Vorwort

In diesem Buch zeigen wir Ihnen den Umgang mit Microsoft SQL Server 2012. Sie lernen, wie Sie den Server installieren und Testumgebungen aufbauen können. Auch die Verwaltung von verschiedenen Bereichen neben den Datenbanken, wie Integration Services, Master Data Services oder Data Quality Services, beschreiben wir. Der Fokus des Buchs liegt in der Administration und dem Betrieb von SQL Server, weniger in der Entwicklung. Wir haben aber dennoch zahlreiche SQL-Befehle mit aufgeführt, die beim Administrieren des Servers helfen. Entwickler profitieren von diesem Buch genauso wie Datenbank- oder Netzwerkadministratoren, die nebenbei noch SQL Server-Computer verwalten sollen.

Ein wichtiger Bestandteil des Buchs ist der Betrieb von SQL Server 2012 zusammen mit SharePoint 2010. Und auch die Installation von SQL Server 2012 auf Servercomputern mit Windows Server 2012 haben wir beschrieben. Betreiben Sie im Unternehmen auch Exchange Server 2010, finden Sie in diesem Buch Hinweise, wie Sie das Datenbank-E-Mail-System von SQL Server 2012 optimal mit Exchange Server verbinden. Natürlich beherrscht SQL Server 2012 auch die Anbindung an andere E-Mail-Systeme.

In den verschiedenen Kapiteln gehen wir zusätzlich darauf ein, wie Sie SQL Server 2012 mit Windows Azure oder SQL Azure verbinden und so Datenbankserver effizient in der Cloud betreiben können.

Nach der Lektüre dieses Buchs können Sie SQL Server 2012 installieren, migrieren und verwalten. Wenn Sie noch nicht so gut mit SQL-Befehlen vertraut sind, lernen Sie in diesem Buch zahlreiche praktische Möglichkeiten der Nutzung kennen, die sich auch leicht bearbeiten und erweitern lassen. Um die einzelnen Bereiche zu verstehen, müssen Sie kein alter Hase sein. Auch Einsteiger, die bereits andere Server verwalten, finden sich mit SQL Server 2012 schnell zurecht.

Wir beschreiben in diesem Buch die verschiedenen Editionen, die Planung und die Einbindung von SQL Server 2012 in komplexe Serverstrukturen. Die Datensicherung ist ein genauso wichtiger Bestandteil, wie zahlreiche kostenlose Zusatztools von Microsoft, welche die Arbeit von Administratoren erleichtern.

Auf dem Begleitmedium zu diesem Buch finden Sie eine ausführliche Linkliste, die auch über die Internetseite des Buchs heruntergeladen werden kann. Diese befindet sich auf *http://www.microsoft-press.de/support.asp?s110=151* oder auf *http://msp.oreilly.de/support/2253/734*. In dieser Liste sind sämtliche Links aufgeführt, die wir in diesem Buch angeben, und Sie können so per einfachem Klick die Software bzw. jeweiligen Informationen bequem herunterladen, ohne lange Links eintippen zu müssen.

Bedanken möchte ich mich bei Florian Helmchen als Projekt-Manager bei Microsoft Press sowie meinem Fachlektor Georg Weiherer. Natürlich gilt auch dem ganzen Microsoft Press-Team und allen Mitarbeitern an diesem Buch mein Dank. Ein ganz besonderer Dank aber geht an Sie, liebe Leserin und lieber Leser, dass Sie sich für dieses Buch entschieden haben. Ich hoffe, Sie lernen bei der Lektüre alles, was Sie benötigen und erhoffen, und empfinden den gleichen Spaß wie ich beim Schreiben.

Ihr *Thomas Joos*
im Juli 2012

Kapitel 6

Überwachung, Optimierung und Fehlerbehebung

In diesem Kapitel:

In diesem Kapitel zeigen wir Ihnen, mit welchen Mitteln und Werkzeugen Sie SQL Server 2012 überwachen und die Ressourcen des Servers optimal für SQL Server 2012 vorbereiten. Wir gehen in diesem Kapitel auf die in SQL Server 2012 integrierten Möglichkeiten ein, geben aber auch Hinweise auf Werkzeuge von Drittherstellern und Tools in Windows Server 2008 R2 und Windows Server 2012 sowie kostenlose Programme von Microsoft.

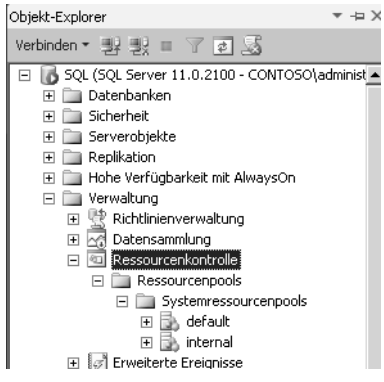
Ressourcenkontrolle im SQL Server Management Studio

SQL Server 2012 kann mit der Ressourcenkontrolle die SQL Server-Arbeitsauslastung und den Systemressourcenverbrauch verwalten. Über die Ressourcenkontrolle können Sie Grenzwerte für die CPU sowie den Speicherplatz festlegen. Mit der Ressourcenkontrolle können Sie also die SQL Server-Arbeitsauslastungen und -Ressourcen verwalten, indem Sie Grenzen für den Ressourcenverbrauch durch eingehende Anforderungen festlegen.

HINWEIS Die Ressourcenverwaltung ist auf das Datenbankmodul beschränkt. Sie können die Ressourcenkontrolle nicht für Analysis Services, Integration Services und Reporting Services verwenden.

Bei der Installation von SQL Server 2012 legt der Assistent einen internen Ressourcenpool (*internal*) und einen Standardressourcenpool (*default*) an. Die Ressourcenkontrolle unterstützt aber auch benutzerdefinierte Ressourcenpools, die Sie selbst erstellen.

Abbildg. 6.1 Verwalten von Ressourcen im SQL Server Management Studio



Bei der Installation von SQL Server 2012 erstellt der Setup-Assistent zusätzlich noch zwei Arbeitsauslastungsgruppen (interne Arbeitsauslastungsgruppe und Standardauslastungsgruppe) mit den dazugehörigen Ressourcenpools. Es gibt interne Regeln, mit denen Sie eingehende Anforderungen klassifizieren und an eine Arbeitsauslastungsgruppe binden. Die Ressourcenkontrolle unterstützt auch benutzerdefinierte Klassifizierungsfunktionen für die Implementierung von eigenen Klassifizierungsregeln.

Dedizierte Administratorverbindungen (Dedicated Administrator Connection, DAC) werden nicht über die Ressourcenkontrolle gesteuert (siehe Kapitel 3). Bei der Anbindung eines Clients finden folgende Vorgänge statt:

1. Es gibt eine eingehende Verbindung für eine Sitzung (Sitzung 1 von n).
2. Die Sitzung wird klassifiziert (Klassifikation).
3. Die Arbeitsauslastung der Sitzung wird an eine Arbeitsauslastungsgruppe geleitet.
4. Die Arbeitsauslastungsgruppe verwendet den ihr zugeordneten Ressourcenpool.
5. Durch den Ressourcenpool werden die von der Anwendung benötigten Ressourcen bereitgestellt und begrenzt.

Ressourcenkontrolle aktivieren und deaktivieren

Ist die Ressourcenkontrolle nach der Installation deaktiviert, erkennen Sie dies am roten Symbol im SQL Server Management Studio. Sie können die Ressourcenkontrolle in SQL Server Management Studio oder mit Transact-SQL-Anweisungen aktivieren. Dazu verwenden Sie das Kontextmenü von Ressourcenkontrolle für die jeweilige Instanz.

Aktivieren Sie die Ressourcenkontrolle, werden neue Verbindungen automatisch mit der Klassifizierungsfunktion behandelt, damit deren Arbeitsauslastungen Arbeitsauslastungsgruppen zugeordnet werden können. Die in der Konfiguration der Ressourcenkontrolle angegebenen Ressourcengrenzwerte werden überprüft und durchgesetzt.

Um die Ressourcenkontrolle über T-SQL zu aktivieren, geben Sie in einer neuen Abfrage die folgenden Befehle ein und lassen sie ausführen:

```
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

Über das Kontextmenü deaktivieren Sie die Ressourcenkontrolle wieder. Auch hier können Sie wiederum mit T-SQL arbeiten. Geben Sie dazu die folgenden Befehle ein:

```
ALTER RESOURCE GOVERNOR DISABLE;
GO
```

Ressourcenpools verstehen und verwalten

Ressourcenpools sind eine Teilmenge der physischen Ressourcen einer Instanz des Datenbankmoduls. Es handelt sich einfach ausgedrückt um virtuelle Server innerhalb von SQL Server-Instanzen. Jeder Ressourcenpool kann wiederum eine oder mehrere Arbeitsauslastungsgruppen enthalten. Wenn eine Sitzung startet, weist die Klassifizierungsfunktion die Sitzung einer bestimmten Arbeitsauslastungsgruppe zu.

Ein Pool besteht immer aus zwei Teilen. Ein Teil überschneidet sich nicht mit anderen Pools und erlaubt eine Reservierung privater Ressourcen. Der andere Teil wird gemeinsam mit anderen Pools verwendet. Poolressourcen legen Sie durch verschiedene Angaben für CPU und Arbeitsspeicher fest:

1. MIN, MAX oder CAP für CPU
2. MIN und MAX für den Arbeitsspeicher

Bei MIN und MAX handelt es sich um die garantierte Mindestverfügbarkeit an Ressourcen für den Pool und die maximale Größe des Pools für die einzelnen Ressourcen. Der CAP-Wert für CPU stellt ein hartes Maximum dar. Die Summe aller MIN-Werte für alle Pools darf 100 Prozent der Serverressourcen nicht übersteigen. Die MAX- und CAP-Werte können Sie zwischen MIN und 100 Prozent festgelegen.

Der interne Pool stellt die von SQL Server 2012 belegten Ressourcen dar. Dieser Pool lässt sich nicht ändern und enthält immer nur die interne Gruppe. Die Ressourcenbelegung durch den internen Pool ist nicht eingeschränkt. Alle Arbeitsauslastungen im Pool gelten als unverzichtbar für die Serverfunktion.

Der Standardpool ist der vordefinierte Benutzerpool in SQL Server 2012. Der Standardpool enthält nach der Aktivierung der Ressourcenkontrolle nur die Standardgruppe. Den Standardpool können Sie ändern, aber nicht löschen oder aus dem Pool entfernen. Er kann neben der Standardgruppe noch benutzerdefinierte Gruppen enthalten.

Erstellen Sie eigene Ressourcenpools, verwenden Sie am besten das SQL Server Management Studio. Gehen Sie dabei folgendermaßen vor:

1. Öffnen Sie in SQL Server Management Studio den Objekt-Explorer, und erweitern Sie den Knoten *Verwaltung/Ressourcenkontrolle*.
2. Klicken Sie mit der rechten Maustaste auf *Ressourcenkontrolle* und wählen Sie im Kontextmenü den Eintrag *Eigenschaften* aus.
3. Klicken Sie bei *Ressourcenpools* in die leere Zeile der ersten Spalte. Diese Spalte ist durch ein Sternchen (*) gekennzeichnet.
4. Geben Sie den Namen für den Ressourcenpool ein.
5. Klicken Sie auf die Zellen in der Zeile, die Sie sich ändern wollen und geben Sie die neuen Werte ein.
6. Klicken Sie auf *OK*, um die Änderungen zu speichern.

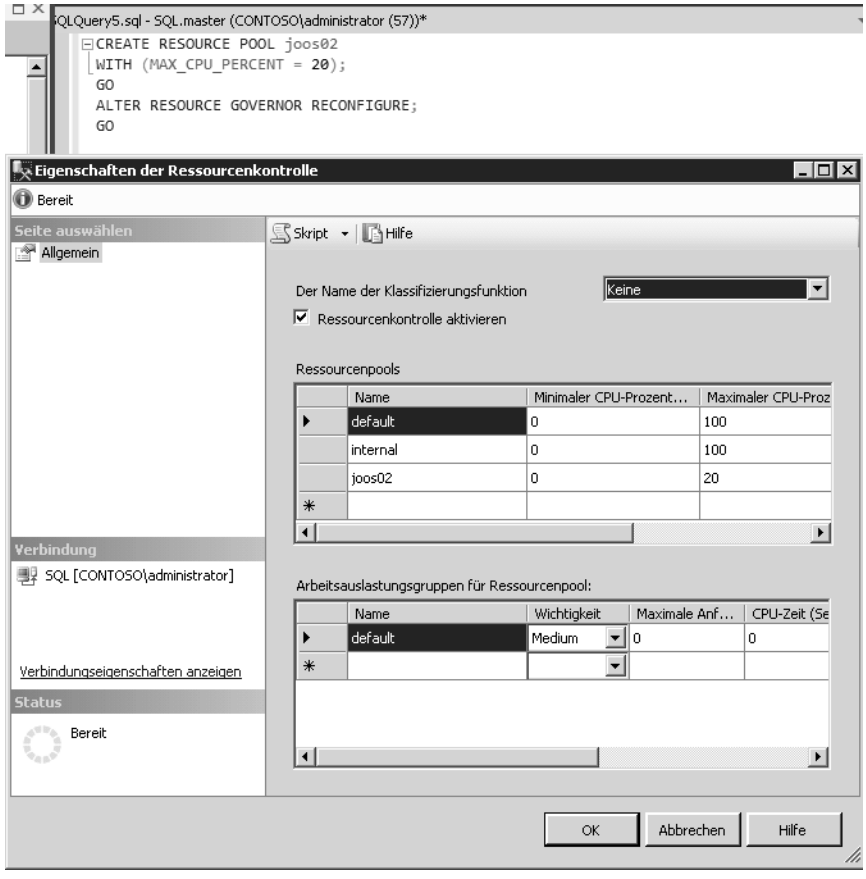
Um einen Pool mit einer T-SQL-Abfrage zu erstellen, verwenden Sie die Syntax wie im folgenden Beispiel:

```
CREATE RESOURCE POOL joos02
WITH (MAX_CPU_PERCENT = 20);
GO
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

In den Eigenschaften der Ressourcenkontrolle können Sie die Einstellungen jederzeit anpassen. Auch die Anpassung über T-SQL-Abfragen ist jederzeit möglich. Um den oben erstellten Ressourcenpool zu ändern, verwenden Sie die Syntax aus dem folgenden Beispiel:

```
ALTER RESOURCE POOL joos02
WITH (MAX_CPU_PERCENT = 25);
GO
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

Abbildg. 6.2 Erstellen und Verwalten eigener Ressourcenpools



Selbst erstellte Ressourcenpools können Sie auch wieder löschen. Dazu entfernen Sie die Spalte in den Eigenschaften der Ressourcenkontrolle im SQL Server Management Studio oder verwenden eine neue T-SQL-Abfrage wie im folgenden Beispiel:

```
DROP RESOURCE POOL joos02;
GO
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

Arbeitsauslastungsgruppen verstehen und verwalten

Arbeitsauslastungsgruppen sind Container für Sitzungsanforderungen mit ähnlichen Klassifizierungskriterien. Arbeitsauslastungen ermöglichen die Überwachung der Sitzungen und definieren Richtlinien für die klassifizierten Sitzungen. Jede Arbeitsauslastungsgruppe ist Teil eines Ressourcenpools. Wenn ein Anwender eine Sitzung startet, weist die Klassifizierungsfunktion der Ressour-

cenkontrolle die Sitzung einer bestimmten Arbeitsauslastungsgruppe zu. Dadurch ist jede Sitzung auch Bestandteil eines Ressourcenpools.

Sie können benutzerdefinierte Arbeitsauslastungsgruppen zwischen Ressourcenpools verschieben. Die Ressourcenkontrolle verfügt nach der Aktivierung über zwei vordefinierte Arbeitsauslastungsgruppen: die *interne Gruppe* und die *Standardgruppe*. Die interne Gruppe können Sie nicht ändern. SQL Server weist Anforderungen der Standardgruppe zu, wenn keine Kriterien zum Klassifizieren einer Anforderung vorhanden sind. Auch beim Versuch der Zuordnung zu einer nicht vorhandenen Gruppe verwendet SQL Server 2012 die Standardgruppe.

Sie können Arbeitsauslastungsgruppen in SQL Server Management Studio oder mit Transact-SQL genauso wie Ressourcenpools erstellen. Gehen Sie dazu folgendermaßen vor:

1. Erweitern Sie im Objekt-Explorer den Knoten *Verwaltung/Ressourcenkontrolle/Ressourcenpools/<Ressourcenpool>/Arbeitsauslastungsgruppen*.
2. Klicken Sie mit der rechten Maustaste auf *Arbeitsauslastungsgruppen* und wählen Sie im Kontextmenü den Eintrag *Neue Arbeitsauslastungsgruppe*.
3. Markieren Sie den Ressourcenpool, für den Sie die neue Arbeitsauslastungsgruppe erstellen wollen.
4. Geben Sie einen Namen für die Arbeitsauslastungsgruppe im unteren Bereich des Fensters ein.
5. Klicken Sie auf beliebige andere Zellen in der Zeile und geben Sie jeweils die neuen Werte ein.
6. Klicken Sie auf *OK*, um die Änderungen zu speichern.

Um eine neue Arbeitsauslastungsgruppe zu erstellen und einem vorhandenen Ressourcenpool hinzuzufügen, können Sie auch T-SQL verwenden:

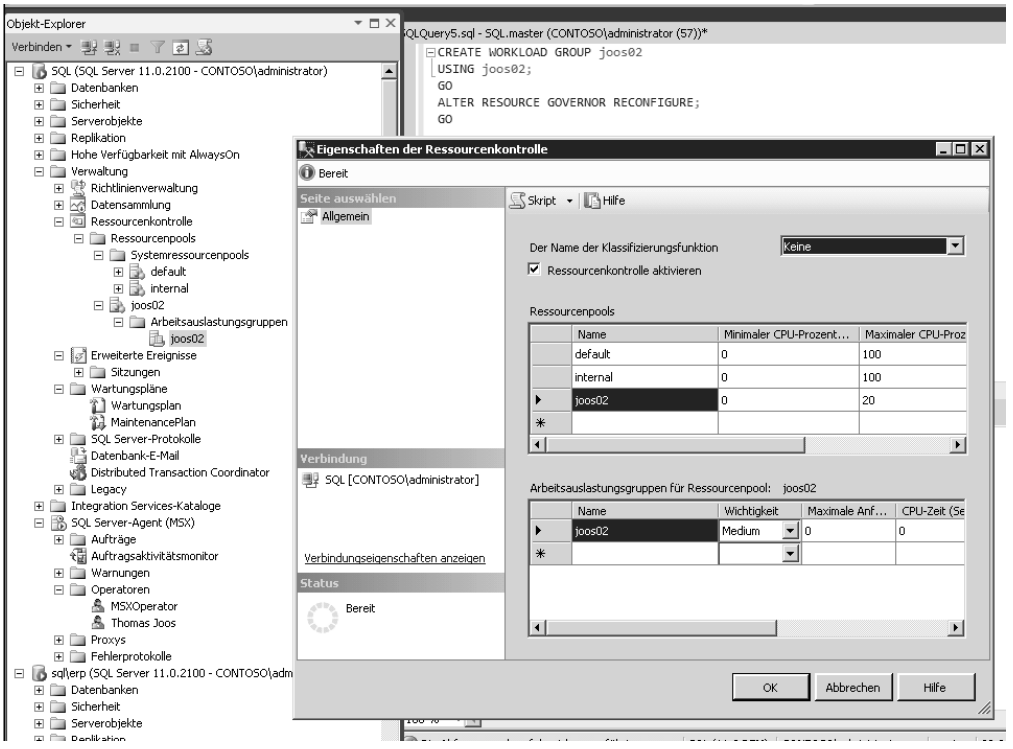
```
CREATE WORKLOAD GROUP joos02
USING joos02;
GO
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

Nach der Aktualisierung von SQL Server Management Studio ist die Gruppe auch hier zu sehen. Über deren Eigenschaften können Sie die Einstellungen der Arbeitsauslastungsgruppe jederzeit wieder ändern.

Wollen Sie Einstellungen mit T-SQL ändern, verwenden Sie zum Beispiel die folgenden Befehle:

```
ALTER WORKLOAD GROUP joos02
WITH (REQUEST_MAX_MEMORY_GRANT_PERCENT = 30);
GO
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

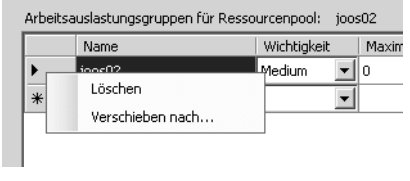
Abbildg. 6.3 Erstellen einer neuen Arbeitsauslastungsgruppe



Arbeitsauslastungsgruppen können Sie jederzeit in andere Ressourcenpools verschieben. Auch hier können Sie das SQL Server Management Studio verwenden oder T-SQL-Abfragen. Arbeitsauslastungsgruppen der Ressourcenkontrolle können Sie in SQL Server Management Studio oder mit Transact-SQL in einen anderen Ressourcenpool verschieben:

1. Öffnen Sie zum Verschieben von Arbeitsauslastungsgruppen die Eigenschaften der *Ressourcenkontrolle* im SQL Server Management Studio.
2. Klicken Sie im Fenster *Ressourcenpools* auf den Ressourcenpool mit der Arbeitsauslastungsgruppe, die Sie verschieben wollen. Im Fenster *Arbeitsauslastungsgruppen* sehen Sie die Arbeitsauslastungsgruppen in diesem Ressourcenpool.
3. Klicken Sie mit der rechten Maustaste links neben der Arbeitsauslastungsgruppe auf den Pfeil nach rechts und wählen Sie im Kontextmenü den Eintrag *Verschieben nach*.
4. Wählen Sie den neuen Ressourcenpool aus und bestätigen Sie anschließend das Verschieben.

Abbildg. 6.4 Verschieben von Arbeitsauslastungsgruppen



Sie können die Verschiebung auch mit T-SQL durchführen. Um zum Beispiel die Gruppe *joos02* in den Standardpool zu verschieben, geben Sie die folgenden Befehle ein:

```
ALTER WORKLOAD GROUP groupAdhoc
USING [default];
GO
ALTER RESOURCE GOVERNOR RECONFIGURE;
GO
```

Klassifizierungsfunktion einsetzen

Die Klassifizierungsfunktion teilt Sitzungen Arbeitsauslastungsgruppen zu. Diese verwenden wiederum die Ressourcenpools, denen sie zugewiesen sind. Verbindet sich ein Client mit dem Server, läuft ein Prozess ab, der auf Basis verschiedener Kriterien festlegt, welcher Arbeitsauslastungsgruppe der Client zugewiesen wird. Die dedizierte Administratorverbindung (Dedicated Administrator Connection, DAC) auf dem Server unterliegt nicht der Klassifizierung (siehe Kapitel 3). Mit dieser Verbindung können Sie Fehler und Probleme bei Serververbindungen und Ressourcenauslastung auch dann noch beheben, wenn der Server nicht mehr ordnungsgemäß reagiert.

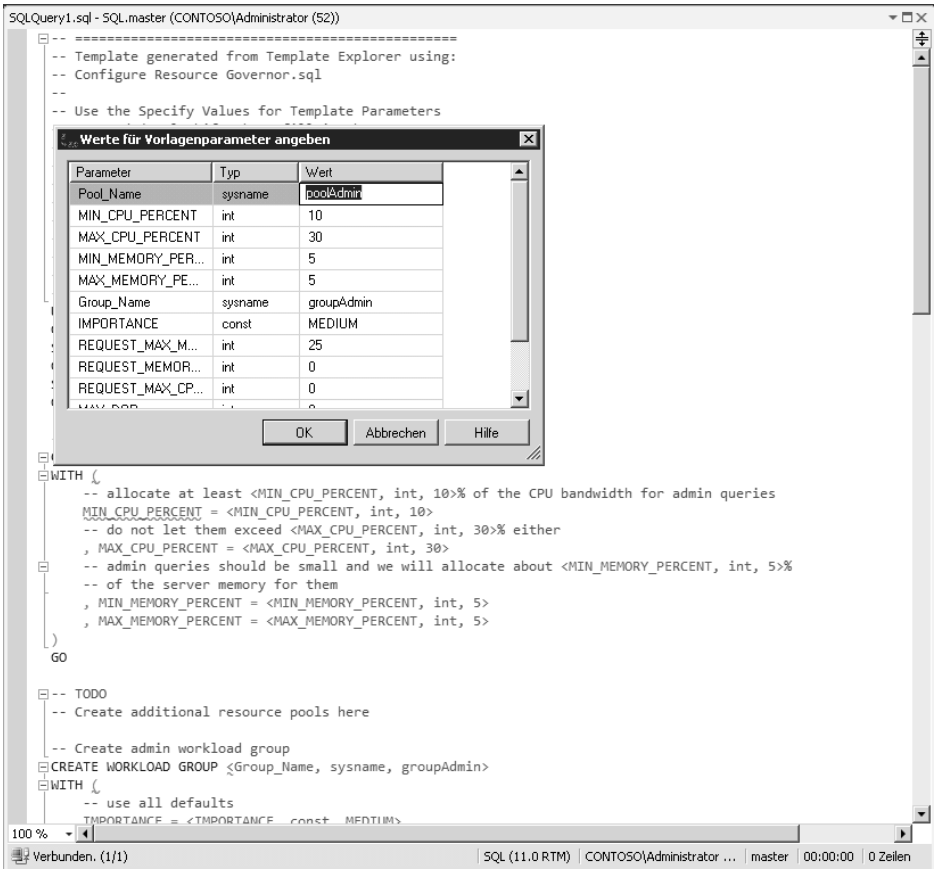
Wenn Sie keine DAC starten können, besteht noch die Möglichkeit, die entsprechende Instanz im Einzelbenutzermodus neu zu starten (siehe Kapitel 3). Der Einzelbenutzermodus unterliegt nicht der Klassifizierung, Sie können aber die Konfiguration der Klassifizierung überprüfen.

Um eigene Klassifizierungsfunktionen zu erstellen, sind einige T-SQL-Kenntnisse erforderlich. Sie müssen benutzerdefinierte Funktionen in T-SQL erstellen. Ein Beispiel für eine solche Abfrage finden Sie auf der Seite *http://msdn.microsoft.com/de-de/library/cc645892.aspx* [Ms151-K06-01].

Sie können die Ressourcenkontrolle mit einer in SQL Server Management Studio bereitgestellten Vorlage konfigurieren. Auf diesem Weg müssen Sie das Skript nicht komplett neu schreiben, sondern können die Vorlage verwenden. Sie können mit dieser Vorlage auch eine benutzerdefinierte Klassifizierungsfunktion erstellen:

1. Klicken Sie im SQL Server Management Studio im Menü *Ansicht* auf *Vorlagen-Explorer*.
2. Erweitern Sie im *Vorlagen-Explorer* den Eintrag *Resource Governor* und klicken Sie doppelt auf *Configure Resource Governor*.
3. Es öffnet sich eine neue Abfrage, über die Sie Ressourcenpools, Auslastungsgruppen und Klassifizierungsfunktionen erstellen können.
4. Drücken Sie die Tastenkombination Strg + ⇧ + M. Es öffnet sich ein neues Fenster, in das Sie die Daten eingeben, die Sie für Ihre Umgebung einsetzen wollen. Der Assistent trägt die Daten in das Skript ein, sodass Sie über keine ausführlichen T-SQL-Kenntnisse verfügen müssen.

Abbildg. 6.5 Ressourcenkontrolle über SQL-Abfragen steuern



5. Klicken Sie auf *OK*, um Änderungen zu speichern.
6. Klicken Sie anschließend auf *Ausführen*, um die Abfrage auszuführen. Die Abfrage erstellt die entsprechenden Ressourcenpools, Auslastungsgruppen und Klassifizierungsfunktionen mit den vorgegebenen Namen und Einstellungen.

Erweiterte Ereignisse verwenden

Mit der Funktion *Erweiterte Ereignisse* in SQL Server 2012 können Sie SQL-Server überwachen, ohne dabei zu viele Ressourcen zu verbrauchen. Dazu erstellen Sie auf dem Server eine eigene Sitzung, zum Beispiel mit dem SQL Server Management Studio. In dieser sammeln Sie verschiedene Ereignisse, die in den Datenbanken und auf dem Server stattfinden. Die Ereignisse können Sie sich in Echtzeit ansehen oder in Dateien protokollieren und entsprechend filtern. Dazu verwenden Sie entweder eine neue Abfrage mit der Anweisung *ALTER EVENT SESSION* oder den Knoten *Erweiterte Ereignisse* im Objekt-Explorer. Die Einstellungen solcher Sitzungen bleiben auf dem Server auch nach dem Beenden weiterhin gespeichert, bis Sie diese löschen. Sie können also beendete Sitzungen jederzeit neu starten, falls Sie diese beendet haben.

Sitzung für erweiterte Ereignisse erstellen

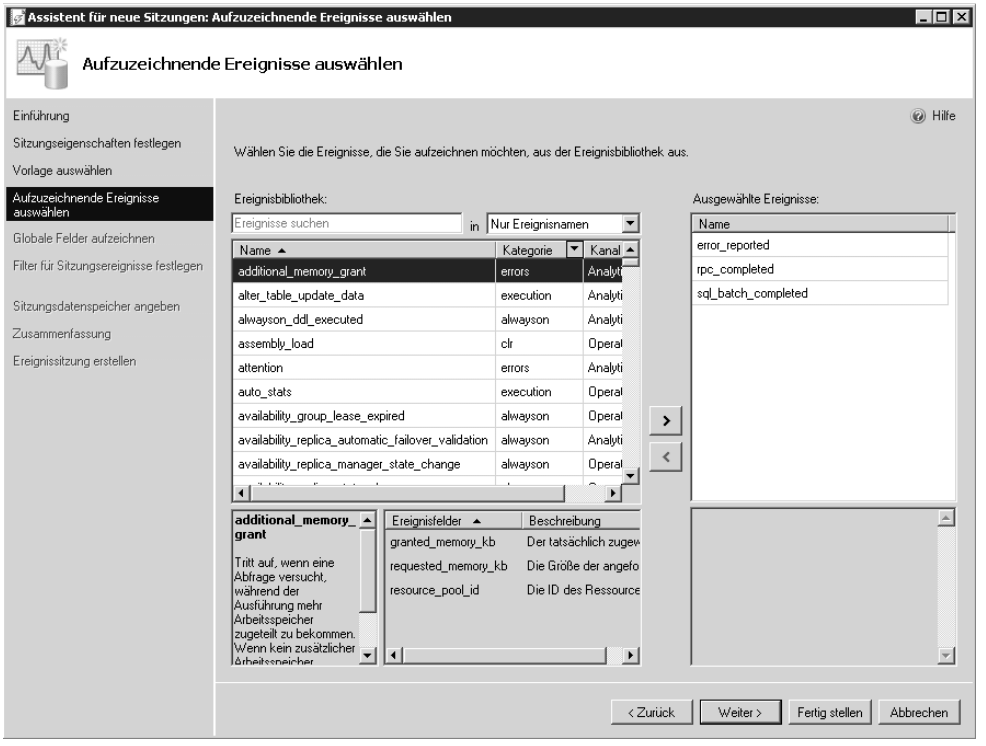
Um eine Sitzung für erweiterte Ereignisse zu erstellen, verwenden Sie am besten das SQL Server Management Studio. Navigieren Sie zu *Verwaltung/Erweiterte Ereignisse/Sitzungen*. Über das Kontextmenü von Sitzungen erstellen Sie entweder manuell Sitzungen und können dabei auch auf Vorlagen zurückgreifen, oder Sie verwenden den Assistenten zum Erstellen von neuen Sitzungen. Dieser führt Sie durch die einzelnen Schritte der Erstellung:

1. Im ersten Schritt geben Sie den Namen der Sitzung ein. Hier können Sie auch festlegen, ob die Sitzung sofort nach dem Erstellen starten soll. Dazu aktivieren Sie das Kontrollkästchen *Ereignissitzung beim Serverstart starten*. Sie können Sitzungen aber auch über das Kontextmenü starten.
2. Auf der nächsten Seite können Sie auswählen, ob Sie eine Vorlage verwenden oder die Einstellungen selbst festlegen wollen. Erstellen Sie eine benutzerdefinierte Sitzung, können Sie diese später über das Kontextmenü als Vorlage speichern und zukünftig über den Assistenten als Vorlage laden lassen.

Abbildg. 6.6 Erstellen einer neuen Sitzung für erweiterte Ereignisse

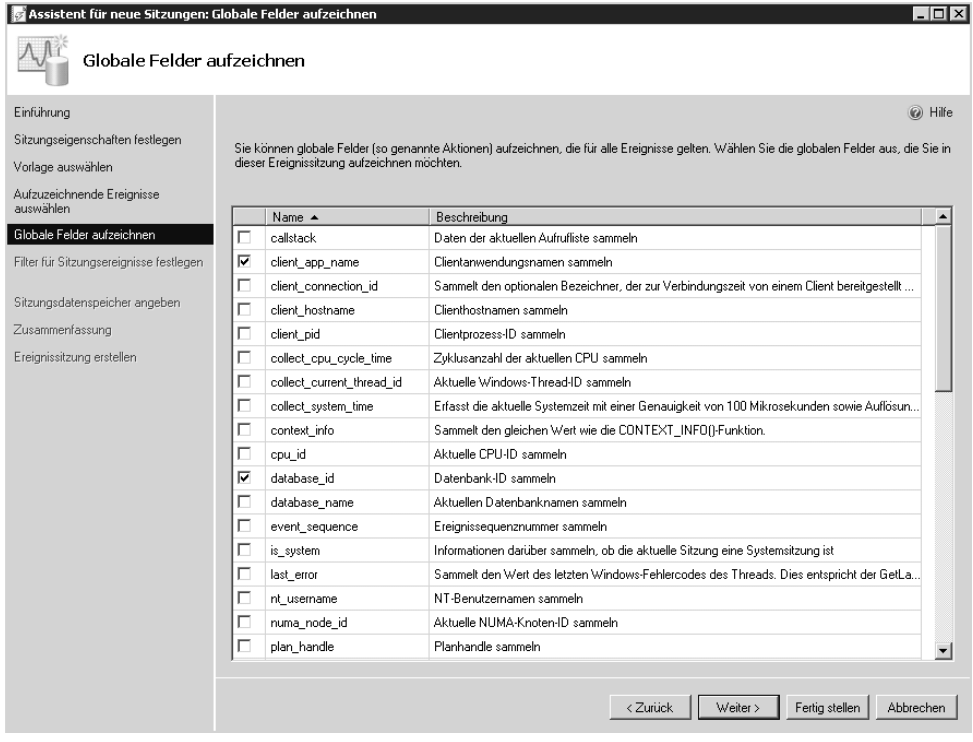
3. Auf der nächsten Seite legen Sie fest, welche Ereignisse die Sitzung zur Überwachung aufzeichnen soll. Wählen Sie die Ereignisse aus, die Sie aufzeichnen möchten, und klicken Sie auf den Pfeil nach rechts. Mit ⇧ oder Strg können Sie mehrere Ereignisse auswählen. Klicken Sie auf ein Ereignis, erhalten Sie im unteren Fensterbereich Informationen darüber, welche Bereiche des Servers das Ereignis überwacht.

Abbildg. 6.7 Auswählen der zu überwachenden Ereignisse



4. Im rechten Bereich wählen Sie aus, auf welcher Basis die Ereignisse gesucht werden sollen, die Sie aufzeichnen wollen. Sie können nach Ereignisnamen oder Beschreibungen suchen oder auch nach beliebigen Wörtern. Alle Ereignisse, die Sie auswählen, erscheinen bei *Ausgewählte Ereignisse*. Hier können Sie diese auch wieder entfernen.
5. Auf der Seite *Globale Felder* legen Sie Aktionen für die ausgewählten Ereignisse fest. Die Aktionen sind in der Vorlage gespeichert, die Sie zu Beginn ausgewählt haben. Aktivieren Sie die Kontrollkästchen bei jenen Aktionen, die Sie für die Ereignisse ausführen lassen wollen.
6. Als Nächstes legen Sie Filter (auch Prädikate genannt) fest, um die Ereignisse zu filtern, falls Sie diese nicht alle anzeigen lassen möchten. Verwenden Sie eine Vorlage, sind hier meist schon Filter hinterlegt. Diese zeigt der Assistent im oberen Bereich an. Um eigene Filter zu erstellen, klicken Sie auf eine freie Zeile im Abschnitt *Zusätzliche Filter*. Die Filter werden aber auf alle Ereignisse angewendet, die Sie im vorderen Fenster festgelegt haben. Mit der Entf-Taste löschen Sie einen selbst erstellten Filter.

Abbildg. 6.8 Auswählen der globalen Felder



7. Auf der nächsten Seite *Sitzungsdatenspeicher* legen Sie fest, wie der Server die Daten speichern soll. Aktivieren Sie das Kontrollkästchen *Dateirollover aktivieren*, überschreibt das System alte Daten mit neuen, wenn die maximale Größe der Datei erreicht ist. Im unteren Bereich nehmen Sie weitere Einstellungen vor, um fortlaufende Daten zu speichern und veraltete Ereignisse zu überschreiben.
8. Auf der letzten Seite erhalten Sie eine Zusammenfassung angezeigt. Klicken Sie auf die Schaltfläche *Skript*, können Sie sich die T-SQL-Befehle für die Erstellung der Sitzung anzeigen lassen. Auf diesem Weg können Sie auch weitere Sitzungen auf Basis von neuen Abfragen erstellen und Einstellungen im Skript selbst ändern. Auch nach der Erstellung können Sie das Skript für die Sitzung über das Kontextmenü aufrufen und zum Erstellen weiterer Sitzungen verwenden.
9. Klicken Sie auf *Fertig stellen*, legt der Assistent die Sitzung an und Sie können auch hier die Sitzung sofort aktivieren. Die Sitzung erscheint im Knoten *Sitzungen*. Über das Kontextmenü starten oder beenden Sie die Sitzung.

HINWEIS Sie können alle Einstellungen einer Sitzung, die Sie beim Erstellen festlegen, später über das Kontextmenü und der Auswahl von *Eigenschaften* ändern.

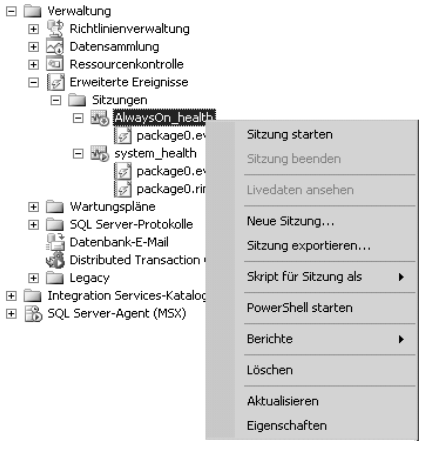
Sitzungen für erweiterte Ereignisse starten, beenden bearbeiten und löschen

Um eine Sitzung für erweiterte Ereignisse zu starten oder zu beenden, klicken Sie im SQL Server Management Studio mit der rechten Maustaste auf eine der Sitzungen im Knoten *Verwaltung/Erweiterte Ereignisse/Sitzungen*. Die Sitzung bleibt auch dann gestartet, wenn Sie sich vom SQL Server Management Studio abmelden. Sie müssen die Sitzung explizit über das Kontextmenü beenden.

TIPP Haben Sie die Sitzung gestartet, können Sie sich die Livedaten der Sammlung über das Kontextmenü der Sitzung anzeigen lassen.

Haben Sie einmal eine Sitzung erstellt, können Sie diese über das Kontextmenü mit dem Befehl *Sitzung exportieren* auch in eine XML-Datei speichern lassen.

Abbildg. 6.9 Starten, beenden oder exportieren von Sitzungen für erweiterte Ereignisse



TIPP Über das Kontextmenü zum Knoten *Verwaltung/Erweiterte Ereignisse/Sitzungen* erstellen Sie über einen Assistenten neue Sitzungen für erweiterte Ereignisse. Haben Sie eine solche Sitzung exportiert und dazu den vorgegebenen Speicherort verwendet, zeigt der Assistent die XML-Datei bei der Erstellung von Sitzungen als Vorlage an, wenn Sie den Befehl *Neue Sitzung* auswählen.

Sitzungen, die Sie über das Kontextmenü von *Verwaltung/Erweiterte Ereignisse/Sitzungen erstellen*, werden aber standardmäßig nicht gestartet. Sie müssen die Sitzung nach der Erstellung über das Kontextmenü zunächst manuell aufrufen. Erstellte Sitzungen können Sie jederzeit nachträglich bearbeiten. Dazu rufen Sie im Kontextmenü den Befehl *Eigenschaften* auf.

Um eine Sitzung zu löschen, verwenden Sie eine neue Abfrage mit den folgenden Befehlen:

```
DROP EVENT SESSION [<Sitzungsname>] ON SERVER
GO
```

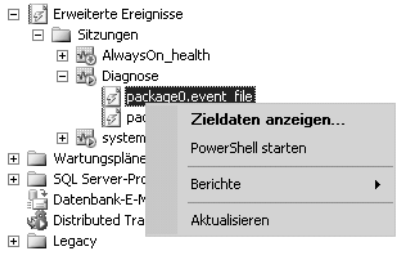
Sie können die Sitzung aber auch über das Kontextmenü der Sitzung löschen lassen.

Ereignissitzungsdaten anzeigen

Starten Sie eine Sitzung, speichert diese Daten in der Datei, die Sie angegeben haben. Über das Kontextmenü der gestarteten Sitzung lassen Sie sich zusätzlich noch die Livedaten über das Kontextmenü anzeigen, indem Sie *Livedaten ansehen* auswählen.

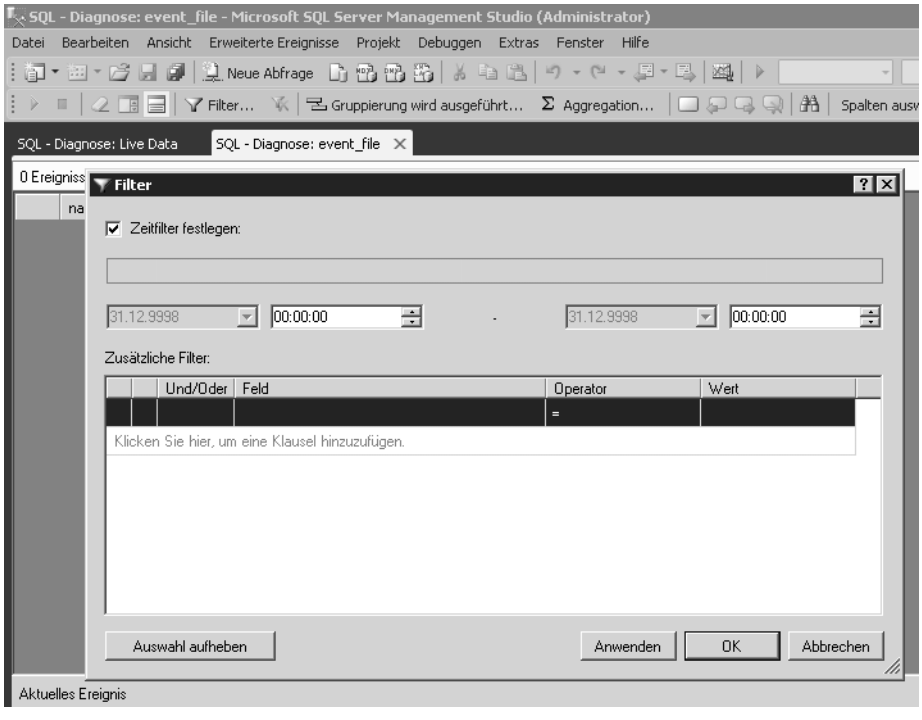
Über das Kontextmenü des Knotens der Speicherdatei der Sitzung lassen Sie sich den Inhalt der Datei anzeigen, indem Sie *Zieldaten anzeigen* auswählen.

Abbildg. 6.10 Anzeigen der Zieldaten einer Diagnosesitzung



Sie können Ablaufverfolgungsergebnisse anzeigen und Filter anwenden, um die Anzeige einzugrenzen. Der Anzeigefilter enthält auch einen Zeitfilter und erweiterte Filter, mit denen Sie die Anzeige besser filtern können.

Abbildg. 6.11 Erstellen von Filtern für die Anzeige der Ereignisüberwachung



Klicken Sie in der Symbolleiste *Erweiterte Ereignisse* auf die Schaltfläche *Aggregation*, lassen sich Ereignisse auch zusammenfassen. Auch die Möglichkeit der Suche haben Sie in der geöffneten Datei. Sie können Zellen, Zeilen und Details aus Ablaufverfolgungsergebnissen kopieren und auch exportieren. Haben Sie verschiedene Einstellungen zur Anzeige der Ansicht geändert, können Sie diese in einer Datei speichern und jederzeit laden lassen. Dazu klicken Sie in der Symbolleiste *Erweiterte Ereignisse* auf die Schaltfläche *Anzeigeeinstellungen*, wenn Sie eine Datei geöffnet haben.

TIPP Erweiterte Ereignisse bieten eine Vielzahl sehr komplexer Überwachungsmöglichkeiten. Diese insgesamt zu beschreiben würde den Rahmen dieses Buchs sprengen. Wollen Sie sich tief gehender mit dem Thema auseinandersetzen, finden Sie eine umfassende Hilfe im MSDN auf der Seite *http://msdn.microsoft.com/de-de/library/bb630282.aspx* [Ms151-K06-02].

Ähnliche Funktionen bietet auch die SQL-Ablaufverfolgung. Hier sammeln Sie ebenfalls verschiedene Ereignisse zur Diagnose. Sie müssen dazu aber T-SQL-Befehle und -Prozeduren verwenden, sich also etwas in der Entwicklung von SQL Server auskennen. Die Ablaufverfolgung ist daher eher für Entwickler geeignet und weniger für Administratoren. Wollen Sie sich die Möglichkeiten ansehen, finden Sie im MSDN auf den Seiten *http://msdn.microsoft.com/de-de/library/hh245121.aspx* [Ms151-K06-03] und *http://msdn.microsoft.com/de-de/library/ms181091.aspx* [Ms151-K06-04] ausführliche Anleitungen zum Thema.

Überwachungen erstellen und verwalten

Mit Überwachungen, auch SQL Server Audit genannt, können Sie Ereignisse auf einem SQL-Server nachverfolgen. Seit SQL Server 2008 Enterprise lässt sich auch eine automatische Überwachung mit einrichten. Die Überwachung einer Instanz oder einer einzelnen Datenbank beinhaltet die Nachverfolgung und Protokollierung von Ereignissen, die im Datenbankmodul auftreten. Überwachte Ereignisse können Sie in die Ereignisprotokolle oder Überwachungsdateien schreiben lassen.

HINWEIS Alle Editionen von SQL Server 2012 unterstützen Überwachungen auf Serverebene. Die Überwachung auf Datenbankebene ist auf die Editionen Enterprise, Developer und Evaluation beschränkt.

Grundlagen zu SQL Server Audit

Eine Überwachungsinfrastruktur in SQL Server 2012 besteht aus mehreren Elementen, die in einem einzelnen Paket für eine bestimmte Gruppe von Server- oder Datenbankaktionen zusammengefasst sind. SQL Server Audit verwendet erweiterte Ereignisse, um eine Überwachung zu erstellen. Die Überwachung wird auf SQL Server-Instanzebene ausgeführt. Sie können auch mehrere Überwachungen pro Instanz konfigurieren. Während der Konfiguration der Überwachung legen Sie die Ausgabe der Ergebnisse fest. Dies ist das Überwachungsziel. Die Überwachung ist nach der Erstellung inaktiv.

Die Serverüberwachungsspezifikation gehört zu der Überwachung. Sie können eine Serverüberwachungsspezifikation pro Überwachung erstellen. Die Serverüberwachungsspezifikation verwendet Aktionsgruppen auf Serverebene, die von erweiterten Ereignissen ausgelöst werden. Sie können Überwachungsaktionsgruppen in eine Serverüberwachungsspezifikation integrieren. Überwachungsaktionsgruppen sind definierte Gruppen von Aktionen, bei denen es sich um Ereignisse han-

delt, die im Datenbankmodul ablaufen. Diese Aktionen werden an die Überwachung gesendet, die sie im Ziel aufzeichnet.

Das Datenbank-Überwachungsspezifikation-Objekt gehört ebenfalls zu SQL Server Audit. Sie können eine Datenbank-Überwachungsspezifikation pro Datenbank und pro Überwachung erstellen. Die Datenbank-Überwachungsspezifikation bietet Überwachungsaktionen auf Datenbankebene, die von erweiterten Ereignissen ausgelöst werden. Sie können entweder Überwachungsaktionsgruppen oder Überwachungsereignisse einer Datenbank-Überwachungsspezifikation hinzufügen. Überwachungsereignisse sind die Aktionen, die vom SQL Server-Modul überwacht werden können. Überwachungsaktionsgruppen sind definierte Aktionsgruppen. Beide befinden sich im SQL Server-Datenbankbereich. Diese Aktionen werden an die Überwachung gesendet, die sie im Ziel aufzeichnet.

Die Ergebnisse einer Überwachung werden an ein Ziel gesendet. Hierbei kann es sich um eine Datei, das Windows-Sicherheitsereignisprotokoll oder das Windows-Anwendungsereignisprotokoll handeln. Wenn Sie in das Windows-Sicherheitsprotokoll schreiben wollen, muss das SQL Server-Dienstkonto der Richtlinie *Generieren von Sicherheitsüberwachungen* hinzugefügt werden. Standardmäßig sind das lokale System, der lokale Dienst und der Netzwerkdienst Teil dieser Richtlinie. Diese Einstellung nehmen Sie mit dem Sicherheitsrichtlinien-Snap-In (*secpol.msc*) oder über Gruppenrichtlinien vor. Zusätzlich müssen Sie die Sicherheitsrichtlinie *Andere Objektzugriffsversuche überwachen* für *Erfolg* und für *Fehler* aktivieren.

Sie können das SQL Server Management Studio oder Transact-SQL verwenden, um die Überwachung zu konfigurieren. Bei Dateizielen können Sie zum Lesen der Zieldatei den Protokolldatei-Viewer in SQL Server Management Studio verwenden. Die Reihenfolge bei der Erstellung ist Folgende:

1. Erstellen Sie eine Überwachung und definieren Sie das Ziel.
2. Erstellen Sie eine Serverüberwachungsspezifikation oder eine Datenbank-Überwachungsspezifikation, die der Überwachung zugeordnet wird. Aktivieren Sie die Überwachungsspezifikation.
3. Aktivieren Sie die Überwachung.
4. Lesen Sie die Überwachungsereignisse mit der Windows-Ereignisanzeige, dem Protokolldatei-Viewer oder der *fn_get_audit_file*-Funktion.

HINWEIS Wenn Sie eine Datenbank an SQL Server 2012 anfügen (siehe Kapitel 4), für die eine Überwachungsspezifikation festgelegt ist, müssen Sie die Überwachungseinstellungen überprüfen und unter Umständen neu erstellen.

Sie können eine Datenbank, für die eine Überwachungsspezifikation angegeben ist, an eine andere Edition von SQL Server 2012 anfügen, die SQL Server Audit nicht unterstützt, zum Beispiel SQL Server 2012 Express. In diesem Fall werden aber keine Überwachungsereignisse mehr aufgezeichnet.

Eine Datenbank, für die eine Datenbank-Überwachungsspezifikation definiert ist und für die Datenbankspiegelung verwendet wird, enthält die Datenbank-Überwachungsspezifikation. Der Spiegelserver muss in diesem Fall über eine Überwachung mit der gleichen GUID verfügen, damit die Datenbank-Überwachungsspezifikation Überwachungsdatensätze schreiben kann. Diese Einstellung können Sie mit dem folgenden Befehl konfigurieren:

```
CREATE AUDIT WITH GUID=<GUID der Quellserverüberwachung>
```

Bei Dateizielen muss das Dienstkonto des Spiegelservers über die erforderlichen Berechtigungen für den Speicherort verfügen. Bei Windows-Ereignisprotokollzielen muss die Sicherheitsrichtlinie für den Computer, auf dem sich der Spiegelserver befindet, den Dienstkontozugriff auf das Sicherheits- oder Anwendungsereignisprotokoll zulassen. Sie können die folgenden DDL-Anweisungen zum Erstellen, Ändern und Löschen von Überwachungsspezifikationen verwenden:

- *ALTER AUTHORIZATION*
- *CREATE SERVER AUDIT*
- *ALTER DATABASE AUDIT SPECIFICATION*
- *CREATE SERVER AUDIT SPECIFICATION*
- *ALTER SERVER AUDIT*
- *DROP DATABASE AUDIT SPECIFICATION*
- *ALTER SERVER AUDIT SPECIFICATION*
- *DROP SERVER AUDIT*
- *CREATE DATABASE AUDIT SPECIFICATION*
- *DROP SERVER AUDIT SPECIFICATION*

SQL Server Audit-Aktionsgruppen und -Aktionen

SQL Server-Überwachungen bestehen aus verschiedenen Überwachungsaktionselementen. Bei diesen Überwachungsaktionselementen kann es sich entweder um eine Aktionsgruppe oder um einzelne Aktionen wie SELECT-Vorgänge in einer Tabelle handeln. Überwachungen auf Serverebene testen Servervorgänge und -änderungen sowie Anmelde- und Abmeldevorgänge. Auf Datenbankebene umfassen Überwachungen DML- (Data Manipulation Language) und DDL-Vorgänge (Data Definition Language). Die Überwachungsebene schließt Aktionen im Überwachungsprozess ein.

Überwachungsaktionsgruppen auf Serverebene sind Aktionen für die Sicherheitsüberwachung. Dabei spielen vor allem die folgenden Aktionsgruppen eine Rolle, die zum größten Teil auch auf Datenbankebene existieren. In diesem Fall können Sie dann aber nur die entsprechende Datenbank überwachen, nicht den kompletten Server:

- **APPLICATION_ROLE_CHANGE_PASSWORD_GROUP** Das Ereignis wird ausgelöst, wenn ein Kennwort für eine Anwendungsrolle geändert wird
- **AUDIT_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn eine Überwachung erstellt, geändert oder gelöscht wird
- **BACKUP_RESTORE_GROUP** Das Ereignis wird ausgelöst, wenn ein Sicherungs- oder Wiederherstellungsbefehl ausgegeben wird
- **BROKER_LOGIN_GROUP** Das Ereignis wird für Berichtsüberwachungsmeldungen zur Service Broker-Transportsicherheit ausgelöst
- **DATABASE_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn eine Datenbank erstellt, geändert oder gelöscht wird
- **DATABASE_LOGOUT_GROUP** Das Ereignis wird ausgelöst, wenn sich der Benutzer einer eigenständigen Datenbank von einer Datenbank abmeldet

- **DATABASE_OBJECT_ACCESS_GROUP** Das Ereignis wird jedes Mal ausgelöst, wenn auf Datenbankobjekte zugegriffen wird
- **DATABASE_OBJECT_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn eine CREATE-, ALTER- oder DROP-Anweisung für Datenbankobjekte ausgeführt wird
- **DATABASE_OBJECT_OWNERSHIP_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn der Besitzer für Objekte im Datenbankbereich geändert wird
- **DATABASE_OBJECT_PERMISSION_CHANGE_GROUP** Dieses Ereignis wird ausgelöst, wenn für Datenbankobjekte eine GRANT-, REVOKE- oder DENY-Anweisung ausgegeben wurde
- **DATABASE_OWNERSHIP_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn Sie die ALTER AUTHORIZATION-Anweisung verwenden, um den Besitzer einer Datenbank zu ändern
- **DATABASE_PRINCIPAL_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn Benutzer in einer Datenbank erstellt, geändert oder aus einer Datenbank gelöscht werden
- **DATABASE_ROLE_MEMBER_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn Anmeldedaten hinzugefügt oder aus einer Datenbankrolle entfernt werden
- **DBCC_GROUP** Das Ereignis wird ausgelöst, wenn ein DBCC-Befehl gestartet wird
- **FAILED_DATABASE_AUTHENTICATION_GROUP** Gibt an, dass ein Anwender vergeblich versucht hat, sich an einer eigenständigen Datenbank anzumelden
- **FAILED_LOGIN_GROUP** Gibt an, dass ein Anwender versucht hat, sich am SQL-Server anzumelden, und diese Anmeldung fehlgeschlagen ist
- **FULLTEXT_GROUP** Gibt an, dass ein Volltextereignis aufgetreten ist
- **LOGIN_CHANGE_PASSWORD_GROUP** Dieses Ereignis wird ausgelöst, wenn das Anmeldekennwort geändert wird
- **LOGOUT_GROUP** Gibt an, dass sich ein Anwender vom SQL-Server abgemeldet hat
- **SERVER_OBJECT_CHANGE_GROUP** Das Ereignis wird für CREATE-, ALTER- oder DROP-Vorgänge auf Serverobjekten ausgelöst
- **SERVER_OBJECT_OWNERSHIP_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn der Besitzer für Objekte im Serverbereich geändert wird
- **SERVER_OBJECT_PERMISSION_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn ein Anwender in SQL Server eine GRANT-, REVOKE- oder DENY-Anweisung für eine Serverobjektberechtigung ausgibt
- **SERVER_PERMISSION_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn eine GRANT-, REVOKE- oder DENY-Anweisung für Berechtigungen im Serverbereich ausgegeben wird, zum Beispiel beim Erstellen eines Anmeldenamens
- **SERVER_PRINCIPAL_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn Serveranmeldungen erstellt, geändert oder gelöscht werden
- **SERVER_ROLE_MEMBER_CHANGE_GROUP** Das Ereignis wird ausgelöst, wenn Anmeldedaten einer Serverrolle hinzugefügt oder daraus entfernt werden
- **SERVER_STATE_CHANGE_GROUP** Dieses Ereignis wird ausgelöst, wenn der SQL Server-Dienststatus geändert wird

- **SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP** Gibt an, dass sich ein Anwender erfolgreich an einer eigenständigen Datenbank angemeldet hat
- **SUCCESSFUL_LOGIN_GROUP** Gibt an, dass sich ein Anwender am SQL-Server angemeldet hat
- **USER_CHANGE_PASSWORD_GROUP** Das Ereignis wird ausgelöst, wenn das Kennwort des Benutzers einer eigenständigen Datenbank mit der ALTER USER-Anweisung geändert wird

Aktionsgruppen auf Serverebene umfassen Aktionen auf einer SQL Server-Instanz. In einer Datenbank-Überwachungsspezifikation sind nur Schemaobjektzugriffe in einer Datenbank integriert. Aktionen auf Serverebene ermöglichen keine detaillierte Filterung für Aktionen auf Datenbankebene.

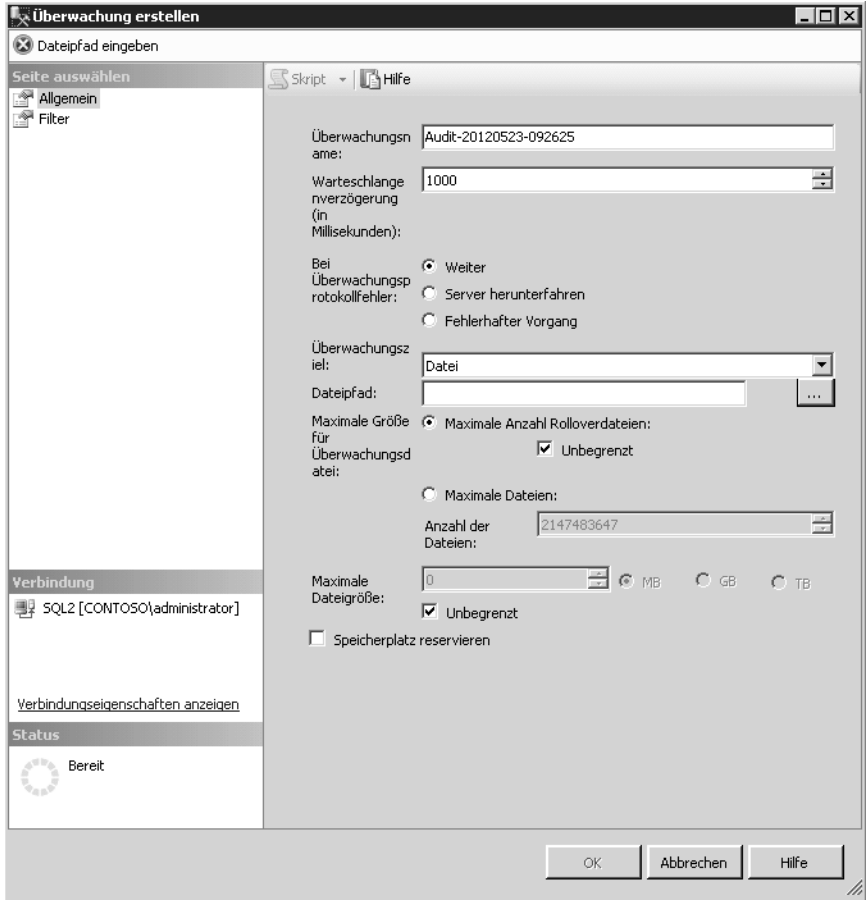
Serverüberwachungen und Serverüberwachungsspezifikationen erstellen

Sie können mehrere Überwachungen pro Instanz festlegen. Das Serverüberwachungsspezifikation-Objekt gehört zu einer Überwachung. Sie können eine Serverüberwachungsspezifikation pro Überwachung erstellen. Eine Überwachung muss bereits vorhanden sein, bevor Sie eine Serverüberwachungsspezifikation erstellen. Benutzer mit der Berechtigung *ALTER ANY SERVER AUDIT* können Serverüberwachungsspezifikationen erstellen und diese an eine beliebige Überwachung binden. So erstellen Sie eine Serverüberwachung:

1. Erweitern Sie im Objekt-Explorer den Knoten *Sicherheit*.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Überwachungen* und wählen Sie im Kontextmenü den Eintrag *Neue Überwachung* aus.
3. Anschließend öffnet sich ein Fenster, über das Sie die Überwachung konfigurieren. Hier geben Sie zunächst einen Namen ein oder verwenden den Standardnamen.
4. Bei *Warteschlangenverzögerung* legen Sie den Zeitraum in Millisekunden fest, nach der die Verarbeitung von Überwachungsaktionen erzwungen wird. Der Wert 0 steht für eine synchrone Übermittlung. Der standardmäßige Wert beträgt 1.000. Der maximale Wert beträgt 2.147.483.647 (24 Tage, 20 Stunden, 31 Minuten, 23 Sekunden und 647 Millisekunden).
5. Über *Bei Überwachungsprotokollfehler* legen Sie fest, wie sich die Überwachung bei Fehlern verhalten soll:
   - **Weiter** Die Überwachung versucht weiter, Ereignisse zu protokollieren. Wählen Sie diese Option aus, wenn die stabile Verwendung des Datenbankmoduls wichtiger ist als die Beibehaltung einer vollständigen Überwachung. Dies ist die Standardauswahl.
   - **Server herunterfahren** Fährt den Server herunter, wenn die Serverinstanz keine Daten in das Überwachungsziel schreiben kann.
   - **Fehlerhafter Vorgang** Es treten keine überwachten Ereignisse auf. Aktionen, die keine überwachten Ereignisse verursachen, können fortgesetzt werden. Die Überwachung versucht weiterhin, Ereignisse zu protokollieren, und wird fortgesetzt, wenn die Fehlerbedingung aufgelöst wurde. Wählen Sie diese Option aus, wenn die Beibehaltung einer vollständigen Überwachung wichtiger ist als der Vollzugriff auf das Datenbankmodul.
6. Bei *Überwachungsziel* wählen Sie aus, wo der Server die Daten der Überwachung speichern soll. Die verfügbaren Optionen sind eine Datei, das Windows-Anwendungsprotokoll oder das Windows-Sicherheitsprotokoll. SQL Server 2012 kann nicht in das Windows-Sicherheitsprotokoll

schreiben, ohne zusätzliche Einstellungen in Windows zu konfigurieren. Lesen Sie in den nächsten Abschnitten, was Sie dazu noch konfigurieren müssen. Um Daten ins Anwendungsprotokoll zu schreiben, ist aber keine weitere Maßnahme notwendig, nur wenn Sie in das Sicherheitsprotokoll der Ereignisanzeige schreiben wollen.

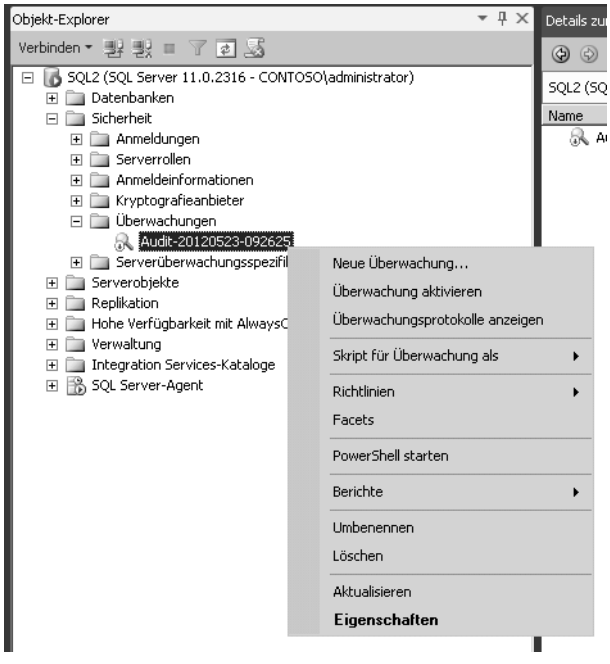
Abbildg. 6.12 Konfigurieren einer Überwachung



7. Über die Option *Maximale Anzahl Rolloverdateien* legen Sie fest, wie viele Überwachungsdateien vom System angelegt werden dürfen. Ist die maximale Anzahl von Überwachungsdateien erreicht, überschreibt der Server die ältesten Überwachungsdateien. Außerdem tritt bei jeder Aktion, durch die zusätzliche Überwachungsereignisse verursacht werden, ein Fehler auf.
8. Über das Kontrollkästchen *Speicherplatz reservieren* legen Sie fest, dass der auf dem Datenträger zugeordnete Speicherplatz der festgelegten maximalen Dateigröße entspricht. Diese Einstellung können Sie nur verwenden, wenn das Kontrollkästchen *Unbegrenzt* bei *Maximale Dateigröße* deaktiviert ist. Diese Option ist standardmäßig deaktiviert.

9. Geben Sie auf der Seite *Filter* optional ein Prädikat oder eine WHERE-Klausel für die Serverüberwachung ein, um Optionen anzugeben, die auf der Seite *Allgemein* nicht verfügbar sind, zum Beispiel *object_name = 'EmployeesTable'*.
10. Sind alle Optionen festgelegt, klicken Sie auf *OK*. Die Überwachung wird jetzt unterhalb des Knotens *Überwachung* angezeigt, ist aber deaktiviert. Sie können die Einstellungen der Überwachung jederzeit anpassen, indem Sie über das Kontextmenü die Eigenschaften aufrufen. Und über das Kontextmenü können Sie auch die Überwachung aktivieren.

Abbildg. 6.13 Verwalten einer Überwachung

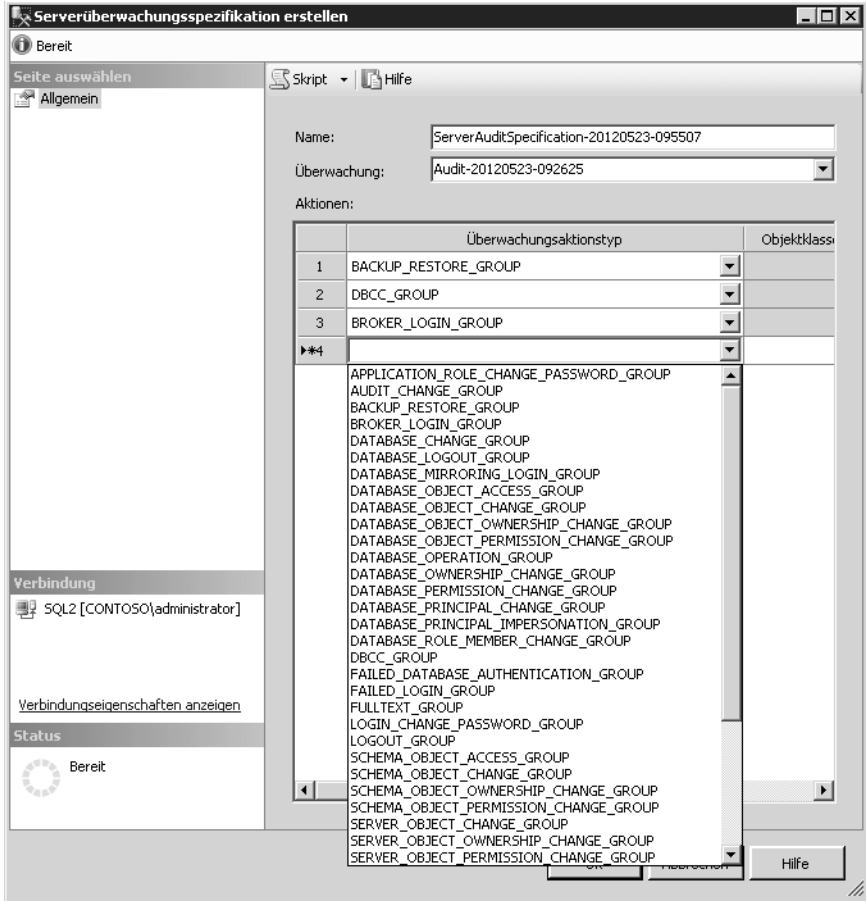


Haben Sie eine Serverüberwachung erstellt, können Sie eine Serverüberwachungsspezifikation erstellen:

1. Erweitern Sie im Objekt-Explorer den Knoten *Sicherheit*.
2. Klicken Sie mit der rechten Maustaste auf den Knoten *Serverüberwachungsspezifikationen* und wählen Sie im Kontextmenü den Eintrag *Neue Serverüberwachungsspezifikation* aus.
3. Geben Sie im neuen Fenster den Namen der Spezifikation an oder belassen Sie die Vorgabe. Wählen Sie anschließend eine Überwachung aus, die Sie mit der *Überwachungsspezifikation* verbinden wollen.
4. Wählen Sie dann aus der Aktionenliste in der Spalte *Überwachungsaktionstyp* die Überwachungsaktionsgruppen auf Serverebene aus. Sie können an dieser Stelle auch mehrere Gruppen auswählen. Mehr zum Thema lesen Sie im Abschnitt »SQL Server Audit-Aktionsgruppen und -Aktionen« ab Seite 369.
5. Für Gruppen können Sie dann verschiedene Einstellungen in der entsprechenden Zeile vornehmen.
6. Klicken Sie auf *OK*, um die Spezifikation zu erstellen.

HINWEIS Damit eine Überwachung mit einer Serverüberwachungsspezifikation durchgeführt wird, aktivieren Sie im SQL Server Management Studio im Knoten *Sicherheit* per Kontextmenü die Überwachungen.

Abbildg. 6.14 Erstellen einer Serverüberwachungsspezifikation



SQL-Serverüberwachungsereignisse in das Sicherheitsprotokoll der Windows-Ereignisanzeige schreiben

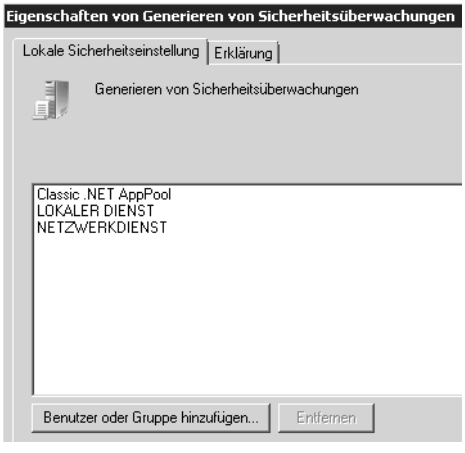
Das Konto, mit dem der SQL Server-Dienst startet, muss über die Berechtigung zum Generieren von Sicherheitsüberwachungen verfügen, um in das Windows-Sicherheitsprotokoll schreiben zu können. Die Windows-Überwachungsrichtlinie kann sich auf die SQL Server-Überwachung auswirken, wenn sie so konfiguriert ist, dass sie in das Windows-Sicherheitsprotokoll schreibt. In diesem Fall besteht bei einer falschen Konfiguration der Überwachungsrichtlinie die Gefahr, dass Ereignisse

verloren gehen. Das Windows-Sicherheitsprotokoll ist standardmäßig so konfiguriert, dass ältere Ereignisse überschrieben werden. Hierdurch werden immer die neuesten Ereignisse beibehalten.

Nehmen Sie Einstellungen lokal am Server vor, besteht die Möglichkeit, dass diese durch Gruppenrichtlinien überschrieben werden können. In diesem Fall nehmen Sie die Einstellungen nicht über lokale Richtlinien vor, sondern mit Gruppenrichtlinien. Die Einstellungen finden Sie an der gleichen Stelle:

1. Starten Sie in der Programmgruppe *Verwaltung* die *Lokale Sicherheitsrichtlinie* oder geben Sie *secpol.msc* im Suchfeld des Startmenüs ein.
2. Erweitern Sie den Knoten *Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrechten*.
3. Doppelklicken Sie im Ergebnisbereich auf *Generieren von Sicherheitsüberwachungen*.
4. Klicken Sie auf der Registerkarte *Lokale Sicherheitseinstellung* auf *Benutzer oder Gruppe hinzufügen*.
5. Geben Sie den Benutzer ein, mit dem Sie die Überwachung durchführen.

Abbildg. 6.15 Konfigurieren der lokalen Sicherheitsrichtlinien auf SQL-Servern



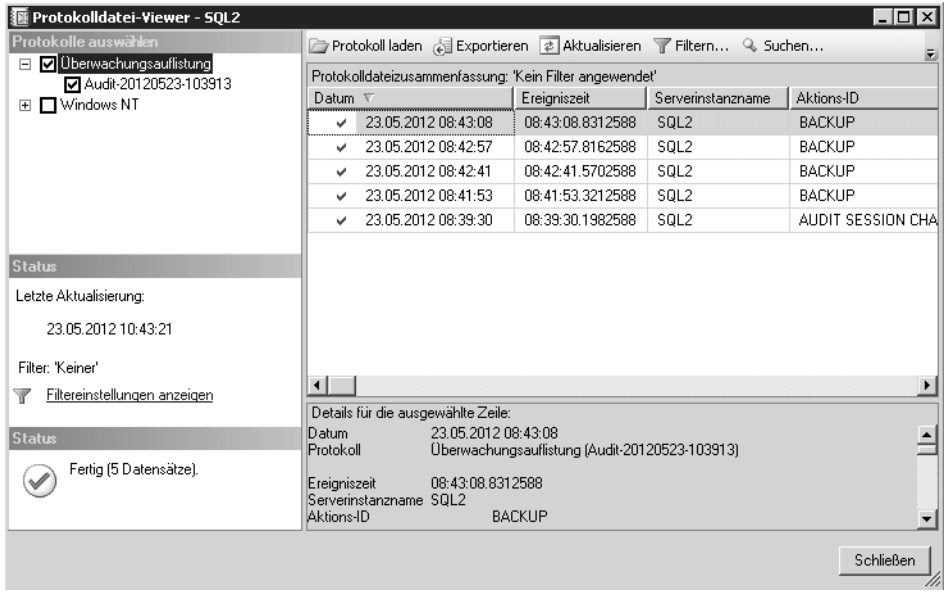
6. Navigieren Sie zum Knoten *Lokale Richtlinien/Überwachungsrichtlinie*.
7. Doppelklicken Sie im Ergebnisbereich auf *Objektzugriffsversuche überwachen*.
8. Wählen Sie auf der Registerkarte *Lokale Sicherheitseinstellung* im Abschnitt *Diese Versuche überwachen* die beiden Kontrollkästchen *Erfolgreich* und *Fehler*.
9. Bestätigen Sie mit *OK*.
10. Starten Sie den SQL-Server neu, um diese Einstellung zu aktivieren.

SQL Server-Überwachungsprotokoll anzeigen

Wenn Sie die Ereignisse der Überwachung in die Ereignisanzeige schreiben lassen, überwachen Sie diese wie die Standardereignisse. Lassen Sie die Daten in eine Datei schreiben, können Sie diese mit dem standardmäßigen Protokoll-Viewer betrachten. Auch eine Anzeige mit SQL-Abfragen ist möglich, um Ergebnisse der Überwachung anzuzeigen:

1. Erweitern Sie im Objekt-Explorer des SQL Server Management Studios den Knoten *Sicherheit*.
2. Erweitern Sie den Knoten *Überwachungen*.
3. Klicken Sie mit der rechten Maustaste auf die Überwachung, deren Protokoll Sie anzeigen wollen, und klicken Sie auf *Überwachungsprotokolle anzeigen*.
4. Es öffnet sich der Protokolldatei-Viewer mit den entsprechenden Daten und Informationen.

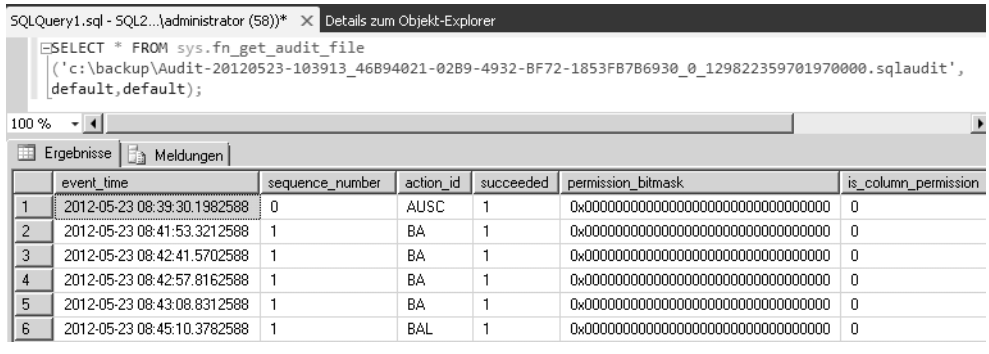
Abbildg. 6.16 Anzeigen der Informationen zu einer Überwachung



Wollen Sie die Daten über eine SQL-Abfrage anzeigen lassen, verwenden Sie die Systemsicht *sys.fn_get_audit_file*. Diese können Sie problemlos mit einer SELECT-Abfrage filtern und anzeigen. Die Syntax dazu lautet:

```
SELECT * FROM sys.fn_get_audit_file ('<Pfad und Name der
Überwachungsdatei>',default,default);
```

Abbildg. 6.17 Anzeige des Überwachungsprotokolls über eine SQL-Abfrage



	event_time	sequence_number	action_id	succeeded	permission_bitmask	is_column_permission
1	2012-05-23 08:39:30.1982588	0	AUSC	1	0x00000000000000000000000000000000	0
2	2012-05-23 08:41:53.3212588	1	BA	1	0x00000000000000000000000000000000	0
3	2012-05-23 08:42:41.5702588	1	BA	1	0x00000000000000000000000000000000	0
4	2012-05-23 08:42:57.8162588	1	BA	1	0x00000000000000000000000000000000	0
5	2012-05-23 08:43:08.8312588	1	BA	1	0x00000000000000000000000000000000	0
6	2012-05-23 08:45:10.3782588	1	BAL	1	0x00000000000000000000000000000000	0

Change Data Capture und Änderungsnachverfolgung im Vergleich

SQL Server 2012 stellt Funktionen bereit, mit denen Sie Änderungen in einer Datenbank nachverfolgen können. Change Data Capture (CDC) und die Änderungsnachverfolgung ermitteln Einfüge-, Aktualisierungs- und Löschvorgänge für Tabellen in Datenbanken.

HINWEIS Die Änderungsverfolgung ist Bestandteil in allen Editionen von SQL Server 2012, auch der kostenlosen Express Edition. Change Data Capture (CDC) ist allerdings nur in der Enterprise Edition von SQL Server 2012 enthalten.

Der Vorteil von Change Data Capture im Vergleich zur Änderungsnachverfolgung ist die Speicherung von Verlaufsdaten. Das heißt, die Änderungsnachverfolgung erfasst, welche Daten geändert wurden, aber nicht die Daten der Änderung. CDC erfasst auch die durchgeführte Änderung. Ansonsten sind sich die beiden Funktionen sehr ähnlich.

Beide Werkzeuge richten sich zwar eher an Entwickler als an Administratoren, dennoch sollten Administratoren die Grundfunktionen der Überwachungsmöglichkeiten beherrschen. Die Änderungsnachverfolgung basiert auf Transaktionen, für die ein Commit ausgeführt wurde. Solche Transaktionen werden vom Transaktionsprotokoll fest in die Datenbank geschrieben.

Grundlagen von Change Data Capture und Änderungsnachverfolgung

Datenbanken, für die Sie Change Data Capture aktivieren, können Sie auch spiegeln. Change Data Capture und Transaktionsreplikation können Sie in einer Datenbank parallel aktivieren. Verwenden Sie in diesem Fall aber die Prozedur *sp_replcmds*, um Änderungen aus dem Transaktionsprotokoll auszulesen. SQL Server 2012 arbeitet aber zuerst die Replikation ab und speichert dann erst die Änderung, um die Leistung des Servers nicht zu beeinträchtigen.

HINWEIS Stellen Sie eine Datenbank wieder her, für die Change Data Capture aktiviert ist, bleibt die Funktion nach der Wiederherstellung weiterhin aktiviert.

Stellen Sie die Datenbank auf einem anderen Server wieder her, wird CDC deaktiviert und die Verlaufsdaten werden gelöscht. Wollen Sie CDC auch in diesem Fall aktiviert belassen, verwenden Sie beim Wiederherstellen der Datenbank die Option *KEEP_CDC*. Auf dem Server muss allerdings die Enterprise Edition von SQL Server 2012 installiert sein.

Die Änderungsnachverfolgung erfasst im Gegensatz zur CDC nicht die geänderten Daten. Die Änderungsnachverfolgung speichert dafür deutlich weniger Daten als CDC.

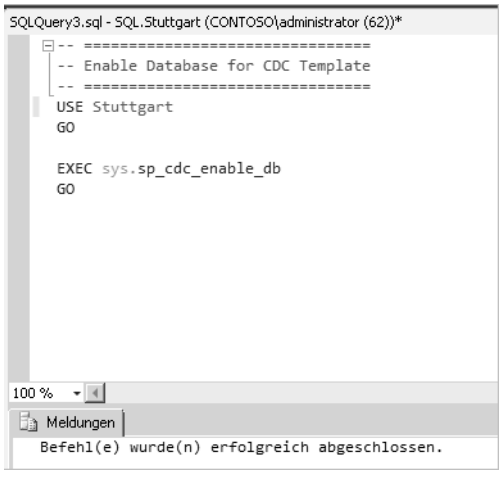
Change Data Capture aktivieren und deaktivieren

Um Change Data Capture (CDC) zu aktivieren, muss ein Benutzer der Serverrolle *sysadmin* zuerst die Datenbank für Change Data Capture aktivieren. Dazu verwenden Sie die gespeicherte Prozedur

sys.sp_cdc_enable_db. Aktivieren Sie Change Data Capture, erstellt SQL Server 2012 das *cdc*-Schema, den *cdc*-Benutzer, Metadatentabellen und andere Systemobjekte für die Datenbank.

Für die Erstellung müssen Sie kein T-SQL-Skript schreiben, sondern können die Vorlage für die Aktivierung von CDC über den Vorlagen-Explorer laden. Wie das geht, lesen Sie in Kapitel 3. Sie finden die Vorlage über *Change Data Capture/Configuration/Enable Database for CDC*. Laden Sie ein Skript aus dem Vorlagen-Explorer in eine neue Abfrage, lassen Sie mit der Tastenkombination Strg+⇧+M ein Fenster anzeigen, in dem Sie bequem alle Variablen im Skript an Ihre Umgebung anpassen können. Anschließend lassen Sie das Skript ausführen und in Ihre Umgebung integrieren. Über diesen Weg können auch weniger geübte Administratoren schnell und einfach komplexe Skripts mit T-SQL erstellen.

Abbildg. 6.18 Aktivieren von CDC für eine Datenbank



Um Change Data Capture für eine Datenbank zu deaktivieren, verwenden Sie die Vorlage *Disable Database for CDC*. Sie müssen nicht CDC für einzelne Tabellen deaktivieren, bevor Sie die Datenbank deaktivieren. Das Skript sieht ähnlich aus, verwendet aber die gespeicherte Prozedur *sys.sp_cdc_disable_db*. Durch das Deaktivieren der Datenbank löschen Sie auch alle mit ihr verbundenen Change Data Capture-Metadaten, einschließlich des *cdc*-Benutzers und -Schemas und der Change Data Capture-Aufträge.

HINWEIS Löschen Sie eine Datenbank, für die Change Data Capture aktiviert ist, löscht der Server auch die Change Data Capture-Aufträge.

Haben Sie eine Datenbank für Change Data Capture aktiviert, können Mitglieder der Datenbankrolle *db_owner* eine Aufzeichnungsinstanz für einzelne Quelltabellen mit der gespeicherten Prozedur *sys.sp_cdc_enable_table* erstellen. Wollen Sie nur einen Teil der Spalten nachverfolgen, verwenden Sie die Option *@captured_column_list*. Standardmäßig befindet sich die Änderungstabelle in der Standarddateigruppe der Datenbank bei den Systemtabellen. Wenn ein Datenbankbesitzer die Position der einzelnen Änderungstabellen steuern will, verwendet dieser die Option *@filegroup_name*. Sie finden auch für diese Maßnahmen entsprechende Vorlagen im Vorlagen-Explorer.

HINWEIS Sie können mit den Änderungsdaten auch arbeiten und diese auswerten. Dazu müssen Sie sich allerdings mit Entwicklerthemen befassen. Wie Sie dabei vorgehen, lesen Sie in MSDN auf der Seite *http://msdn.microsoft.com/de-de/library/cc645858.aspx* [Ms151-K06-05].

Change Data Capture verwalten und überwachen

Der Aufzeichnungsauftrag von CDC startet mit der gespeicherten Prozedur *sp_MScdc_capture_job*. Wichtig sind die konfigurierten Werte für *maxtrans*, *maxscans*, *continuous* und *pollinginterval* für den Aufzeichnungsauftrag aus *msdb.dbo.cdc_jobs*. Die jeweiligen Werte übergibt die Prozedur als Option an die gespeicherte Prozedur *sp_cdc_scan*. Diese Prozedur wiederum verwenden Sie, um *sp_replcmds* aufzurufen.

Mit der Option *maxtrans* wird die maximale Anzahl von Transaktionen festgelegt, die während eines einzelnen Scanzyklus des Protokolls verarbeitet werden können. Die *maxscans*-Option gibt die maximale Anzahl der Scanzyklen an, die der Server versucht, um das Protokoll zu leeren. Die Einstellung *continuous* steuert, ob *sp_cdc_scan* die Steuerung nach dem Leeren des Protokolls oder nach dem Ausführen der maximalen Anzahl von Scanzyklen beendet.

Der Einmalmodus ist nützlich, wenn die Anzahl der Transaktionen bekannt ist. Der Modus ist daher nur für Testzwecke sinnvoll, nicht für produktive Umgebungen. Im kontinuierlichen Modus fordert der Aufzeichnungsauftrag das ständige Ausführen von *sp_cdc_scan* an. In diesem Modus bleibt der Aufzeichnungsauftrag aktiv und führt zwischen Protokollscanvorgängen eine WAITFOR-Anweisung aus. Sie können für den Aufzeichnungsauftrag statt eines Abrufintervalls andere Logiken anwenden, um festzulegen, ob er einen neuen Scan beginnen oder warten soll.

Change Data Capture verwendet einen SQL Server-Agent-Transact-SQL-Auftrag zum Verwalten der Größe der Änderungstabellen. Dieser startet durch die gespeicherte Prozedur *sp_MScdc_cleanup_job*.

CDC überwachen

Jede Zeile in *sys.dm_cdc_log_scan_sessions* stellt eine Ausführung von *sp_cdc_scan* dar. Während einer Sitzung kann der Scan Änderungen oder ein leeres Ergebnis zurückgeben. Gibt es keine Änderung, wird die Spalte *empty_scan_count* in *sys.dm_cdc_log_scan_sessions* auf den Wert 1 gesetzt. Mit einer SQL-Abfrage können Sie die leeren Ergebnisse anzeigen lassen:

```
SELECT * FROM sys.dm_cdc_log_scan_sessions WHERE empty_scan_count <> 0
```

Die Latenzzeit ist die Zeitspanne zwischen dem Ausführen des Commit für eine Transaktion und dem Ausführen des Commit für die letzte aufgezeichnete Transaktion in der Änderungstabelle. Auch diese Zeit können Sie abfragen, um die Leistung des Prozesses zu überwachen. Dazu verwenden Sie die folgende Abfrage:

```
SELECT latency FROM sys.dm_cdc_log_scan_sessions WHERE session_id = 0
```

Wichtig ist auch der Durchsatz. Dies ist die durchschnittliche Anzahl von Befehlen pro Sekunde. Den Durchsatz einer Sitzung erhalten Sie durch Teilen des Werts in der Spalte *command_count* durch den Wert in der Spalte mit der Bezeichnung *duration*. Die folgende Abfrage gibt den durchschnittlichen Durchsatz für die letzten Sitzungen zurück:

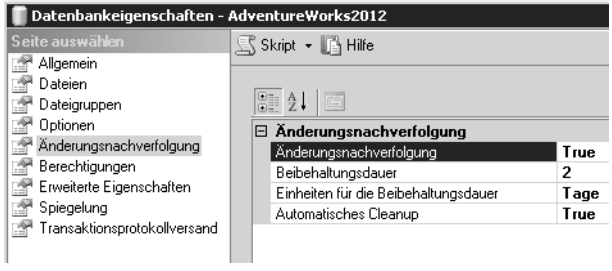
```
SELECT command_count/duration AS [Throughput] FROM sys.dm_cdc_log_scan_sessions WHERE
session_id = 0
```

Mit dem SQL Server-Datensammler können Sie Momentaufnahmen (Snapshots) von Daten aus Tabellen erfassen und ein Data Warehouse für die Leistung erstellen. Sie sollten in regelmäßigen Abständen Momentaufnahmen der Sichten *sys.dm_cdc_log_scan_sessions*-Sicht und *sys.dm_cdc_errors* erstellen.

Änderungsnachverfolgung aktivieren und deaktivieren

Die Änderungsnachverfolgung erfasst geänderte Zeilen, aber nicht den Wert der Änderungen. Sie aktivieren die Änderungsnachverfolgung am einfachsten im SQL Server Management Studio in den Eigenschaften der Datenbank über die Seite *Änderungsnachverfolgung*.

Abbildg. 6.19 Aktivieren und Verwalten der Änderungsnachverfolgung

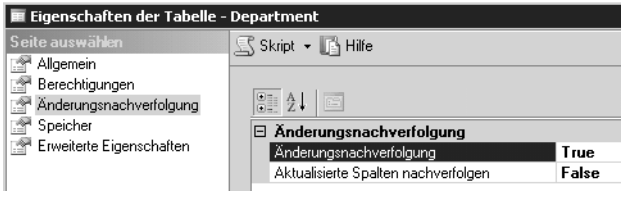


Sobald Sie die Änderungsnachverfolgung aktivieren, setzt der Assistent auch die automatischen Einstellungen für die Funktion. Diese können Sie an Ihre Bedürfnisse anpassen und diese Einstellungen auch als Abfrage steuern. Dazu verwenden Sie die folgenden Befehle:

```
ALTER DATABASE AdventureWorks2012
SET CHANGE_TRACKING = ON
(CHANGE_RETENTION = 2 DAYS, AUTO_CLEANUP = ON)
```

Beibehaltungsdauer gibt den Zeitraum an, für den Änderungsnachverfolgung Daten speichern soll. Daten, die älter sind, entfernt der Server aus den Datenbanken. Die Änderungsnachverfolgung müssen Sie für jede nachzuverfolgende Tabelle getrennt aktivieren. Die Einstellung finden Sie in den Eigenschaften für die Tabellen über *Änderungsnachverfolgung*.

Abbildg. 6.20 Änderungsnachverfolgung für Tabellen aktivieren



Über T-SQL können Sie die Änderungsnachverfolgung auch aktivieren. Dazu verwenden Sie die folgenden Anweisungen:

```
ALTER TABLE <Tabelle>
ENABLE CHANGE_TRACKING
WITH (TRACK_COLUMNS_UPDATED = ON)
```

HINWEIS Wird einer Tabelle mit aktivierter Änderungsnachverfolgung eine neue Spalte hinzugefügt, wird das Hinzufügen der Spalte nicht verfolgt. Die Änderungen in der Spalte protokolliert die Änderungsnachverfolgung aber mit. Es existiert eine interne Änderungstabelle für jede Tabelle, für die die Änderungsnachverfolgung aktiviert ist. Zusätzlich gibt es eine interne Transaktionstabelle für die Datenbank.

Wenn Sie *Aktualisierte Spalten nachverfolgen* auf *True* festlegen, speichert der SQL-Server zusätzliche Informationen in der internen Änderungsnachverfolgungstabelle zu den aktualisierten Spalten. Die Spaltennachverfolgung kann eine Anwendung aktivieren, um nur Spalten zu synchronisieren, die aktualisiert wurden. Dadurch verbessert sich sowohl die Effizienz als auch die Leistung. Die Option ist standardmäßig deaktiviert.

HINWEIS Möchten Sie die Änderungsnachverfolgung deaktivieren, müssen Sie zuerst die Option für die Tabellen ändern, und dann erst für die ganze Datenbank.

Eine Datenbank mit aktivierter Änderungsnachverfolgung verfügt über einen internen Zähler für die Versionen. Dieser zählt die Änderungen an den nachverfolgten Tabellen mit. Jede geänderte Zeile verfügt über eine eigene Versionsnummer. Die Spaltennachverfolgung ermöglicht es Anwendungen, Daten anstatt für die gesamte Zeile nur für die geänderten Spalten abzurufen.

SQL Server-Protokolle analysieren

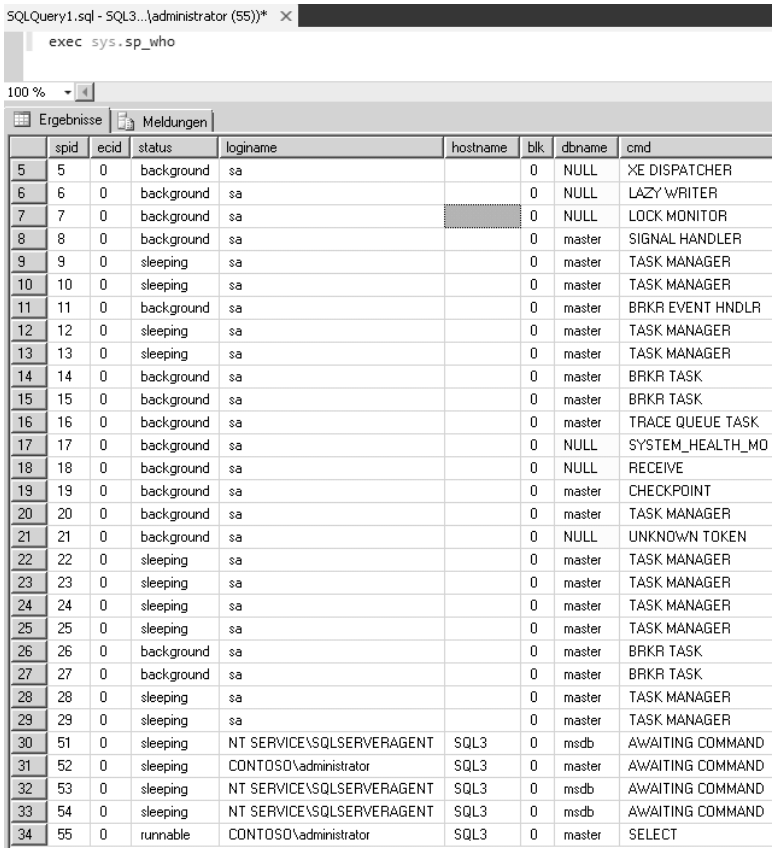
Mit dem Protokolldatei-Viewer in SQL Server Management Studio können Sie auf Fehlermeldungen und Protokolle von den verschiedenen Serverdiensten zugreifen und Fehler entsprechend analysieren. Der Viewer unterstützt die folgenden Serverdienste:

- *Überwachungsauflistung*
- *Datensammlung*
- *Datenbank-E-Mail*
- *Auftragsverlauf*
- *SQL Server*
- *SQL Server-Agent*

Windows-Ereignisse können Sie über diesen Weg zwar ebenfalls auslesen, allerdings ist hier die Ansicht der Ereignisanzeige unter Umständen besser geeignet.

TIPP Sie können sich auch mit einer SQL-Abfrage einen Überblick über die aktuell laufenden Prozesse auf dem Server und deren Ressourcennutzung verschaffen. Dazu geben Sie den Befehl *exec sys.sp_who2* ein.

Abbildg. 6.21 Anzeige der laufenden Prozesse in einer SQL Server-Instanz



SQLQuery1.sql - SQL3...\administrator (55))*

```
exec sys.sp_who
```

100 %

Ergebnisse | Meldungen

	spid	ecid	status	loginame	hostname	blk	dbname	cmd
5	5	0	background	sa		0	NULL	XE DISPATCHER
6	6	0	background	sa		0	NULL	LAZY WRITER
7	7	0	background	sa		0	NULL	LOCK MONITOR
8	8	0	background	sa		0	master	SIGNAL HANDLER
9	9	0	sleeping	sa		0	master	TASK MANAGER
10	10	0	sleeping	sa		0	master	TASK MANAGER
11	11	0	background	sa		0	master	BRKR EVENT HNDLR
12	12	0	sleeping	sa		0	master	TASK MANAGER
13	13	0	sleeping	sa		0	master	TASK MANAGER
14	14	0	background	sa		0	master	BRKR TASK
15	15	0	background	sa		0	master	BRKR TASK
16	16	0	background	sa		0	master	TRACE QUEUE TASK
17	17	0	background	sa		0	NULL	SYSTEM_HEALTH_MO
18	18	0	background	sa		0	NULL	RECEIVE
19	19	0	background	sa		0	master	CHECKPOINT
20	20	0	background	sa		0	master	TASK MANAGER
21	21	0	background	sa		0	NULL	UNKNOWN TOKEN
22	22	0	sleeping	sa		0	master	TASK MANAGER
23	23	0	sleeping	sa		0	master	TASK MANAGER
24	24	0	sleeping	sa		0	master	TASK MANAGER
25	25	0	sleeping	sa		0	master	TASK MANAGER
26	26	0	background	sa		0	master	BRKR TASK
27	27	0	background	sa		0	master	BRKR TASK
28	28	0	sleeping	sa		0	master	TASK MANAGER
29	29	0	sleeping	sa		0	master	TASK MANAGER
30	51	0	sleeping	NT SERVICE\SQLSERVERAGENT	SQL3	0	msdb	AWAITING COMMAND
31	52	0	sleeping	CONTOSO\administrator	SQL3	0	master	AWAITING COMMAND
32	53	0	sleeping	NT SERVICE\SQLSERVERAGENT	SQL3	0	msdb	AWAITING COMMAND
33	54	0	sleeping	NT SERVICE\SQLSERVERAGENT	SQL3	0	msdb	AWAITING COMMAND
34	55	0	runnable	CONTOSO\administrator	SQL3	0	master	SELECT

Protokolle im SQL Server Management Studio anzeigen

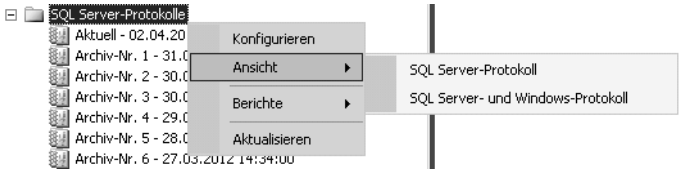
In SQL Server 2012 können Sie SQL Server-Protokolldateien aus lokalen oder Remoteinstanzen von SQL-Servern mit der Option *Registrierte Server* anzeigen lassen (siehe Kapitel 3).

HINWEIS Zum Zugreifen auf Protokolldateien müssen Sie Mitglied der Serverrolle *securityadmin* sein. Um auf Protokolldateien für Offlineinstanzen zuzugreifen, müssen Sie über Lesezugriff für den WMI-Namespace *Root\Microsoft\SqlServer\ComputerManagement10* und den Ordner mit den Protokolldateien verfügen.

Um Protokolle anzuzeigen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das SQL Server Management Studio und navigieren Sie zum Knoten *Verwaltung*.
2. Klicken Sie mit der rechten Maustaste auf *SQL Server-Protokolle*, öffnen Sie im Kontextmenü das Untermenü *Sicht* und wählen Sie dann entweder den Eintrag *SQL Server-Protokoll* oder den Eintrag *SQL Server- und Windows-Protokoll* aus.

Abbildg. 6.22 Öffnen von Protokolldateien in SQL Server 2012

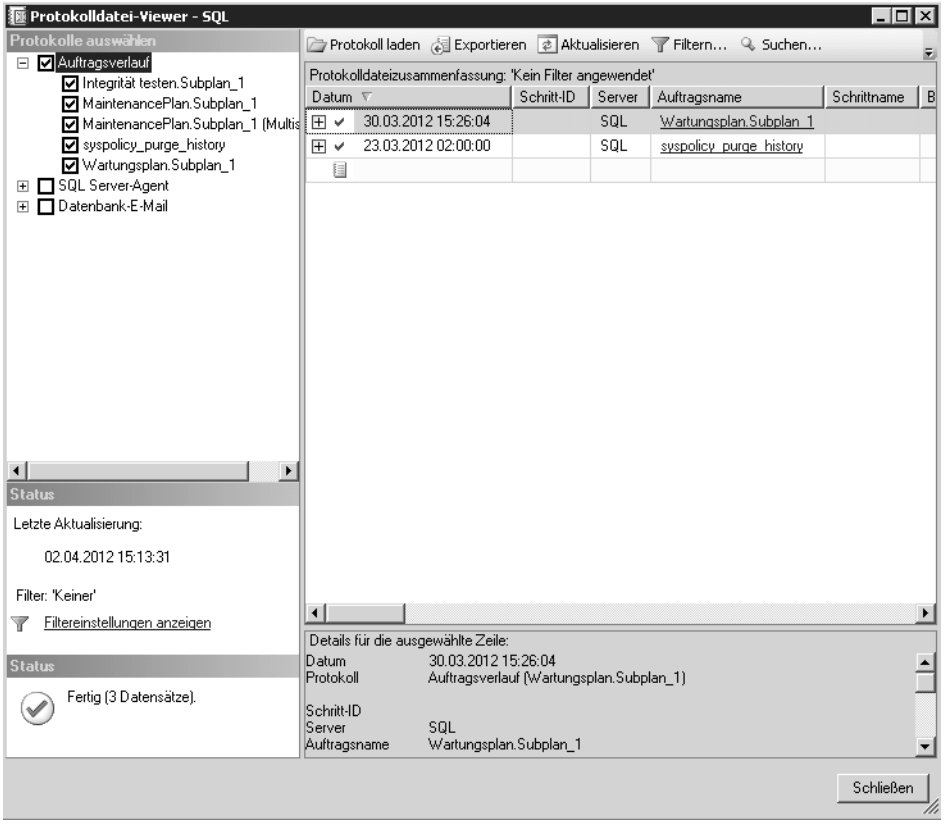


Alternativ klicken Sie mit der rechten Maustaste auf den Knoten *SQL Server-Protokolle* und wählen im Kontextmenü eine der Protokolldateien aus. Sie können auch auf Protokolldateien doppelklicken. Die Protokolle enthalten Daten zu Datenbank-E-Mail, SQL Server, SQL Server-Agent und Windows-Ereignisse.

Protokolle der Aufträge anzeigen

Um Protokolle von Aufträgen anzuzeigen, verwenden Sie ebenfalls das SQL Server Management Studio. Erweitern Sie im Objekt-Explorer den Knoten *SQL Server-Agent*, klicken Sie mit der rechten Maustaste auf *Aufträge* und wählen Sie im Kontextmenü den Eintrag *Verlauf anzeigen*.

Abbildg. 6.23 Anzeigen von Protokollen für den SQL Server-Agent



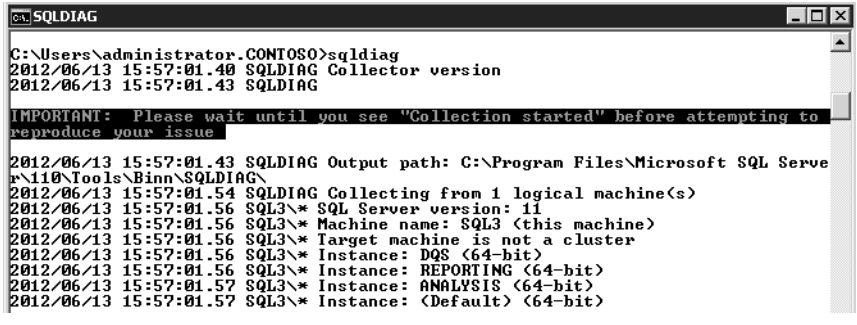
Protokolle von Wartungsplänen, Datensammlungen und mehr

Die Protokolle der Wartungspläne finden Sie wiederum an anderen Stellen. Um diese zu öffnen, gehen Sie dann folgendermaßen vor:

1. Erweitern Sie zunächst im Objekt-Explorer den Knoten *Verwaltung*, klicken Sie mit der rechten Maustaste auf *Wartungspläne* und wählen Sie im Kontextmenü den Eintrag *Verlauf anzeigen*.
2. Klicken Sie mit der rechten Maustaste auf *Datensammlung* und dann im Kontextmenü auf *Protokolle anzeigen*, sehen Sie die Protokolldateien von Datensammlungen.
3. Klicken Sie mit der rechten Maustaste auf *Datenbank-E-Mail* und dann im Kontextmenü auf *Datenbank-E-Mail-Protokoll anzeigen*, zeigt das SQL Server Management Studio Meldungen zu Datenbank-E-Mails an.
4. Erweitern Sie im Objekt-Explorer den Knoten *Sicherheit/Überwachungen*, klicken Sie mit der rechten Maustaste auf eine Überwachung und wählen Sie im Kontextmenü den Eintrag *Überwachungsprotokolle anzeigen* aus, wenn Sie die Protokollierung der Überwachung anzeigen lassen wollen.

Das Befehlszeilentool *SQLdiag* zeigt allgemeine Diagnoseinformationen an und kann als Befehlszeilen-Tool oder als Dienst starten. Mit *SQLdiag* können Sie Protokolle und Datendateien von SQL Server 2012 und anderen Servertypen sammeln. Eine Liste aller Möglichkeiten des Tools finden Sie auf der Seite *http://msdn.microsoft.com/de-de/library/ms162833* [Ms151-K06-06].

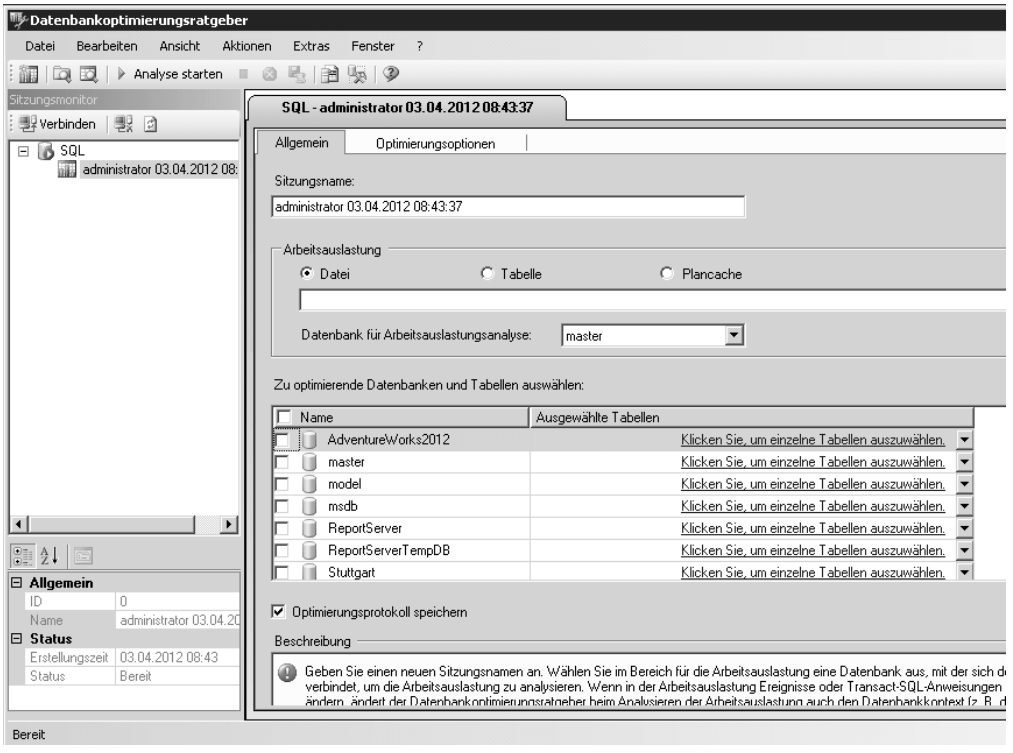
Abbildg. 6.24 SQL-Server überprüfen mit *sqldiag.exe*



Datenbankoptimierungsratgeber einsetzen

Der Datenbankoptimierungsratgeber (DTA) ist dafür zuständig, die Datenbanken auf dem Server zu analysieren und Verbesserungsvorschläge für den Aufbau des Index zu erstellen. Der Index ist der Schlüssel für schnelle Abfragen in SQL Server. Aus diesem Grund muss dieser optimal an die jeweilige Datenbank angepasst sein. Genau genommen richtet sich der Datenbankoptimierungsratgeber an Entwickler, die ihre Datenbank optimal an die Bedürfnisse im Unternehmen anpassen müssen. Dennoch sollten sich Administratoren zumindest grundlegend mit dem Thema auseinandersetzen.

Abbildg. 6.25 Datenbanken mit dem Datenbankoptimierungsratgeber (DTA) optimieren



Grundlagen und Tipps zum Datenbankoptimierungsratgeber

Der Datenbankoptimierungsratgeber kann optimale Empfehlungen für Indizes, indizierte Sichten oder Tabellenpartitionen erstellen. Der Vorteil dabei ist, dass auch weniger geübte Entwickler oder Administratoren einiges an Leistung herausholen können. Auch erfahrene SQL-Entwickler sollten Datenbanken mit dem DTA überprüfen und optimieren lassen. In vielen Fällen lässt sich die Leistung des Servers deutlich erhöhen.

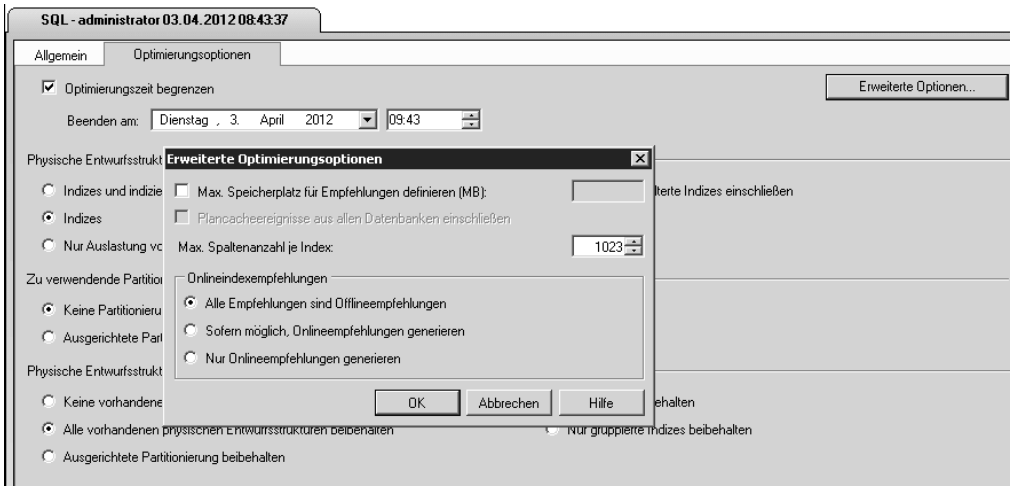
TIPP Der DTA bietet auch eine Befehlszeilenversion. Mit dem Tool *dta* können Sie die Funktionalität des Datenbankoptimierungsratgebers in Anwendungen und Skripts integrieren.

Da das SQL Server-Setup den Pfad der ausführbaren Dateien von SQL Server 2012 in den Befehlszeilenpfad einträgt, können Sie an jeder Stelle der Befehlszeile *dta* starten. Eine Hilfe zur Syntax erhalten Sie mit *dta /?*

In SQL Server 2012 können Sie den Plancache als Arbeitsauslastung angeben, um Datenbanken zu optimieren. Sie können aber auch weiterhin Dateien auf Basis des XML-Formats verwenden, um den DTA zu konfigurieren und Beispielabfragen mitzugeben. Die XML-Eingabedatei unterstützt erweiterte Optimierungsoptionen, die weder über die GUI noch im Befehlszeilentool *dta* verfügbar sind.

Der DTA kann keine eindeutigen Indizes oder Indizes, die PRIMARY KEY- oder UNIQUE-Einschränkungen erzwingen, bearbeiten. Datenbanken im Einzelbenutzermodus lassen sich nicht analysieren (siehe Kapitel 3). Sie können den maximalen Datenträgerspeicher über die Option *–B* des Befehlszeilentools von *dta* verwenden oder in der grafischen Oberfläche einen Wert im Dialgfeld *Erweiterte Optimierungsoptionen* vorgeben.

Abbildg. 6.26 Der DTA bietet zahlreiche Optionen zur Optimierung von Datenbanken an



Wenn Sie eine Einschränkung bezüglich der Optimierungszeit angeben, zum Beispiel mit der Option *–A* oder auf der Registerkarte *Optimierungsoptionen* über die Option *Optimierungszeit begrenzen*, besteht die Möglichkeit, dass der Datenbankoptimierungsratgeber das Zeitlimit überschreitet, um eine optimale Verbesserung zu erreichen.

HINWEIS Der Benutzer, der den Datenbankoptimierungsratgeber startet, muss Mitglied der Datenbankrolle *db_owner* oder der Serverrolle *sysadmin* sein. Die Abfragen zur Optimierung führt der DTA im Sicherheitskontext des Benutzers aus, der den Datenbankoptimierungsratgeber ausführt.

Der Datenbankoptimierungsratgeber speichert Daten in der *msdb*-Datenbank. Aus diesem Grund sollten Sie die Datenbank auch immer in die Sicherungsstrategie des Servers einbinden.

Der DTA kann die Leistung des SQL-Servers stark beeinträchtigen. Sie sollten ihn daher nicht starten, wenn Benutzer am Server arbeiten oder Wartungstasks laufen. Am besten starten Sie den DTA, wenn keinerlei andere Aufgaben anstehen.

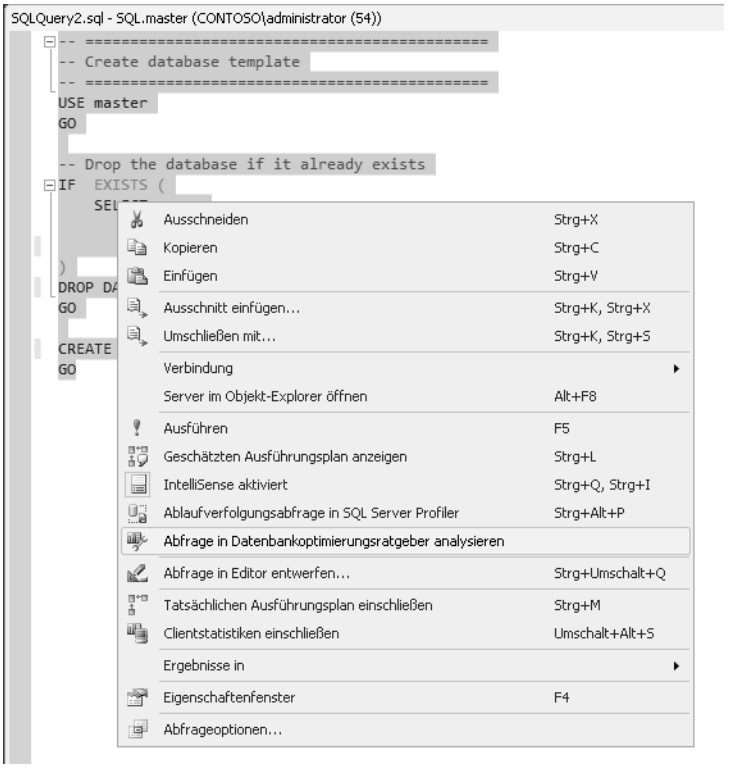
Der Datenbankoptimierungsratgeber ist von der gespeicherten Prozedur *xp_msver* abhängig. Diese gespeicherte Prozedur ist standardmäßig aktiviert. Die Prozedur ermöglicht es dem DTA, die Anzahl der Prozessoren und den verfügbaren Speicher auf dem Server einzubinden.

Datenbankoptimierungsratgeber starten

Beim ersten Start des DTA muss der Benutzer Mitglied der Serverrolle *sysadmin* sein. Bei jedem weiteren Start reicht es aus, das Recht *db_owner* für die zu optimierende Datenbank zu erhalten. Beim ersten Start legt der DTA einige Tabellen in der Systemdatenbank *msdb* an. Bei allen weiteren Starts ist dies nicht mehr notwendig und *db_owner* können die Tabellen verwenden.

Starten Sie daher den Datenbankoptimierungsratgeber und melden Sie sich an der Instanz an in der Sie eine Datenbank optimieren wollen. Sie finden in Windows Server 2008 R2 die Verknüpfung über *Microsoft SQL Server 2012/Leistungstools* im Startmenü. In SQL Server Management Studio finden Sie den Datenbankoptimierungsratgeber im Menü *Extras*. Darüber starten Sie das Tool in Windows Server 2012 am besten.

Abbildg. 6.27 Abfragen lassen sich auch mit dem Datenbankoptimierungsratgeber analysieren



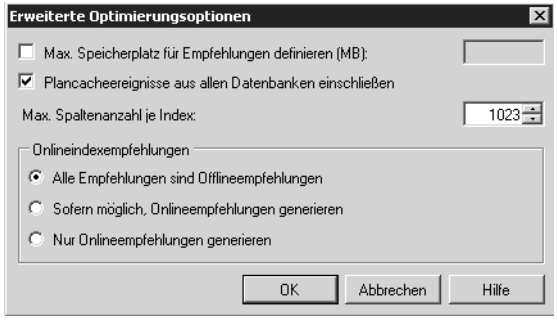
TIPP Alternativ wählen Sie in einem beliebigen Transact-SQL-Skript eine Abfrage oder das gesamte Skript aus, klicken mit der rechten Maustaste auf die Auswahl und wählen *Abfrage in Datenbankoptimierungsratgeber analysieren*.

Die GUI des Datenbankoptimierungsratgebers wird geöffnet und importiert das Skript als Arbeitsauslastung aus einer XML-Datei. Sie können einen Namen für die Sitzung und Optimierungsoptionen angeben, um die ausgewählten Transact-SQL-Abfragen als Arbeitsauslastung zu optimieren.

Ein wichtiger Teil des Datenbankoptimierungsratgebers sind die Arbeitsauslastungen. Eine Arbeitsauslastung ist ein Satz von Transact-SQL-Anweisungen, die der DTA für Datenbanken ausführen soll. Der Datenbankoptimierungsratgeber analysiert diese Arbeitsauslastungen und gibt auf dieser Basis Empfehlungen, um Indizes optimal aufzubauen oder den Server besser zu partitionieren. Arbeitsauslastungen können Sie selbst erstellen, den Plancache verwenden oder über den SQL Server Profiler (Menü *Extras* im SQL Server Management Studio) Datenbanken und Tabellen einlesen. Diesen finden Sie auch in den Leistungstools auf dem SQL-Server. Dazu ist aber etwas Wissen im Bereich T-SQL und der Entwicklung von Datenbanken notwendig.

Geben Sie nach dem Start des Datenbankoptimierungsratgebers auf der Registerkarte *Allgemein* einen Namen ein, um eine neue Optimierungssitzung zu erstellen. Wählen Sie die gewünschte Option für die Arbeitsauslastung aus. Verwenden Sie den Plancache einer Datenbank, gibt DTA die ersten 1.000 Ereignisse aus. Öffnen Sie noch die Registerkarte *Optimierungsoptionen*, klicken Sie auf die Schaltfläche *Erweiterte Optionen* und aktivieren Sie *Plancacheereignisse aus allen Datenbanken einschließen*.

Abbildg. 6.28 Konfigurieren der erweiterten Optionen des DTA



Haben Sie alle Einstellungen vorgenommen, klicken Sie in der Symbolleiste von DTA auf *Analyse starten*.

Datenbanken mit Skripts über die Befehlszeile optimieren

Wollen Sie eine Datenbank mit dem Befehlszeilentool *dta* analysieren, geben Sie in SQL Server 2012 zum Beispiel die neue Option *–ip* für die Verwendung des Plancaches an:

```
dta –E –D <Datenbank> –ip –s <Name der Sitzung>
```

HINWEIS Der Aufruf von *dta* in der Befehlszeile unterscheidet teilweise bei den Optionen zwischen Groß- und Kleinschreibung. Die Optionen lassen Sie sich mit *dta /?* anzeigen.

Die Option *–E* stellt eine Verbindung auf Basis der Anmeldung her, mit der Sie sich am Server angemeldet haben. Sie können sich im *dta*-Befehlszeilentool auch direkt am Server anmelden. Dazu verwenden Sie die Option *–U* und den Benutzernamen, mit dem Sie sich anmelden wollen, sowie die

Option *–P* für das Kennwort. Geben Sie zum Ändern der Anzahl der für die Analyse zu verwendenden Ereignisse die Option *–n* an:

```
dta –S <Servername> –E –D <Datenbank> –ip –n 2000 –s <Sitzung>
```

Geben Sie zum Analysieren der Ereignisse aller Datenbanken in der Instanz die Option *–ipf* an.

Abbildg. 6.29 Analysieren von Datenbanken mit dem DTA in der Befehlszeile

Standardmäßig nutzt DTA eine Verbindung zur Standardinstanz des Servers. Verwenden Sie die Option *–S*, um eine Remotedatenbank oder eine benannte Instanz zu verwenden. Die Option *–if* legt den Namen und den Pfad zu einer Arbeitsauslastungsdatei fest. Die Option *–it* gibt den Namen der Arbeitsauslastungstabelle an, wenn Sie diese Option verwenden.

HINWEIS Standardmäßig verwendet DTA eine Optimierungsdauer von acht Stunden. Wenn Sie eine Arbeitsauslastung für einen unbegrenzten oder anderen Zeitraum verwenden wollen, geben Sie 0 für die Option *–A* an.

Die Option *–ix* legt die XML-Eingabedatei an, die für diese Optimierungssitzung verwendet werden soll.

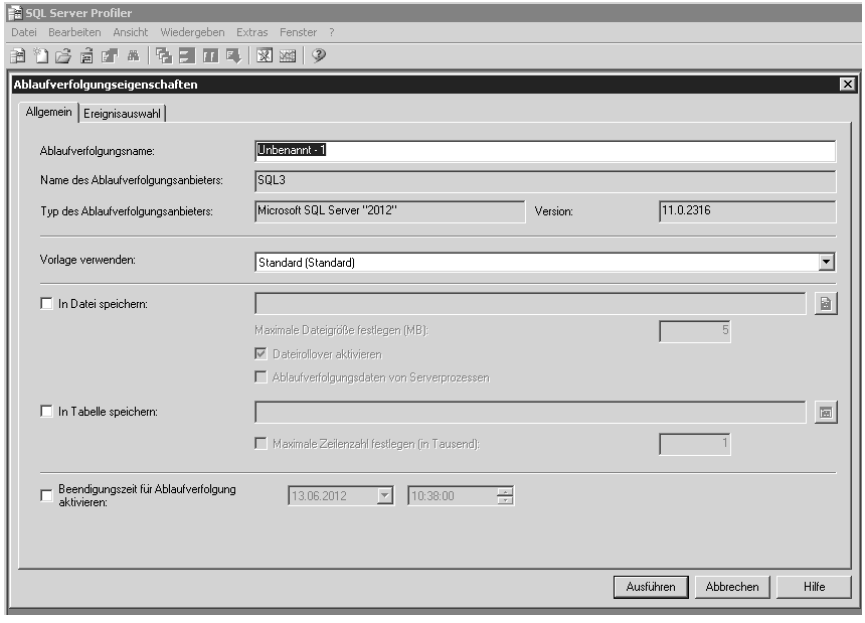
Ablaufverfolgung mit SQL Server Profiler

Um Abfragen und Indizes zu optimieren, können Sie auch den SQL Server Profiler nutzen. Dieser hilft dabei interne Abläufe im Datenbankmodul zu analysieren und anzuzeigen. Das Tool ist allerdings weniger für Administratoren sinnvoll, sondern vor allem für Entwickler zur Optimierung der Abfragen von Datenbankanwendungen.

Sie finden den SQL Server Profiler in der Programmgruppe *Leistungstools* innerhalb der Gruppe *Microsoft SQL Server 2012* oder über den Menüpunkt *Extras* im Management Studio. Über diesen Weg starten Sie das Tool auch in Windows Server 2012. Nach dem Start des Tools verbinden Sie sich zunächst mit der SQL Server-Instanz, die Sie überwachen wollen. Nutzen Sie dazu das Symbol oben links in der Symbolleiste von SQL Server Profiler.

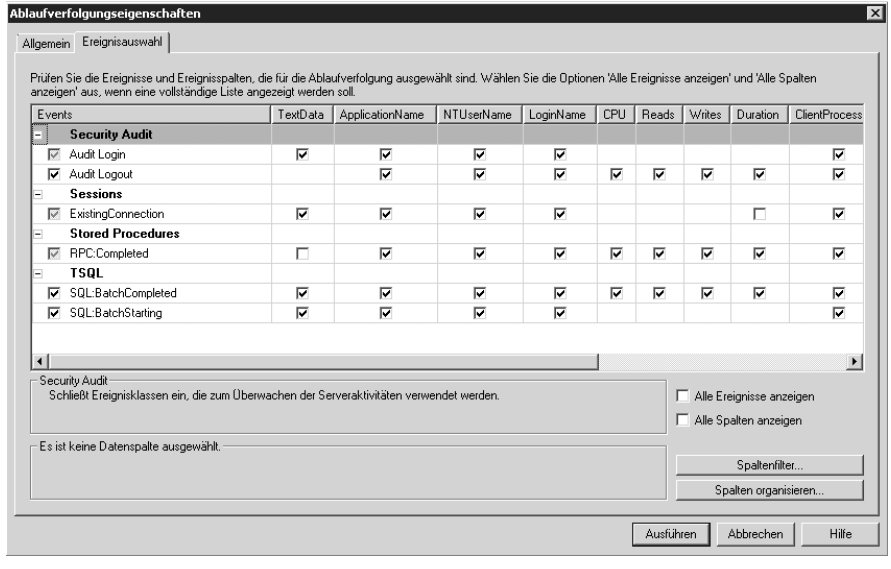
Auf der Registerkarte *Allgemein* legen Sie fest, wo die Daten der Ablaufverfolgung abgelegt werden sollen. Sie können an dieser Stelle die Daten in einer Datei oder in einer Datenbanktabelle speichern.

Abbildg. 6.30 Verwenden von SQL Server Profiler für das Erstellen einer Ablaufverfolgung in SQL Server 2012



Auf der Registerkarte *Ereignisauswahl* nehmen Sie die wichtigsten Einstellungen vor. Hier wählen Sie die Ereignisse und Spalten aus, welche die Ablaufverfolgung verwenden soll. In den Standardeinstellungen überwacht SQL Server Profiler die Daten der vorhandenen Verbindungen, An- und Abmeldungen und Beginn und Abschluss von Abfragen. Für die meisten Bedürfnisse reichen die Standardeinstellungen zumindest für einen ersten Überblick aus.

Abbildg. 6.31 Konfigurieren der zu überwachenden Ereignisse mit SQL Server Profiler

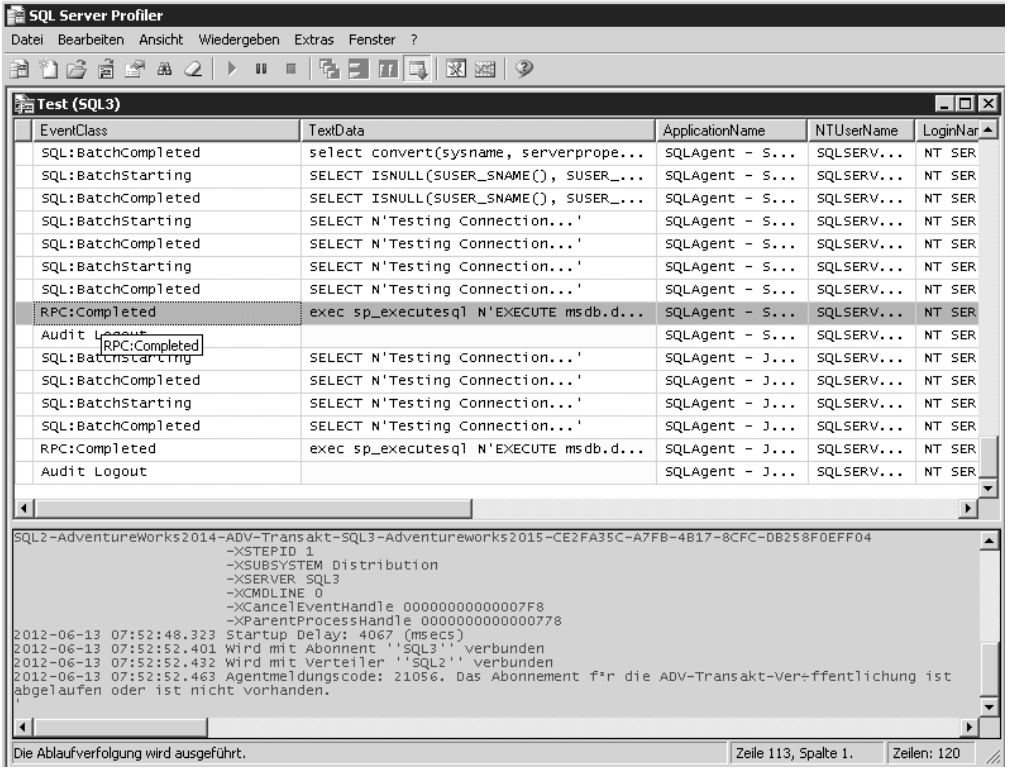


Sobald Sie auf *Ausführen* klicken, sehen Sie in Echtzeit, was auf dem Server abläuft. Sie können die einzelnen Spalten der Abfrage jederzeit ändern und auch Filter einbauen.

Zusätzlich speichert der Profiler die Daten in der Datei oder der Tabelle, die Sie in den Einstellungen festgelegt haben. Diese Daten öffnen Sie über die Symbolleiste.

Ändern Sie die Standardeinstellungen einer Ablaufverfolgung, können Sie diese über *Datei/Speichern unter* als Vorlagendatei speichern und zukünftig auf der Registerkarte *Allgemein* die von Ihnen erstellte Vorlage auswählen. In dieser sind die Einstellungen, Filter und Ereignisse hinterlegt.

Abbildg. 6.32 Anzeigen der Daten der Ablaufverfolgung



Fehlerbehebung in Windows Server – Ereignisanzeige

Alle Fehler und Aktionen von Windows und SQL Server werden in den Ereignisanzeigen festgehalten und stehen Administratoren zur Verfügung, um Fehler zu beheben. Anhand des Ereignisprotokolls können Sie nach Ereignissen suchen, die auf Probleme hinweisen. Darüber hinaus dienen diese Informationen zur Diagnose von Problemen. Sie können nach Programm- und Systemaktionen suchen, die zu einem Problem führen, und Details herausfinden, die Ihnen bei der Ermittlung der Grundursache behilflich sind. Zugleich lassen sich anhand dieser Informationen auch Leistungspro-

bleme beurteilen und beheben. Sie sollten in regelmäßigen Abständen auf Datenbankservern nach Einträgen suchen, da Sie hier frühzeitig Fehler erkennen können.

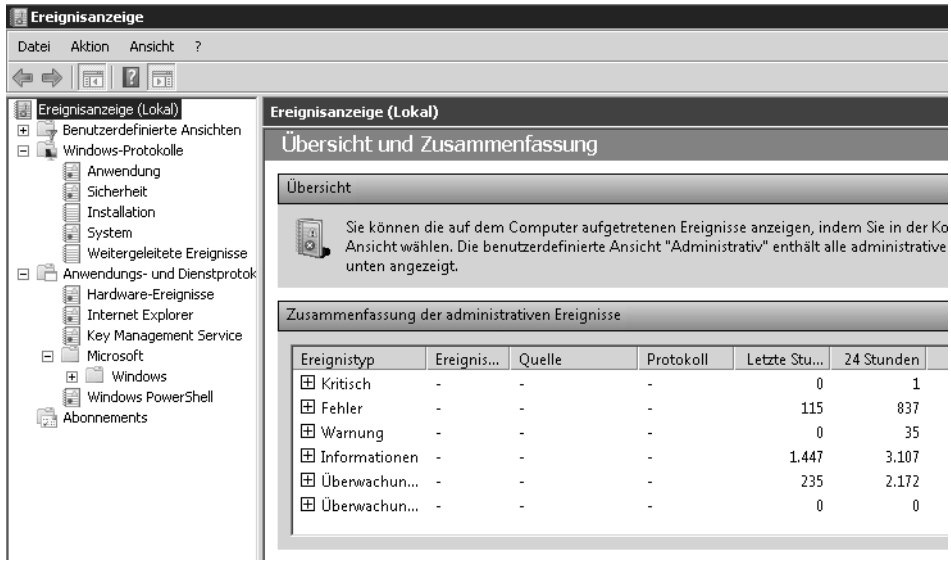
Ereignisanzeige nutzen

Sie starten die Ereignisanzeige durch Eingabe von *eventvwr.msc* im Suchfeld des Startmenüs oder über die Programmgruppe *Verwaltung*.

HINWEIS Unter Windows Server 2012 können Sie auf der Metro-Oberfläche direkt mit dem Tippen von »eventvwr.msc« beginnen oder über ⊞ + R das Dialogfeld *Ausführen* aufrufen und dort den Programmnamen eingeben.

Die Ereignisanzeige sehen Sie auch unterhalb des Knotens *Diagnose* im Server-Manager. In Windows Server 2012 finden Sie die Ereignisanzeige im Menüpunkt *Tools*. Unter dem Knoten *Windows-Protokolle* ist auch weiterhin der Zugriff auf die vertrauten Anwendungs-, System- und Sicherheitsprotokolle möglich.

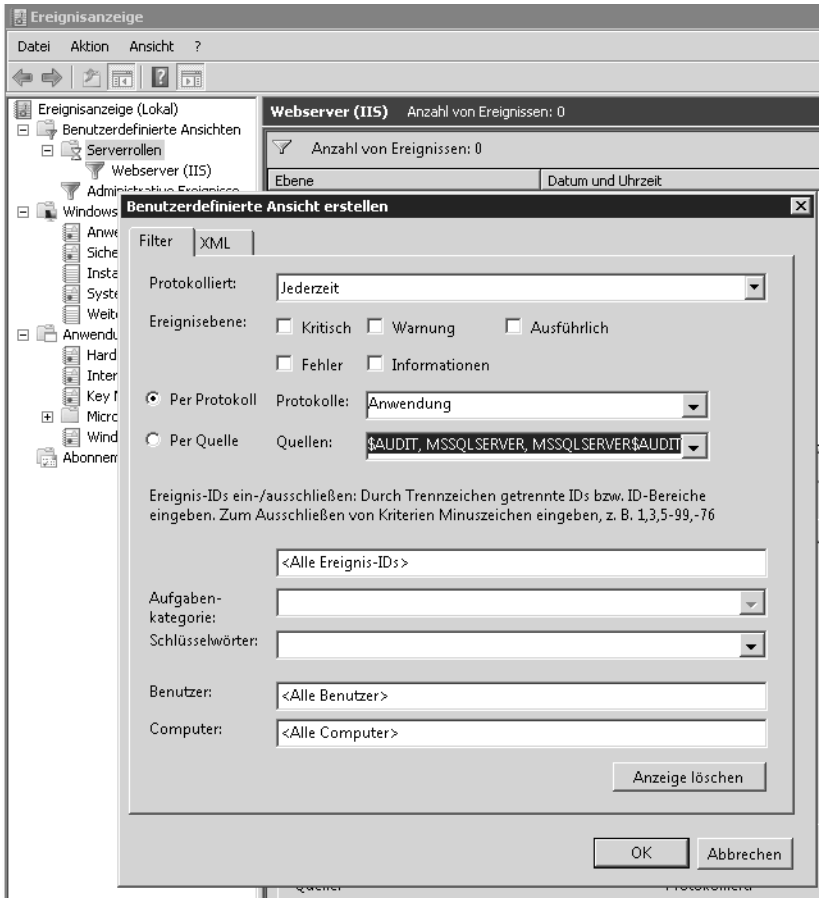
Abbildg. 6.33 Anzeigen der Ereignisprotokolle in Windows Server 2008 R2



Klicken Sie direkt auf den Knoten *Ereignisanzeige*, sehen Sie eine Zusammenfassung aller Serverfehler im rechten Bereich. Im Knoten *Anwendungs- und Dienstprotokolle* finden Sie zahlreiche Protokolle zu den einzelnen Serverdiensten in Windows Server 2008 R2 und Windows Server 2012, allerdings keine Einträge für SQL Server 2012. Diese sind im Knoten *Anwendungen* zu finden.

Über den Knoten *Benutzerdefinierte Ansichten* lassen Sie sich Filter für alle installierten Serverrollen anzeigen. Auf diese Weise können Sie auch Filter für die SQL-Instanzen erstellen lassen.

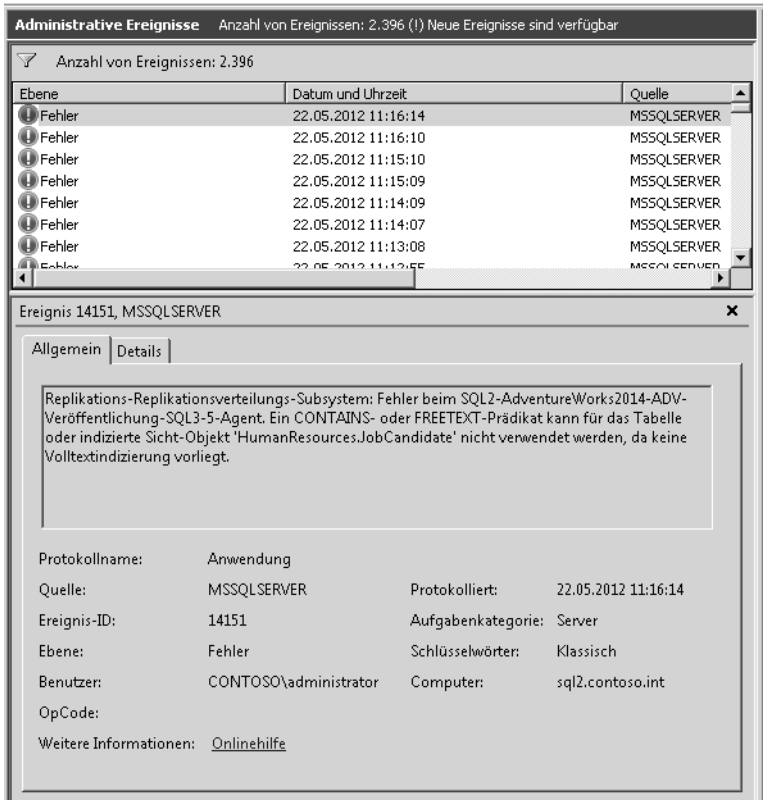
Abbildg. 6.34 Anzeigen von Meldungen gefiltert nach Serverrollen



HINWEIS Der Speicherort der Standardprotokolle in der Ereignisanzeige ist *%SystemRoot%\System32\winevt\Logs*. Die Protokolldateien erhalten die Endung *.evtx*, da diese XML-basiert sind.

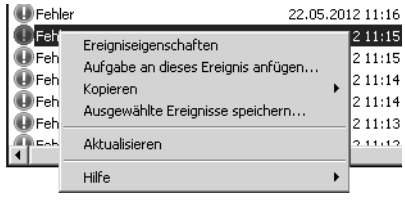
Unter dem Knoten *Benutzerdefinierte Ansichten* werden administrative Ereignisse angezeigt. Hier finden sich alle Fehler und Warnungen aus den verschiedenen Protokolldateien, die für Administratoren von Interesse sind. Windows Server 2008 R2 bzw. Windows Server 2012 bietet die Möglichkeit, weniger interessante Ereignisse herauszufiltern, sodass Sie sich auf jene Ereignisse konzentrieren können, die wichtig sind. Klicken Sie eine Meldung an, erhalten Sie im unteren Bereich ausführlichere Informationen.

Abbildg. 6.35 Anzeigen von Informationen zu einer Ereignismeldung



Mit dem Windows-Aufgabenplaner können Sie einem Ereignis eine Aufgabe hinzufügen. Jedes Mal, wenn ein Ereignis erscheint, das der Abfrage entspricht, startet anschließend die entsprechende Aufgabe. Dazu klicken Sie mit der rechten Maustaste auf das Ereignis und wählen *Aufgabe an dieses Ereignis anfügen*. In diesem Fall startet Windows die Aufgabe immer genau dann, wenn die Datensicherung erfolgreich abgeschlossen ist.

Abbildg. 6.36 Aufgaben anhängen



Wenn Sie ein Ereignisprotokoll aufrufen, erhalten Sie im mittleren Bereich des Fensters eine Zusammenfassung aller Einträge, deren detaillierte Informationen Sie per Doppelklick auf einzelne Meldungen anzeigen lassen können. Auf Basis dieser Fehlermeldung können Sie erkennen, welche Probleme Windows Server 2008 R2 oder Windows Server 2012 mit einzelnen Komponenten erkannt

hat. Sie sollten durchaus regelmäßig die Ereignisanzeigen auf Fehler überprüfen, da Sie hier schnell Probleme erkennen können, bevor diese gravierendere Auswirkungen haben.

TIPP Haben Sie den Fehler genauer eingegrenzt und Fehlermeldungen in der Ereignisanzeige und der Diagnose festgestellt, suchen Sie auf der Internetseite *http://www.eventid.net* [Ms151-K06-07] gezielt nach diesen Fehlern. Auf dieser Seite gibt es zu so gut wie jedem Eintrag der Ereignisanzeige Hinweise und mögliche Lösungsansätze.

Außerdem können Sie den Fehler in einer Suchmaschine oder in speziellen Supportseiten eingeben, wie zum Beispiel *http://www.experts-exchange.com* [Ms151-K06-08]. Auch die Suche in der Microsoft Knowledge Base unter *http://support.microsoft.com* [Ms151-K06-09] hilft oft weiter. Suchen Sie allerdings in der englischen Knowledge Base immer nur nach englischen Begriffen, da Sie hier mehr Antworten erhalten.

Klicken Sie ein Protokoll mit der rechten Maustaste an, können Sie weitere Einstellungen vornehmen. Im Kontextmenü werden Ihnen zahlreiche Möglichkeiten angezeigt:

- **Gespeicherte Protokolldatei öffnen** Über diesen Menübefehl können Sie eine Protokolldatei öffnen, die Sie über die Option *Ereignisse speichern unter* abgespeichert haben. Dadurch lassen sich Protokolle per E-Mail versenden und andere Benutzer können den Inhalt überprüfen.
- **Benutzerdefinierte Ansicht erstellen** Über diesen Menübefehl können Sie die Anzeige der Ereignisanzeigen anpassen und als benutzerdefinierten Filter ablegen. In diesem Fall werden Ihnen nur noch die Ereignisse in Ihrer gespeicherten Ansicht angezeigt.
- **Benutzerdefinierte Ansicht importieren** Mit dieser Optionen werden zuvor exportierte Ansichten auf einem Server wieder importiert und sind auf diese Weise schnell verfügbar.
- **Protokoll löschen** Wählen Sie diesen Menübefehl aus, wird nicht das Protokoll gelöscht, sondern der Inhalt des Protokolls. Sie erhalten zuvor noch eine Meldung, ob das Protokoll wirklich gelöscht werden soll und ob Sie das Protokoll vorher speichern möchten. Speichern Sie das Protokoll zuvor, entspricht dies der Option *Ereignisse speichern unter*.
- **Aktuelles Protokoll filtern** Dieser Menübefehl wird verwendet, wenn Sie keine eigene Ansicht des Protokolls erstellen möchten, sondern nur die aktuelle Ansicht gefiltert werden soll. Dadurch können Sie zum Beispiel nach einem bestimmten Fehler suchen und überprüfen, wann dieser aufgetreten ist.
- **Eigenschaften** Über die Eigenschaften können Sie die Größe der einzelnen Protokolle festlegen bzw. bestimmen, wie sich Windows Server 2008 R2 oder Windows Server 2012 beim Erreichen der maximalen Ereignisprotokollgröße verhalten soll.
- **Aufgabe an dieses Protokoll anfügen** Mit dieser Option können Sie über die Aufgabenplanung automatisch bestimmte Aktionen und Skripts starten, wenn in den Ereignisanzeigen bestimmte Fehler auftauchen. Solche Aufgaben lassen sich auch an einzelne Ereignisse anfügen.

TIPP Überprüfen Sie in der Ereignisanzeige, ob Fehler gemeldet werden, die mit dem Problem in Zusammenhang stehen können, wenn Sie eine Fehlerbehebung durchführen. Überprüfen Sie auch, ob parallel zu diesem Fehler in anderen Protokollen der Ereignisanzeige Fehler auftreten, die zur gleichen Zeit gemeldet werden, also unter Umständen auf einen Zusammenhang schließen lassen. Stellen Sie fest, wann der Fehler in der Ereignisanzeige das erste Mal aufgetreten ist. Überlegen Sie genau, ob zu diesem Zeitpunkt irgend etwas verändert wurde (auch auf Basis der Ereignisprotokolle).

Schauen Sie auch in anderen Protokollen der Ereignisanzeige nach, ob der Fehler mit anderen Ursachen zusammenhängt. Ein Fehler tritt selten ohne vorherige Änderung der Einstellung oder aufgrund defekter Hardware auf, sondern meist durch Änderungen am System oder der Installation von Applikationen und Tools. Durch die Filtermöglichkeiten der Ereignisanzeige in Windows Server 2008 R2 und Windows Server 2012 können Fehler oft sehr genau eingegrenzt werden.

Ereignisprotokolle im Netzwerk einsammeln

Nicht jedes Unternehmen setzt auf professionelle und teure Überwachungslösungen, um Server im Netzwerk zu überwachen. Selbst beim Einsatz solcher Lösungen kann es sinnvoll sein, zusätzlich noch Protokolldateien und Ereignisanzeigen zu überwachen. Es gibt zahlreiche kostenlose Möglichkeiten, um die Ereignisanzeigen und Protokolle der Server an einer zentralen Stelle zu sammeln und zu analysieren. Zunächst bieten Windows Server 2008 R2 und Windows Server 2012 die Möglichkeit, Ereignisse von Servern im Netzwerk zu sammeln, Abonnement genannt. Darüber hinaus gibt es Freewaretools, die ebenfalls in der Lage sind, Ereignisse in den Protokollen von Windows-Servern zu sammeln und Administratoren zentral zur Verfügung zu stellen. Nachfolgend zeigen wir Ihnen, welche Möglichkeiten es gibt. Achten Sie aber darauf, dass derartige Tools teilweise auch den Server belasten und vorsichtig eingesetzt werden sollten

Echtzeitüberwachung der Ereignisprotokolle – EventSentry

EventSentry (*http://www.eventsentry.com* [Ms151-K06-10]) ist eine Monitoring-Software zur Erfassung, Analyse und Anzeige von Systemereignissen. Es besteht auch die Möglichkeit, Informationen per E-Mail zu versenden, wenn bestimmte Ereignismeldungen in den Protokollen der Server auftauchen. In der E-Mail ist die auslösende Ereignismeldung mit allen Daten enthalten. Die Lizenz der Anwendung für einen Host kostet 85 Dollar. Es gibt auch eine komplett kostenlose, aber etwas eingeschränkte Light-Variante von EventSentry. Diese kann ebenfalls Ereignisanzeigen überwachen und E-Mails versenden, aber nicht so umfassend laufende Dienste oder Protokolldateien auf Servern überwachen. Die genauen Unterschiede finden Sie auf der Seite des Herstellers (*http://www.eventsentry.com/downloads/full-vs-light* [Ms151-K06-11]). In vielen Fällen reichen die Funktionen der kostenlosen Light-Edition aber aus.

Der Hauptvorteil von EventSentry liegt darin, dass Sie die Ereignisanzeigen aller Ihrer Server in Echtzeit überwachen können. Abhängig von Fehlermeldungen, die in den verschiedenen Ereignisanzeigen auftreten, können Sie Aktionen durchführen lassen, zum Beispiel E-Mails an Administratoren verschicken, die den Inhalt der Ereignismeldung enthalten. Mit diesem Tool können Sie Fehler und drohende Ausfälle in Ihrem Netzwerk sehr früh erkennen. Sie können sich eine 30-Tage-Testversion oder die kostenlose Light-Version von der Seite *http://www.eventsentry.com* [Ms151-K06-10] herunterladen.

Zur Überwachung installieren Sie auf den zu überwachenden Servern das Tool mit den entsprechenden Agenten zur Überwachung. Auf einem Computer im Netzwerk installieren Sie die Verwaltungsoberfläche, auf jedem Server, den Sie überwachen möchten, den entsprechenden Agenten. Die Auswahl zur Installation nehmen Sie im Setup-Assistenten vor. Nach dem Start erscheint ein Agent, der Sie bei der Einrichtung der Anwendung unterstützt.

Im Rahmen der Einrichtung legen Sie fest, auf welche Arten von Ereignissen in den Ereignisanzeigen das Tool achten soll. In der Verwaltungsoberfläche können Sie direkt die Ereignisanzeigen *Application*, *Security* und *System* auf den angebundenen Server öffnen. Im Bereich *Packages/Event*

Log Packages/Default legen Sie fest, welche Ereignisse das Tool auf den Servern überwachen soll, auf denen der Agent installiert ist. Auf diesem Weg können Sie auch gezielt nach einzelnen IDs oder nach Ereignisquellen filtern lassen. Im Bereich *Actions* legen Sie fest, welche Aufgaben das Tool durchführen soll, wenn Ereignisse auftreten, die den konfigurierten Filtern entsprechen.

Die einzelnen Aktionen wiederum, zum Beispiel die Konfiguration der Warn-E-Mails, nehmen Sie im Bereich *Actions* im linken Abschnitt der Verwaltungsoberfläche vor. Nach der Einrichtung sollten Sie eine Test-E-Mail versenden lassen, um sicherzustellen, dass der E-Mail-Fluss funktioniert. Nach der Installation blendet EventSentry auch ein Informationsfenster ein, sobald ein Fehler auf dem Server auftaucht.

Ereignisanzeigen sammeln – PsLogList

Mit PsLogList aus der PsTools-Sammlung von Sysinternals (*http://technet.microsoft.com/de-de/sysinternals* [Ms151-K06-12]) können Sie über die Befehlszeile die Ereignisanzeigen verschiedener Computer einsammeln, anzeigen und vergleichen. Wenn Sie das Tool ohne Optionen aufrufen, zeigt PsLogList alle Einträge des lokalen Systemereignisprotokolls an. Das Programm verfügt darüber hinaus über zahlreiche Optionen, welche beim Abfragen der Ereignisanzeigen viele verschiedene Vergleichsmöglichkeiten bieten:

```
psloglist [\\<Computer>[,<Computer>[,...] | @<Datei> [–u <Benutzername>[–p <Kennwort>]]]
[–s [–t delimiter]] [–m #|–n #|–h #|–d #|–w][–c][–x][–r][–a mm/dd/yy][–b mm/dd/yy][–f
filter] [–i ID[,ID[,...] | –e ID[,ID[,...]]] [–o event source[,event source][,..]]] [–q
event source[,event source][,..]]] [–l event log file] <eventlog>
```

Tabelle 6.1 Optionen von PsLogList

Option	Auswirkung
@<Datei>	Führt den Befehl auf allen Computern aus, die in der Datei aufgelistet sind. Jeder Computer muss dazu in einer eigenen Spalte in der Textdatei stehen. Die entsprechenden Ereignisse der Computer werden hierüber also gesammelt.
–a	Zeigt die Einträge nach dem genannten Datum an. Als Format wird *dd/mm/yy* verwendet.
–b	Zeigt die Einträge vor dem genannten Datum an
–c	Löscht die entsprechenden Ereignisanzeigen nach der Anzeige über PsLoglist. Dies ist zum Beispiel bei der Abfrage über eine Batchdatei sinnvoll.
–d	Zeigt nur die Einträge der letzten n Tage an. Dabei werden die letzten Tage als *<n>* hinter der Option mit angegeben.
–e	Filtert Einträge mit definierten IDs aus. Die Syntax entspricht der Option *–i* weiter unten.
–f	Filtert Ereignisse mit bestimmten Typen aus (*–f w* filtert Warnungen). Es können beliebige Buchstaben verwendet werden. Es werden nur Ereignisse angezeigt, die mit den entsprechenden Buchstaben anfangen.
–h	Zeigt nur Einträge der letzten n Stunden. Die Syntax entspricht der Option *–d* weiter oben.
–i	Zeigt nur Einträge mit den definierten IDs. Es können auch mehrere IDs kommagetrennt angezeigt werden.
–l	Speichert Einträge der definierten Ereignisanzeige
–m	Zeigt nur Einträge der letzten n Minuten

Tabelle 6.1 Optionen von PsLogList *(Fortsetzung)*

Option	Auswirkung
–n	Zeigt nur die aktuellsten definierten Einträge an
–o	Zeigt nur die Einträge der spezifizierten Ereignisquelle (zum Beispiel \–*o cdrom*\). Diese Option schließt in der Ausgabe also zusätzliche Informationen ein.
–p	Gibt das Kennwort für den konfigurierten Benutzer an. Geben Sie kein Kennwort ein, fragt das Tool notfalls nach. Dabei wird das Kennwort nicht in Klartext angezeigt oder über das Netzwerk geschickt.
–q	Zeigt die Einträge der spezifizierten Ereignisquelle nicht an (zum Beispiel \–*q cdrom*\). Benutzerdefinierte Einträge werden so von der Ausgabe ausgeschlossen. Sollen mehrere Quellen von der Ausgabe ausgeschlossen werden, müssen diese durch Komma voneinander getrennt werden.
–r	Speichert die Einträge aufsteigend ab
–s	Hier werden die Einträge kommabasiert angezeigt, um diese zum Beispiel in einer Excel-Tabelle oder SQL-Datenbank zu speichern. Nach der Auswertung kann zum Beispiel über den Befehl start die *.csv*-Datei sofort geöffnet und angezeigt werden.
–t	Definiert das Trennzeichen
–u	Legt den Benutzernamen fest, mit dem Sie auf die Server zugreifen
–w	Wartet auf neue Einträge und speichert sie, sobald diese in der Ereignisanzeige angezeigt werden. Das funktioniert aber nur für das lokale System.
–x	Speichert erweiterte Daten, die standardmäßig nicht angezeigt werden. Hierbei handelt es sich meistens um binäre Rohdaten.

Standardmäßig verwendet das Tool das Systemereignisprotokoll. Sie können die Ereignisanzeige auswählen, wenn Sie die ersten Buchstaben oder die entsprechende Abkürzung angeben. Allerdings müssen auch auf deutschen Windows-Servern die englischen Abkürzungen, also beispielsweise »sec« für »security«, eingegeben werden, wenn das Ereignisprotokoll »Sicherheit« geöffnet werden soll. Eine wichtige Funktion des Tools ist, dass es in der Lage ist, direkt auf die Quell-DLLs auf den Remotesystemen zuzugreifen. Allerdings muss dazu auf dem entfernten System die administrative Freigabe (Admin$) aktiviert sein.

Geben Sie zum Beispiel den Befehl *psloglist system* ein, listet das Tool in der Befehlszeile alle Ereignisse des Systemereignisprotokolls auf. Der Befehl *psloglist application* zeigt das Anwendungsprotokoll an. Wollen Sie nur die aktuellsten fünf Einträge sehen, verwenden Sie den Befehl *psloglist system –n 5*. Die fünf ältesten Einträge zeigen Sie mit *psloglist system –r –n 5* an.

Um effizient Daten anzuzeigen, sollten Sie die Anzeige filtern, da ansonsten zu viele Informationen auf dem Bildschirm erscheinen. Dazu verwenden Sie die Option *–f*. Wollen Sie zum Beispiel nur Fehlermeldungen erfassen, geben Sie den Befehl *psloglist system –f e* ein. Fehler und Warnungen erhalten Sie mit der Option *–f ew* angezeigt. Um nur Meldungen einer bestimmten ID anzuzeigen, verwenden Sie *–i*, gefolgt von einer kommagetrennten Liste der IDs, die Sie anzeigen wollen.

Eine weitere Möglichkeit ist das Exportieren der Ausgabe in eine *.evt*-Datei, die Sie wiederum mit der Ereignisanzeige in Windows öffnen können. Dazu verwenden Sie zusätzlich die Option *–g .\<.evt-Datei>*.

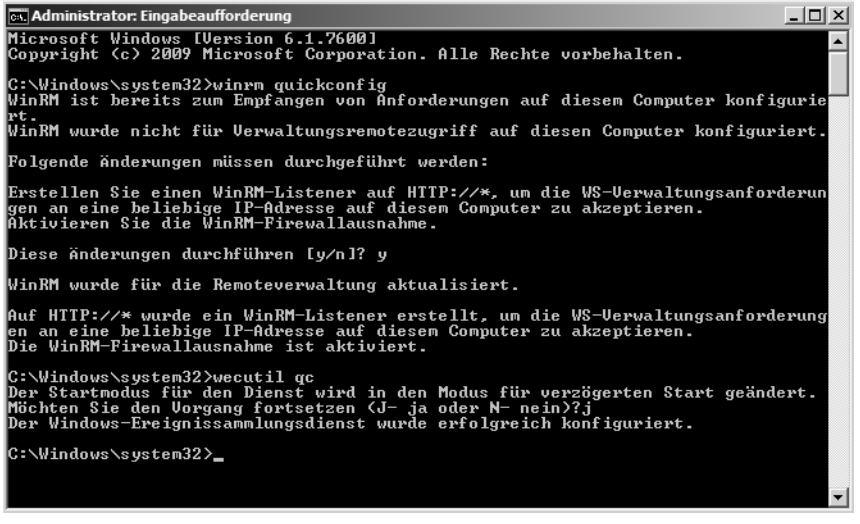
Mit PsLogList können Sie auch die Ereignisanzeigen von Computern im Netzwerk auslesen. Dazu verwenden Sie zunächst die Option *psloglist \\<Computer>* und dann die verschiedenen Optionen des Tools, um die Anzeige zu aktivieren. Dabei gehen Sie genauso vor wie bei der Abfrage lokaler Ereignisanzeigen.

Ereignis-Abonnements verwalten

Windows Server 2008 R2 und Windows Server 2012 können auch mit Bordmitteln die Ereignisanzeigen verschiedener Server im Netzwerk zusammentragen und anzeigen. Diese Funktion trägt die Bezeichnung *Abonnements* und lässt sich direkt in der Ereignisanzeige einrichten. Basis ist der Systemdienst *Windows-Ereignissammeldienst*. Dieser muss auf dem Server gestartet sein, der die verschiedenen Ereignisse sammeln soll, sowie auf allen beteiligten Servern. Damit die Sammlung von Ereignisanzeigen funktioniert, müssen Sie die beteiligten Computer vorbereiten, das Abonnement erstellen und dann in der Ereignisanzeige die Fehler der entsprechenden Server anzeigen.

Die Sammlung von Ereignisanzeigen basiert auf zwei Grundlagen. Es gibt einen Server, der die Daten sammelt (Sammlungscomputer) und Server, die an den Sammlungsserver angebunden sind (Quellcomputer). Die Sammlung von Ereignisanzeigen führen Sie am besten auf Servern durch, die in einer gemeinsamen Active Directory-Gesamtstruktur positioniert sind.

Abbildg. 6.37 Konfigurieren der Remoteverwaltung und des Windows-Ereignissammeldienstes in Windows Server 2008 R2



Im ersten Schritt müssen Sie die Remoteverwaltung auf den einzelnen Servern aktivieren. Dazu führen Sie auf jedem Quellcomputer und dem Sammlungscomputer in einer Befehlszeile mit Administratorrechten (über das Kontextmenü gestartet) den Befehl *winrm quickconfig* aus. Im nächsten Schritt führen Sie noch den Befehl *wecutil qc* aus. Das Tool konfiguriert das Weiterleiten von Ereignissen über das Netzwerk zu einem Sammlungscomputer. Nehmen Sie anschließend das Computer-

konto des Sammlungscomputers, auf dem Sie die Ereignisse aller angebundenen Server anzeigen wollen, in die lokalen Administratorgruppen der einzelnen Server auf.

Die lokale Benutzerverwaltung starten Sie am schnellsten durch die Eingabe von *lusrmgr.msc* im Suchfeld des Startmenüs. Rufen Sie die Eigenschaften der lokalen Administratorgruppe auf, klicken Sie auf die Schaltfläche *Hinzufügen* und im daraufhin geöffneten Dialogfeld auf die Schaltfläche *Objekttypen*, um auch Computerkonten in die Gruppe aufnehmen zu können.

Wollen Sie Ereignisabonnements in Arbeitsgruppen erstellen, müssen Sie manuell eine Ausnahme in der Windows-Firewall für *Remote-Ereignisprotokollverwaltung* auf jedem Quellcomputer hinzufügen. Das Konto, mit dem Sie die Ereignisse auf den Quellcomputern sammeln, müssen Sie anschließend bei der Einrichtung des Abonnements hinterlegen. Zusätzlich ist auf dem Sammlungscomputer der folgende Befehl einzugeben:

```
winrm set winrm/config/client @{TrustedHosts="<Alle Quellcomputer, durch Komma getrennt>"}
```

Die Sammlung nehmen Sie am besten mit einem Konto vor, das über Administratorrechte in der Domäne verfügt. Wollen Sie ein eigenes Konto dafür anlegen, müssen Sie dieses in die lokale Administratorgruppe auf allen Quellcomputern aufnehmen. Normalerweise reicht es aus, wenn nur das Computerkonto des Sammlungscomputers Mitglied der Administratorgruppe auf den Quellcomputern ist.

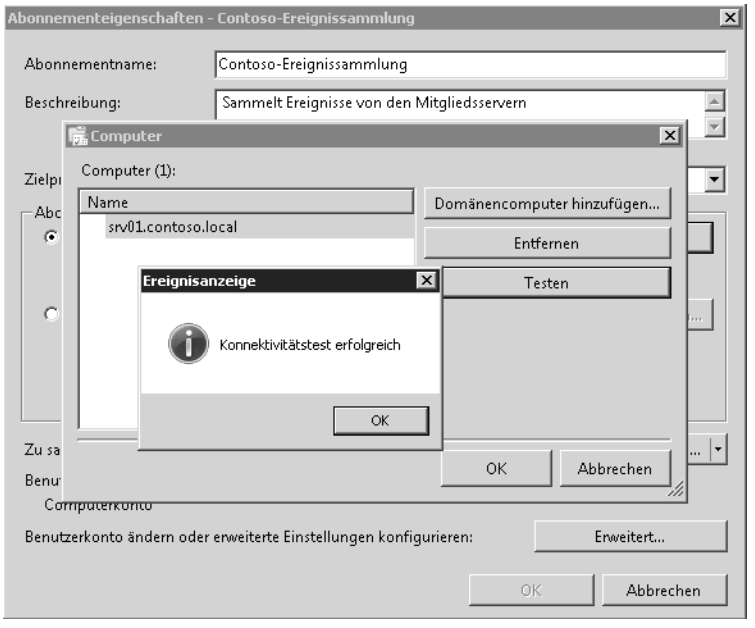
Haben Sie alle Vorbereitungen getroffen, starten Sie auf dem Sammlungscomputer die Ereignisanzeige und klicken auf *Abonnements*. Ist der Systemdienst *Windows-Ereignissammlungsdienst* nicht gestartet, erhalten Sie eine entsprechende Meldung. Lassen Sie in diesem Fall den Dienst starten. Anschließend klicken Sie mit der rechten Maustaste auf *Abonnements* und dann auf *Abonnement erstellen*. Alternativ können Sie auch im Menü *Aktionen* auf *Abonnement erstellen* klicken.

Im neuen Fenster konfigurieren Sie jetzt das Abonnement. Bei *Abonnementname* geben Sie eine Bezeichnung und auf Wunsch auch eine Beschreibung ein. Bei *Zielprotokoll* wählen Sie aus, wo auf dem Sammlungsserver die Ereignisse der Quellcomputer gesammelt werden sollen. Standardmäßig ist hier das Protokoll *Weitergeleitete Ereignisse* auswählt.

Anschließend wählen Sie die Art des Abonnements aus. Aktivieren Sie die Option *Sammlungsinitiiert* und klicken Sie auf die Schaltfläche *Computer auswählen*. Anschließend wählen Sie die Quellcomputer aus, die das Abonnement erfassen soll. Sie sollten für jeden Computer, den Sie hinzufügen, auf die Schaltfläche *Testen* klicken, um sicherzustellen, dass der Sammlungscomputer eine Verbindung aufbauen kann.

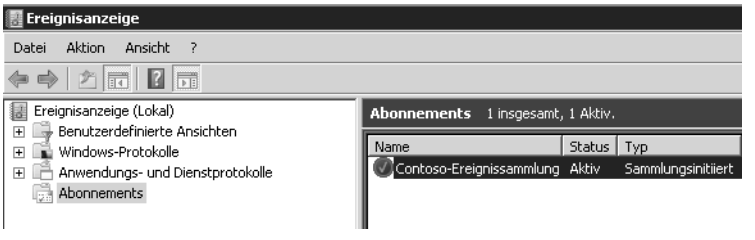
Über die Schaltfläche *Ereignisse auswählen* erstellen Sie neue Filter, über die Sie festlegen, welche Ereignisse auf den Quellcomputern der Sammlungscomputer angezeigt werden sollen. Grundsätzlich legen Sie fest, welche Ereignisse von welchen Protokollen erfasst werden sollen. Haben Sie den Filter erstellt, klicken Sie auf *OK*. Bevor Sie weitere Einstellungen vornehmen, klicken Sie auf *OK*, um das Abonnement zu überprüfen.

Abbildg. 6.38 Konfigurieren eines neuen Abonnements



Nach der Erstellung muss das Abonnement als *Aktiv* gekennzeichnet sein. Auf diesem Weg können Sie auch mehrere Abonnements erstellen, die verschiedene Computer mit verschiedenen Abfragefiltern erfassen. Mit einem Doppelklick auf das Abonnement können Sie dieses jederzeit wieder anpassen.

Abbildg. 6.39 Erfolgreich erstelltes Abonnement

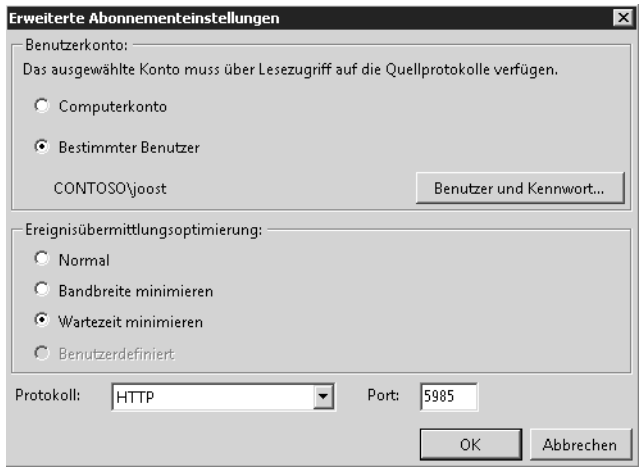


Anschließend können Sie die Ereignisse im ausgewählten Protokoll anzeigen. Haben Sie das Standardprotokoll *Weitergeleitete Ereignisse* ausgewählt, finden Sie dieses im Bereich *Windows-Protokolle*. Bis die ersten Ereignisse eintreffen, kann es allerdings eine Weile dauern. Von welchem Server die Ereignisse stammen, sehen Sie in der Spalte *Computer*.

Neben den Standardeinstellungen für Abonnements können Sie über die Schaltfläche *Erweitert* in den Eigenschaften des Abonnements einige Einstellungen ändern. Sie können an dieser Stelle zum Beispiel festlegen, dass die Abfrage der Ereignisse nicht durch das Computerkonto des Servers erfolgt, sondern mit einem speziellen Benutzerkonto, dessen Daten Sie in den erweiterten Einstellungen des Abonnements hinterlegen. Achten Sie aber darauf, dieses Konto in die lokale Administratorengruppe der Quellcomputer aufzunehmen.

Außerdem können Sie in den erweiterten Einstellungen noch festlegen, wie der Sammlungscomputer die Daten abrufen soll. Hier stehen die drei Optionen *Normal*, *Bandbreite minimieren* und *Wartezeit minimieren* zur Verfügung.

Abbildg. 6.40 Konfigurieren von Abonnements



Bei der Standardeinstellung *Normal* verwendet das Abonnement den Pullzustellungsmodus. Dabei fasst das Abo immer fünf Elemente zusammen und überträgt diese vom entsprechenden Quellcomputer auf den Sammlungsserver. Die Option *Bandbreite minimieren* begrenzt die Bandbreite, die dem Abo zur Verfügung steht. Mit der Option *Wartezeit minimieren* wird sichergestellt, dass Ereignisse möglichst schnell auf dem Sammlungsserver zur Verfügung stehen.

In den erweiterten Einstellungen legen Sie auch den Port und die Übertragungsart fest. Wenn Sie diese ändern, müssen Sie in den Firewalleinstellungen der Quellcomputer ebenfalls entsprechende Regeln definieren. In Active Directory-Umgebungen können Sie dazu auch Gruppenrichtlinien verwenden, um Regeln auf den Servern zu erstellen.

Neben den Abonnements können Sie auch mit der Standardereignisanzeige problemlos Ereignisanzeigen von Computern im Netzwerk abrufen. Sie können dazu die Ereignisanzeige selbst verwenden oder das Befehlszeilentool *wevtutil* an einer Eingabeaufforderung eingeben, um Ereignisprotokolle auf einem Remotecomputer zu verwalten. Starten Sie dazu die Ereignisanzeige und klicken Sie mit der rechten Maustaste auf *Ereignisanzeige (Lokal)*. Anschließend können Sie durch Auswahl von *Verbindung mit anderem Computer herstellen* die Ereignisanzeige beliebiger Server öffnen. Wollen Sie auf diesem Weg eine Verbindung mit mehreren Servern aufbauen, müssen Sie eine neue Management Console erstellen und das Snap-In der Ereignisanzeige mehrmals integrieren.

Wollen Sie eine Verbindung mit einem anderen Benutzerkonto aufbauen, aktivieren Sie noch die Option *Verbindung unter anderem Benutzerkonto herstellen* und wählen das entsprechende Konto aus. Sie können den Benutzernamen und das Kennwort für die Verbindung festlegen.

Sie können die Ereignisanzeige eines Servers auch direkt durch Eingabe des Befehls *eventvwr<Computername>* öffnen.

Ereignisanzeige in der Systemsteuerung steuern – Wevtutil

Sie können auch in der Befehlszeile eine Verbindung zur Ereignisanzeige eines anderen Servers aufbauen. Dazu verwenden Sie den folgenden Befehl:

```
wevtutil <Option> /r:<Computername> /u:<Benutzername> /p:<Kennwort>
```

Verwenden Sie die Optionen */u* und */p* nicht, verbindet Sie *wevtutil* mit dem Benutzer, mit dem Sie angemeldet sind.

Welche Optionen zur Verfügung stehen, sehen Sie, wenn Sie *wevtutil* eingeben. Das Tool dient nicht dazu, die Ereignisanzeige über das Netzwerk zu öffnen, sondern Einstellungen vorzunehmen oder das Protokoll zu löschen. Mit Aufruf von *wevtutil el /r:sbs.contoso.local* lassen Sie sich zum Beispiel alle verfügbaren Protokolle auf dem Remotecomputer anzeigen. Sie können mit *wevtutil* auch Ereignisanzeigen ohne Rücksprache löschen lassen. Dazu verwenden Sie den Befehl *wevtutil cl <Name des Protokolls>*. Der Befehl *wevtutil cl System /r:sql* löscht zum Beispiel das Systemprotokoll auf dem Server *sql* ohne weitere Rücksprache. Natürlich können Sie mit dem Tool auch Protokolle über das Netzwerk auf den lokalen Computer in *.evtx*-Dateien exportieren. Dazu verwenden Sie den Befehl *wevtutil epl*.

Performance Analysis of Logs (PAL) Tool

Auf der Seite *http://pal.codeplex.com* [Ms151-K06-13] erhalten Sie das Freewaretool Performance Analysis of Logs (PAL), welches bei der Auswertung von Leistungsberichten eine gute Hilfe sein kann. Das Tool ist allerdings kein Gelegenheitstool, sondern nur geeignet, wenn Sie einen englischen Server betreiben und eine ausführliche Analyse von Logdateien durchführen wollen, die über die normalen Möglichkeiten hinausgehen. Grundsätzlich sollten Sie das Tool nur auf Testservern installieren und nicht auf produktiven Servern. Auf der genannten Seite erhalten Sie das Tool und finden auch weiterführende Hilfe und Dokumentationen zum Thema Leistungsüberwachung von Servern. Sie benötigen für das Tool zusätzlich noch die folgenden ebenfalls frei erhältlichen Zusatzprogramme:

- **Log Parser 2.2** *http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&DisplayLang=en* [Ms151-K06-14]
- **Microsoft Chart Controls für Microsoft .NET Framework 3.5** *http://www.microsoft.com/download/en/details.aspx?DisplayLang=en&id=14422* [Ms151-K06-15]
- **Office 2003-Add-In: Office Web Components** *http://www.microsoft.com/downloads/details.aspx?FamilyID=7287252c-402e-4f72-97a5-e0fd290d4b76&DisplayLang=en* [Ms151-K06-16]

Fehler in Windows nachstellen und beheben – Problemaufzeichnung

Windows 7 und Windows Server 2008 R2, sowie Windows 8 und Windows Server 2012 bieten die Möglichkeit, Fehler in Windows aufzuzeichnen und für Spezialisten so aufzubereiten, dass diese den Fehler leicht nachstellen und überprüfen können. Diese Schritt-für-Schritt-Aufzeichnung von Fehlern hat die Bezeichnung Problemaufzeichnung. Am schnellsten starten Sie die Problemaufzeichnung, indem Sie *psr* im Suchfeld des Startmenüs eingeben. Es öffnet sich eine Symbolleiste, mit der Sie die Aufzeichnung durchführen.

Abbildg. 6.41 Probleme aufzeichnen in Windows 7 und Windows Server 2008 R2

Um einen Fehler aufzuzeichnen und weitergeben zu können, gehen Sie folgendermaßen vor:

1. Tippen Sie *psr* im Suchfeld des Startmenüs ein.

HINWEIS Unter Windows Server 2012 können Sie auf der Metro-Oberfläche direkt mit dem Tippen beginnen oder über ⊞ + R das Dialogfeld *Ausführen* aufrufen.

2. Klicken Sie nach dem Start des Tools auf *Aufzeichnung starten*.
3. Führen Sie exakt die Schritte in Windows oder dem jeweiligen Programm durch, die den Fehler verursacht haben.
4. Per Klick auf *Kommentar hinzufügen* können Sie eigene Hinweise einfügen, falls der Fehler nicht direkt offensichtlich ist.
5. Haben Sie den Fehler nachgestellt, klicken Sie auf *Aufzeichnung beenden*.
6. Speichern Sie die Datei als ZIP-Archiv ab.
7. Das Tool speichert die Aufzeichnung als *.mht*-Datei, die Sie mit dem Internet Explorer öffnen können. Extrahieren Sie die *.zip*-Datei per Klick mit der rechten Maustaste oder klicken Sie doppelt auf die *.zip*-Datei und dann auf die *.mht*-Datei. Sie sehen die Aufzeichnung des Problems als Dokument, das jeder nachvollziehen kann.

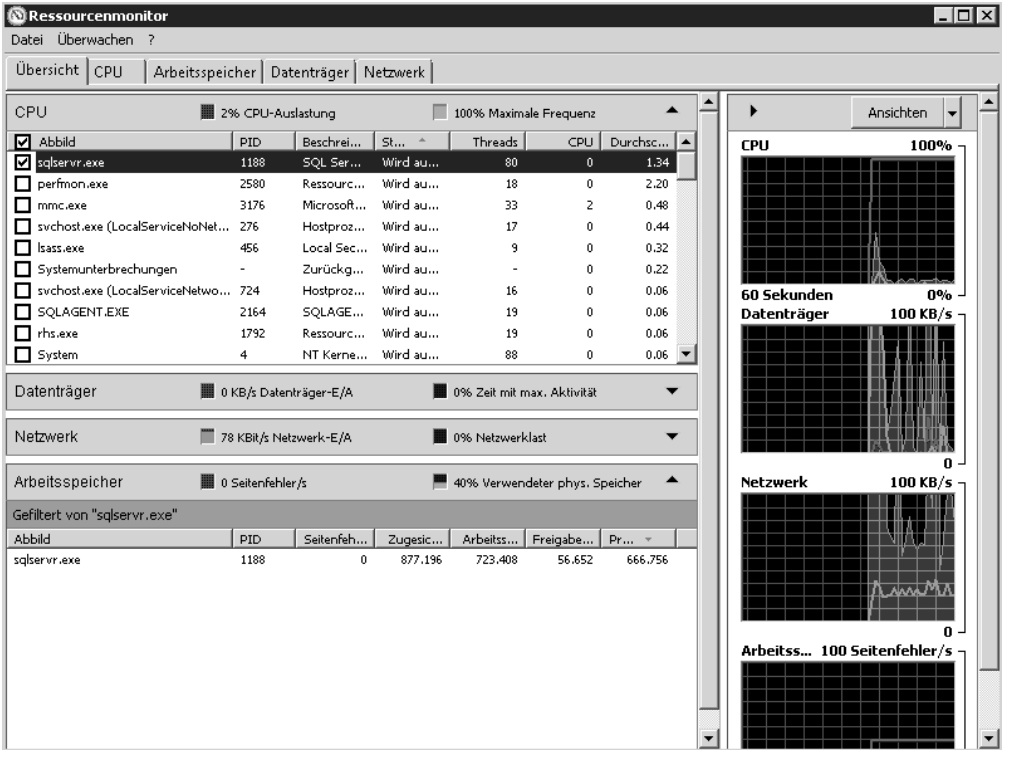
Überwachung der Systemleistung

Über den Eintrag *Leistung* in der Konsolenstruktur des Server-Managers können Sie sich die aktuelle Systemleistung Ihres Servers mit verschiedenen Tools und Ansichten anzeigen lassen. Über den Link *Ressourcenmonitor öffnen* lässt sich eine detaillierte Ansicht des aktuellen CPU-Verbrauchs, des Arbeitsspeichers, der Datenträger und des Netzwerkverkehrs anzeigen. In Windows Server 2012 finden Sie das Programm über den Menüpunkt *Tools* im Server-Manager.

Die Gesamtleistung eines Systems wird durch verschiedene Faktoren begrenzt. Hierzu zählen etwa die Zugriffsgeschwindigkeit der physischen Datenträger, die für alle laufenden Prozesse zur Verfügung stehende Speichermenge, die Prozessorgeschwindigkeit und der Datendurchsatz der Netzwerkschnittstellen. Mehr zu diesem Thema lesen Sie auch in Kapitel 1.

Nachdem die einschränkenden Faktoren auf der Hardwareseite identifiziert wurden, kann der Ressourcenverbrauch einzelner Anwendungen und Prozesse überprüft werden. Anhand einer umfassenden Leistungsanalyse, die sowohl die Auswirkungen von Anwendungen als auch die Gesamtkapazität berücksichtigt, können IT-Experten einen Bereitstellungsplan entwickeln und an die jeweiligen Anforderungen anpassen. Alternativ können Sie diese Funktion auch über *perfmon /res* starten. Durch Erweitern der *Ressourcenübersicht* können Sie zusätzliche Informationen anzeigen und überprüfen, welche Ressourcen von welchen Prozessen genutzt werden.

Abbildg. 6.42 Anzeige des Ressourcenmonitors in Windows Server 2008 R2



Der Bereich mit der Ressourcenübersicht enthält vier animierte Diagramme, die die Auslastung der CPU-, Datenträger-, Netzwerk- und Speicherressourcen des lokalen Computers in Echtzeit anzeigen. Unter den Diagrammen befinden sich vier erweiterbare Bereiche, in denen Einzelheiten zur jeweiligen Ressource angezeigt werden können. Klicken Sie zur Anzeige dieser Informationen auf den Abwärtspfeil rechts neben dem jeweiligen Balken.

Die Leistungsüberwachung

Klicken Sie in der Konsolenstruktur (die linke Fensterspalte) des Server-Managers auf den Eintrag *Leistung/Überwachungstools/Leistungsüberwachung*, können Sie den Server noch genauer überwachen lassen, indem Sie verschiedene Leistungsindikatoren hinzufügen. In Windows Server 2012 finden Sie das Programm im Menüpunkt *Tools*. In den verschiedenen Kapiteln dieses Buchs, zum Beispiel in Kapitel 7 gehen wir auf die Indikatoren und Objekte ein, die Sie mit der Leistungsüberwachung nachverfolgen können.

In der Leistungsüberwachung werden die integrierten Leistungsindikatoren grafisch dargestellt. Sie können Daten in Echtzeit oder Verlaufsdaten anzeigen und Leistungsindikatoren entweder per Drag & Drop hinzufügen oder benutzerdefinierte Datensammlergruppen (Data Collector Sets, DCS) erstellen. Die Leistungsüberwachung unterstützt verschiedene Ansichten für die visuelle Überprüfung der Daten in Leistungsprotokollen.

Abbildg. 6.43 Ändern der Ansicht in der Leistungsüberwachung

Vor allem die Auswahl *Bericht* bietet oft mehr Übersicht als die anderen Optionen in der Liste. Außerdem können Sie benutzerdefinierte Ansichten in Form von Datensammlergruppen für die Verwendung in Leistungs- und Protokollfunktionen exportieren. Über das grüne Pluszeichen in der Symbolleiste können Sie weitere Leistungsindikatoren einblenden lassen. Für SQL-Server gibt es einige solcher Indikatoren, die wir in den einzelnen Kapiteln genauer besprechen. Den Zustand von Verfügbarkeitsgruppen (siehe Kapitel 7) können Sie zum Beispiel nicht nur im SQL Server Management Studio überwachen, sondern auch mit der Leistungsüberwachung von Windows Server 2008 R2 und Windows Server 2012. Dazu stehen einige neue Leistungsindikatoren zur Verfügung, die bei der Überwachung hilfreich sind. Das Leistungsobjekt *SQLServer:Database Replica* verfügt über Leistungsindikatoren, die Informationen zu den sekundären Verfügbarkeitsdatenbanken messen. Das *SQLServer:Databases*-Objekt in SQL Server stellt Indikatoren zum Überwachen von Transaktionsprotokollaktivitäten zur Verfügung. Die folgenden Indikatoren sind besonders für die Überwachung der Transaktionsprotokollaktivität von Verfügbarkeitsdatenbanken interessant:

- *Schreibdauer für Protokollleerungen (ms)*
- *Protokollleerungen/Sekunde*
- *Protokollpool-Cachefehlversuche/Sekunde*
- *Protokollpool-Lesevorgänge auf dem Datenträger/Sekunde*
- *Protokollpoolanforderungen/Sekunde*

Sie können auch die Windows-Leistungsmessung (*perfmon.msc*) verwenden, um die Spiegelung zu überwachen. Mit Leistungsindikatoren können Sie dazu die Leistung der Datenbankspiegelung überwachen. Der Indikator *Transaktionsverzögerung* testet, ob die Datenbankspiegelung Auswirkungen auf die Leistung des Prinzipalservers hat. Die Indikatoren *Wiederholungswarteschlange* und *Protokollsende-Warteschlange* untersuchen, wie die Spiegeldatenbank mit der Prinzipaldatenbank übereinstimmt. Durch Analyse des Leistungsindikators *Gesendete Protokollbytes/Sekunde* können Sie überwachen, wie viele Protokollbytes pro Sekunde gesendet wurden.

Sie haben auch die Möglichkeit, die Replikation zu überwachen. Dazu stehen ebenfalls verschiedene Indikatoren zur Verfügung:

- **Alle Agents** *SQLServer:Replications Agents*
- **Momentaufnahme-Agent** *SQLServer:Replication Snapshot*
- **Protokolllese-Agent** *SQLServer:Replication Logreader*
- **Verteilungs-Agent** *SQLServer:Replication Dist.*
- **Merge-Agent** *SQL Server:Replication Merge*

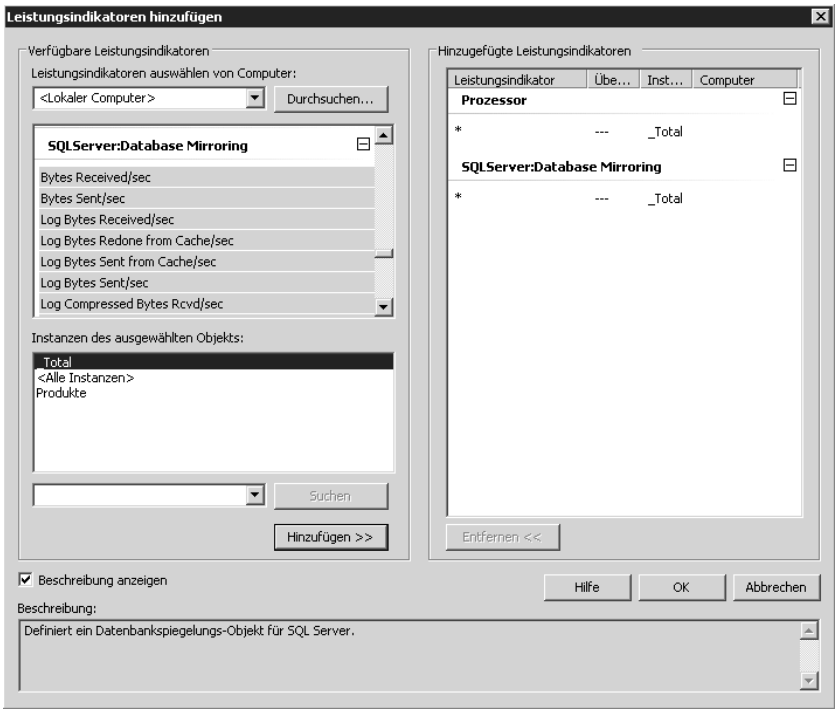
Datensicherungen lassen sich bereits beim Erstellen komprimieren. Da eine komprimierte Sicherung kleiner als eine unkomprimierte Sicherung ist, wird für das Komprimieren einer Sicherung in den meisten Fällen weniger Geräte-E/A benötigt. Aus diesem Grund steigt die Sicherungsgeschwindigkeit in den meisten Fällen. Komprimierte und nicht komprimierte Sicherungen können Sie nicht parallel in einem Mediensatz speichern. Die CPU-Nutzung steigt durch die Komprimierung erheblich.

Mit den Windows-Leistungsindikatoren *Device Throughput Bytes/sec* des Objekts *SQLServer:Backup Device* und *Backup/Restore Throughput/sec* des Objekts *SQLServer:Databases* messen Sie die Übertragungsgeschwindigkeit auf das Sicherungsmedium. Auf diesem Weg können Sie die Übertragungsrate für komprimierte im Vergleich zu nicht komprimierten Sicherungen messen und auf dieser Basis entscheiden, ob die Komprimierung die höhere CPU-Last rechtfertigt

Wählen Sie zunächst den entsprechenden Indikator aus und klicken Sie auf *Hinzufügen*. Sie können eine Beschreibung der Indikatorengruppe anzeigen, die aktuell in der Liste ausgewählt ist. Aktivieren Sie dazu das Kontrollkästchen *Beschreibung anzeigen* in der unteren linken Ecke des Fensters. Wenn Sie eine andere Gruppe auswählen, wird die zugehörige Beschreibung angezeigt.

Sie können die verfügbaren Indikatoren einer Gruppe anzeigen, indem Sie auf den Abwärtspfeil rechts neben dem Gruppennamen klicken. Zum Hinzufügen einer Indikatorengruppe markieren Sie den Gruppennamen und klicken auf die Schaltfläche *Hinzufügen*.

Abbildg. 6.44 Hinzufügen von Leistungsindikatoren zur Leistungsüberwachung



Nachdem Sie einen Gruppennamen markiert haben, können Sie die enthaltenen Leistungsindikatoren anzeigen. Markieren Sie einen Indikator in der Liste, bevor Sie auf *Hinzufügen* klicken, wird nur dieser Indikator hinzugefügt.

Sie können einen einzelnen Indikator hinzufügen, indem Sie auf das Pluszeichen neben dem Gruppennamen klicken, den gewünschten Indikator markieren und danach auf *Hinzufügen* klicken. Möchten Sie mehrere Indikatoren einer Gruppe auswählen, klicken Sie bei gedrückter Strg-Taste auf die Namen in der Liste. Sobald alle gewünschten Indikatoren ausgewählt sind, klicken Sie auf *Hinzufügen*.

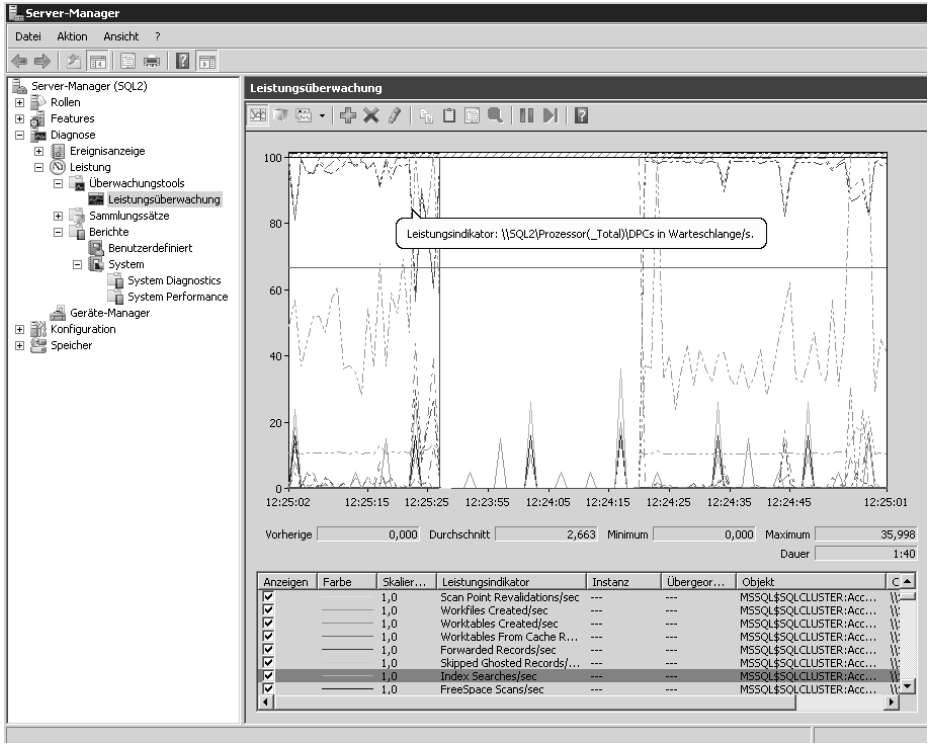
Möchten Sie nur eine bestimmte Instanz eines Indikators hinzufügen, markieren Sie einen Gruppennamen in der Liste, wählen den gewünschten Prozess in der Liste im Bereich Instanzen des gewählten Objekts aus und klicken auf *Hinzufügen*. Derselbe Indikator kann von mehreren Prozessen generiert werden. Bei Auswahl einer Instanz protokolliert der Server nur die Indikatoren, die der gewählte Prozess erzeugt. Wenn Sie keine Instanz auswählen, protokolliert der Server alle Instanzen des Indikators.

Sie können nach Instanzen eines Indikators suchen, indem Sie die Indikatorengruppe markieren oder die Gruppe erweitern und den gewünschten Indikator markieren, den Prozessnamen in das Feld unterhalb der Instanzenliste für das gewählte Objekt eingeben und auf *Suchen* klicken. Der eingegebene Prozessname wird in der Dropdownliste für eine weitere Suche angeboten.

Indikatorendaten in der Leistungsüberwachung beobachten

Standardmäßig zeigt die Leistungsüberwachung die Daten in Form eines Liniendiagramms an. Abgebildet werden Daten über einen Zeitraum von zwei Minuten. Die Abtastung erfolgt von links nach rechts. Die X-Achse ist beschriftet. Mithilfe des Diagramms lassen sich Änderungen an den Aktivitäten der einzelnen Indikatoren über einen kurzen Zeitraum beobachten. Sie können Details für einen bestimmten Indikator anzeigen, indem Sie im Diagramm mit der Maus auf die entsprechende Indikatorlinie zeigen. Mit dem Dropdownlistenfeld in der Symbolleiste können Sie die Anzeige für die aktuelle Datensammlergruppe ändern.

Abbildg. 6.45 Anzeigen der Überwachungsdaten



In der Histogrammansicht sehen Sie Daten ebenfalls in Echtzeit und Balkenform. In dieser Ansicht lassen sich Änderungen an den Aktivitäten der einzelnen Indikatoren beobachten. Die Berichtansicht enthält die Werte für den ausgewählten Indikator in Textform. Unter dem Ansichtsfenster befindet sich eine Legende mit Angaben zu den einzelnen Leistungsindikatoren. Über die Kontrollkästchen der einzelnen Zeilen können Sie steuern, welche Indikatoren in der Ansicht dargestellt werden.

Ist eine Zeile in der Legende ausgewählt, lässt sich die zugehörige Indikatorlinie optisch hervorheben, indem Sie auf der Symbolleiste auf die Schaltfläche *Markierung* klicken. Durch erneutes Klicken auf diese Schaltfläche wird die ursprüngliche Anzeige wiederhergestellt.

Abbildg. 6.46 Markieren von Indikatoren in der Leistungsüberwachung

Sie können die Eigenschaften für die Anzeige eines Indikators ändern. Klicken Sie dazu mit der rechten Maustaste auf die entsprechende Zeile in der Legende und wählen Sie im Kontextmenü den Eintrag *Eigenschaften*. Daraufhin wird das Dialogfeld *Eigenschaften von Leistungsüberwachung* mit aktivierter Registerkarte *Daten* geöffnet. Passen Sie die Eigenschaften mithilfe der Einträge in den Listenfeldern an. Mit der Schaltfläche *Anzeige fixieren* auf der Symbolleiste können Sie die Anzeige einfrieren, um die aktuelle Aktivität zu überprüfen. Wenn Sie die Anzeige wieder aktivieren möchten, klicken Sie auf die Schaltfläche *Fixierung der Anzeige aufheben*. Per Klick auf die Schaltfläche *Daten aktualisieren* kann die Anzeige schrittweise durchlaufen werden.

Halten Sie die Anzeige des Liniendiagramms an und starten diese wieder, ändert sich der auf der X-Achse dargestellte Zeitraum. Die Leistungsüberwachung arbeitet mit *Objekten*, die sich beobachten lassen. Für jedes dieser Objekte, wie zum Beispiel den Prozessor, gibt es eine Reihe von Leistungsindikatoren wie *Prozessorzeit* oder *Interrupts/s*. Für einzelne Objekte gibt es zudem mehrere Instanzen. Dies ist zum Beispiel beim Prozessor der Fall, wenn mit einem Multiprozessorsystem gearbeitet wird. Beim Objekt *Prozesse* wird eine Instanz für jeden aktiven Prozess definiert.

Sammlungssätze nutzen

Die Echtzeitanzeige ist nur eine Möglichkeit, die Leistungsüberwachung zu nutzen. Nachdem Sie eine Kombination aus Indikatoren zusammengestellt haben, können Sie diese als *Sammlungssätze* (Data Collector Set, DCS) speichern. Um einen Sammlungssatz zu erstellen, beginnen Sie mit der Anzeige der Leistungsindikatoren. Erweitern Sie in der Konsole die Hierarchiestruktur, klicken Sie mit der rechten Maustaste auf *Leistungsüberwachung* und rufen Sie im Kontextmenü den Untermenübefehl *Neu/Sammlungssatz* auf. In Windows Server 2012 trägt die Funktion die Bezeichnung *Datensammlersatz*. Daraufhin wird der Assistent für die Erstellung einer neuen Datensammlergruppe gestartet. Die neue Datensammlergruppe enthält alle Indikatoren, die in der aktuellen Ansicht ausgewählt sind. Möchten Sie nicht den Standardbenutzer verwenden, klicken Sie im dritten Schritt des Assistenten auf die Schaltfläche *Ändern* und geben den Namen und das Kennwort des gewünschten Benutzers ein. Der Sammlungssatz muss unter dem Konto eines Benutzers mit Administratorrechten ausgeführt werden. Über das Kontextmenü starten Sie einen Datensammlersatz. Nach dem Beenden erstellt der Satz einen Bericht, den Sie sich im Server-Manager anzeigen lassen können.

Ein Sammlungssatz erstellt eine Protokolldatei. Diese können Sie sich nach dem Beenden über den Knoten *Berichte/Benutzerdefiniert* anzeigen lassen. In Windows Server 2012 finden Sie den Bereich

über *Datensammlersätze/Benutzerdefiniert*. Sie haben die Möglichkeit, für jeden Satz Speicheroptionen zu konfigurieren. Klicken Sie in der Liste des Fensters mit der rechten Maustaste auf den Namen des Sammlungssatzes, und wählen Sie im Kontextmenü den Eintrag *Eigenschaften*.

Auf der Registerkarte *Allgemein* können Sie eine Beschreibung oder Schlüsselwörter für die Datensammlergruppe eingeben. Auf der Registerkarte *Verzeichnis* ist der Stammordner als Standardordner festgelegt, in dem alle Protokolldateien für die Datensammlergruppe gespeichert sind. Mit *Zeitplan* geben Sie an, wann mit der Datensammlung begonnen wird. Auf der Registerkarte *Stoppbedingung* können Sie Kriterien für Bedingungen angeben, bei denen die Datensammlung angehalten wird. Wenn Sie auf der Registerkarte *Zeitplan* ein Ablaufdatum festgelegt haben, das nach einer auf der Registerkarte *Stoppbedingung* definierten Bedingung liegt, hat die Stoppbedingung Vorrang.

Speicherengpässe beheben

Performanceprobleme können eine Reihe unterschiedlicher Ursachen haben. Ein Problem bei der Performanceanalyse ist, dass die Beseitigung eines Engpasses oft zum nächsten Engpass führt. Dafür gibt es viele Beispiele. Wenn mehr Speicher bereit steht, zeigt sich oft, dass auch die Prozessorauslastung bereits an der Kapazitätsgrenze ist. Es gibt nun einige grundsätzliche Regeln für den Einsatz von Hauptspeicher. Die erste Regel lautet: Viel hilft viel, sowohl beim Hauptspeicher als auch beim Cache. Dies hat für Windows Server 2008 R2/2012 und SQL Server 2012 noch mehr Gültigkeit als unter Windows Server 2003/2008.

Die zweite Regel besagt, dass die Auslagerungsdatei am besten auf einer anderen physischen Festplatte als der Systempartition, die Datenbankdateien und die Transaktionsprotokolle aufgehoben ist.

Auslagerungsdatei und Ressourcenmonitor

Sie sollten die Auslagerungsdatei auf eine andere physische Festplatte des Servers verschieben, damit Schreibzugriffe auf die Auslagerungsdatei nicht von Schreibzugriffen auf der Festplatte ausgebremst werden. Falls keine physische Festplatte zur Verfügung steht, ist ein Verschieben nicht sinnvoll, da die Auslagerung auf eine Partition, die auf derselben Platte liegt, keine positiven Auswirkungen hat. Sie sollten die Auslagerungsdatei aber nicht auf Datenträger auslagern, die Datenbanken oder Transaktionsprotokolle benutzen.

Die Einstellungen für die Auslagerungsdatei finden Sie über *Start/Systemsteuerung/System und Sicherheit/System/Erweiterte Systemeinstellungen*. Wechseln Sie auf die Registerkarte *Erweitert* und klicken Sie bei *Leistung* auf *Einstellungen.* In Windows Server 2012 tippen Sie im Startbildschirm *erweiterte system ein,* wechseln von *Apps* zu *Einstellungen* und klicken dann auf *Erweiterte Systemeinstellungen anzeigen.*

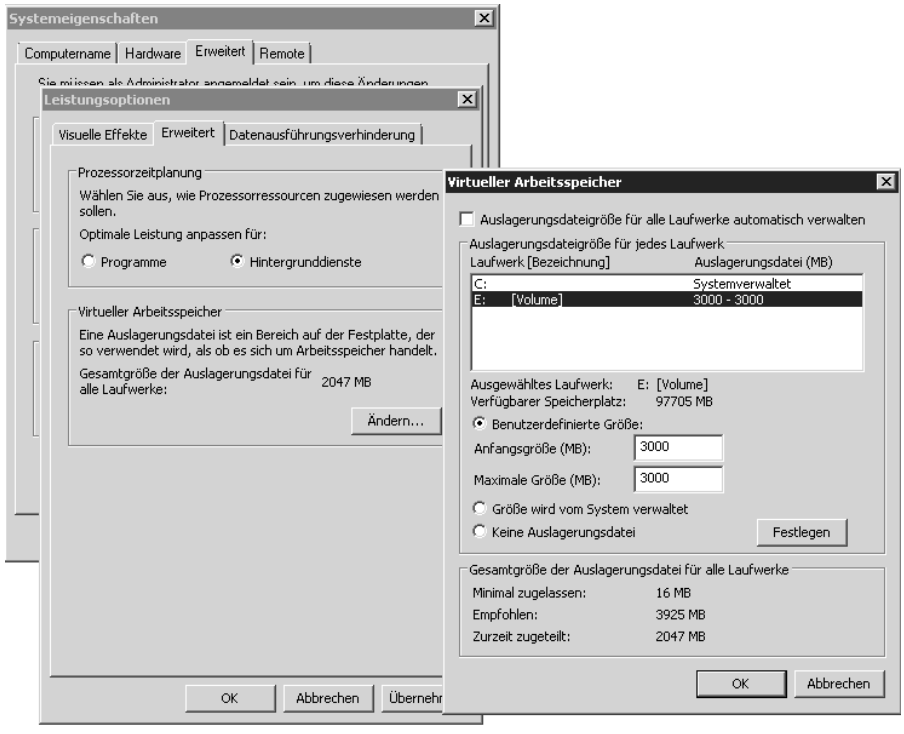
Auf der Registerkarte *Erweitert* klicken Sie bei *Virtueller Arbeitsspeicher* auf *Ändern*. Sie können an dieser Stelle auch eine feste Größe für die Auslagerungsdatei festlegen sowie die Laufwerke bestimmen, auf denen Auslagerungsdateien zur Verfügung stehen sollen. Klicken Sie auf *Festlegen*, nachdem Sie für das jeweilige Laufwerk die gewünschten Einstellungen vorgenommen haben. Zum Abschluss müssen Sie den Server neu starten.

Dies hat den Vorteil, dass diese Datei nicht fragmentiert, da Windows immer auf die komplette Größe zugreifen darf. In der Vergangenheit hat sich etwa eine Größe von »Physischer Arbeitsspeicher * 2,5« als optimal herausgestellt. Sie können in der grafischen Oberfläche aber keine Auslagerungsdatei erstellen, die größer als 2 TB ist. Wenn Sie eine größere Datei verwenden wollen, müssen Sie die Einstellungen in der Befehlszeile vornehmen. Wie Sie dabei vorgehen, zeigen wir Ihnen im nächsten Abschnitt.

Verwenden Sie als Speicherort am besten eine zusätzliche Festplatte und trennen Sie Betriebssystem, Datenbankdateien, Transaktionsprotokolle und die Auslagerungsdatei. Deaktivieren Sie dazu das Kontrollkästchen *Auslagerungsdateigröße für alle Laufwerke automatisch verwalten* und deaktivieren Sie die Auslagerungsdatei für alle Datenträger, auf die SQL Server 2012 zugreifen muss.

Die Auslagerungsdatei speichert Windows in der versteckten Systemdatei *pagefile.sys* im Stammordner des entsprechenden Laufwerks.

Abbildg. 6.47 Anpassen der Auslagerungsdatei



TIPP Sie können die Konfiguration der Auslagerungsdatei auch in der Befehlszeile vornehmen. Dies ist zum Beispiel notwendig, wenn die Datei größer als 2 TB sein soll, oder wenn Sie die Einstellungen skripten möchten. Zum Erstellen einer Auslagerungsdatei führen Sie den folgenden Befehl aus:

```
wmic.exe pagefileset create name="<Laufwerksbuchstabe>:\pagefile.sys"
```

Zum Festlegen der Größe der Auslagerungsdatei verwenden Sie den Befehl:

```
wmic.exe pagefileset where name="<Laufwerksbuchstabe>:\\pagefile.sys" set
InitialSize=<MB>,MaximumSize=<MB>
```

Bitte beachten Sie den doppelten Backslash »\\«!

Mit dem folgenden Befehl deaktivieren Sie die Auslagerungsdatei auf einem Laufwerk:

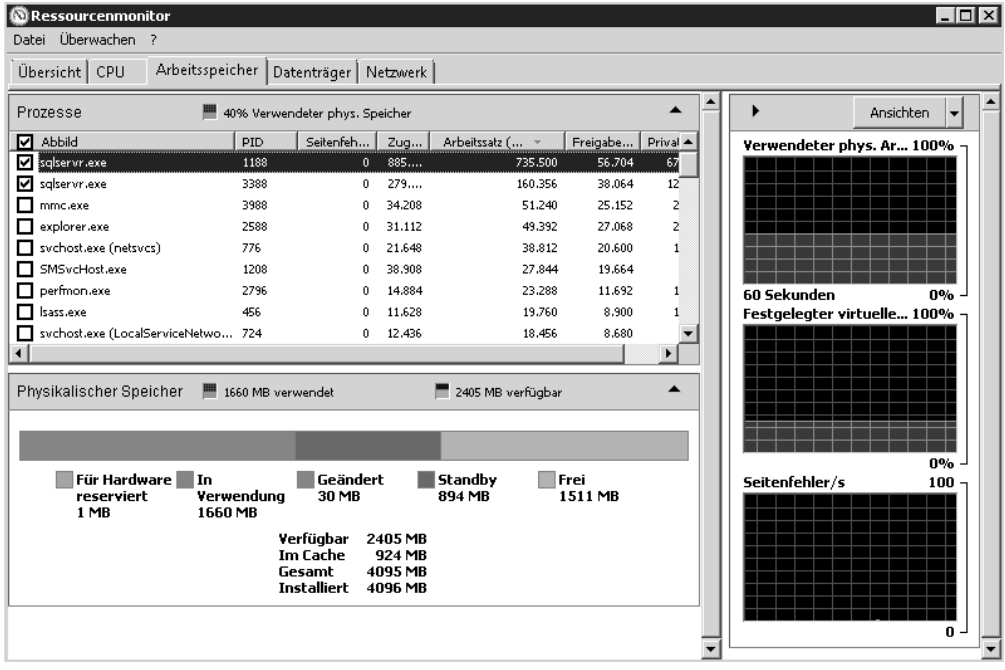
```
wmic.exe pagefileset where name="<Laufwerksbuchstabe>:\\pagefile.sys" delete
```

Haben Sie die Datei bereits gelöscht, erscheint die Meldung *Keine Instanzen verfügbar*. Auf diese Weise überprüfen Sie daher auch, ob auf einem Laufwerk eine Auslagerungsdatei vorhanden ist.

Abbildg. 6.48 Steuern der Auslagerungsdatei in der Befehlzeile

Im Ressourcenmonitor sehen Sie auf der Registerkarte *Arbeitsspeicher* die verschiedenen laufenden Prozesse und deren verbrauchten Arbeitsspeicher. Am schnellsten starten Sie den Ressourcenmonitor durch Eingabe von *perfmon /res* im Suchfeld des Startmenüs oder direkt auf dem Startbildschirm in Windows Server 2012. Mit einem Klick auf die Spalte *Arbeitssatz* lassen Sie sich den Arbeitsspeicherverbrauch der Prozesse sortiert anzeigen.

Abbildg. 6.49 Überprüfen des Arbeitsspeicherverbrauchs einzelner Prozesse auf dem SQL-Server



Arbeitsspeicher mit der Leistungsüberwachung optimieren und überwachen

Die Überwachung des Arbeitsspeichers übernehmen Sie am besten ebenfalls mit der Leistungsüberwachung. Auf SQL-Servern bieten sich folgende Leistungsindikatoren an:

- **Arbeitsspeicher: Verfügbare Bytes** Gibt an, wie viele Bytes an Arbeitsspeicher derzeit für die Verwendung durch Prozesse verfügbar sind. Niedrige Werte können ein Anzeichen dafür sein, dass insgesamt zu wenig Arbeitsspeicher auf dem Server vorhanden ist oder dass eine Anwendung keinen Arbeitsspeicher freigibt.
- **Arbeitsspeicher: Seiten/s** Gibt die Anzahl der Seiten an, die wegen Seitenfehlern vom Datenträger gelesen oder auf den Datenträger geschrieben wurden, um Speicherplatz aufgrund von Seitenfehlern freizugeben. Ein hoher Wert kann auf überhöhte Auslagerungen hindeuten. Überwachen Sie noch *Seitenfehler/s*, um sicherzustellen, dass die Datenträgeraktivität nicht durch das Auslagern verursacht wird.

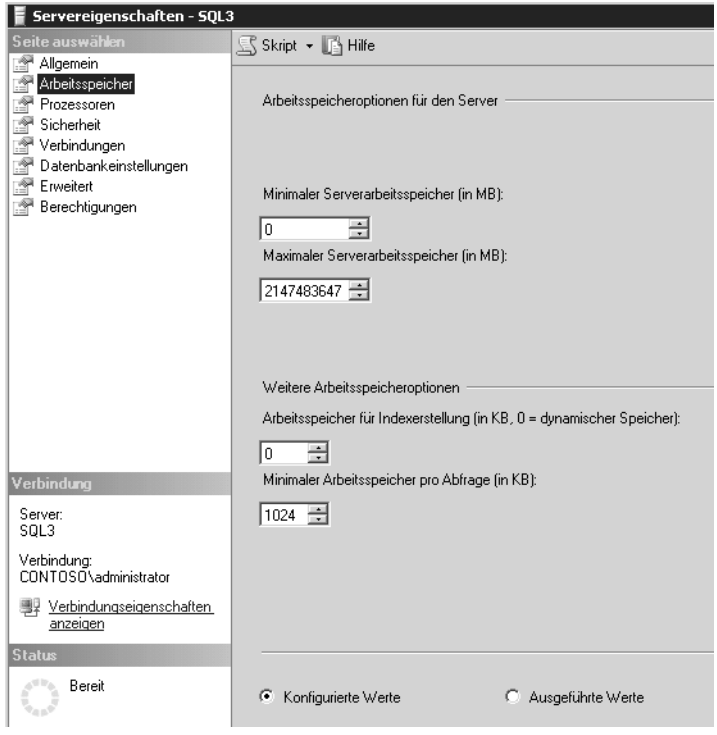
Der Manager für virtuellen Arbeitsspeicher (VMM) entnimmt Seiten von SQL Server 2012 und anderen Prozessen, um die Größen der Arbeitsspeicherbereiche dieser Prozesse anzupassen. Um festzustellen, ob die überhöhten Auslagerungen von SQL Server 2012 oder einem anderen Prozess verursacht werden, sollten Sie *Seitenfehler/s* der SQL Server-Prozessinstanz überprüfen.

In der Standardkonfiguration werden Arbeitsspeicheranforderungen von SQL Server 2012 auf Basis der verfügbaren Systemressourcen dynamisch geändert. Wenn der SQL-Server mehr Arbeitsspeicher benötigt, wird das Betriebssystem nach der Verfügbarkeit von freiem physischen Arbeitsspeicher abgefragt. Wenn SQL Server 2012 den zugeordneten Arbeitsspeicher nicht benötigt, wird der Arbeitsspeicher für das Betriebssystem freigegeben. Sie können die Option zur dynamischen Verwendung des Arbeitsspeichers jedoch mit den Serverkonfigurationsoptionen *minservermemory* und *maxservermemory* überschreiben.

Die Standardeinstellung für *minservermemory* ist 0, die für *maxservermemory* 2.147.483.647 MB (gleich 2 Petabyte). Wenn sich SQL Server 2012 nach dem Ändern der Optionen nicht starten lässt, müssen Sie den Serverdienst mit der Startoption *–f* starten. Mehr zum Thema lesen Sie in Kapitel 3. Generell ist es empfehlenswert, die dynamische Verwendung des Arbeitsspeichers beizubehalten. Sie können die Speicheroptionen aber auch manuell festlegen und den Umfang des für SQL Server 2012 zugreifbaren Arbeitsspeichers einschränken. *minservermemory* wird dem SQL-Server nicht gleich beim Start zugeordnet. Wenn der Wert nicht benötigt wird, ruft der SQL-Server ihn auch nicht komplett ab. So definieren Sie eine feste Arbeitsspeichergröße:

1. Klicken Sie im Objekt-Explorer des SQL Server Management Studios mit der rechten Maustaste auf den Server und wählen Sie *Eigenschaften*.
2. Öffnen Sie die Seite *Arbeitsspeicher*.
3. Geben Sie im Abschnitt *Arbeitsspeicheroptionen für den Server* den gewünschten Wert für *Minimaler Serverarbeitsspeicher* und *Maximaler Serverarbeitsspeicher* ein.

Abbildg. 6.50 Konfigurieren des Arbeitsspeichers eines Servers



Durch Sperren von Seiten im Arbeitsspeicher können Sie die Leistung eines SQL-Servers teilweise auch nach Auslagerung von Arbeitsspeicherdaten auf die Festplatte verbessern. Die SQL Server-Option *Sperren von Seiten im Speicher* wird bei SQL Server 2012 auf *ON* gesetzt, wenn dem Dienstkonto der Instanz das Windows-Benutzerrecht *Lock Pages in Memory (LPIM)* erteilt wurde. Entfernen Sie zum Deaktivieren der Option *Sperren von Seiten im Speicher* für SQL Server 2012 das Benutzerrecht *Lock Pages in Memory* für das SQL Server-Startkonto. In diesem Fall kann der Server selbst die entsprechenden Seiten nicht mehr steuern, sondern das Betriebssystem übernimmt diese Aufgabe:

Erstellen Sie für die Einstellung entweder eine Gruppenrichtlinie, die Sie den SQL-Servern zuweisen, oder nehmen Sie die Einstellungen lokal auf dem Server vor:

1. Geben Sie im Suchfeld des Startmenüs den Befehl *gpedit.msc* ein.

HINWEIS Unter Windows Server 2012 können Sie auf der Metro-Oberfläche direkt mit dem Tippen beginnen oder über ⊞ + R das Dialogfeld *Ausführen* aufrufen.

2. Erweitern Sie *Computerkonfiguration/Windows-Einstellungen/Sicherheitseinstellungen/Lokale Richtlinien/Zuweisen von Benutzerrechten*.
3. Klicken Sie doppelt auf *Sperren von Seiten im Speicher*.
4. Entfernen Sie das Konto des SQL-Servers in diesem Bereich, wenn es angezeigt wird.

Um die Menge des von SQL Server 2012 speziell verwendeten Arbeitsspeichers zu überwachen, überwachen Sie die folgenden Leistungsindikatoren:

- **Prozess: Arbeitsseiten** Gibt die Menge an Arbeitsspeicher an, die ein Prozess verwendet. Wenn dieser Wert konstant unter der Menge an Arbeitsspeicher liegt, die in den Serveroptionen in den Eigenschaften des SQL-Servers festgelegt sind, haben Sie den SQL-Server so konfiguriert, dass er zu viel Arbeitsspeicher beansprucht.
- **SQLServer:Buffer-Manager: Buffer cache hit ratio** Eine Rate von 90 Prozent oder höher ist hier empfohlen. Erhöhen Sie so lange Arbeitsspeicher, bis der Wert konstant über 90 Prozent liegt. Ein Wert von über 90 Prozent bedeutet, dass mehr als 90 Prozent aller Datenanforderungen vom Datencache erfüllt wurden. Aktivieren Sie zur besseren Übersicht in der Windows-Leistungsüberwachung die Ansicht *Bericht*.

Abbildg. 6.51 Überwachen des Arbeitsspeichers von SQL Server 2012 mit der Windows-Leistungsüberwachung

Karte des Arbeitsspeichers – RAMMap und VMMap

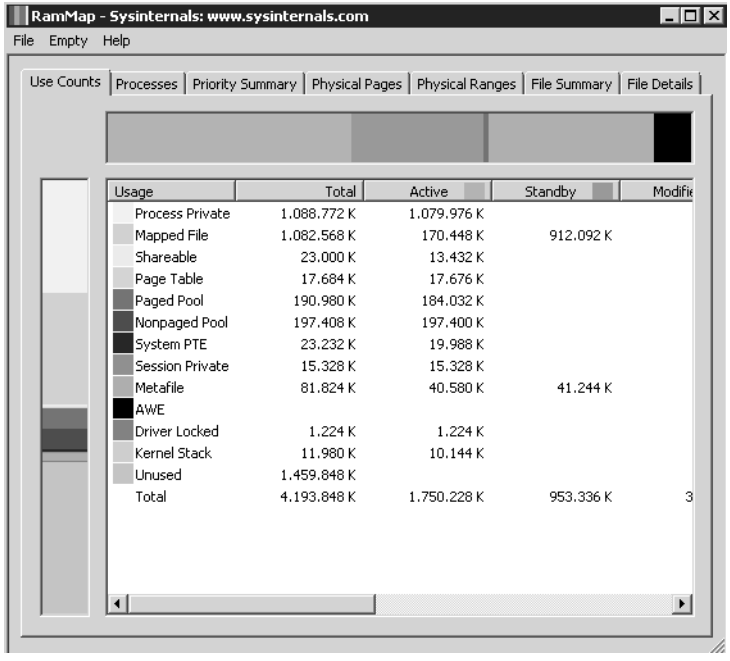
Für die Fehleranalyse oder Leistungsmessung eines Computers kann es sinnvoll sein, die aktuelle Auslastung des Arbeitsspeichers zu kennen. Das Sysinternals-Tool *RAMMap* (*http://technet.microsoft.com/de-de/sysinternals/ff700229* [Ms151-K06-17]) zeigt die aktuelle Zuteilung des Arbeitsspeichers in einer grafischen Oberfläche an.

Mit dem Tool erkennen Sie, wie viel Arbeitsspeicher aktuell für den Kernel reserviert sind und welchen Arbeitsspeicher die Treiber des Computers verbrauchen. Auf verschiedenen Registerkarten zeigt das Tool ausführliche Informationen zum Arbeitsspeicher an:

- **Use Counts** Zusammenfassung
- **Processes** Prozesse
- **Priority Summary** Priorisierte Standbylisten
- **Physical Pages** Seitenübersicht für den kompletten Arbeitsspeicher
- **Physical Ranges** Adressen zum Arbeitsspeicher
- **File Summary** Dateien im Arbeitsspeicher
- **File Details** Individuelle Seiten im Arbeitsspeicher nach Dateien sortiert

Das Tool hilft vor allem Technikern und Entwicklern dabei, zu verstehen, wie die aktuellen Windows-Versionen den Arbeitsspeicher verwalten und an die verschiedenen Anwendungen, Treiber und Prozesse verteilen. Das Tool funktioniert ab Windows Vista/Windows Server 2008, allerdings nicht in den Vorgängerversionen.

Abbildg. 6.52 Anzeige der Arbeitsspeicherverteilung in Windows Server 2008 R2



Noch ausführlicher bezüglich der Arbeitsspeicheranalyse ist VMMAP (*http://technet.microsoft.com/en-us/sysinternals/dd535533* [Ms151-K06-18]). Das Tool zeigt sehr detailliert den Arbeitsspeicherverbrauch von Prozessen an. Durch die ausführlichen Filtermöglichkeiten geht *VMMap* bei der Analyse also wesentlich weiter als *RAMMap*. Beide Tools sind nicht nur für Administratoren geeignet, sondern auch für Entwickler oder Techniker, die genau das Aufteilen der Ressourcen verstehen wollen.

VMMap hat die Möglichkeit, auch anzuzeigen, ob ein Prozess Arbeitsspeicher durch den physischen Arbeitsspeicher zugewiesen bekommt oder durch Windows in die Auslagerungsdatei ausgelagert wird. VMMap listet sehr detailliert auf, welche Daten eines Programms oder eines Prozesses in welchen Bereichen des Arbeitsspeichers oder der Auslagerungsdatei liegen. Das Tool ermöglicht auch das Erstellen von Momentaufnahmen und dadurch von Vorher-Nachher-Beobachtungen.

Durch die ausführlichen Analysemöglichkeiten kann das Tool in der grafischen Oberfläche genau anzeigen, wie viel Arbeitsspeicher einzelne Funktionen in einem Prozess benötigen. Über den Menübefehl *View/String* lässt sich anzeigen, welche Daten ein einzelner Speicherbereich enthält. Gescannte Ergebnisse lassen sich über das Menü *File* abspeichern.

Neben dem Standardformat von VMMap (*.mmp*) lassen sich die Daten auch im *.txt*-Format sowie als *.csv*-Datei abspeichern. Mit diesen Möglichkeiten können Sie also auch Analysen mit Excel durchführen. Im Gegensatz zu RAMMap können Sie VMMap aber auch unter Windows 2000, XP und Windows Server 2003 nutzen.

Diagnose des Arbeitsspeichers

Häufig sind die Probleme auf einem Server auf defekten Arbeitsspeicher zurückzuführen. In Windows Server 2008 R2 und Windows Server 2012 wurde daher ein spezielles Diagnoseprogramm integriert, welches den Arbeitsspeicher ausführlich auf Fehler überprüft. Sie können das Tool über *mdsched* aufrufen. Das Tool steht auch in der Programmgruppe *Verwaltung* zur Verfügung und – wenn Sie den Server mit der 2008-DVD starten – über die *Computerreparaturoptionen*.

Sie können entweder den Server sofort neu starten und eine Diagnose durchführen oder festlegen, dass die Diagnose erst beim nächsten Systemstart durchgeführt werden soll. Während der Speicherdiagnose prüft das Programm, ob der eingebaute Arbeitsspeicher Fehler aufweist, was eine häufige Ursache für ungeklärte Abstürze ist.

Nachdem der Test abgeschlossen ist, startet der Server automatisch neu und meldet das Ergebnis über ein Symbol im Infobereich der Taskleiste. Über die Funktionstaste F1 gelangen Sie zu den Optionen der Überwachung und können verschiedene Überprüfungsmethoden auswählen und mit F10 starten. Ist der Test beendet, startet der Server automatisch wieder. Sie müssen daher nicht warten, bis der Test abgeschlossen ist, damit der Server wieder zur Verfügung steht.

Für andere Windows-Versionen oder ausführlichere Tests, hilft Windows Memory Diagnostic, das kostenlos auf der Seite *http://oca.microsoft.com/de/windiag.asp* [Ms151-K06-19] zur Verfügung steht. Das Tool erstellt eine Boot-Diskette oder eine bootfähige CD, von der Sie starten und dann den Arbeitsspeicher ausführlich testen lassen. Lassen Sie den Assistenten ein CD-Image als ISO-Datei erstellen. Auf der Ultimate Boot CD (*http://www.ultimatebootcd.com/* [Ms151-K06-20]) befinden sich übrigens im Bereich *Memory* ebenfalls einige Testtools für den Arbeitsspeicher. Mehr zu diesem Thema lesen Sie in Kapitel 5.

Prozessorauslastung messen und für SQL Server 2012 optimieren

Auch die Prozessorleistung kann einen Flaschenhals darstellen. Zu wenig Hauptspeicher kann die Konsequenz haben, dass auch der Prozessor sehr stark belastet wird. Denn die Auslagerung von Seiten und viele andere Vorgänge gehen natürlich nicht spurlos am Prozessor vorbei. Er hat an der Verwaltung des Arbeitsspeichers einen relativ hohen Anteil. Da Engpässe beim Hauptspeicher typischerweise deutlich kostengünstiger zu beheben sind, als solche beim Prozessor, sollte diese Situation zunächst untersucht werden.

Die Auslastung ist kein Problem, wenn sie kurzzeitig über 90 % liegt oder wenn das gelegentlich vorkommt. Zum Problem wird sie, wenn sie über längere Zeiträume in diesem Bereich liegt. Aber auch dann muss man mit der Analyse noch etwas vorsichtig sein. Bei Mehrprozessorsystemen gilt das Augenmerk vor allem den Leistungsindikatoren aus dem Objekt *System*. Dort werden Informationen von mehreren Systemkomponenten zusammengefasst. So kann dort beispielsweise die Gesamtbelastung aller Prozessoren ermittelt werden. Ergänzend ist aber auch hier der Leistungsindikator *Prozessorzeit* des Objekts *Prozessor* von Bedeutung. Wenn viele verschiedene Prozesse ausgeführt werden, ist eine einigermaßen gleichmäßige Lastverteilung fast sicher. Bei einem einzelnen Prozess ist dagegen die Aufteilung in einigermaßen gleichgewichtige Threads wichtig. Ein Thread ist eine Ausführungseinheit eines Prozesses. Wenn ein Prozess mehrere Threads verwendet, können diese auf unterschiedlichen Prozessoren ausgeführt werden. Die Verteilung erfolgt entsprechend der Auslastung der einzelnen Prozessoren durch das System.

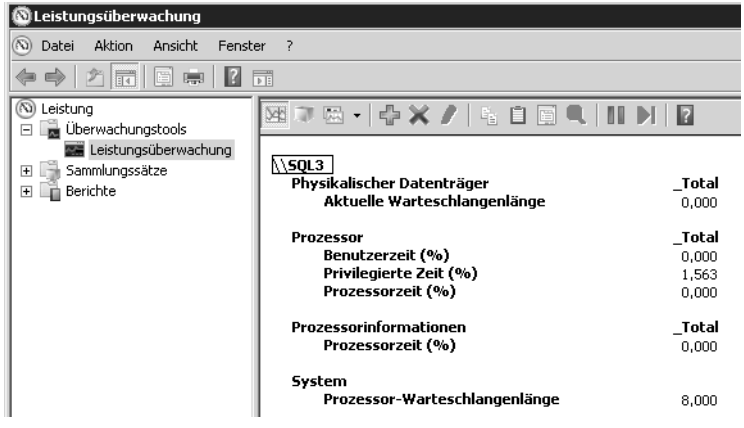
Eine hohe Zahl von Warteschlangen bedeutet, dass mehrere Threads rechenbereit sind, ihnen aber vom System noch keine Rechenzeit zugewiesen wurde. Die Faustregel für diesen Wert ist, dass er nicht allzu häufig über 2 liegen sollte. Wenn die Auslastung des Prozessors im Durchschnitt relativ gering ist, spielt dieser Wert nur eine untergeordnete Rolle.

Eine konstant hohe CPU-Nutzungsrate macht deutlich, dass der Prozessor eines Servers überlastet ist. Überwachen Sie in der Leistungsüberwachung von Windows Server 2008 R2 und Windows Server 2012 den Leistungsindikator *Prozessor: Prozessorzeit (%)*. Dieser Leistungsindikator überwacht die Zeit, welche die CPU zur Verarbeitung eines Threads benötigt, der sich nicht im Leerlauf befindet. Ein konstanter Status von 80 bis 90 % ist zuviel. Bei Multiprozessorsystemen sollten Sie für jeden Prozessor eine eigene Instanz dieses Leistungsindikators überwachen. Dieser Wert stellt die Summe der Prozessorzeit für einen bestimmten Prozessor dar.

Zusätzlich können Sie die Prozessornutzung aber auch über *Prozessor: Privilegierte Zeit (%)* überwachen. Dieser gibt den prozentualen Zeitanteil an der Gesamtzeit an, die der Prozessor benötigt, um Windows-Kernelbefehle, wie die Verarbeitung von E/A-Anforderungen von SQL Server 2012, auszuführen. Sollte dieser Leistungsindikator bei hohen Werten für die Leistungsindikatoren *Physischer Datenträger* dauerhaft hoch sein, sollten Sie die Installation eines schnelleren oder effizienteren Datenträgers planen.

- **Prozessor: Benutzerzeit** (%) Gibt den prozentualen Zeitanteil an der Gesamtzeit an, die der Prozessor benötigt, um Benutzerprozesse des SQL-Servers auszuführen
- **System: Prozessor-Warteschlangenlänge** Zählt die Threads, die auf Prozessorzeit warten. Ein Prozessorengpass entsteht, wenn die Threads eines Prozesses mehr Prozessorzyklen benötigen, als zur Verfügung stehen. Wenn viele Prozesse versuchen, Prozessorzeit zu beanspruchen, sollten Sie einen schnelleren Prozessor installieren.

Abbildg. 6.53 Überwachen der Prozessoren eines SQL-Servers



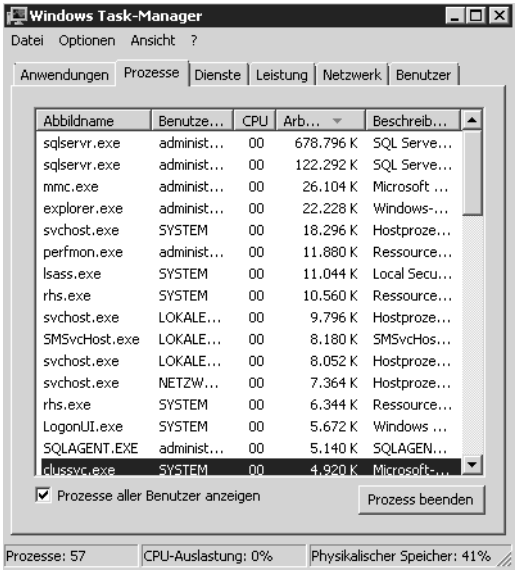
Der Task-Manager als Analysewerkzeug

Ein weiteres wichtiges Werkzeug für die Analyse der Performance ist der Windows Task-Manager. Dieser zeichnet sich dadurch aus, dass er mit sehr wenig Aufwand genutzt werden kann. Sie können den Task-Manager durch einen Klick mit der rechten Maus auf die Taskleiste über dessen Kontextmenü aufrufen. Alternativ können Sie den Task-Manager auch über das Menü aufrufen, das mit der

Tastenkombination Strg+Alt+Entf erscheint oder über *taskmgr* im Suchfeld des Startmenüs. Direkt lässt sich der Task-Manager über die Tastenkombination Strg+⇧+Esc starten. Der Task-Manager stellt in Windows Server 2008 R2 sechs Registerkarten bereit, in Windows Server 2012 nur noch 5. Da die Bedienung der beiden Systeme recht ähnlich ist, auch wenn die Oberfläche unterschiedlich aussieht, beschreiben wir nachfolgend die Bedienung in Windows Server 2008 R2:

- **Anwendungen** Gibt einen Überblick über die aktuell laufenden Anwendungen. Angezeigt wird der Status dieser Anwendungen. Darüber hinaus können Sie über das Kontextmenü der Anwendungen steuern, wie diese Anwendungen angezeigt werden sollen. Außerdem können Sie hier laufende Anwendungen (Tasks) beenden, zu Anwendungen wechseln oder über die Schaltfläche *Neuer Task* auch neue Anwendungen starten.
- **Prozesse** Hier erhalten Sie einen Überblick über die derzeit aktiven Prozesse. Dabei handelt es sich nicht nur um Anwendungen, sondern auch um die gesamten Systemdienste, die im Hintergrund ausgeführt werden. Zu jedem dieser Prozesse werden Informationen über die Prozess-ID (PID), den aktuellen Anteil an der Nutzung der CPU, die insgesamt in dieser Arbeitssitzung konsumierte CPU-Zeit sowie die aktuelle Speichernutzung angezeigt. Gerade diese letzte Information ist von besonderem Interesse, da sie darüber informiert, in welchem Umfang Anwendungen den Hauptspeicher tatsächlich nutzen – ohne dass man komplexe Parameter überwachen muss. Auch hier können Prozesse über die entsprechende Schaltfläche wieder beendet werden. Sie sollten damit allerdings sehr vorsichtig sein, da das Beenden eines Diensts dazu führen kann, dass Ihr System nicht mehr korrekt ausgeführt wird.

Abbildg. 6.54 Systemüberwachung von Windows Server 2008 R2 mit dem Task-Manager



- **Dienste** Listet den Ressourcenverbrauch der gestarteten Dienste auf
- **Leistung** Gibt einen schnellen Überblick zum aktuellen Leistungsverbrauch des Servers. Dahinter verbirgt sich ein kleiner Systemmonitor, der die wichtigsten Informationen zur Systemauslastung in grafischer Form zur Verfügung stellt. In kleinen Fenstern wird die Auslastung der CPU und des Speichers zum aktuellen Zeitpunkt und im Zeitablauf dargestellt. Darunter findet

sich eine Fülle von Informationen rund um die aktuelle Speichernutzung. Von besonderem Interesse ist dabei das Verhältnis von insgesamt zugesichertem virtuellen Speicher und dem physisch vorhandenen Hauptspeicher. Wenn mehr virtueller Speicher zugesichert ist, als im System vorhanden ist, muss auf jeden Fall ausgelagert werden. Eine optimale Systemgestaltung führt dazu, dass ausreichend physischer Hauptspeicher vorhanden ist beziehungsweise der Mittelwert des zugesicherten virtuellen Speichers zumindest nicht wesentlich über dem physischen Hauptspeicher liegt

- **Netzwerk** Zeigt Informationen zum aktuellen Datenverkehr über das Netzwerk an
- **Benutzer** Liefert Informationen über die aktuell gestarteten Programme der angemeldeten Benutzer auf dem Server

Bei den Prozessen fällt vor allem der Prozess *svchost.exe* auf. Die Datei liegt im *System32*-Ordner und wird beim Systemstart von Windows automatisch als allgemeiner Prozess gestartet. Der Prozess durchsucht beim Systemstart die Registry nach Diensten, die beim Systemstart geladen werden müssen. Dienste, die nicht eigenständig lauffähig sind, sondern über Dynamic Link Library (DLL)-Dateien geladen werden, werden mithilfe der *svchost.exe* geladen. Auch wenn Windows läuft, kommt die *svchost.exe* immer dann ins Spiel, wenn Dienste über DLL-Dateien geladen werden müssen. Das Betriebssystem startet SVCHOST-Sessions, sobald solche benötigt werden, und beendet sie auch wieder, sobald sie nicht mehr gebraucht werden. Da unter Windows die unterschiedlichsten Dienste parallel laufen, können auch mehrere Instanzen der *svchost.exe* gleichzeitig in der Prozessliste auftauchen.

Über den Befehl *tasklist /svc* in der Eingabeaufforderung können Sie sich anzeigen lassen, welche Anwendungen auf *svchost.exe* zurückgreifen. Alternativ können Sie die mit *svchost.exe* verbundenen Dienste auch im Task-Manager anzeigen lassen. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie den Task-Manager.
2. Holen Sie die Registerkarte *Prozesse* in den Vordergrund. In Windows Server 2012 verwenden Sie die Registerkarte *Details*.
3. Klicken Sie mit der rechten Maustaste auf eine Instanz von *svchost.exe* und klicken Sie dann auf *Zu Dienst(en) wechseln*. Die dem betreffenden Prozess zugeordneten Dienste werden auf der Registerkarte *Dienste* hervorgehoben. Das Ganze funktioniert auch für andere Prozesse.

Eine weitere Option, die über den Befehl *Priorität festlegen* im Kontextmenü der verschiedenen Prozesse zur Verfügung steht, ist die Möglichkeit zur Prioritätssteuerung laufender Prozesse. Eine höhere Priorität führt dazu, dass ein Prozess mehr Rechenzeit zugewiesen erhält. Bei der Priorität *Echtzeit* erhält der Prozess die gesamte zuteilbare Rechenzeit. Die manuelle Zuordnung von Prioritäten sollte allerdings generell nur von Experten vorgenommen werden, da sie auch die gegenteilige Wirkung – nämlich ein deutlich langsameres System – haben kann, wenn hier falsche Einstellungen getroffen werden.

Laufwerke und Datenträger überwachen – Leistungsüberwachung und Zusatztools

Der folgende Abschnitt geht auf Tools ein, mit denen Sie Datenträger und Laufwerke in Windows Server 2008 R2 und Windows Server 2012 optimal überwachen können. Auf diesem Weg können Sie eventuellen Problemen mit den Datenbankdateien vorgreifen. Sie können aber auch mit der Windows-Leistungsüberwachung, die wir in diesem Kapitel an den verschiedenen Stellen behandelt

haben, ebenfalls die Datenträger im System überwachen. In Kapitel 1 gehen wir ebenfalls auf verschiedene Tools ein, die bei der Optimierung der Datenträger für SQL Server 2012 helfen.

Datenträger mit der Windows-Leistungsüberwachung prüfen

SQL Server 2012 verwendet Aufrufe für die Windows-Betriebssystemeingabe/-ausgabe, um Lese- und Schreibvorgänge auf dem Datenträger auszuführen. SQL Server 2012 verwaltet zwar, wann und wie Datenträger-E/A ausgeführt werden, aber das Betriebssystem führt E/A-Vorgänge aus. Das E/A-Teilsystem umfasst Systembus, Datenträgercontroller, Datenträger, CD/DVD-ROM-Laufwerk und zahlreiche andere E/A-Geräte. Datenträger-E/A ist häufig die Ursache von Engpässen in einem System, vor allem beim Einsatz von SQL-Servern.

Die folgenden zwei Leistungsindikatoren können überwacht werden, um die Datenträgeraktivität zu bestimmen:

- **Physikalischer Datenträger:Zeit (%)** Prozentsatz der Zeit, den der Datenträger für Lese-/Schreibaktivitäten benötigt. Wenn der Leistungsindikator einen hohen Wert besitzt, überprüfen Sie noch *Physikalischer Datenträger:Aktuelle Warteschlangenlänge*, um festzustellen, wie viele Anforderungen auf einen Datenträgerzugriff warten. Die Anzahl der wartenden E/A-Anforderungen sollte das Anderthalbfache bis Zweifache der Anzahl der Spindeln, aus denen sich der physische Datenträger zusammensetzt, nicht überschreiten. Wenn *Aktuelle Warteschlangenlänge* und *Zeit (%)* durchgängig sehr hoch sind, müssen Sie den Datenträger entlasten, weitere Datenträger einsetzen und die verschiedenen Datenbankdateien aufteilen oder einen weiteren Server hinzufügen (siehe Kapitel 4).
- **Physikalscher Datenträger:Durchschnittliche Warteschlangenlänge des Datenträgers** Überwachen Sie den *Arbeitsspeicher:Seitenfehler/s*, um sicherzustellen, dass die Datenträgeraktivität nicht durch Auslagern verursacht wird. In diesem Fall liegt das Problem nicht am Datenträger, sondern an fehlendem Arbeitsspeicher.

Wenn Sie über mehr als eine logische Partition auf derselben Festplatte verfügen, sollten Sie statt den Leistungsindikatoren für physische Arbeitsspeicher die Leistungsindikatoren für logische Datenträger verwenden. Haben Sie die Datenträger mit hoher Lese-/Schreibaktivität festgestellt, können Sie zum Beispiel mit *Logischer Datenträger:Bytes geschrieben/s* den Fehler weiter eingrenzen.

Sie können zusätzlich die folgenden zwei Leistungsindikatoren überwachen, um den durch SQL Server-Komponenten erstellten E/A-Umfang zu ermitteln:

- *SQLServer:Buffer Manager:Page reads/sec*
- *SQLServer:Buffer Manager:Page writes/sec*

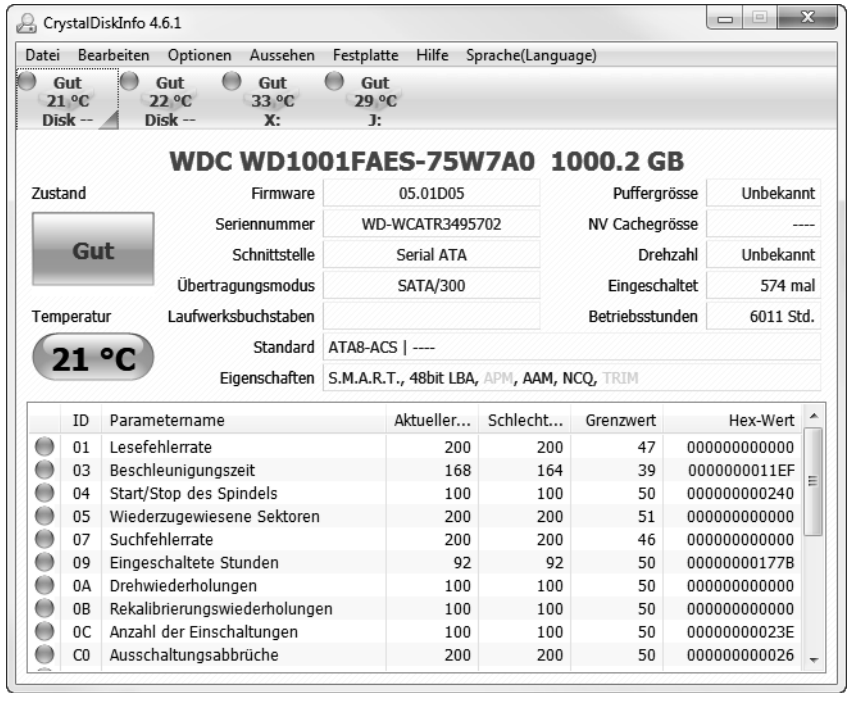
Sie können auch den Datenbankoptimierungsratgeber (DTA) im SQL Server Management Studio oder über die Befehlszeile verwenden, um typische SQL Server-Arbeitsauslastungen zu analysieren.

Zusatztools für Datenträger

Unabhängig davon, ob Sie eine neue Festplatte einbauen oder vorhandene Festplatten testen wollen, ist das Messen der Leistung von Festplatten ein wichtiger Indikator für die Leistung eines Servers und dem Datenbanksystem. In vielen Fällen liegt der Flaschenhals bei langsamen Servern an der Festplatte und den Schreib-/Lesezugriffen. Über kostenlose Tools lassen sich aber recht einfach die Geschwindigkeiten von verschiedenen Festplatten messen.

Ein Tool zum Messen der Leistung von SSD- und herkömmlichen Festplatten ist CrystalDiskInfo von der Seite *http://crystalmark.info/?lang=en* [Ms151-K06-21]. Das Tool gibt es als installierbare Version und auch transportabel für USB-Sticks. Sobald Sie CrystalDiskInfo gestartet haben, sehen Sie auch die Temperatur der Festplatten. Diese sind ein wichtiger Indikator für eine gute Kühlung im Server. Werden die Festplatten bei Beanspruchung zu heiß, können Sie schnell zerstört werden. Das Tool listet außerdem die SMART-Meldungen der installierten Festplatten auf und gibt auch Warnungen aus, wenn eine Festplatte nicht mehr ordnungsgemäß funktioniert.

Abbildg. 6.55 Anzeigen von Informationen zu Festplatten



Über *Optionen/Diagramm* lassen Sie sich grafisch die verschiedenen Daten und den Zustand der Festplatte anzeigen. Über die Oberfläche können Sie sich alle eingebauten Festplatten des Systems anzeigen lassen.

Ein wichtiges Tool, welches Ihnen genau anzeigt, welche Festplatte sich an welchem Controller befindet, ist *DriveControllerInfo* von der Seite *http://download.orbmu2k.de/download.php?id=48* [Ms151-K06-22]. Sie müssen das Tool nicht installieren, sondern können es direkt starten. Nach dem Einlesen der Informationen sehen Sie die wichtigsten Angaben zu den Laufwerken und den geladenen Treibern. Diese Informationen stellen die Grundlage zu Festplattentests dar.

Festplattenaktivität überwachen – DiskMon

Das Sysinternals-Tool DiskMon (*http://technet.microsoft.com/de-de/sysinternals/bb896646* [Ms151-K06-23]) zeigt alle Schreib- und Lesevorgänge der Festplatte in einem Fenster an. Sie sehen auf diese Weise den physischen Zugriff und die aktuellen Vorgänge der Festpatte. Sie sehen die Aktion, Sektor, Zeit, Dauer und auf welcher Festplatte der Computer aktuell etwas schreibt. Sie haben die Möglich-

keit, die Ausgabe auch in eine Protokolldatei zu speichern. Aktivieren Sie die Funktion *Minimize to Tray Disk Light* im Menü *Options*, minimiert sich das Tool direkt in die Taskleiste und zeigt Ihnen die aktuelle Nutzung der Festplatte wie das LED-Symbol an. Auf diese Weise sehen Sie den Festplattenzugriff auf den Server auch in einer Remotesitzung. In der minimierten Ansicht sehen Sie Schreibzugriffe als rote Anzeige und Lesezugriffe in Grün. Klicken Sie auf das Symbol, öffnet sich wieder die ausführliche Ansicht. Wollen Sie das Tool gleich als Symbol starten, verwenden Sie die Option *diskmon /l* (kleines L).

Damit das Tool Daten auslesen kann, müssen Sie es mit Administratorrechten starten, wenn Sie die Benutzerkontensteuerung aktiviert haben. Windows Server 2008 R2, Windows Server 2012 und Windows 7/8 blenden das Symbol nach einiger Zeit aus. Um es dauerhaft einzublenden, klicken Sie in der Taskleiste auf die zwei kleinen Pfeile, um auch die ausgeblendeten Symbole anzuzeigen. Wählen Sie *Anpassen* und dann für das Symbol die Option *Symbol und Benachrichtigungen anzeigen*. Um die Echtzeitanzeige zu deaktivieren, klicken Sie auf die kleine Lupe. Fahren Sie mit der Maus über ein Symbol, erhalten Sie eine kleine Hilfe zur entsprechenden Schaltfläche.

Sie können innerhalb des Capture-Fensters auch nach bestimmten Einträgen suchen. Mit *History Depth* legen Sie die maximale Anzahl an Daten fest, die Sie in der grafischen Oberfläche anzeigen lassen wollen. DiskMon ermöglicht auch den Start mehrerer Instanzen. Lassen Sie das Tool zum Beispiel automatisch als LED minimiert starten, lässt es sich dennoch noch einmal parallel aufrufen, sodass die LED aktiv bleibt, auch wenn Sie mit DiskMon arbeiten.

Leistungsmessung für Profis – Windows Performance Toolkit

Mit dem kostenlosen Windows Performance Toolkit von Microsoft können Sie die Leistung eines Systems sehr effizient messen und Performance-Probleme beheben. Mit dem Toolkit lassen sich Leistungsengpässe messen sowie Startprobleme und Verzögerungen von Anwendungen. Auch die Bootzeit und damit verbundene Verzögerungen können Sie auf diesem Weg überprüfen. Vor allem erfahrene Anwender und Entwickler erhalten mit dem Toolkit auch die Möglichkeit, Ressourcenmessungen von Anwendungen und Interrupts zu messen.

Im Gegensatz zur Windows-internen Leistungsüberwachung arbeitet das Tool nicht mit Indikatoren, die Sie starten müssen, sondern verwendet integrierte Messpunkte. Zusätzlich zu diesem Tool können Sie mit dem ebenfalls kostenlosen *Windows System State Analyzer* Änderungen am System genau überprüfen. Mit den beiden Tools ist eine effiziente Überwachung und Analyse von Servern möglich, die auch Entwicklern dabei hilft, Auswirkungen ihrer Programme auf Windows-Servern zu verstehen. Die beiden Tools erstellen exportierbare Protokolldateien, sodass sich beide auch für das Troubleshooting eignen. Dazu muss der entsprechende Administrator nur die Messung durchführen und diese dem Spezialisten zukommen lassen, der den Fehler analysiert. Auf diesem Weg arbeitet unter anderem auch der Microsoft-Support, um Leistungsprobleme von Kunden feststellen zu können.

Das Windows Performance Toolkit ist Bestandteil des Windows Software Development Toolkit (SDK), welches Sie kostenlos von der Seite *http://msdn.microsoft.com/de-de/performance/cc752957* [Ms151-K06-24] herunterladen können. Sie benötigen für den Betrieb .NET Framework 4, welches Sie über die Seite *http://go.microsoft.com/fwlink/?LinkID=187668* [Ms151-K06-25] erhalten. Wollen Sie Windows 7 oder Windows Server 2008 R2/2012 mit dem Tool messen, benötigen Sie das Windows Performance Toolkit 4.7, welches zum Windows Software Development Toolkit 7.1 gehört. Sie

müssen auf einem Server aber nicht das komplette SDK installieren, sondern können auch einfach aus dem Ordner *Setup\ WinSDKPerformanceToolKit_amd64 (64-Bit)* oder *WinSDKPerformance-ToolKit (32-Bit)* die Installation starten. Die Installation besteht lediglich aus dem Bestätigen einiger Fenster; eine Konfiguration ist nicht notwendig. Das Tool installiert auch keine Treiber oder ständig laufende Hintergrundprozesse. Lediglich die Messungen (Traces) laufen im Hintergrund, wenn Sie diese gestartet haben.

Das Windows Performance Toolkit besteht vor allem aus den drei Tools *Xperf.exe*, *Xperfview.exe* und *Xbootmgr.exe*. Leistungsmessungen nehmen Sie zunächst mit dem Befehlszeilentool *Xperf.exe* vor, indem Sie dem Tool beim Starten verschiedene Optionen mitgeben. Während der Analyse speichert das Tool eine Tracedatei, die Sie später mit *Xperfview.exe* analysieren. Die Analyse selbst findet in einer grafischen Oberfläche statt, die sehr gute Filtermöglichkeiten und Zoomstufen bietet. Mit *Xbootmgr.exe* können Sie wiederum den Bootvorgang des Rechners messen beziehungsweise die Vorgänge nach einem Standby oder dem Ruhezustand. Microsoft stellt dazu auch ein umfangreiches Whitepaper zur Verfügung, welches Sie von der Seite *http://msdn.microsoft.com/en-us/windows/hardware/gg463386.aspx* [Ms151-K06-26] herunterladen können.

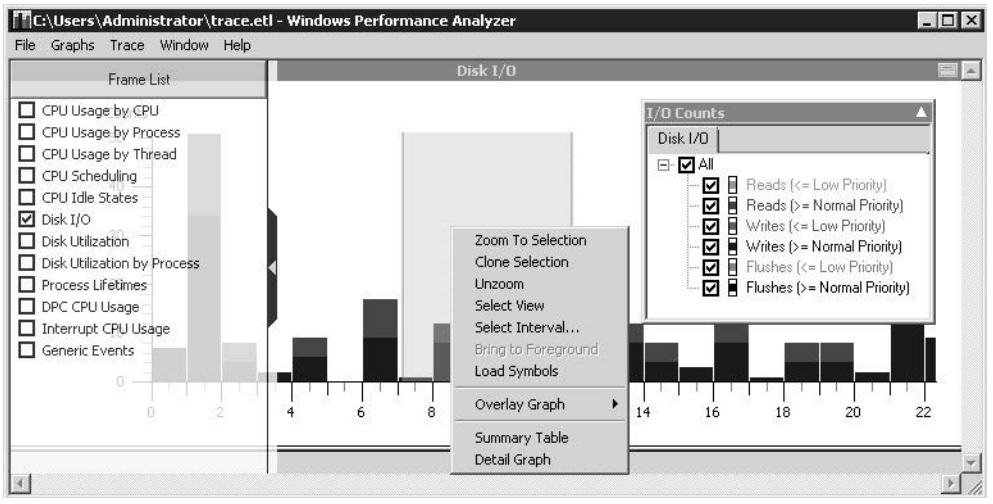
Um Messungen durchzuführen, müssen Sie sich aber nicht erst durch Hunderte Seiten Whitepaper lesen, sondern können nach der Installation schon recht schnell ein Messergebnis erhalten. Haben Sie das Windows SDK mit dem Windows Performance Toolkit installiert, beziehungsweise das WPT alleine, können Sie eine einfache Systemanalyse auf folgendem Weg ausführen:

1. Öffnen Sie eine Eingabeaufforderung mit Administratorrechten.
2. Geben Sie den Befehl *xperf –start –on diageasy* ein. Alternativ reicht auch die Eingabe von *xperf –on diageasy*.
3. Anschließend läuft das Tool im Hintergrund und misst die Systemleistung.
4. Starten Sie die Programme und Tools, deren Leistung Sie messen wollen. Im Hintergrund misst das Tool die Reaktionszeiten des Computers.
5. Haben Sie alle Aufgaben durchgeführt, die Sie in der Messung berücksichtigen wollen, geben Sie den Befehl *xperf –stop* ein, um die Messung zu beenden. Sie können die Messung auch mit *xperf –d trace.etl* beenden und alle Daten in die Datei *trace.etl* übernehmen.

Nach dem Beenden der erhalten Sie die Meldung, dass das Windows Performance Toolkit die Messdatei *C:\kernel.etl* erstellt hat. Beenden Sie mit *xperf –d trace.etl*, liegt die Datei *trace.etl* vor. Um diese zu öffnen, reicht es wenn Sie *xperf trace.etl* eingeben. Reagiert Windows beim Start zum Beispiel zu langsam, haben Sie die Möglichkeit, verschiedene Tracevorgänge zu starten.

Mit *xperf.exe –on –f kernel.etl* starten Sie einen Tracevorgang für den Windows-Basisstart und anschließend mit *xperf.exe –start UserTrace –on Microsoft-Windows-Win32k –f user.etl* einen weiteren Vorgang parallel zum ersten für die Anmeldung und Messung der Benutzeraktionen. Starten Sie Anwendungen, die langsam reagieren und beenden dann die Tracevorgänge mit den Befehlen *xperf.exe –stop UserTrace* und *xperf.exe –stop*. Die beiden gespeicherten *.etl*-Dateien können Sie zusätzlich noch zusammenfügen. Dazu verwenden Sie den Befehl *xperf –merge user.etl kernel.etl <NeueDatei>.etl*. Diese Datei können Sie analysieren, um mit den verschiedenen Mitteln festzustellen, warum der Computer langsam reagiert.

Abbildg. 6.56 Analysieren einer Tracedatei nach der Messung



Wollen Sie zusätzlich noch den Bootvorgang und die damit verbundenen Abläufe messen, verwenden Sie das Tool *xbootmgr.exe*. Geben Sie den Befehl *xbootmgr –trace boot –resultpath c:\temp* in der Befehlszeile an. Anschließend startet das Tool den Computer neu und misst den Bootvorgang. Auch hier speichert das Tool eine *.etl*-Datei direkt im Pfad *C:\temp*. Den Pfad können Sie dabei frei wählen. Sobald der Bootvorgang abgeschlossen ist, stehen die *.etl*-Dateien zur Analyse zur Verfügung. Den Bootvorgang können Sie auch auf Basis verschiedener anderer Optionen messen lassen, abhängig von der Umgebung, die Sie testen lassen wollen. Folgende Beispiele erstellen vernünftige Analysen:

- **Bootvorgang erweitert** *xbootmgr –trace boot –traceFlags BASE+CSWITCH+DRIVERS+POWER –resultPath C:\temp*
- **Herunterfahren** *xbootmgr –trace shutdown –traceFlags BASE+CSWITCH+DRIVERS+POWER –resultPath C:\temp*
- **Standby** *xbootmgr –trace standby –traceFlags BASE+CSWITCH+DRIVERS+POWER –resultPath C:\temp*
- **Start nach Ruhezustand** *xbootmgr –trace hibernate –traceFlags BASE+CSWITCH+DRIVERS+POWER –resultPath C:\temp*

Neben der einfachen Standardanalyse können Sie mit *Xperf.exe* auch erweiterte Messungen durchführen. Alle wichtigen Optionen des Tools lassen Sie sich mit dem Befehl *xperf –help start* anzeigen. Wie Sie Messvorgänge beenden und welche Optionen das Windows Performance Toolkit dafür zur Verfügung stellt, erfahren Sie mit dem Befehl *xperf –help stop*. Für Entwickler und sehr erfahrene Administratoren besteht auch die Möglichkeit, mit *xperf –providers k* eine Liste der Kernel Flags anzuzeigen, die das Tool verwendet. Der erste Ansatz für eine Messung ist immer der Befehl *xperf –start –on diageasy*. Dieser erstellt automatisch die Datei *kernel.etl*. Wollen Sie den Namen und Pfad der Messdatei selbst bestimmen, verwenden Sie noch die Option *–f <Dateiname>*.

Die erstellten Dateien können Sie mit dem Windows Performance Analyzer öffnen, den Sie in der Programmgruppe Windows Performance Toolkit finden. Um die Messungen anzuzeigen, öffnen Sie die Datei *C:\kernel.etl* oder die *.etl*-Datei des Bootvorgangs über *File/Open*. Die Messdateien sind

transportabel. Das heißt Sie können nach der Leistungsmessung durch *Xperf.exe* oder *Xbootmgr.exe* die Analyse mit *Xperfview.exe* auch auf einem anderen Computer durchführen, in dem Sie die *.etl*-Dateien kopieren und öffnen. In manchen Fällen erhalten Sie beim Öffnen eine Fehlermeldung. Öffnen Sie in diesem Fall eine Befehlszeile mit Administratorrechten und geben Sie den Befehl *xperfview <Pfad und Name der Datei> –tti* ein.

Die Anzeige der verschiedenen Bereiche filtern Sie über den Menübereich, den Sie durch Anklicken des linken Teils des Fensters einblenden. Klicken Sie dazu auf das Symbol am linken Rand in der Mitte des Fensters. Ihnen stehen an dieser Stelle die verschiedenen Messbereiche zur Verfügung, die Sie einblenden lassen können. Entfernen Sie das Häkchen bei einem Kontrollkästchen, ist das entsprechende Diagramm im Viewer ebenfalls verschwunden. Auf diese Weise blenden Sie genau die Inhalte ein, die Sie benötigen. Die Anzeige ist dynamisch, das heißt, einmal eingeblendete Diagramme können Sie jederzeit ausblenden und umgekehrt. So müssen Sie nur genau die Daten betrachten, die Sie aktuell analysieren wollen. Lassen Sie sich zum Beispiel beim Messen des Bootvorgangs nur *CPU Usage by Process* anzeigen, sehen Sie, wie viel CPU-Last die einzelnen Prozesse verursachen. Mit *Disk I/O* sehen Sie die Festplattenzugriffe.

Klicken Sie auf die Grafik in einem Diagramm, können Sie zu Teilen der Anzeige heranzoomen. Dazu markieren Sie den Bereich mit der Maus, den Sie zoomen wollen, und klicken diesen mit der rechten Maustaste an. Mit dem Kontextmenübefehl *Zoom to Selection* starten Sie den Zoomvorgang. Neben Grafiken können Sie auch Tabellen erstellen, indem Sie im Kontextmenü die Option *Summary Table* auswählen. In der Tabelle sehen Sie Informationen ähnlich zum Task-Manager über den gemessenen Zeitraum. Sie erkennen auf diese Weise sehr schnell, welche Prozesse zum Beispiel über den Messzeitraum die meiste CPU-Last verursacht haben.

Die Ansicht lässt sich sortieren, indem Sie auf die entsprechende Spalte der Tabelle klicken. Markieren Sie verschiedene Zeilen der Tabelle, können Sie im Kontextmenü durch Auswahl von *Export Selection* die Daten in eine *.csv*-Datei exportieren. Diese können Sie dann später mit Excel weiterbearbeiten. In diesem Zusammenhang ist auch ein weiteres Tool zur Leistungsmessung interessant. Zur Fehlersuche und Analyse reicht es nicht immer aus, die Echtzeitdaten im Task-Manager oder Zusatztools einzulesen. Hier stellt die Excel-Tabelle *Taskmanager.xls* von der Seite *http://blog.didierstevens.com/2011/02/03/taskmanager-xls/* [Ms151-K06-27] eine wertvolle Hilfe dar. Starten Sie die Tabelle in Excel, können Sie einfach die aktuellen Prozesse und deren Daten aus dem Task-Manager in Excel einlesen. In die Tabelle können Sie dann noch die *.csv*-Dateien des Windows Performance Toolkits importieren, zum Beispiel um Vergleiche anzustellen.

Eine weitere Möglichkeit der Analyse ist die Überlagerung von Diagrammen im Fenster des Viewers. Dazu klicken Sie mit der rechten Maustaste in das Diagramm, in welches Sie ein anderes Diagramm überlagern wollen. Wählen Sie im Kontextmenü die Option *Overlay Graph* und die gewünschte Grafik aus, die Sie einblenden wollen. Auf diesem Weg können Sie zum Beispiel im Diagramm für die CPU-Messung, noch das Diagramm der Festplattenbenutzung integrieren. Benötigen Sie noch detaillierte Informationen, können Sie zum Beispiel über das Kontextmenü der Anzeige *Disk I/O oder Disk Utilization* die Option *Detail Graph* auswählen Mit dieser Option zeigen Sie genaue Schreib- und Lesezugriffe während des Messvorgangs an. Diese Daten helfen sehr effizient, um zu verstehen, welche Vorgänge eine Festplatte aktuell belastet haben. Für die Überwachung der Festplattennutzung helfen auch andere Zusatztools von Microsoft ergänzend zum Windows Performance Toolkit. In den meisten Fällen ist es sinnvoll, parallel weitere Tools einzusetzen, um die Messergebnisse besser analysieren zu können.

Mit dem Befehl *xbootmgr –trace boot* messen Sie die Dauer des Bootvorgangs. Wollen Sie die Ergebnisdatei nicht im Ordner des Windows Performance Toolkit ablegen, verwenden Sie den Befehl *xbootmgr –trace boot –resultpath c:\temp*. Anschließend startet Windows sofort neu und das Tool

misst den Bootvorgang. Beenden Sie daher vorher alle Programme, mit denen Sie arbeiten. Nach dem Windows-Start und der Anmeldung eines Benutzers misst das Tool noch zwei Minuten weiter. Führen Sie hier keine Aktionen durch und lassen Sie den PC in Ruhe weiterarbeiten. Nur so ist sichergestellt, dass alle Tools und Treiber erfasst sind.

Unter manchen Umständen erhalten Sie bei der Analyse Fehlermeldungen in der Art *Couldn't find user-mode logger in active logger list*. Diese Fehler lassen sich schwer beheben und liegen meistens an Tools oder Programmen, die sich mit dem Windows Performance Toolkit ins Gehege kommen. Testweise können Sie einen neuen Benutzer anlegen und mit diesem das Tool starten. Funktioniert das nicht, können Sie zur weiteren Analyse nicht das Toolkit verwenden, oder zumindest eingeschränkt beziehungsweise mit etwas Zusatzarbeit. Ist der Bootvorgang abgeschlossen, öffnen Sie noch einmal eine Befehlszeile und wechseln in den Ordner des Windows Performance Toolkit. Geben Sie den Befehl *xbootmgr –remove* ein, ansonsten misst das Tool jeden Bootvorgang.

Führen Sie eine Messung von mehreren Servern mit dem Windows Performance Toolkit durch, ist es auch interessant, zu wissen, wie die Systemkonfiguration des gemessenen Computers ist und zu welchem Computer die Messdatei gehört, die Sie aktuell überprüfen. Diese Informationen speichert das Windows Performance Toolkit ebenfalls in der *.etl*-Datei. Klicken Sie im Viewer auf *Trace/System Configuration*, öffnet sich ein neues Fenster, in dem Sie ausführliche Informationen zum Computer erhalten. Das Fenster zeigt den Namen des Computers, die Domäne, das installierte Betriebssystem, den Versionsstand, die Taktung des Prozessors und die Größe des Arbeitsspeichers an. Auf verschiedenen Registerkarten erhalten Sie weitere Hinweise, deren Informationsgehalt vielen Tools zur Systemanalyse in nichts nachstehen. Auch hier haben Sie durch Markieren und Rechtsklick die Möglichkeit, Daten in *.csv*-Dateien zu exportieren und damit in Excel zu importieren. Auf der Registerkarte *Traces* sehen Sie, wann Sie die Messung genau durchgeführt haben.

In der Befehlszeile aktualisieren Sie die Systemkonfiguration mit dem Befehl *xperf –i trace.etl –a sysconfig*. Mit dem Befehl *systeminfo* in der Befehlszeile zeigen Sie alle Informationen eines Servers in der Eingabeaufforderung an, darunter finden sich Infos über Hotfixes, Netzwerkkarten, Prozessor, Betriebssystem, Hersteller, usw. – sogar die aktuelle Systembetriebszeit (also wie lange der Rechner bereits läuft) und das ursprüngliche Installationsdatum lässt sich anzeigen. Hier empfiehlt sich die Umleitung in eine Textdatei, wobei Sie zusätzlich den Parameter */FO list* angeben sollten, um die Informationen formatiert zu speichern. Um alle Infos in die Textdatei *C:\sysinfo.txt* zu speichern, müssen Sie den Befehl *systeminfo /FO list > C:\sysinfo.txt* verwenden. Diese Datei können Sie anschließend mit der *.etl*-Datei des Windows Performance Toolkits zur Analyse verwenden.

Zusammenfassung

In diesem Kapitel haben wir Ihnen verschiedene Möglichkeiten in SQL Server 2012 zur Überwachung der eigenen Systemleistung aufgezeigt. Wir sind auf SQL-Funktionen wie beispielsweise die Ressourcenverwaltung eingegangen und haben gezeigt, wie die Ablaufverfolgung und der SQL Profiler funktioniert. Auch die Windows-Leistungsüberwachung und die verschiedenen Überwachungsindikatoren von SQL Server 2012 waren Thema dieses Kapitels. Auch über interessante Zusatztools von Sysinternals und anderen Herstellern, um Server und Hardware zu überwachen, haben Sie alles Wissenswerte erfahren.

Im nächsten Kapitel erfahren Sie, wie Sie SQL Server 2012 mit verschiedenen Mitteln hochverfügbar zur Verfügung stellen und die Replikation sowie die Datenbankspiegelung nutzen. Auch Cluster, Hyper-V und die neuen AlwaysOn-Verfügbarkeitsgruppen zeigen wir Ihnen im nächsten Kapitel.