weiter**.
8. Wählen Sie auf der Seite **Profilsicherheit verwalten** den Wert **Öffentlich** für das Profil **SQL Server Agent-Profil** aus, ändern Sie die Einstellung **Standardprofil** in **Ja**, und klicken Sie auf **Weiter**.
9. Klicken Sie auf der Seite **Systemparameter konfigurieren** auf **Weiter**.
10. Klicken Sie auf der Seite **Assistenten abschließen** auf **Fertig stellen**, warten Sie, bis die Konfiguration abgeschlossen wurde, und klicken Sie anschließend auf **Schließen**.

Verschicken einer E-Mail-Testnachricht

1. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Datenbank-E-Mail**, und klicken Sie auf **Test-E-Mail senden**.
2. Vergewissern Sie sich im Dialogfeld **Test-E-Mail senden von MIA-SQL**, dass das Datenbank-E-Mail-Profil **SQL Server Agent-Profil** ausgewählt ist.

3. Geben Sie im Feld **An** den Wert **student@adventureworks.msft** ein, und klicken Sie auf **Test-E-Mail senden**.
4. Navigieren Sie im Datei-Explorer zum Ordner **C:\inetpub\mailroot\Drop**, und vergewissern Sie sich, dass eine E-Mail-Nachricht verschickt wurde.
5. Doppelklicken Sie auf die Nachricht, um sie in Outlook zu öffnen. Lesen Sie die Nachricht, schließen Sie sie, und minimieren Sie das Fenster mit dem Ordner **Drop**.
6. Klicken Sie im Dialogfeld **Test-E-Mail von Datenbank-E-Mail** (befindet sich möglicherweise hinter SQL Server Management Studio) auf **OK**.

#### Abfragen der Datenbank-E-Mail-Systemtabellen

1. Zeigen Sie in SSMS im Menü **Datei** auf **Öffnen**, und klicken Sie auf **Projekt/Projektmappe**.
2. Navigieren Sie im Dialogfeld **Projekt öffnen** zu **D:\Demofiles\Mod10\Demo**, klicken Sie auf **Demo.ssmssl** und anschließend auf **Öffnen**.
3. Erweitern Sie im Projektmappen-Explorer den Eintrag **Abfragen**, doppelklicken Sie auf **Demo 2 - database mail.sql**, überprüfen Sie den Code, und klicken Sie auf **Ausführen**.
4. Überprüfen Sie die Ergebnisse. Das erste Resultset enthält Systemereignisse für Datenbank-E-Mail, und das zweite Resultset enthält Einträge mit den verschickten E-Mail-Nachrichten.
5. Lassen Sie die Projektmappe und SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 3

# Operatoren, Warnungen und Benachrichtigungen

### Inhalt:

Fragen und Antworten	9
Ressourcen	9
Vorführung: Konfigurieren von SQL Server-Agent-Operatoren	9
Vorführung: Konfigurieren von SQL Server-Agent-Warnungen	10

## Fragen und Antworten

**Frage:** Richtig oder falsch? Datenbank-E-Mail in SQL Server kann nur zum Versand von Warnungen und Benachrichtigungen verwendet werden.

- ( ) Richtig  
( ) Falsch

**Antwort:**

- ( ) Richtig  
(√) Falsch

## Ressourcen

### Übersicht über SQL Server-Warnungen



**Bewährte Methoden:** Konfigurieren Sie nach Möglichkeit Benachrichtigungen für alle Fehlermeldungen mit Schweregrad 19 und höher.

## Vorführung: Konfigurieren von SQL Server-Agent-Operatoren

### Vorführungsschritte

Aktivieren eines E-Mail-Profiles für den SQL Server-Agent

1. Klicken Sie im Objekt-Explorer unter **MIA-SQL** mit der rechten Maustaste auf **SQL Server-Agent**, und klicken Sie auf **Eigenschaften**.
2. Wählen Sie im Dialogfeld **Eigenschaften des SQL Server-Agents** auf der Seite **Warnungssystem** die Option **E-Mail-Profil aktivieren** aus.
3. Wählen Sie in der Dropdownliste **E-Mail-Profil** den Eintrag **SQL Server Agent-Profil** aus, und klicken Sie auf **OK**.
4. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **SQL Server-Agent**, und klicken Sie auf **Neu starten**.
5. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
6. Klicken Sie im Dialogfeld **Microsoft SQL Server Management Studio** auf **Ja**.

Erstellen eines Operators

1. Doppelklicken Sie im Projektmappen-Explorer auf **Demo 3 - operators.sql**.
2. Markieren Sie den Code unter dem Kommentar, der mit **Task 2** beginnt, und klicken Sie auf **Ausführen**, um einen neuen Operator mit dem Namen **Student** zu erstellen.

Konfigurieren eines Auftrags zum Benachrichtigen eines Operators

1. Erweitern Sie im Objekt-Explorer nacheinander die Einträge **SQL Server-Agent** und **Aufträge**, und sehen Sie sich die vorhandenen Aufträge an.
2. Klicken Sie mit der rechten Maustaste auf **Back Up Database - AdventureWorks**, und klicken Sie auf **Eigenschaften**.
3. Wählen Sie im Dialogfeld **Auftrageigenschaften - Back Up Database - AdventureWorks** auf der Seite **Benachrichtigungen** die Option **E-Mail** aus.

4. Klicken Sie in der ersten Dropdownliste auf **Student**.
5. Klicken Sie in der zweiten Dropdownliste auf **Beim Abschluss des Auftrags**, und klicken Sie auf **OK**.
6. Erweitern Sie im Objekt-Explorer den Eintrag **Operatoren**, klicken Sie mit der rechten Maustaste auf **Student**, und klicken Sie auf **Eigenschaften**.
7. Klicken Sie im Dialogfeld **Eigenschaften von Student** auf der Seite **Benachrichtigungen** auf **Aufträge**, beachten Sie die Auftragsbenachrichtigungen, die für diesen Operator definiert wurden, und klicken Sie auf **Abbrechen**.
8. Klicken Sie unter **Aufträge** mit der rechten Maustaste auf **Back Up Database - AdventureWorks**, und klicken Sie auf **Auftrag starten bei Schritt**.
9. Warten Sie, bis der Auftrag abgeschlossen wurde, und klicken Sie auf **Schließen**.
10. Klicken Sie unter **Operatoren** mit der rechten Maustaste auf **Student**, und klicken Sie auf **Eigenschaften**.
11. Beachten Sie im Dialogfeld **Eigenschaften von Student** auf der Seite **Verlauf** den aktuellen Benachrichtigungsversuch per E-Mail, und klicken Sie auf **Abbrechen**.
12. Vergewissern Sie sich im Datei-Explorer, dass eine neue E-Mail-Nachricht im Ordner **C:\inetpub\mailroot\Drop** erstellt wurde.
13. Doppelklicken Sie auf die neueste Datei, um sie in Outlook zu öffnen. Lesen Sie die Nachricht, schließen Sie sie, und minimieren Sie das Fenster mit dem Ordner **Drop**.
14. Lassen Sie die Projektmappe und SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Konfigurieren von SQL Server-Agent-Warnungen

### Vorführungsschritte

#### Erstellen einer Warnung

1. Klicken Sie im Objekt-Explorer unter **SQL Server-Agent** mit der rechten Maustaste auf **Warnungen**, und klicken Sie auf **Neue Warnung**.
2. Geben Sie im Dialogfeld **Neue Warnung** auf der Seite **Allgemein** im Feld **Name** den Wert **Warnung: Protokoll voll** ein.
3. Beachten Sie, dass Sie in der Dropdownliste **Typ** Warnungen für Ereignisse, Leistungsüberwachungsbedingungen und SQL Server-Ereignisse konfigurieren können, und klicken Sie auf **SQL Server-Ereigniswarnung**.
4. Klicken Sie auf **Fehlernummer**, und geben Sie **9002** in das Feld ein (SQL Server löst diese Fehlernummer aus, wenn ein Datenbanktransaktionsprotokoll voll ist).
5. Wählen Sie auf der Seite **Antwort** die Option **Operatoren benachrichtigen** aus, und wählen Sie das Kontrollkästchen **E-Mail** für den Operator **Student** aus.
6. Wählen Sie auf der Seite **Optionen** unter **Fehlermeldungstext übermitteln mit:** die Option **E-Mail** aus, und klicken Sie auf **OK**.

### Testen einer Warnung

1. Doppelklicken Sie im Projektmappen-Explorer auf **Demo 4 - alerts.sql**, und klicken Sie auf **Ausführen**. Warten Sie, während das Skript eine Tabelle in der Datenbank **TestAlertDB** füllt. Wenn die Protokolldatei für diese Datenbank voll ist, tritt der Fehler 9002 auf.
2. Erweitern Sie im Objekt-Explorer den Eintrag **Warnungen**, klicken Sie mit der rechten Maustaste auf **Warnung: Protokoll voll**, und klicken Sie auf **Eigenschaften**.
3. Beachten Sie im Dialogfeld **Warnungseigenschaften für „Warnung: Protokoll voll“** auf der Seite **Verlauf** die Werte unter **Datum der letzten Warnung** und **Datum der letzten Antwort**, und klicken Sie auf **Abbrechen**.
4. Vergewissern Sie sich im Datei-Explorer, dass eine neue E-Mail-Nachricht im Ordner **C:\inetpub\mailroot\Drop** erstellt wurde.
5. Doppelklicken Sie auf die neueste Nachricht, um sie in Outlook zu öffnen. Lesen Sie die Nachricht, schließen Sie sie, und schließen Sie das Fenster mit dem Ordner **Drop**.
6. Lassen Sie die Projektmappe und SSMS für die nächste Vorführung geöffnet.

## Lektion 4

# Warnungen in Azure SQL-Datenbank

### Inhalt:

Fragen und Antworten	12
Vorführung: Konfigurieren von Warnungen in Azure SQL-Datenbank	12

## Fragen und Antworten

**Frage:** Welche der folgenden Metriken kann **nicht** als Basis für eine Azure SQL-Datenbank-Warnung verwendet werden?

- DTU-Prozentsatz
- SQL Server-Fehlernummer 9002
- Datenbankgröße gesamt
- CPU-Prozentsatz
- Durch Firewall blockiert

**Antwort:**

- DTU-Prozentsatz
- SQL Server-Fehlernummer 9002
- Datenbankgröße gesamt
- CPU-Prozentsatz
- Durch Firewall blockiert

## Vorführung: Konfigurieren von Warnungen in Azure SQL-Datenbank

### Vorführungsschritte

1. Öffnen Sie Internet Explorer und gehen Sie zu <https://portal.azure.com/>.
2. Melden Sie sich mit Ihrem Azure Pass oder den Anmeldeinformationen Ihres Microsoft-Kontos beim Azure-Portal an.
3. Klicken Sie im Menü auf **SQL-Datenbanken**, und klicken Sie im Blatt **SQL-Datenbanken** auf **AdventureWorksLT**.
4. Klicken Sie im Blatt **Einstellungen** unter **Überwachung** auf **Warnungsregeln**.
5. Klicken Sie im Blatt **Warnungsregeln** auf **Warnung hinzufügen**.
6. Beachten Sie im Blatt **Warnungsregel hinzufügen**, dass das Feld **Ressource** automatisch mit dem Datenbanknamen vorausgefüllt wird.
7. Konfigurieren Sie die Warnung mit den folgenden Werten, und klicken Sie auf **OK**:
  - **Name:** AdventureWorksLT DTU-Nutzungswarnung.
  - **Metrik:** DTU-Prozentsatz.
  - **Bedingung:** größer als.
  - **Schwellenwert:** 1.
  - **Zeitraum:** Letzte 5 Minuten.
  - **Zusätzliche Administrator-E-Mail-Adressen:** Oder geben Sie Ihre E-Mail-Adresse ein, um die Warnung zu erhalten.
8. Doppelklicken Sie in SSMS im Projektmappen-Explorer auf **Demo 5 - azure.sql**.
9. Zeigen Sie im Menü **Abfrage** auf **Verbindung**, und klicken Sie auf **Verbindung ändern**.

10. Stellen Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** eine Verbindung mit dem Azure SQL-Datenbankserver her, auf dem Ihre Kopie der **AdventureWorksLT**-Datenbank gehostet wird. (Verwenden Sie für diese Verbindung die Anmeldeinformationen, die Sie beim Konfigurieren des Azure SQL-Datenbankservers festgelegt haben. Sie finden den Servernamen im Blatt **AdventureWorksLT** im Azure-Portal.)
11. Klicken Sie auf der Symbolleiste in der Liste **Verfügbare Datenbanken** auf **AdventureWorksLT**.
12. Klicken Sie auf der Symbolleiste auf **Ausführen**. Die Abfrage führt eine einfache SELECT-Anweisung 200 Mal aus. Dieser Vorgang sollte den DTU-Verbrauch in der Datenbank über 1 Prozent erhöhen.
13. Warten Sie im Azure-Portal, bis das Blatt **Warnungsregeln** aktualisiert wurde, und unter **ZULETZT AKTIV** ein anderer Wert als **Nie** angezeigt wird, was darauf hindeutet, dass die Warnung ausgelöst wurde. Dieser Vorgang kann mehrere Minuten dauern, und Sie müssen die Seite möglicherweise aktualisieren.
14. Klicken Sie im Blatt **Warnungsregeln** auf **AdventureWorksLT DTU-Nutzungswarnung**. Beachten Sie, dass die Warnungsmetrik über den Zeitraum als Liniendiagramm, und der Schwellenwert als gepunktete Linie dargestellt wird.
15. Klicken Sie auf **Löschen**, und klicken Sie auf **Ja**, um die Regel zu entfernen.
16. Falls Sie den Inhalt einer Warnungs-E-Mail zeigen möchten, melden Sie sich bei Ihrem Postfach an, und sehen Sie sich die von **Microsoft Azure-Warnungen** empfangene E-Mail an.
17. Schließen Sie Internet Explorer, und schließen Sie SSMS, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

Berücksichtigen Sie die folgenden bewährten Methoden, wenn Sie Datenbank-E-Mail verwenden und Benachrichtigungen und Warnungen in SQL Server planen:

- Konfigurieren Sie separate Datenbank-E-Mail-Profile für unterschiedliche Verwendungsszenarios.
- Schränken Sie die Berechtigung zum Versand von E-Mail-Nachrichten aus der Datenbank-Engine ein.
- Implementieren Sie eine Aufbewahrungsrichtlinie für Datenbank-E-Mail-Protokolle und E-Mail-Überprüfungen.
- Erstellen Sie einen Ausfallsicherheitsoperator.
- Definieren Sie Warnungen für Fehlermeldungen mit hohem Schweregrad.

## Fragen zur Lernzielkontrolle

**Frage:** Richtig oder falsch? Sie möchten einen Kollegen aus dem IT-Team als Operator zuweisen, aber dieser Kollege hat keine Anmeldung für die SQL Server-Instanz. Sie müssen eine Anmeldung für Ihren Kollegen definieren, bevor Sie ihn als Operator konfigurieren können.

Richtig

Falsch

**Antwort:**

Richtig

Falsch

**Frage:** Sie möchten Benachrichtigungen von SQL Server verschicken und sind der Ansicht, dass NET SEND-Benachrichtigungen praktischer sind als E-Mails. Warum sollten Sie diese Benachrichtigungen nicht verwenden?

**Antwort:** Broadcastnachrichten sind in den meisten modernen Betriebssystemen deaktiviert, daher werden die NET SEND-Nachrichten möglicherweise nicht angezeigt. Die NET SEND-Benachrichtigungsfunktion ist veraltet und wird in einer zukünftigen Version von SQL Server entfernt.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Überwachen von SQL Server mithilfe von Warnungen und Benachrichtigungen

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Unter welchen Umständen werden E-Mail-Benachrichtigungen an den von Ihnen erstellten Operator DBA-Team verschickt?

**Antwort:** Der Operator DBA-Team ist der Ausfallsicherheitsoperator. Der Ausfallsicherheitsoperator erhält Benachrichtigungen und Warnungen, wenn **msdb** nicht erreichbar ist, oder wenn kein Pager-Operator im Dienst ist.

Als Ausfallsicherheitsoperator wird der Operator DBA-Team benachrichtigt, wenn SQL Server aufgrund eines Fehlers nicht auf die Konfigurationstabellen von Datenbank-E-Mail in der **msdb**-Datenbank zugreifen kann. Wenn Pagerbenachrichtigungen aktiviert sind und kein anderer Operator im Dienst ist, werden Warnungen stattdessen an den Ausfallsicherheitsoperator verschickt.

# Unterrichtseinheit 11

## **Einführung in die Verwaltung von SQL Server mithilfe von PowerShell**

### **Inhalt:**

<b>Lektion 1:</b> Erste Schritte mit Windows PowerShell	2
<b>Lektion 2:</b> Konfigurieren von SQL Server mithilfe von PowerShell	5
<b>Lektion 3:</b> Verwalten und Warten von SQL Server mit PowerShell	7
<b>Lektion 4:</b> Verwalten von Azure SQL-Datenbank mit PowerShell	9
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	12
Fragen und Antworten zur Zusammenfassung der Übungseinheit	13

## Lektion 1

# Erste Schritte mit Windows PowerShell

### Inhalt:

Fragen und Antworten	3
Ressourcen	3
Vorführung: Erkunden von SQL Server Management Objects	3

## Fragen und Antworten

**Frage:** Was ist ein PowerShell-Alias?

- Eine PowerShell-Variable.
- Die Unix-Alternative zu PowerShell-Cmdlets.
- Eine vertraute Befehlszeilenverknüpfung für ein PowerShell-Cmdlet.
- Eine Möglichkeit, um weitere Informationen über ein Cmdlet abzurufen.
- Die vollständige Version eines Cmdlets.

**Antwort:**

- Eine PowerShell-Variable.
- Die Unix-Alternative zu PowerShell-Cmdlets.
- Eine vertraute Befehlszeilenverknüpfung für ein PowerShell-Cmdlet.
- Eine Möglichkeit, um weitere Informationen über ein Cmdlet abzurufen.
- Die vollständige Version eines Cmdlets.

## Ressourcen

### PowerShell-Anbieter

 **Weitere Informationen:** Weiterführende Informationen zu Windows PowerShell erhalten Sie im Buch *Learn Windows PowerShell in a Month of Lunches* (Don Jones und Jeffery D. Hicks, in Englischer Sprache). Dieses Buch wird von Manning veröffentlicht, und ist als E-Book erhältlich.

## Vorführung: Erkunden von SQL Server Management Objects

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie **Setup.cmd** im Ordner **D:\Demofiles\Mod11** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Klicken Sie auf der Taskleiste mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie auf **Als Administrator ausführen**.
5. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
6. Vergewissern Sie sich, dass in der Titelleiste der PowerShell-Konsole Folgendes angezeigt wird: **Administrator: Windows PowerShell**.
7. Geben Sie an der Eingabeaufforderung **cd \** ein, und drücken Sie die EINGABETASTE.
8. Geben Sie an der Eingabeaufforderung **Get-Alias** ein, und drücken Sie die EINGABETASTE, um herauszufinden, warum normale Befehle in PowerShell zu funktionieren scheinen.
9. Geben Sie an der Eingabeaufforderung **Get-Alias c\*** ein, und drücken Sie die EINGABETASTE.
10. Geben Sie an der Eingabeaufforderung **Update-Help -Force -ErrorAction SilentlyContinue** ein, und drücken Sie die EINGABETASTE. Warten Sie, bis die Hilfedateien installiert wurden.

11. Geben Sie an der Eingabeaufforderung **Get-Help** ein, und drücken Sie die EINGABETASTE.
12. Geben Sie an der Eingabeaufforderung **Get-Help Get-Help** ein, und drücken Sie die EINGABETASTE.
13. Geben Sie an der Eingabeaufforderung **Get-Help Get-Item** ein, und drücken Sie die EINGABETASTE.
14. Geben Sie für die folgenden Cmdlets an der Eingabeaufforderung zunächst das Cmdlet ein, und drücken Sie die EINGABETASTE, um die jeweiligen Parameter anzuzeigen:

**Get-Help Get-Item -Examples**

**Get-Help Get-Item -Detailed**

**Get-Help Get-Item -ShowWindow**

15. Schließen Sie das „Get-Item“-Hilfefenster.
16. Geben Sie an der Eingabeaufforderung **Get-I** ein, und drücken Sie TAB.
17. Drücken Sie TAB mehrmals, um alle Cmdlets anzuzeigen, die mit „Get-I“ beginnen.
18. Drücken Sie UMSCHALT+TAB, um die Cmdlets rückwärts zu durchlaufen. Beachten Sie, dass die Groß- und Kleinschreibung automatisch korrigiert wird.
19. Drücken Sie ESC.
20. Geben Sie an der Eingabeaufforderung **Get-PSProvider** ein, und drücken Sie die EINGABETASTE.
21. Geben Sie an der Eingabeaufforderung **Get-PSDrive** ein, und drücken Sie die EINGABETASTE.
22. Geben Sie an der Eingabeaufforderung **Import-Module SQLPS** ein, und drücken Sie die EINGABETASTE.
23. Wiederholen Sie die Schritte 20 und 21, und beachten Sie die neuen Einträge in der Liste.
24. Geben Sie an der Eingabeaufforderung **Set-Location SQLSERVER:\** oder **cd SQLSERVER:\** ein, und drücken Sie die EINGABETASTE.
25. Geben Sie an der Eingabeaufforderung **Get-ChildItem** ein, und drücken Sie die EINGABETASTE.
26. Geben Sie an der Eingabeaufforderung **Set-Location SQL** ein, und drücken Sie die EINGABETASTE.
27. Geben Sie an der Eingabeaufforderung **Get-ChildItem** ein, und drücken Sie die EINGABETASTE.
28. Geben Sie an der Eingabeaufforderung **Set-Location MIA-SQL** ein, und drücken Sie die EINGABETASTE.
29. Geben Sie an der Eingabeaufforderung **Get-ChildItem** ein, und drücken Sie die EINGABETASTE.
30. Geben Sie an der Eingabeaufforderung **Set-Location Default** ein, und drücken Sie die EINGABETASTE.
31. Geben Sie an der Eingabeaufforderung **Get-ChildItem** ein, und drücken Sie die EINGABETASTE.
32. Überprüfen Sie die Liste der Objekte, und machen Sie sich deren Zuordnung zu Objekten in SQL Server bewusst.
33. Geben Sie an der Eingabeaufforderung **Set-Location Databases** ein, und drücken Sie die EINGABETASTE.
34. Geben Sie an der Eingabeaufforderung **Get-ChildItem** ein, und drücken Sie die EINGABETASTE.
35. Geben Sie an der Eingabeaufforderung **exit** ein, und drücken Sie die EINGABETASTE.

## Lektion 2

# Konfigurieren von SQL Server mithilfe von PowerShell

### **Inhalt:**

Fragen und Antworten

6

## Fragen und Antworten

Bringen Sie die folgenden Schritte in die richtige Reihenfolge, indem Sie sie durchnummerieren.

Schritte
Importieren des SQL PowerShell-Moduls.
Verwenden des SQL PowerShell-Anbieters, um zu einem SMO-Objekt zu navigieren.
Zuweisen eines SMO-Objekts zu einer Variable.
Abrufen der Objekteigenschaften mit „Get-Member“.
Ändern einer Eigenschaft.
Übernehmen der Änderung mit der Methode „Alter“.

**Antwort:**

Schritte	
1	Importieren des SQL PowerShell-Moduls.
2	Verwenden des SQL PowerShell-Anbieters, um zu einem SMO-Objekt zu navigieren.
3	Zuweisen eines SMO-Objekts zu einer Variable.
4	Abrufen der Objekteigenschaften mit „Get-Member“.
5	Ändern einer Eigenschaft.
6	Übernehmen der Änderung mit der Methode „Alter“.

## Lektion 3

# Verwalten und Warten von SQL Server mit PowerShell

### Inhalt:

Ressourcen	8
Vorführung: PowerShell für die Problembehandlung	8

## Ressourcen

### Verwalten von Benutzern und Rollen

 **Weitere Informationen:** Weitere Informationen zum Automatisieren von SQL-Aufgaben finden Sie im Buch *SQL Server 2014 with PowerShell v5 Cookbook* (Donabel Santos, Packt Publishing, in Englischer Sprache).

### Vorführung: PowerShell für die Problembehandlung

#### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Geben Sie im Startmenü **Windows PowerShell ISE** ein, klicken Sie mit der rechten Maustaste auf **Windows PowerShell ISE**, und klicken Sie auf **Als Administrator ausführen**.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Klicken Sie im Menü **Datei** auf **Öffnen**.
5. Navigieren Sie im Dialogfeld **Öffnen** zu **D:\Demofiles\Mod11**, klicken Sie auf **InspectSqlInstances.ps1**, und dann auf **Öffnen**.
6. Markieren Sie den Code unter dem Kommentar **#1#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um das SQL-Modul zu importieren.
7. Markieren Sie den Code unter dem Kommentar **#2#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um den Speicherort zu laden.
8. Markieren Sie den Code unter dem Kommentar **#3#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um die SQL Server-Instanzen anzuzeigen.
9. Markieren Sie den Code unter dem Kommentar **#4#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um eine formatierte Liste der SQL Server-Instanzen anzuzeigen.
10. Markieren Sie den Code unter dem Kommentar **#5#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um eine Liste der Datenbanken in absteigender Reihenfolge nach deren Größe anzuzeigen.
11. Markieren Sie den Code unter dem Kommentar **#6#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um eine tabellarische Liste der Datenbanken in absteigender Reihenfolge nach deren Größe anzuzeigen.
12. Markieren Sie den Code unter dem Kommentar **#7#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um die Informationen in eine Textdatei zu schreiben.
13. Markieren Sie den Code unter dem Kommentar **#8#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um die Informationen in eine XML-Datei zu schreiben.
14. Markieren Sie den Code unter dem Kommentar **#9#**, und klicken Sie auf der Symbolleiste auf **Auswahl ausführen**, um die Informationen in eine Excel-Datei zu schreiben.
15. Schließen Sie die PowerShell-ISE, ohne die Änderungen zu speichern.

## Lektion 4

# Verwalten von Azure SQL-Datenbank mit PowerShell

### Inhalt:

Fragen und Antworten	10
Vorführung: Erstellen einer Azure SQL-Datenbank mithilfe von PowerShell	10

## Fragen und Antworten

**Frage:** Welche Vorteile bietet die Nutzung von PowerShell zusammen mit Microsoft Azure?

**Antwort:** Die Antworten hängen von den Erfahrungen der Kursteilnehmer mit Microsoft Azure ab. Ein Vorteil ist die Möglichkeit, standardisierte und getestete Skripts zu erstellen, um identische Datenbanken oder virtuelle Computer einzurichten. Dies ist hilfreich in Umgebungen mit mehreren Instanzen oder in Unternehmen, die ihre Datenbanken oder VMs (Virtuelle Computer, oder Virtual Machines) schnell und exakt erstellen möchten. Speicherkonten können ebenfalls mit PowerShell verwaltet werden.

## Vorführung: Erstellen einer Azure SQL-Datenbank mithilfe von PowerShell

### Vorführungsschritte

Installieren des AzureRM PowerShell-Moduls

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Geben Sie im Startmenü **Windows PowerShell** ein, klicken Sie mit der rechten Maustaste auf **Windows PowerShell**, und klicken Sie auf **Als Administrator ausführen**.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Geben Sie an der Eingabeaufforderung **Install-Module Azure** ein, und drücken Sie die EINGABETASTE.
5. Geben Sie in der Meldung **Der NuGet-Anbieter ist erforderlich, um den Vorgang fortzusetzen Ja** ein, und drücken Sie die EINGABETASTE.
6. Drücken Sie in der Meldung **Nicht vertrauenswürdiges Repository** auf **A**, und drücken Sie die EINGABETASTE.
7. Warten Sie, bis die Installation abgeschlossen ist, und schließen Sie dann das PowerShell-Fenster.
8. Geben Sie an der Eingabeaufforderung **cd\** ein, und drücken Sie die EINGABETASTE.
9. Geben Sie an der Eingabeaufforderung **cls** ein, und drücken Sie die EINGABETASTE.

Erstellen einer Azure SQL-Datenbank

1. Geben Sie an der Eingabeaufforderung das folgende Cmdlet, um Ihr Azure-Konto mit PowerShell zu verknüpfen, und drücken Sie die EINGABETASTE:

```
Add-AzureRmAccount
```

2. Geben Sie **J** ein, um die Datensammlung zu aktivieren.
3. Geben Sie im Azure-Anmeldebildschirm den Benutzernamen und das Kennwort ein, mit denen Sie sich beim Azure-Portal anmelden, und klicken Sie auf **Anmelden**.
4. Geben Sie das folgende Cmdlet an der Eingabeaufforderung ein, um Ihr Azure-Konto mit der PowerShell auf dieser VM zu verknüpfen:

```
Login-AzureRmAccount
```

5. Warten Sie, bis der Azure-Anmeldebildschirm angezeigt wird, geben Sie den Benutzernamen und das Kennwort ein, mit denen Sie sich beim Azure-Portal anmelden, und klicken Sie auf **Anmelden**.
6. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, und drücken Sie die EINGABETASTE: Ersetzen Sie **<IhreAbonnementID>** durch die im vorherigen Schritt zurückgegebene **SubscriptionID**:

```
Select-AzureRmSubscription -SubscriptionID <IhreAbonnementID>
```

7. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, um eine Liste der Azure-Rechenzentrumsstandorte zurückzugeben, und drücken Sie die EINGABETASTE:

```
(Get-AzureRmResourceProvider -ListAvailable | Where-Object {$_.ProviderNamespace -eq 'Microsoft.Sql'}).Locations
```

8. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, um eine Ressourcengruppe zu erstellen, und drücken Sie die EINGABETASTE. Ersetzen Sie <Standort> durch einen Standort aus der Liste aus dem vorherigen Schritt:

```
New-AzureRmResourceGroup -Name "21764CTest" -Location "<Standort>"
```

9. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, um einen neuen Server in der soeben erstellten Ressourcengruppe zu erstellen, und drücken Sie die EINGABETASTE. Ersetzen Sie <Standort> durch den Standort, den Sie im vorherigen Schritt verwendet haben. Ersetzen Sie <Name Ihres Servers> durch einen eindeutigen Servernamen. Dieser Name muss im gesamten Azure-Dienst eindeutig sein, und kann daher hier nicht angegeben werden. Ein empfohlenes Format ist sql2016ps-<Ihre Initialen> <eine oder mehrere Ziffern>. Zum Beispiel sql2016ps-js123. Alle Buchstaben müssen Kleinbuchstaben sein.

```
New-AzureRmSqlServer -ResourceGroupName "21764CTest" -ServerName "<Name Ihres Servers>" -Location "<Standort>" -ServerVersion "12.0"
```

10. Geben Sie im Dialogfeld **Bei Windows PowerShell anmelden** im Feld **Benutzername** den Wert **psUser** und im Feld **Kennwort** den Wert **Pa55w.rd** ein, und klicken Sie auf **OK**. Warten Sie, bis Azure den Administrator für Ihren Server erstellt hat und die Informationen in der Ko angezeigt werden.
11. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, um eine Variable zum Speichern Ihrer externen IP-Adresse zu erstellen, und drücken Sie die EINGABETASTE. Ersetzen Sie den Parameter <Ihre externe IP> durch Ihre eigene IP-Adresse:

```
$currentIP = "<Ihre externe IP>"
```



**Hinweis:** Sie können Ihre aktuelle externe IP-Adresse entweder im Azure-Portal (über den Wert, den die Schaltfläche „Client-IP hinzufügen“ in der Firewall für einen vorhandenen Server zurückgibt) oder über einen externen Dienst wie [www.whatismyip.com](http://www.whatismyip.com) herausfinden.

12. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, um eine Firewallregel zu erstellen, die Verbindungen zum Server erlaubt, und drücken Sie die EINGABETASTE. Ersetzen Sie den Parameter <Name Ihres Servers> durch den Namen Ihres Servers:

```
New-AzureRmSqlServerFirewallRule -ResourceGroupName "21764CTest" -ServerName "<Name Ihres Servers>" -FirewallRuleName "Firewall1" -StartIpAddress $currentIP -EndIpAddress $currentIP
```

13. Geben Sie an der Eingabeaufforderung das folgende Cmdlet ein, um eine neue Azure SQL-Datenbank auf dem soeben erstellten Server zu erstellen, und drücken Sie die EINGABETASTE. Ersetzen Sie <Name Ihres Servers> durch den Namen Ihres Servers:

```
New-AzureRmSqlDatabase -ResourceGroupName "21764CTest" -ServerName "<Name Ihres Servers>" -DatabaseName "testpsdb" -Edition Standard -RequestedServiceObjectiveName "S1"
```

Dieser Vorgang wird einige Minuten dauern. Warten Sie, bis die Details der neuen Datenbank zurückgegeben werden, um anzuzeigen, dass die Datenbank erstellt wurde.

14. Schließen Sie Windows PowerShell.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

Verwenden Sie Aliase bei der Arbeit im Konsolenfenster, und verwenden Sie die korrekte Groß- und Kleinschreibung in Cmdlet-Namen, um die Lesbarkeit Ihrer Skripts zu verbessern.

## Fragen zur Lernzielkontrolle

**Frage:** Welche Aufgaben eignen sich für die Automatisierung mit PowerShell in Ihrer SQL Server-Umgebung?

**Antwort:** Verschiedene Antworten sind möglich, darunter: Melden von Problemen aus den Fehlerprotokollen, Melden von Problemen aus anderen installierten Microsoft-Produkten, die sich auf SQL Server auswirken können, und Berichte zu SQL Server-Instanzen.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Verwalten von SQL Server mithilfe von PowerShell

### Fragen und Antworten

#### Erste Schritte mit PowerShell

**Frage:** Richtig oder falsch? PowerShell-Anbieter sind eine Alternative zur Verwendung von SQL Server Management Objects.

- Richtig
- Falsch

**Antwort:**

- Richtig
- Falsch

#### Zusammenfassung der Übungseinheit

**Frage:** Was ist ein SMO-Objekt?

- Ein SQL PowerShell-Anbieter.
- Ein Objekt zur programmgesteuerten Verwaltung von SQL Server-Komponenten.
- Eine SQL Server-Funktion zur Verbesserung der Leistung.
- Ein Teil des Windows-Betriebssystems.
- Das Objekt auf der obersten Ebene der SQL Server-Hierarchie.

**Antwort:**

- Ein SQL PowerShell-Anbieter.
- Ein Objekt zur programmgesteuerten Verwaltung von SQL Server-Komponenten.
- Eine SQL Server-Funktion zur Verbesserung der Leistung.
- Ein Teil des Windows-Betriebssystems.
- Das Objekt auf der obersten Ebene der SQL Server-Hierarchie.

**Frage:** Kennen Sie drei Möglichkeiten, um Informationen über ein Cmdlet abzurufen?

**Antwort:** Vervollständigung mit der TAB-TASTE, „Get-Help“ und „Get-Command“.

**Frage:** In welchem Fall würden Sie einen PowerShell-Anbieter verwenden?

**Antwort:** Für den Zugriff auf Datenspeicher wie SMO-Objekte, das Dateisystem oder die Registrierung. Der SQL PowerShell-Anbieter ist im SQLPS-Modul enthalten. Dieses Modul muss importiert werden, um SMO-Objekte verwenden zu können.

# Unterrichtseinheit 12

## Verfolgen des Zugriffs auf SQL Server mit erweiterten Ereignissen

### Inhalt:

Lektion 1: Grundkonzepte von erweiterten Ereignissen	2
Lektion 2: Arbeiten mit erweiterten Ereignissen	5
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	9
Fragen und Antworten zur Zusammenfassung der Übungseinheit	10

## Lektion 1

# Grundkonzepte von erweiterten Ereignissen

### Inhalt:

Fragen und Antworten	3
Vorführung: Erstellen einer erweiterten Ereignissitzung	3

## Fragen und Antworten

**Frage:** Welche System-DMV enthält die Liste aller Ereignisse, die in einer aktiven erweiterten Ereignissitzung definiert wurden?

- sys.dm\_xe\_session\_targets
- sys.dm\_xe\_session\_events
- sys.dm\_xe\_sessions
- sys.dm\_xe\_session\_event\_actions

**Antwort:**

- sys.dm\_xe\_session\_targets
- sys.dm\_xe\_session\_events
- sys.dm\_xe\_sessions
- sys.dm\_xe\_session\_event\_actions

## Vorführung: Erstellen einer erweiterten Ereignissitzung

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie im Ordner **D:\Demofiles\Mod12** die Datei **Setup.cmd** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**, und warten Sie, bis das Skript beendet wurde.
4. Starten Sie SQL Server Management Studio, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine-Instanz **MIA-SQL** her.
5. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie auf **Projekt/Projektmappe**.
6. Navigieren Sie im Dialogfeld **Projekt öffnen** zum Ordner **D:\Demofiles\Mod12**, klicken Sie auf **Demo.ssmssl** und anschließend auf **Öffnen**.
7. Erweitern Sie im Projektmappen-Explorer den Bereich **Abfragen**, und doppelklicken Sie auf **Demo 1 - create xe session.sql**.
8. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 1** beginnt, und klicken Sie auf **Ausführen**, um eine erweiterte Ereignissitzung zu erstellen.
9. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 2** beginnt, und klicken Sie auf **Ausführen**, um zu überprüfen, ob die Sitzungsmetadaten sichtbar sind.
10. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 3** beginnt, und klicken Sie auf **Ausführen**, um die Sitzung zu starten und einige Abfragen auszuführen.
11. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 4** beginnt, und klicken Sie auf **Ausführen**, um die Sitzungsdaten abzufragen.
12. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 5** beginnt, und klicken Sie auf **Ausführen**, um die Sitzungsdatenabfrage zu verfeinern.
13. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** nacheinander die Einträge **Verwaltung**, **Erweiterte Ereignisse**, **Sitzungen**, und **SqlStatementCompleted**, und doppelklicken Sie auf **package0.ring\_buffer**.

14. Klicken Sie in der Spalte **Data** auf den XML-Wert, und beachten Sie, dass hier derselbe Wert steht, den auch die Abfrage unter dem Kommentar zurückgegeben hat, der mit **Schritt 4** beginnt (außerdem wurden weitere Anweisungen erfasst, weil Sie den Code bereits zuvor ausgeführt haben).
15. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **SqlStatementCompleted**, und klicken Sie auf **Livedaten ansehen**.
16. Markieren Sie im Abfragebereich **Demo 1 - create xe sessions.sql** den Code unter dem Kommentar, der mit **Schritt 7** beginnt, und klicken Sie auf **Ausführen**, um einige SQL-Anweisungen auszuführen.
17. Kehren Sie zum Bereich **MIA-SQL - SqlStatementCompleted: Livedaten** zurück. Warten Sie einige Sekunden, bis die Ereignisse erfasst und angezeigt werden. Möglicherweise werden noch weitere SQL-Anweisungen aus Hintergrundprozessen von der Sitzung erfasst.
18. Wiederholen Sie die Schritte 16 und 17, falls die Ergebnisse nicht angezeigt werden.
19. Markieren Sie im Abfragebereich **Demo 1 - create xe sessions.sql** den Code unter dem Kommentar, der mit **Schritt 8** beginnt, und klicken Sie auf **Ausführen**, um die Sitzung zu beenden.
20. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **SqlStatementCompleted**, und klicken Sie auf **Eigenschaften**.
21. Überprüfen Sie im Dialogfeld **Sitzungseigenschaften** die Einstellungen auf den Seiten **Allgemein**, **Ereignisse**, **Datenspeicher** und **Erweitert**, und beachten Sie bei Bedarf die Sitzungsdefinition unter dem Kommentar, der mit **Schritt 1** beginnt.
22. Klicken Sie im Dialogfeld **Sitzungseigenschaften** auf **Abbrechen**.
23. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 10** beginnt, und klicken Sie auf **Ausführen**, um die Sitzung zu verwerfen.
24. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Arbeiten mit erweiterten Ereignissen

### Inhalt:

Fragen und Antworten	6
Vorführung: Nachverfolgen von Wartestatistiken auf Sitzungsebene	7

## Fragen und Antworten

Ordnen Sie die einzelnen Zieltypen für erweiterte Ereignisse in die passende Kategorie ein. Geben Sie Ihre Antwort an, indem Sie rechts neben jedem Element die Kategorienummer notieren.

Elemente	
1	Ringpuffer-Ziel
2	Ereignisdatei-Ziel
3	Histogramm-Ziel
4	Ereignisablaufverfolgung für Windows-Ziel
5	Ereignispaar-Ziel
6	Ereigniszähler-Ziel

Kategorie 1	Kategorie 2
Schreibt in Speicherpuffer	Schreibt in eine Datei auf dem Datenträger

**Antwort:**

Kategorie 1	Kategorie 2
Schreibt in Speicherpuffer	Schreibt in eine Datei auf dem Datenträger
Ringpuffer-Ziel Histogramm-Ziel Ereignispaar-Ziel Ereigniszähler-Ziel	Ereignisdatei-Ziel Ereignisablaufverfolgung für Windows-Ziel

**Vorführung: Nachverfolgen von Wartestatistiken auf Sitzungsebene****Vorführungsschritte**

1. Doppelklicken Sie in SSMS im Projektmappen-Explorer auf **Demo 2 - track waits by session.sql**.
2. Erweitern Sie im Objekt-Explorer nacheinander die Einträge **Verwaltung** und **Erweiterte Ereignisse**, klicken Sie mit der rechten Maustaste auf **Sitzungen**, und klicken Sie auf **Neue Sitzung**.
3. Geben Sie im Dialogfeld **Neue Sitzung** auf der Seite **Allgemein** im Feld **Sitzungsname** den Wert **Wartevorgänge pro Sitzung** ein.
4. Geben Sie auf der Seite **Ereignisse** im Feld **Ereignisbibliothek** den Wert **wait** ein, und doppelklicken Sie in der Liste darunter auf **wait\_info**, um diesen Wert zur Liste **Ausgewählte Ereignisse** hinzuzufügen.
5. Klicken Sie auf **Konfigurieren**, um die Liste **Optionen für die Ereigniskonfiguration** anzuzeigen.
6. Wählen Sie in der Liste **Optionen für die Ereigniskonfiguration** auf der Registerkarte **Globale Felder (Aktionen)** den Wert **session\_id** aus.
7. Klicken Sie auf der Registerkarte **Filter (Prädikat)** auf **Klicken Sie hier, um eine Klausel hinzuzufügen**.
8. Klicken Sie in der Liste **Feld** auf **sqlserver.session\_id**, klicken Sie in der Liste **Operator** auf **>**, und geben Sie im Feld **Wert** den Wert **50** ein. Dieser Filter schließt die meisten Systemsitzungen aus der Sitzung aus.
9. Klicken Sie auf der Seite **Datenspeicher** auf **Klicken Sie hier, um ein Ziel hinzuzufügen**.
10. Klicken Sie in der Liste **Typ** auf **event\_file**, geben Sie im Feld **Dateiname auf Server** den Wert **D:\Demofiles\Mod12\waitbysession** ein, geben Sie im ersten Feld **Maximale Dateigröße** den Wert **5** ein, klicken Sie im zweiten Feld **Maximale Dateigröße** auf **MB**, und klicken Sie anschließend auf **OK**.
11. Erweitern Sie im Objekt-Explorer den Eintrag **Sitzungen**, klicken Sie mit der rechten Maustaste auf **Wartevorgänge pro Sitzung**, und klicken Sie auf **Sitzung starten**.

12. Klicken Sie im Datei-Explorer im Ordner **D:\Demofiles\Mod12** mit der rechten Maustaste auf **start\_load\_1.ps1**, und klicken Sie auf **Mit PowerShell ausführen**. Wenn Sie aufgefordert werden, eine Änderung an der Ausführungsrichtlinie zu bestätigen, drücken Sie auf **J**, und drücken Sie die EINGABETASTE. Lassen Sie die Arbeitsauslastung etwa eine Minute lang laufen, bevor Sie fortfahren.
13. Markieren Sie in SSMS im Bereich **Demo 2 - track waits by session.sql** den Code unter dem Kommentar, der mit **Schritt 14** beginnt, klicken Sie auf **Ausführen**, und sehen Sie sich das Resultat an.
14. Markieren Sie den Code unter dem Kommentar, der mit **Schritt 15** beginnt, und klicken Sie auf **Ausführen**, um die Sitzung zu beenden und zu löschen, und um die Arbeitsauslastung zu beenden.
15. Beachten Sie im Datei-Explorer im Ordner **D:\Demofiles\Mod12**, dass eine oder mehrere Dateien mit dem Namensmuster **waitbysession\*.xel** erstellt wurden.
16. Schließen Sie den Datei-Explorer, schließen Sie SSMS, ohne die Änderungen zu speichern, und drücken Sie die EINGABETASTE im Windows PowerShell-Fenster, um das Fenster zu schließen.

## Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

**Frage:** Welche der folgenden Quellen enthält **keine** ausführlichen Informationen zu den erweiterten Ereignisdefinitionen?

- ( ) Die GUI für erweiterte Ereignisse in SQL Server Management Studio.
- ( ) Die DMV „sys.dm\_xe\_objects“.
- ( ) Die technische SQL Server-Dokumentation.

**Antwort:**

- ( ) Die GUI für erweiterte Ereignisse in SQL Server Management Studio.
- ( ) Die DMV „sys.dm\_xe\_objects“.
- (✓) Die technische SQL Server-Dokumentation.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Erweiterte Ereignisse

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Wie können Sie die von einer erweiterten Ereignissitzung generierten Daten anzeigen, wenn für die Sitzung keine Ziele definiert sind?

**Antwort:** Mit der Funktion **Livedaten ansehen** in SSMS. Rechtsklick auf den Sitzungsnamen in SSMS, und Klick auf **Livedaten ansehen**.

# Unterrichtseinheit 13

## Überwachen von SQL Server

### Inhalt:

Lektion 1: Überwachen der Aktivität	2
Lektion 2: Erfassen und Verwalten von Leistungsdaten	7
Lektion 3: Analysieren der gesammelten Leistungsdaten	10
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	14
Fragen und Antworten zur Zusammenfassung der Übungseinheit	15

## Lektion 1

# Überwachen der Aktivität

### Inhalt:

Fragen und Antworten	3
Vorführung: Anzeigen von Aktivitäten mithilfe von DMOs	3
Vorführung: Verwenden des Aktivitätsmonitors in SQL Server Management Studio	4
Vorführung: Verwenden der Leistungsüberwachung	5

## Fragen und Antworten

**Frage:** Aus welchem Grund kann es Sinn machen, die System-DMV **sys.dm\_os\_performance\_counters** anstelle der Leistungsüberwachung zu verwenden, um auf SQL Server-Zähler zuzugreifen?

**Antwort:** Mit Abfragen an die System-DMV **sys.dm\_os\_performance\_counters** können Sie Informationen aus den Systemleistungsindikatoren mit Daten aus internen Leistungstools wie anderen DMOs vergleichen. Die Übersichtsinformationen aus den Leistungsindikatoren können mit den ausführlichen Informationen zum Verhalten einzelner Sitzungen und Abfragebatches aus anderen DMOs kombiniert werden. Auf diese Weise erhalten Sie detaillierte Einblicke in die Auswirkungen unterschiedlicher Arbeitsauslastungen auf die Leistung von SQL Server und können automatisierte Prozesse erstellen, um die Leistungsdaten zu überwachen und auf Änderungen zu reagieren.

## Vorführung: Anzeigen von Aktivitäten mithilfe von DMOs

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Klicken Sie im Ordner **D:\Demofiles\Mod13** mit der rechten Maustaste auf **Setup.cmd**, und klicken Sie dann auf **Als Administrator ausführen**.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**, und warten Sie, bis das Skript beendet wurde.
4. Doppelklicken Sie im Ordner **D:\Demofiles\Mod13** auf **Workload1.cmd**.
5. Starten Sie **SQL Server Management Studio**, und stellen Sie unter Verwendung der Windows-Authentifizierung eine Verbindung mit der Datenbank-Engine-Instanz **MIA-SQL** her.
6. Zeigen Sie im Menü **Datei** auf **Öffnen**, und klicken Sie auf **Projekt/Projektmappe**.
7. Navigieren Sie im Dialogfeld **Projekt öffnen** zum Ordner **D:\Demofiles\Mod13\Demo**, und doppelklicken Sie auf **Demo.ssmssl.n**.
8. Erweitern Sie im Projektmappen-Explorer den Bereich **Abfragen**, und doppelklicken Sie auf **Demo 1 - DMO.sql**.
9. Führen Sie den Code unter der Überschrift aus, die mit **Task 2** beginnt, um die aktuell ausgeführten Anfragen anzuzeigen. Daraufhin sollten etwa 50 Zeilen zurückgegeben werden, von denen die meisten jedoch Systemanfragen sind.
10. Führen Sie den Code unter der Überschrift aus, die mit **Task 3** beginnt, um die aktuell Benutzerprozesse anzuzeigen.
11. Führen Sie den Code unter der Überschrift aus, die mit **Task 4** beginnt, um die ausgeführten Anfragen nach Benutzersitzungen zu filtern, um nur Aktivitäten von Benutzern anzuzeigen.
12. Führen Sie den Code unter der Überschrift aus, die mit **Task 5** beginnt, um Details zu den Transact-SQL-Batches der einzelnen Anfragen anzuzeigen.
13. Führen Sie den Code unter der Überschrift aus, die mit **Task 6** beginnt, um Details zu den Transact-SQL-Anweisungen anzuzeigen, die momentan in den einzelnen Batches ausgeführt werden. Diese Anweisung ist komplex, gibt aber im Grunde genommen eine Teilzeichenfolge aus dem Ergebnis des vorherigen Schritts zurück.

14. Führen Sie den Code unter der Überschrift aus, die mit **Task 7** beginnt, um das Skript für die Arbeitsauslastung zu beenden. (Die Arbeitsauslastung ist so konfiguriert, dass sie beendet wird, wenn die globale temporäre Tabelle **##stopload** erstellt wird.)
15. Führen Sie den Code unter der Überschrift aus, die mit **Task 8** beginnt, um den Inhalt des Abfrageplan-cache anzuzeigen.
16. Führen Sie den Code unter der Überschrift aus, die mit **Task 9** beginnt, um die 10 teuersten Abfragen im Abfrageplan-cache basierend auf durchschnittlichen logischen Schreibvorgängen zu identifizieren.
17. Führen Sie den Code unter der Überschrift aus, die mit **Task 10** beginnt, um E/A-Statistiken für die Datenbankdateien anzuzeigen.
18. Führen Sie den Code unter der Überschrift aus, die mit **Task 11** beginnt, um Statistiken zu Wartevorgängen anzuzeigen. An dieser Abfrage erkennen Sie den Bereich von Wartetypen, für die Statistiken erhoben werden.
19. Klicken Sie im Menü **Datei** auf **Schließen**.
20. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Verwenden des Aktivitätsmonitors in SQL Server Management Studio

### Vorführungsschritte

1. Doppelklicken Sie in SQL Server Management Studio im Projektmappen-Explorer auf **Demo 2a - blocker.sql**.
2. Lesen Sie den Inhalt der Datei, beachten Sie, dass in der Datei eine Transaktion ohne anschließenden Commit begonnen wird, und klicken Sie auf **Ausführen**.
3. Doppelklicken Sie im Projektmappen-Explorer auf **Demo 2b - blocked.sql**, und klicken Sie auf **Ausführen**. Dabei wird kein Resultset zurückgegeben, und die Abfrage wird nicht zu Ende ausgeführt. Der Zugriff dieser Abfrage auf die Tabelle **HR.Employees** wird durch die Transaktion blockiert, die Sie im vorherigen Schritt geöffnet haben.
4. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **MIA-SQL**, und klicken Sie auf **Aktivitätsmonitor**.
5. Klicken Sie im Bereich **MIA-SQL-Aktivitätsmonitor** auf **Prozesse**, um den Bereich **Prozesse** zu erweitern.
6. Klicken Sie im Bereich **Prozesse** in der Spalte **Datenbankname** in der Spaltenüberschrift auf die Schaltfläche **Filter**, und klicken Sie auf **InternetSales**.
7. Beachten Sie, dass für einen der Prozesse der **Taskstatus** als **ANGEHALTEN** angezeigt wird. Dabei handelt es sich um die Abfrage aus dem Abfragebereich „Demo 2b - blocked.sql“.
8. Zeigen Sie auf die Überschrift der Spalte **Blockiert durch**, um zu zeigen, dass in der QuickInfo für die Spalte die DMO-Spalte angezeigt wird, aus der die Informationen stammen:  
**sys.dm\_os\_waiting\_tasks.blocking\_session\_id**.
9. Beachten Sie den Wert in der Spalte **Blockiert durch** in der Zeile **ANGEHALTEN**. Hier sehen Sie die Sitzungs-ID der blockierenden Sitzung: die Abfrage aus dem Abfragebereich „Demo 2a - blocker.sql“.
10. Klicken Sie im Bereich **Prozesse** in der Spalte **Sitzungs-ID** in der Spaltenüberschrift auf die Schaltfläche **Filter**, und klicken Sie auf den Wert der Sitzung, die Sie im vorherigen Schritt als Ursache für die Blockierung identifiziert haben. Im Bereich **Prozesse** sollte jetzt nur noch eine Zeile angezeigt werden. Beachten Sie, dass in der Spalte **Kopfzeilenblockierung** der Wert **1** angezeigt wird. Dieser Wert bedeutet, dass die Sitzung die erste in einer Blockierungskette ist.

11. Klicken Sie im Bereich **Prozesse** mit der rechten Maustaste auf die Zeile, und klicken Sie mit der rechten Maustaste auf **Prozess abbrechen**.
12. Klicken Sie im Dialogfeld **Prozess abbrechen** auf **Ja**, um einen Rollback für die Abfrage im Abfragebereich „Demo 2a - blocker.sql“ auszuführen.



**Hinweis:** Prozesse sollten nur als letzter Ausweg abgebrochen werden.

13. Schließen Sie den MIA-SQL-Aktivitätsmonitor.
14. Beachten Sie im Bereich **Demo 2b - blocked.sql**, dass die Abfrage abgeschlossen wurde, da die Blockierung entfernt wurde.
15. Schließen Sie beide Bereiche.
16. Klicken Sie im Dialogfeld **Microsoft SQL Server Management Studio** auf **Nein**.
17. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Verwenden der Leistungsüberwachung

### Vorführungsschritte

1. Klicken Sie auf **Start**, klicken Sie auf **Verwaltung**, und doppelklicken Sie anschließend auf **Leistungsüberwachung**.
2. Erweitern Sie im Fenster **Leistungsüberwachung** im linken Bereich nacheinander die Einträge **Datensammlungssätze** und **System**, und klicken Sie auf **Systemleistung**.
3. Doppelklicken Sie im rechten Bereich auf **Leistungsindikator**.
4. Sehen Sie sich im Dialogfeld **Eigenschaften der Leistungsindikatoren** die verschiedenen Leistungsindikatoren an, die dieser Satz sammelt, und klicken Sie auf **Abbrechen**.
5. Klicken Sie im linken Bereich mit der rechten Maustaste auf **Systemleistung**, und klicken Sie auf **Start**. Daraufhin ändert sich das Symbol für den Sammlersatz **Systemleistung**, um anzuzeigen, dass der Satz ausgeführt wird. Der Sammlersatz sammelt eine Minute lang Daten, und wird anschließend automatisch beendet. Warten Sie, bis der Sammlersatz abgeschlossen wurde, und das Symbol wieder zu seiner ursprünglichen Form wechselt.
6. Klicken Sie im Menü **Aktion** auf **Aktuellster Bericht**. Beachten Sie, dass in der Baumstruktur im linken Bereich neue Knoten hinzugefügt werden. Erweitern Sie im rechten Bereich die einzelnen Abschnitte des Berichts, um die gesammelten Informationen zu zeigen.
7. Sehen Sie sich den Bericht an, und klicken Sie im linken Bereich anschließend auf **Leistungsüberwachung**. Daraufhin wird im rechten Bereich ein Diagramm angezeigt, in dem der Zähler **Prozessorzeit (%)** bereits ausgewählt ist.
8. Klicken Sie mit der rechten Maustaste an eine beliebige Stelle im rechten Bereich, und klicken Sie auf **Zähler hinzufügen**.
9. Klicken Sie im Dialogfeld **Zähler hinzufügen** in der Liste **Verfügbare Zähler** auf die folgenden Zähler, und klicken Sie anschließend auf **Hinzufügen >>**, um die Zähler hinzuzufügen:
  - a. **SQLServer:Speicher-Manager: Serverspeicher gesamt (KB)**
  - b. **SQLServer:Speicher-Manager: Zielserverspeicher (KB)**
  - c. **SQLServer:Datenbanken: Prozentsatz der Protokollverwendung** (Instanz **InternetSales**)
  - d. **MSSQL\$SQL2:Speicher-Manager: Serverspeicher gesamt (KB)**
10. Klicken Sie auf **OK**.

11. Sehen Sie sich die Änderungen im Diagramm der Leistungsüberwachung an, und schließen Sie die Leistungsüberwachung.
12. Doppelklicken Sie in SQL Server Management Studio im Projektmappen-Explorer auf **Demo 3 - counters.sql**.
13. Führen Sie den Code in der Datei aus, um zu zeigen, dass die SQL Server-Leistungsüberwachungszähler über die System-DMV **sys.dm\_os\_performance\_counters** erreichbar sind.
14. Klicken Sie im Menü **Datei** auf **Schließen**.
15. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Lektion 2

# Erfassen und Verwalten von Leistungsdaten

### Inhalt:

Fragen und Antworten	7
Vorführung: Konfigurieren von Datensammlern	7

## Fragen und Antworten

**Frage:** Richtig oder falsch? Sie können den SQL Server-Datensammler für die Echtzeitüberwachung verwenden.

- ( ) Richtig
- ( ) Falsch

**Antwort:**

- ( ) Richtig
- (√) Falsch

## Vorführung: Konfigurieren von Datensammlern

### Vorführungsschritte

Konfigurieren des Verwaltungs-Data Warehouses

1. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** den Eintrag **Verwaltung**, klicken Sie mit der rechten auf **Datensammlung**, zeigen Sie auf **Tasks**, und klicken Sie auf **Verwaltungs-Data Warehouse konfigurieren**.
2. Klicken Sie im Fenster **Assistent für die Konfiguration des Verwaltungs-Data Warehouses** auf **Weiter**.
3. Klicken Sie auf der Seite **Speicher des Verwaltungs-Data Warehouses konfigurieren** auf **Neu**.
4. Geben Sie im Dialogfeld **Neue Datenbank** im Feld **Datenbankname** den Wert **MDW** ein, und klicken Sie auf **OK**.
5. Klicken Sie auf der Seite **Speicher des Verwaltungs-Data Warehouses konfigurieren** auf **Weiter**.
6. Sehen Sie sich auf der Seite **Anmeldennamen und Benutzer zuordnen** die verfügbaren Optionen an, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite **Assistenten abschließen** auf **Fertig stellen**.
8. Warten Sie, bis die Konfiguration abgeschlossen wurde, und klicken Sie auf **Schließen**.

Registrieren der Instanz **MIA-SQL** für die Datensammlung

1. Klicken Sie im Objekt-Explorer unter **Verwaltung** mit der rechten Maustaste auf **Datensammlung**, zeigen Sie auf **Tasks**, und klicken Sie auf **Datensammlung konfigurieren**.
2. Klicken Sie im Fenster **Assistent für die Konfiguration der Datensammlung** auf **Weiter**.
3. Klicken Sie auf der Seite **Datensammlungssätze einrichten** neben dem Feld **Servername** auf die Schaltfläche mit den **Auslassungszeichen (...)**.
4. Vergewissern Sie sich im Dialogfeld **Verbindung mit Server herstellen**, dass im Feld **Servername** der Wert **MIA-SQL** steht, und klicken Sie auf **Verbinden**.
5. Klicken Sie auf der Seite **Datensammlungssätze einrichten** in der Liste **Datenbankname** auf **MDW**.
6. Wählen Sie unter **Zu aktivierende Datensammlungssätze auswählen** das Kontrollkästchen **Systemdaten-Sammlungssätze** aus, und klicken Sie auf **Weiter**.
7. Klicken Sie auf der Seite **Assistenten abschließen** auf **Fertig stellen**.

Konfigurieren eines Datensammlungssatzes

1. Erweitern Sie im Objekt-Explorer unter **Verwaltung** nacheinander die Einträge **Datensammlung** und **Systemdaten-Sammlungssätze**. Beachten Sie, dass einer der vier verfügbaren Sammlungssätze angehalten ist.
2. Klicken Sie mit der rechten Maustaste auf **Datenträgerverwendung**, und klicken Sie auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften für Datensammlungssätze** auf der Seite **Allgemein** auf **Auswählen**.
4. Klicken Sie im Dialogfeld **Zeitplan für Auftrag auswählen** auf **CollectorSchedule\_Every\_5min** (die Zeile mit **ID = 2**), und klicken Sie auf **OK**.
5. Klicken Sie im Dialogfeld **Eigenschaften für Datensammlungssätze** auf **OK**.
6. Doppelklicken Sie im Projektmappen-Explorer unter **Abfragen** auf **SSRS Fix 2017.sql**.
7. Klicken Sie auf **Ausführen**.
8. Führen Sie im Ordner **D:\Demofiles\Mod13** die Datei **Workload1.cmd** aus, und warten Sie das Ende der Ausführung ab. Dieses Skript generiert Aktivitäten für die Datensammlungsberichte in den Vorführungen der nächsten Lektion.

## Lektion 3

# Analysieren der gesammelten Leistungsdaten

### Inhalt:

Fragen und Antworten	11
Vorführung: Anzeigen des Berichts zur Datenträgerverwendung	11
Vorführung: Anzeigen des Berichts zur Serveraktivität	12
Vorführung: Anzeigen des Berichts zu Abfragestatistiken	12

## Fragen und Antworten

**Frage:** Mit welchem Systemdaten-Sammlungssatzbericht können Sie den Verlauf der Arbeitsspeicherverwendung abrufen?

- ( ) Der Bericht zur Serveraktivität.
- ( ) Der Bericht zu Abfragestatistiken.
- ( ) Der Bericht zur Datenträgerverwendung.

**Antwort:**

- (√) Der Bericht zur Serveraktivität.
- ( ) Der Bericht zu Abfragestatistiken.
- ( ) Der Bericht zur Datenträgerverwendung.

## Vorführung: Anzeigen des Berichts zur Datenträgerverwendung

### Vorführungsschritte

Erzwingen einer Datensammlung

1. Klicken Sie in SQL Server Management Studio im Objekt-Explorer unter **Verwaltung** unter **Datensammlung** unter **Systemdaten-Sammlungssätze** mit der rechten Maustaste auf **Datenträgerverwendung**, und klicken Sie auf **Auflisten und jetzt hochladen**.
2. Klicken Sie im Dialogfeld **Datensammlungssatz auflisten und hochladen** auf **Schließen**.
3. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Abfragestatistiken**, und klicken Sie mit der rechten Maustaste **Auflisten und jetzt hochladen**.
4. Klicken Sie im Dialogfeld **Datensammlungssatz auflisten und hochladen** auf **Schließen**.
5. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Serveraktivität**, und klicken Sie mit der rechten Maustaste **Auflisten und jetzt hochladen**.
6. Klicken Sie im Dialogfeld **Datensammlungssatz auflisten und hochladen** auf **Schließen**.

Zugreifen auf den Bericht zur Datenträgerverwendung

1. Erweitern Sie im Objekt-Explorer unter **MIA-SQL** den Eintrag **Datenbanken**, klicken Sie mit der rechten Maustaste auf **MDW**, zeigen Sie auf **Berichte**, zeigen Sie auf **Verwaltungs-Data Warehouse**, und klicken Sie auf **Verwaltungs-Data Warehouse - Übersicht**.
2. Sehen Sie sich die Hyperlinks unter den einzelnen Berichtsnamen mit dem Datum und der Uhrzeit der letzten Sammlung an. Klicken Sie unter **Datenträgerverwendung** auf den Hyperlink mit Datum und Uhrzeit.
3. Vergewissern Sie sich im Bericht **Sammlungssatz zur Datenträgerverwendung**, dass die Daten verfügbar sind, und klicken Sie auf **InternetSales**.
4. Beachten Sie die verfügbaren Informationen im Bericht **Datenträgerverwendung für Datenbank: InternetSales**, und klicken Sie im Berichtsbereich in der oberen linken Ecke auf die Schaltfläche **Rückwärts navigieren**, um zum Bericht **Sammlungssatz zur Datenträgerverwendung** zurückzukehren.
5. Klicken Sie in der Spalte **Trend protokollieren** auf die Trendlinie für die Datenbank **MDW**. Achten Sie darauf, genau auf die Linie zu klicken, der restliche Bereich der umgebenden Zelle hat nicht denselben Effekt.

6. Beachten Sie die verfügbaren Informationen im Bericht **Sammlungssatz zur Datenträgerverwendung - Protokoll: [MDW]**. Das Diagramm in diesem Bericht basiert auf den Prozentwerten für den freien Speicherplatz in der Datendatei.
7. Klicken Sie auf die Schaltfläche **Rückwärts navigieren**, um zum Bericht **Sammlungssatz zur Datenträgerverwendung** zurückzukehren.
8. Klicken Sie im Berichtsbereich auf die Schaltfläche **Rückwärts navigieren**, um zum Bericht **Verwaltungs-Data Warehouse - Übersicht: MDW** zurückzukehren.
9. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Anzeigen des Berichts zur Serveraktivität

### Vorführungsschritte

1. Klicken Sie in SQL Server Management Studio im Bereich **Verwaltungs-Data Warehouse - Übersicht** in der oberen linken Ecke des Berichtsbereichs auf die Schaltfläche **Aktualisieren**.
2. Klicken Sie im Hauptbericht unter **Serveraktivität** auf den Hyperlink mit Datum und Uhrzeit.
3. Sehen Sie sich im Bericht **Serveraktivität - Verlauf** die Zeitachse und die sechs Diagramme an. Erklären Sie, dass manche Diagramme leer sind, weil noch keine relevante Aktivität stattgefunden hat.
4. Zeigen Sie die Verwendung der Zeitachse, indem Sie unter der Zeitachse zweimal auf die Schaltfläche **Vergrößern** klicken. Beachten Sie, dass die dunkelblauen Vierecke, die jeweils einen Datensammlungspunkt darstellen, mit jedem Klick reduziert werden, und der Bereich der Daten in den Diagrammen an den ausgewählten Zeitbereich angepasst wird.
5. Klicken Sie im Diagramm **Arbeitsspeicherverwendung** auf die untere Linie, um einen Drillthrough auszuführen.
6. Führen Sie im Bericht **SQL Server-Arbeitsspeicherverwendung** einen Bildlauf nach unten durch, bis Sie zum Diagramm **Interne SQL Server-Arbeitsspeichernutzung nach Typ** gelangen.
7. Erweitern Sie den Bereich **Durchschnittliche Arbeitsspeicherverwendung nach Komponente** des Berichts, um ausführliche Informationen zur Arbeitsspeicherverwendung für die einzelnen SQL Server-Komponenten anzuzeigen.
8. Klicken Sie im Berichtsbereich in der oberen linken Ecke auf die Schaltfläche **Rückwärts navigieren**, um zum Bericht **Serveraktivität - Verlauf** zurückzukehren.
9. Klicken Sie im Berichtsbereich in der oberen linken Ecke fünfmal auf die Schaltfläche **Rückwärts navigieren**, um zum Bericht **Verwaltungs-Data Warehouse - Übersicht** zurückzukehren.
10. Lassen Sie SQL Server Management Studio für die nächste Vorführung geöffnet.

## Vorführung: Anzeigen des Berichts zu Abfragestatistiken

### Vorführungsschritte

1. Klicken Sie in SQL Server Management Studio im Bereich **Verwaltungs-Data Warehouse - Übersicht** in der oberen linken Ecke des Berichtsbereichs auf die Schaltfläche **Aktualisieren**.
2. Klicken Sie im Hauptbericht unter **Abfragestatistiken** auf den Hyperlink mit Datum und Uhrzeit.
3. Beachten Sie, dass der Bericht **Abfragestatistik - Verlauf** dasselbe Zeitachsensteuerelement zum Navigieren in den Daten verwendet wie der **Bericht zur Serveraktivität**.
4. Klicken Sie unter **Navigieren Sie mithilfe der Zeitachse unten durch die Verlaufsmomentaufnahmen von Daten** auf das Symbol .

5. Klicken Sie im Diagramm **Erste Abfragen nach CPU gesamt** auf **Dauer**, klicken Sie auf **E/A gesamt**, klicken Sie auf **Physische Lesevorgänge**, und klicken Sie anschließend auf **Logische Schreibvorgänge**, um die verschiedenen Datenansichten vorzuführen.
6. Klicken Sie auf **CPU**, um zur ursprünglichen Ansicht zurückzukehren.
7. Klicken Sie unter dem Bericht in der Spalte **Abfrage** in der Datentabelle auf die erste Zeile.
8. Führen Sie im Bericht **Abfragedetails** einen Bildlauf nach unten durch, um die verschiedenen Komponenten des Berichts anzuzeigen.
9. Klicken Sie am Ende des Berichts in der Tabelle **Erste Abfragepläne nach durchschnittlicher CPU-Zeit pro Ausführung** in der Spalte **Plan #** auf die erste Zeile.
10. Führen Sie im Bericht **Abfrageplandetails** einen Bildlauf nach unten durch, und klicken Sie im Bereich **Abfrageausführungsstatistik** auf **Grafischen Abfrageausführungsplan anzeigen**.
11. Daraufhin wird der Abfrageplan in einem neuen Bereich geöffnet.
12. Schließen Sie SQL Server Management Studio, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

In dieser Unterrichtseinheit haben Sie verschiedenen Möglichkeiten kennengelernt, um die Aktivität in SQL Server Datenbank-Engines zu überwachen:

- Verwenden von DMOs für Überwachung und Problembehandlung in Echtzeit.
- Verwenden des Aktivitätsmonitors für einfachen Zugriff auf die wichtigsten Informationen.
- Verwenden der Leistungsüberwachung zum Sammeln von Metriken für Windows und SQL Server.
- Erstellen eines zentralen Verwaltungs-Data Warehouse zum Speichern der gesammelten Leistungsinformationen.

## Fragen zur Lernzielkontrolle

**Frage:** Welche Tools für die Aktivitätsüberwachung in SQL Server eignen sich am besten für die Anforderungen Ihres Unternehmens?

**Antwort:** Es gibt unterschiedliche Antworten. DMOs und Aktivitätsmonitor sind besonders hilfreich für die Behebung von soeben aufgetretenen Problemen. Leistungsüberwachung und Datensammlung ermöglichen langfristige Einblicke in übergreifende Trends. Die meisten Unternehmen profitieren von einer Kombination dieser Tools.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Überwachen von SQL Server

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Welche Vorteile bietet ein zentrales Data Warehouse für SQL Server-Leistungsdaten gegenüber der lokalen Sammlung auf den einzelnen Servern?

**Antwort:** Es macht Sinn, Leistungsdaten an einem zentralen Ort zu speichern, um den Zugriff und die Berichterstellung zu vereinfachen.

Wenn sich die Leistungsdaten für Ihre SQL Server-Instanzen an einem einzigen zentralen Ort befinden, können Sie viel leichter auf die Daten zugreifen und Berichte erstellen. Außerdem können die Benutzer Leistungsdaten abfragen, ohne dafür Verbindungsberechtigungen für sämtliche Datenbank-Engine-Instanzen zu benötigen.

Mit zentral gespeicherten Leistungsdaten können Sie außerdem instanzübergreifende Muster erkennen und die Leistung ähnlicher Instanzen viel einfacher miteinander vergleichen, als wenn jede Instanz ihre eigenen Leistungsdaten enthielte.

# Unterrichtseinheit 14

## Problembehandlung für SQL Server

### Inhalt:

Lektion 1: Problembehandlungsmethodik für SQL Server	2
Lektion 2: Beheben dienstbezogener Probleme	4
Lektion 3: Beheben von Konnektivitäts- und Anmeldeproblemen	7
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	9
Fragen und Antworten zur Zusammenfassung der Übungseinheit	10

## Lektion 1

# Problembehandlungsmethodik für SQL Server

### **Inhalt:**

Fragen und Antworten

3

## Fragen und Antworten

Nummerieren Sie jede einzelne der folgenden Problembehandlungsphasen, um ihre richtige Reihenfolge anzugeben.

	Schritte
	Untersuchungsphase
	Analysephase
	Implementierungsphase
	Überprüfungsphase
	Erstellen der Dokumentation

**Antwort:**

	Schritte
1	Untersuchungsphase
2	Analysephase
3	Implementierungsphase
4	Überprüfungsphase
5	Erstellen der Dokumentation

## Lektion 2

# Beheben dienstbezogener Probleme

### Inhalt:

Fragen und Antworten	5
Vorführung: Problembehandlung bei dienstbezogenen Problemen	5

## Fragen und Antworten

**Frage:** In welchem/welchen Protokoll(en) finden Sie die meisten Informationen, wenn der SQL Server-Dienst nicht gestartet wird?

- Im Windows-Systemprotokoll.
- Im Windows-Anwendungsprotokoll.
- Im SQL Server-Fehlerprotokoll.
- Im SQL Server-Fehlerprotokoll und im Windows-Systemprotokoll.
- Im SQL Server-Fehlerprotokoll und im Windows-Anwendungsprotokoll.

**Antwort:**

- Im Windows-Systemprotokoll.
- Im Windows-Anwendungsprotokoll.
- Im SQL Server-Fehlerprotokoll.
- Im SQL Server-Fehlerprotokoll und im Windows-Systemprotokoll.
- Im SQL Server-Fehlerprotokoll und im Windows-Anwendungsprotokoll.

## Vorführung: Problembehandlung bei dienstbezogenen Problemen

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie **Setup.cmd** im Ordner **D:\Demofiles\Mod14** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Klicken Sie auf die Schaltfläche **Start**, geben Sie dann **Konfigurations-Manager** ein, und klicken Sie auf **SQL Server-Konfigurations-Manager**.
5. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
6. Klicken Sie im SQL Server-Konfigurations-Manager im linken Bereich auf **SQL Server-Dienste**.
7. Beachten Sie im rechten Bereich, dass der Dienst **SQL Server (SQL2)** nicht ausgeführt wird.
8. Klicken Sie mit der rechten Maustaste auf **SQL Server (SQL2)**, und klicken Sie auf **Start**. Beachten Sie, dass der Dienst nicht erfolgreich gestartet und eine Fehlermeldung zurückgegeben wird.
9. Klicken Sie im Dialogfeld **SQL Server-Konfigurations-Manager** auf **OK**.
10. Klicken Sie zum Überprüfen des Windows-Systemprotokolls auf **Start**, geben Sie **Ereignisanzeige** ein, und drücken Sie die EINGABETASTE.
11. Erweitern Sie in der Ereignisanzeige im linken Bereich **Windows-Protokolle**, und klicken Sie dann auf **System**.
12. Klicken Sie auf die neueste Meldung mit **Fehler** als **Ebene** und **Dienststeuerungs-Manager** als **Quelle**.
13. Beachten Sie auf der Registerkarte **Details**, ob die Fehlermeldung besagt, dass kein dienstspezifischer Fehler vorliegt, und nur die folgenden Details bereitstellt:

```
SQL Server (SQL2)
%%17113
```

14. Schließen Sie das Ereignisanzeige-Fenster.
15. Starten Sie zum Überprüfen des SQL Server-Fehlerprotokolls den Datei-Explorer, und navigieren Sie zu **C:\Programme\Microsoft SQL Server\MSSQL14.SQL2\MSSQL\Log**.
16. Wenn das Dialogfeld **Protokoll** angezeigt wird, klicken Sie auf **Weiter**.
17. Klicken Sie mit der rechten Maustaste auf **ERRORLOG**, klicken Sie auf **Öffnen mit**, und klicken Sie dann auf **Editor**. Beachten Sie, dass in den letzten drei Zeilen der Datei die im Windows-Systemprotokoll (17113) angezeigte Fehlernummer sowie eine detaillierte Beschreibung des Problems (scrollen Sie nach rechts, um die vollständige Fehlermeldung zu lesen) enthalten sind. Die Meldung gibt an, dass die Datendatei für die **Masterdatenbank** nicht gefunden werden kann.
18. Navigieren Sie im Datei-Explorer zum in der Fehlermeldung erwähnten Ordnerspeicherort (**C:\Programme\Microsoft SQL Server\MSSQL14.SQL2\MSSQL\DATA**).
19. Klicken Sie auf **Weiter**, sofern das Dialogfeld **DATA** angezeigt wird. Beachten Sie, dass im Ordner die Datei **master.AV0001** enthalten ist. Die Vorführung simuliert die Situation, in der die Datei **master.mdf** durch eine Antivirenanwendung in Quarantäne verschoben wurde, die sie in **master.AV0001** umbenannt hat.  
  
(In einem echten Szenario müssten Sie die Datei aus dem Quarantänesystem wiederherstellen und verhindern, dass die Antivirenanwendung diesen Ordner überprüft, bevor Sie versuchen, den Dienst neu zu starten.)
20. Benennen Sie zum Zwecke dieser Vorführung die Datei von **master.AV0001** in **master.mdf** um. Klicken Sie mit der rechten Maustaste auf **master.AV0001**, und klicken Sie dann auf **Umbenennen**.
21. Ersetzen Sie die Dateierweiterung **AV0001** durch **mdf**, und drücken Sie die EINGABETASTE.
22. Klicken Sie im Dialogfeld **Umbenennen** auf **Ja**.
23. Schließen Sie den Datei-Explorer.
24. Klicken Sie im SQL Server-Konfigurations-Manager im rechten Bereich mit der rechten Maustaste auf **SQL Server (SQL2)**, und klicken Sie dann auf **Start**. Beachten Sie, dass der Dienst erfolgreich gestartet wird.
25. Schließen Sie den SQL Server-Konfigurations-Manager und Editor.

## Lektion 3

# Beheben von Konnektivitäts- und Anmeldeproblemen

### Inhalt:

Fragen und Antworten

8

Ressourcen

8

## Fragen und Antworten

**Frage:** Sie möchten einen Alias für eine benannte Instanz der Datenbank-Engine definieren. Der Alias wird von Clients verwendet, die native Clienttreiber mit 32 und 64 Bit verwenden. Wo sollten Sie im SQL Server-Konfigurations-Manager den Alias definieren?

- Unter der SQL Native Client 11.0-Konfiguration.
- Unter der SQL Native Client 11.0-Konfiguration (32 Bit).
- Unter der SQL Native Client 11.0-Konfiguration (32 und 64 Bit).

**Antwort:**

- Unter der SQL Native Client 11.0-Konfiguration.
- Unter der SQL Native Client 11.0-Konfiguration (32 Bit).
- Unter der SQL Native Client 11.0-Konfiguration (32 und 64 Bit).

## Ressourcen



**Bewährte Methoden:** Durch auf der Windows-Authentifizierung basierende Benutzeranmeldungen entfällt für Sie als Datenbankadministrator die Notwendigkeit, sich um die meisten kennwort- und authentifizierungsbezogenen Probleme zu kümmern.

## Problembehandlung bei Konnektivitätsproblemen



**Bewährte Methoden:** Wenn Sie ein Netzwerkkonnektivitätsproblem in einem TCP-/IP-Netzwerk vermuten, sollten Sie zunächst unter Verwendung der IP-Adresse des Servers und ggf. der TCP-Portnummer eine Verbindung vom Client zum Server herstellen. Sollte eine Verbindung nach IP-Adresse fehlschlagen, hängt das Problem wahrscheinlich mit dem Netzwerk zusammen, etwa mit einem Routing- oder Firewallproblem. Wenn eine Verbindung nach IP-Adresse erfolgreich ist, die Verbindung nach Name jedoch fehlschlägt, hängt das Problem wahrscheinlich mit der Namensauflösung zusammen, also entweder mit dem DNS, dem SQL Server-Browserdienst oder den SQL Server-Aliasen.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Fragen zur Lernzielkontrolle

**Frage:** Wie bewerten Sie Ihre Problembehandlungsfähigkeiten? Wie können Sie sie verbessern?

**Antwort:** Es gibt jeweils unterschiedliche Antworten.

## Tools

Sie sollten sich in Onlineforen beteiligen, in denen Entwickler und Administratoren Fragen zu SQL Server-Problemen stellen, um Ihre Problembehandlungsfertigkeiten zu trainieren und um Einblicke hinsichtlich der von anderen Problemlösern verwendeten Methoden zu erhalten.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

Übungseinheit: Problembehandlung bei häufig auftretenden Problemen

Fragen und Antworten

Zusammenfassung der Übungseinheit

**Frage:** Welche Tools können Sie zum Überwachen eines zeitweiligen oder langfristigen Problems verwenden?

**Antwort:** Beim SQL Server-Datensammler, erweiterten Ereignissen und bei der SQL-Ablaufverfolgung handelt es sich um Beispiele von Tools, die Sie zur langfristigen Überwachung verwenden können.

# Unterrichtseinheit 15

## Importieren und Exportieren von Daten

### Inhalt:

Lektion 1: Übertragen von Daten in und aus SQL Server	2
Lektion 2: Importieren und Exportieren von Tabellendaten	6
Lektion 3: Verwenden von bcp und BULK INSERT zum Importieren von Daten	10
Lektion 4: Bereitstellen und Aktualisieren von Datenschichtenanwendungen	13
Lernzielkontrolle und Kernpunkte der Unterrichtseinheit	16
Fragen und Antworten zur Zusammenfassung der Übungseinheit	17

## Lektion 1

# Übertragen von Daten in und aus SQL Server

### Inhalt:

Fragen und Antworten	3
Ressourcen	3
Vorführung: Deaktivieren und Aktivieren von Einschränkungen	3
Vorführung: Wechseln von Partitionen für die Datenübertragung	4

## Fragen und Antworten

**Frage:** Wie wirkt sich das Deaktivieren des gruppierten Indizes auf eine Rowstore-Tabelle aus?

- ( ) Der Index wird ignoriert, die Tabelle kann jedoch aktualisiert werden.
- ( ) Die Tabelle wird schreibgeschützt.
- ( ) Die Tabelle ist vollständig unzugänglich.
- ( ) Die Tabelle wird gelöscht.

**Antwort:**

- ( ) Der Index wird ignoriert, die Tabelle kann jedoch aktualisiert werden.
- ( ) Die Tabelle wird schreibgeschützt.
- (✓) Die Tabelle ist vollständig unzugänglich.
- ( ) Die Tabelle wird gelöscht.

## Ressourcen

### Deaktivieren und Aktivieren von Einschränkungen



**Bewährte Methoden:** Im Allgemeinen sollten Sie die Primärschlüssel- oder Unique-Einschränkungen im Rahmen von Masseladevorgängen nur dann deaktivieren, wenn dies unbedingt erforderlich ist. Beide Einschränkungstypen sind kritisch für die Integrität Ihrer Daten. Es ist wahrscheinlich einfacher zu verhindern, dass ungültige Daten geladen werden, indem die gegebenen Primärschlüssel- und Unique-Einschränkungen beibehalten werden, als eine Korrektur nach einem Masseladevorgang vorzunehmen.

### Vorführung: Deaktivieren und Aktivieren von Einschränkungen

#### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-W2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** ausgeführt werden. Melden Sie sich anschließend als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Starten Sie **SQL Server Management Studio**, und stellen Sie mithilfe der SQL Server-Authentifizierung eine Verbindung mit Ihrer Azure-Instanz her, in der die **AdventureWorksLT**-Datenbank ausgeführt wird.
3. Öffnen Sie die Projektmappe **Demo.ssmssl** im Ordner **D:\Demofiles\Mod15\Demo**.
4. Öffnen Sie die Abfragedatei **Demo 01 - constraints.sql**.
5. Stellen Sie zwischen dem Abfragefenster und Ihrer Kopie der **AdventureWorksLT**-Datenbank eine Verbindung her.
6. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um zwei Tabellen für diese Vorführung zu erstellen.
7. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um den aktuellen Zustand der Check-Einschränkung anzuzeigen.
8. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um die Check-Einschränkung zu deaktivieren.

9. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um anzuzeigen, dass die Check-Einschränkung deaktiviert und als nicht vertrauenswürdig markiert ist.
10. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um die Check-Einschränkung mit CHECK zu aktivieren.
11. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, um anzuzeigen, dass die Einschränkung aktiviert und als nicht vertrauenswürdig markiert ist.
12. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um die Check-Einschränkung WITH CHECK CHECK zu aktivieren.
13. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um anzuzeigen, dass die Einschränkung aktiviert und vertrauenswürdig ist.
14. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um einen nicht gruppierten Primärschlüssel zu deaktivieren.
15. Führen Sie den Code unter der Überschrift für **Schritt 11** aus, um den Zustand der Indizes für die Tabelle anzuzeigen.
16. Führen Sie den Code unter der Überschrift für **Schritt 12** aus, um zu zeigen, dass die Daten weiterhin in die Tabelle eingefügt werden können.
17. Führen Sie den Code unter der Überschrift für **Schritt 13** aus, um den Index zu aktivieren.
18. Führen Sie den Code unter der Überschrift für **Schritt 14** aus, um den Zustand der Indizes für die Tabelle anzuzeigen.
19. Führen Sie den Code unter der Überschrift für **Schritt 15** aus, um eine gruppierte Primärschlüsseleinschränkung zu deaktivieren. Beachten Sie die durch diesen Befehl generierten Warnungen.
20. Führen Sie den Code unter der Überschrift für **Schritt 16** aus, um anzuzeigen, dass alle Indizes für die Tabelle deaktiviert sind.
21. Führen Sie den Code unter der Überschrift für **Schritt 17** aus, um den gruppierten Index zu aktivieren.
22. Führen Sie den Code unter der Überschrift für **Schritt 18** aus, um anzuzeigen, dass die nicht gruppierten Indizes deaktiviert bleiben.
23. Führen Sie den Code unter der Überschrift für **Schritt 19** aus, um den nicht gruppierten Index zu aktivieren.
24. Führen Sie den Code unter der Überschrift für **Schritt 20** aus, um die Fremdschlüsseleinschränkung zu aktivieren, die auf den gruppierten Primärschlüssel verweist.
25. Führen Sie den Code unter der Überschrift für **Schritt 21** aus, um die Vorführungsobjekte zu verwerfen.
26. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Vorführung: Wechseln von Partitionen für die Datenübertragung

### Vorführungsschritte

1. Öffnen Sie im Projektmappen-Explorer die Abfragedatei **Demo 02 - partition switch.sql**.
2. Stellen Sie zwischen dem Abfragefenster und Ihrer Kopie der **AdventureWorksLT**-Datenbank eine Verbindung her.
3. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine Partitionsfunktion, ein Partitionsschema und eine partitionierte Tabelle zu erstellen.

4. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um Daten zu erstellen und sie der nicht partitionierten Tabelle hinzuzufügen, die mit dem Schema der partitionierten Tabelle übereinstimmt.
5. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um Partition eins der partitionierten Tabelle mit der nicht partitionierten Tabelle zu wechseln.
6. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um die Auswirkung des Wechsels vorzuführen.
7. Führen Sie den Code unter der Überschrift für **Schritt 6** aus, um drei identische nicht partitionierte Tabellen zu erstellen und um **SalesLT.ShippingRate** Daten hinzuzufügen.
8. Führen Sie den Code unter der Überschrift für **Schritt 7** aus, der Datenlast **SalesLT.ShippingRateStaging** Daten hinzuzufügen.
9. Führen Sie den Code unter der Überschrift für **Schritt 8** aus, um die Partitionen zu wechseln. Beachten Sie die Verwendung der dritten Tabelle, sodass einer der Teilnehmer an einem Wechsel immer leer ist.
10. Führen Sie den Code unter der Überschrift für **Schritt 9** aus, um die Auswirkung des Wechsels vorzuführen.
11. Führen Sie den Code unter der Überschrift für **Schritt 10** aus, um die Vorführungsobjekte zu verwerfen.
12. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Lektion 2

# Importieren und Exportieren von Tabellendaten

### Inhalt:

Fragen und Antworten	7
Vorführung: Arbeiten mit SSIS	7
Vorführung: Verwenden des SQL Server-Import/Export-Assistenten	8

## Fragen und Antworten

**Frage:** Richtig oder falsch? Der Datenimport-/export-Assistent kann nur verwendet werden, um Daten in Microsoft-Formaten (wie Excel, Access und SQL Server) zu importieren und zu exportieren.

- ( ) Richtig  
( ) Falsch

**Antwort:**

- ( ) Richtig  
(v) Falsch

## Vorführung: Arbeiten mit SSIS

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Führen Sie **Setup.cmd** im Ordner **D:\Demofiles\Mod15** als Administrator aus.
3. Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.
4. Starten Sie Visual Studio, und öffnen Sie die Projektmappe **SSISProject.sln** im Ordner **D:\Demofiles\Mod15\SSISProject**.
5. Führen Sie die unterschiedlichen Bereiche eines SSIS-Projekts in Visual Studio kurz vor.
6. Doppelklicken Sie im Projektmappen-Explorer auf **Package.dtsx**.
7. Klicken Sie im Menü **SSIS** auf **SSIS-Toolbox**.
8. Klicken Sie auf **Datenflusstask**, und ziehen Sie die Option aus der SSIS-Toolbox in den Bereich „Package.dtsx [Design]“. Legen Sie **Datenflusstask** an einer beliebigen Position auf der Registerkarte **Ablaufsteuerung** des Bereichs „Package.dtsx [Design]“ ab.
9. Klicken Sie mit der rechten Maustaste auf **Datenflusstask**, klicken Sie auf **Umbenennen**, geben Sie **Namensimport auf oberster Domänenebene** ein, und drücken Sie die EINGABETASTE.
10. Doppelklicken Sie auf **Namensimport auf oberster Domänenebene**, um zur Registerkarte **Datenfluss** des Designers zu wechseln.
11. Klicken Sie im Bereich „SSIS-Toolbox“ auf **Quellen-Assistent**, und ziehen Sie diese Option auf die Registerkarte **Datenfluss** des Bereichs „Package.dtsx [Design]“.
12. Klicken Sie im Dialogfeld **Quellen-Assistent - Neue Quelle hinzufügen** im Feld **Quellentyp auswählen** auf **Flatfile**.
13. Doppelklicken Sie im Feld **Verbindungs-Manager auswählen** auf **Neu**.
14. Geben Sie im Dialogfeld **Verbindungs-Manager-Editor für Flatfiles** auf der Seite **Allgemein** im Feld **Name des Verbindungs-Managers** den Text **TLD-Datei** ein.
15. Geben Sie im Feld **Dateiname** den Pfad **D:\Demofiles\Mod15\Data\top\_level\_domains.txt** ein.
16. Geben Sie im Feld **Auszulassende Kopfzeilen** den Wert **1** ein.
17. Deaktivieren Sie das Kontrollkästchen **Spaltennamen in der ersten Datenzeile**.
18. Überprüfen Sie auf der Seite **Spalten** die Vorschau, um sich zu vergewissern, dass zwei Spalten angezeigt werden.

19. Ändern Sie auf der Seite **Erweitert** für **Spalte 0** den Wert **OutputColumnWidth** in **100**, und klicken Sie dann auf **OK**.
20. Klicken Sie mit der rechten Maustaste auf **Flatfilequelle**, klicken Sie auf **Umbenennen**, geben Sie **TLD-Dateiquelle** ein, und drücken Sie die EINGABETASTE.
21. Klicken Sie im Bereich „SSIS-Toolbox“ auf **Ziel-Assistent**, und ziehen Sie diese Option auf die Registerkarte **Datenfluss**.
22. Bestätigen Sie im Dialogfeld **Ziel-Assistent - Neues Ziel hinzufügen**, dass **SQL Server** für **Zieltyp auswählen** ausgewählt ist.
23. Klicken Sie im Feld **Verbindungs-Manager auswählen** auf **Neu** und dann auf **OK**.
24. Geben Sie im Dialogfeld **Verbindungs-Manager** im Feld **Servername** den Text **MIA-SQL** ein.
25. Klicken Sie in der Liste **Datenbanknamen eingeben oder auswählen** auf **salesapp1** und dann auf **Verbindung testen**.
26. Beachten Sie im Dialogfeld **Verbindungs-Manager**, ob der Test erfolgreich war, und klicken Sie dann auf **OK**.
27. Klicken Sie im Dialogfeld **Verbindungs-Manager** auf **OK**.
28. Klicken Sie mit der rechten Maustaste auf **OLE DB-Ziel**, klicken Sie auf **Umbenennen**, geben Sie **salesapp1 DB** ein, und drücken Sie die EINGABETASTE.
29. Klicken Sie auf **TLD-Dateiquelle**. Klicken Sie anschließend auf den linken (blauen) Pfeil unten auf dem Objekt **TLD-Dateiquelle**, und klicken Sie dann auf das Objekt **salesapp1 DB**.
30. Doppelklicken Sie auf das Objekt **salesapp1 DB**.
31. Klicken Sie im Dialogfeld **Ziel-Editor für OLE DB** auf der Seite **Verbindungs-Manager** in der Liste **Name der Tabelle oder Sicht** auf **[dbo].[TopLevelDomain]**. Heben Sie die Kontrollkästchen **Tabellensperre** und **Einschränkungen überprüfen** hervor, und verweisen Sie dabei auf die vorherige Lektion.
32. Klicken Sie auf der Seite **Zuordnungen** im ersten Feld **Eingabespalte** auf **Spalte 0**.
33. Klicken Sie im zweiten Feld **Eingabespalte** auf **Spalte 1** und dann auf **OK**.
34. Klicken Sie im Menü **Debuggen** auf die Option zum **Starten des Debugvorgangs**.
35. Klicken Sie im Menü **Debuggen** auf die Option zum **Anhalten des Debugvorgangs**, sobald das Paket abgeschlossen wurde.
36. Öffnen Sie in SQL Server Management Studio die Abfragedatei **Demo 03 - SSIS.sql**.
37. Zeigen Sie im Menü **Abfrage** auf **Verbindung**, und klicken Sie dann auf **Verbindung ändern**.
38. Geben Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** im Feld **Servername** den Text **MIA-SQL** ein, und klicken Sie in der Liste **Authentifizierung** auf **Windows-Authentifizierung** und dann auf **Verbinden**.
39. Führen Sie die Abfrage in der Datei aus, um den hochgeladenen Inhalt der Tabelle **dbo.TopLevelDomain** anzuzeigen.
40. Schließen Sie Visual Studio, ohne die Änderungen zu speichern. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Vorführung: Verwenden des SQL Server-Import/Export-Assistenten

### Vorführungsschritte

1. Vergewissern Sie sich, dass die virtuellen Computer **MT17B-WS2016-NAT**, **21764C-MIA-DC** und **21764C-MIA-SQL** laufen, und melden Sie sich als **ADVENTUREWORKS\Student** mit dem Kennwort **Pa55w.rd** bei **21764C-MIA-SQL** an.
2. Klicken Sie in **SQL Server Management Studio** im **Objekt-Explorer** auf **Verbinden**, und klicken Sie dann auf **Datenbankmodul**.
3. Geben Sie im Dialogfeld **Verbindung mit Datenbankmodul herstellen** im Feld **Servername** den Text **MIA-SQL** ein, und klicken Sie dann auf **Verbinden**.
4. Erweitern Sie im Objekt-Explorer **Datenbanken** unter **MIA-SQL**, klicken Sie mit der rechten Maustaste auf **salesapp1**, zeigen Sie auf **Tasks**, und klicken Sie dann auf **Daten exportieren**.
5. Klicken Sie im Fenster **SQL Server-Import/Export-Assistent** auf **Weiter**.
6. Klicken Sie auf der Seite **Datenquelle auswählen** im Feld **Datenquelle** auf **SQL Server Native Client 11.0**.
7. Vergewissern Sie sich, dass im Feld **Datenbank** der Wert **salesapp1** vorhanden ist, und klicken Sie dann auf **Weiter**.
8. Klicken Sie auf der Seite **Ziel auswählen** im Feld **Ziel** auf **Flatfileziel**.
9. Geben Sie im Feld **Dateiname** den Pfad **D:\Demofiles\Mod15\export.txt** ein, und klicken Sie dann auf **Weiter**.
10. Vergewissern Sie sich auf der Seite **Tabelle kopieren oder Datenbank abfragen**, dass **Daten aus mindestens einer Tabelle oder Sicht kopieren** ausgewählt ist, und klicken Sie dann auf **Weiter**.
11. Klicken Sie auf der Seite **Flatfileziel konfigurieren** in der Liste **Quelltabelle oder -sicht** auf **[Production].[Categories]** und dann auf **Weiter**.
12. Überprüfen Sie auf der Seite **Paket speichern und ausführen**, ob **Sofort ausführen** ausgewählt ist, und klicken Sie dann auf **Fertig stellen**.
13. Klicken Sie auf der Seite **Assistenten abschließen** auf **Fertig stellen**, um den Export auszuführen.
14. Klicken Sie auf **Schließen**, sobald der Export fertig ist.
15. Öffnen Sie mit dem Datei-Explorer **D:\Demofiles\Mod15\export.txt**, um das Exportergebnis zu überprüfen.
16. Schließen Sie den Editor.
17. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Lektion 3

# Verwenden von bcp und BULK INSERT zum Importieren von Daten

### Inhalt:

Fragen und Antworten	11
Vorführung: Arbeiten mit bcp	11
Vorführung: Arbeiten mit BULK INSERT	11
Vorführung: Arbeiten mit OPENROWSET	12

## Fragen und Antworten

**Frage:** Richtig oder falsch? Standardmäßig ignorieren **bcp** und BULK INSERT beim Importieren von Daten Check-Einschränkungen, Fremdschlüsseinschränkungen und Trigger.

- ( ) Richtig  
( ) Falsch

**Antwort:**

- (√) Richtig  
( ) Falsch

## Vorführung: Arbeiten mit bcp

### Vorführungsschritte

1. Öffnen Sie eine Eingabeaufforderung, geben Sie den folgenden Befehl ein, und drücken Sie die EINGABETASTE, um die **bcp**-Syntaxhilfe anzuzeigen:

```
bcp -?
```

2. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie dann die EINGABETASTE, um eine Textformatdatei zu erstellen:

```
bcp salesapp1.HR.Employees format nul -S MIA-SQL -T -w -t ^| -r \n -f
D:\Demofiles\Mod15\bcp\EmployeesFmt.txt
```

3. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie dann die EINGABETASTE, um eine XML-Formatdatei zu erstellen:

```
bcp salesapp1.HR.Employees format nul -S MIA-SQL -T -w -t ^| -r \n -x -f
D:\Demofiles\Mod15\bcp\EmployeesFmt.xml
```

4. Öffnen Sie mit dem Editor **D:\Demofiles\Mod15\bcp\EmployeesFmt.txt** und **D:\Demofiles\Mod15\bcp\EmployeesFmt.xml**. Überprüfen und vergleichen Sie den Inhalt der Dateien, und schließen Sie den Editor anschließend.

5. Geben Sie an der Eingabeaufforderung den folgenden Befehl ein, und drücken Sie dann die EINGABETASTE, um Daten mit der XML-Formatdatei zu exportieren:

```
bcp salesapp1.HR.Employees out D:\Demofiles\Mod15\bcp\Employees.csv -S MIA-SQL -T -f
D:\Demofiles\Mod15\bcp\EmployeesFmt.xml
```

6. Schließen Sie die Eingabeaufforderung.
7. Öffnen Sie mit dem Editor die Datei **D:\Demofiles\Mod15\bcp\Employees.csv**, und zeigen Sie die Daten an, die exportiert wurden. Beachten Sie, dass die in verschiedenen Datenfeldern vorhandenen Kommas die Daten für das Exportieren mit einem Komma als Feldtrennzeichen unbrauchbar machen. Schließen Sie den Editor, sobald Sie die Überprüfung abgeschlossen haben.

## Vorführung: Arbeiten mit BULK INSERT

### Vorführungsschritte

1. Öffnen Sie in SQL Server Management Studio die Abfragedatei **Demo 06 - BULK INSERT.sql**.
2. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um aufzuzeigen, dass die Tabelle **Finance.dbo.Currency** leer ist.

3. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine Anweisung BULK INSERT zum Laden von **Finance.dbo.Currency** mit Daten auszuführen.
4. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um zu überprüfen, ob die Tabelle mit Daten geladen wurde.
5. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Vorführung: Arbeiten mit OPENROWSET

### Vorführungsschritte

1. Öffnen Sie in SQL Server Management Studio die Abfragedatei **Demo 07 - OPENROWSET.sql**.
2. Führen Sie den Code unter der Überschrift für **Schritt 1** aus, um aufzuzeigen, dass die Tabelle **Finance.dbo.SalesTaxRate** leer ist.
3. Führen Sie den Code unter der Überschrift für **Schritt 2** aus, um eine SELECT-Anweisung mit dem OPENROWSET BULK-Anbieter aufzuzeigen.
4. Führen Sie den Code unter der Überschrift für **Schritt 3** aus, um aufzuzeigen, dass die Ausgabe einer OPENROWSET-Anweisung mit einer WHERE-Klausel gefiltert werden kann.
5. Führen Sie den Code unter der Überschrift für **Schritt 4** aus, um eine OPENROWSET-Anweisung zum Einfügen von Daten in die Tabelle **Finance.dbo.SalesTaxRate** zu verwenden.
6. Führen Sie den Code unter der Überschrift für **Schritt 5** aus, um aufzuzeigen, dass die Tabelle **Finance.dbo.SalesTaxRate** nun Daten enthält.
7. Lassen Sie SSMS für die nächste Vorführung geöffnet.

## Lektion 4

# Bereitstellen und Aktualisieren von Datenschichtanwendungen

### Inhalt:

Fragen und Antworten	14
Ressourcen	14
Vorführung: Arbeiten mit Datenschichtanwendungen	14

## Fragen und Antworten

**Frage:** Welche der im Folgenden genannten ist *keine* Aktion, die Sie für ein DACPAC ausführen können?

- ( ) EXTRAHIEREN
- ( ) UPGRADE
- ( ) BEREITSTELLEN
- ( ) REGISTRIEREN
- ( ) EXPORT

**Antwort:**

- ( ) EXTRAHIEREN
- ( ) UPGRADE
- ( ) BEREITSTELLEN
- ( ) REGISTRIEREN
- (√) EXPORT

## Ressourcen

### Ausführen von direkten Upgrades der Datenschichtenanwendungen



**Bewährte Methoden:** Sie sollten eine vollständige Datenbanksicherung vornehmen, bevor Sie mit einem direkten Upgrade einer DAC fortfahren.

## Vorführung: Arbeiten mit Datenschichtenanwendungen

### Vorführungsschritte

1. Erweitern Sie in SQL Server Management Studio im Objekt-Explorer unter **MIA-SQL** den Knoten **Datenbanken**, klicken Sie mit der rechten Maustaste auf **Finanzen**, zeigen Sie auf **Tasks**, und klicken Sie dann auf **Datenschichtenanwendung extrahieren**.
2. Klicken Sie im Dialogfeld **Datenschichtenanwendung extrahieren** auf **Weiter**.
3. Geben Sie auf der Seite **Eigenschaften festlegen** im Feld **In DAC-Paketdatei speichern (Erweiterung '.dacpac' in den Dateinamen aufnehmen)** den Pfad **D:\Demofiles\Mod15\dacpac\Finance.dacpac** ein, und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite **Überprüfung und Zusammenfassung** auf **Weiter**. Die Extrahierung wird gestartet.
5. Klicken Sie auf der Seite **Paket erstellen** nach abgeschlossenem Extrahierungsprozess auf **Fertig stellen**.
6. Navigieren Sie im Datei-Explorer zu **D:\Demofiles\Mod15\dacpac**, um die exportierte DACPAC-Datei anzuzeigen.
7. Klicken Sie zum Importieren des DACPACs in SSMS im Objekt-Explorer unter **MIA-SQL** mit der rechten Maustaste auf **Datenbanken**, und klicken Sie dann auf **Datenschichtenanwendung bereitstellen**.
8. Klicken Sie im Fenster **Datenschichtenanwendung bereitstellen** auf **Weiter**.

9. Geben Sie auf der Seite **Paket auswählen** im Feld **DAC-Paket (Dateiname mit der Erweiterung '.dacpac')** den Pfad **D:\Demofiles\Mod15\dacpac\Finance.dacpac** ein, und klicken Sie dann auf **Weiter**.
10. Geben Sie auf der Seite **Konfiguration aktualisieren** im Feld **Name (der Name der bereitgestellten DAC und Datenbank)** den Text **FinanceDAC** ein, und klicken Sie dann auf **Weiter**.
11. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**. Die Bereitstellung wird ausgeführt.
12. Klicken Sie auf der Seite **DAC bereitstellen** nach abgeschlossener Bereitstellung auf **Fertig stellen**.
13. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf **Datenbanken**, und klicken Sie dann auf **Aktualisieren**. Vergewissern Sie sich, dass die Datenbank **FinanceDAC** vorhanden ist.
14. Erweitern Sie **FinanceDAC**, erweitern Sie **Tabellen**, klicken Sie mit der rechten Maustaste auf **dbo.Currency**, und klicken Sie dann auf **Erste 1000 Zeilen auswählen**, um zu überprüfen, ob die Tabelle ohne Daten erstellt wurde.
15. Schließen Sie SSMS, ohne die Änderungen zu speichern.

# Lernzielkontrolle und Kernpunkte der Unterrichtseinheit

## Bewährte Methoden

- Wählen Sie das richtige Tool für Massenimportvorgänge aus.
- Verwenden Sie SSIS für komplexe Transformationen.
- Verwenden Sie **bcp** oder BULK INSERT für schnelle Import- und Exportvorgänge.
- Verwenden Sie OPENROWSET, wenn Daten gefiltert werden müssen, bevor sie eingefügt werden.
- Versuchen Sie, die minimale Protokollierung zu erzielen, um den Datenimport zu beschleunigen.

## Fragen zur Lernzielkontrolle

**Frage:** Welche anderen Faktoren sollten Sie beim Importieren oder Exportieren von Daten berücksichtigen?

**Antwort:** Die Antwort variiert entsprechend den Gegebenheiten.

Es gibt viele Überlegungen, einschließlich der Auswirkung auf die Benutzer- und Anwendungsauslastung und der Sicherheit.

# Fragen und Antworten zur Zusammenfassung der Übungseinheit

## Übungseinheit: Importieren und Exportieren von Daten

### Fragen und Antworten

#### Zusammenfassung der Übungseinheit

**Frage:** Welche alternativen Methoden zu einem SSIS-Paket können Sie verwenden, um die Ausgabe der gespeicherten Prozedur **Sales.usp\_prospect\_list** in eine Datei zu exportieren?

**Antwort:** Verschiedene unterschiedliche Optionen bieten möglicherweise geeignete Alternativen.

Mögliche Alternativen:

- Verwenden Sie **bcp** mit der Anweisung **queryout**.
- Verwenden Sie **sqlcmd**.
- Schreiben Sie eine benutzerdefinierte Anwendung oder ein Skript.

**Frage:** Wenn in der Tabelle **HR.JobCandidate** eine Spalte für eine Zusammenfassung im Microsoft Word-Dokumentformat enthalten ist, welchen der folgenden Befehle würden Sie dann verwenden, um das Dokument in eine Spalte in einer Tabelle zu importieren?

- Der BULK-Anbieter im Befehl OPENROWSET mit der Option SINGLE\_BLOB.
- Der BULK-Anbieter im Befehl OPENROWSET mit der Option SINGLE\_CLOB.
- Der BULK-Anbieter im Befehl OPENROWSET mit der Option SINGLE\_NCLOB.
- Keine der genannten Optionen.

**Antwort:**

- Der BULK-Anbieter im Befehl OPENROWSET mit der Option SINGLE\_BLOB.
- Der BULK-Anbieter im Befehl OPENROWSET mit der Option SINGLE\_CLOB.
- Der BULK-Anbieter im Befehl OPENROWSET mit der Option SINGLE\_NCLOB.
- Keine der genannten Optionen.