SOPHOS

Security made simple.

Sophos Enterprise Console
Benutzeranleitung zur Überwachung

Produktversion: 5.5

Inhalt

1 Einleitung

Diese Anleitung enthält Informationen zur Nutzung der Überwachungsfunktion in Sophos Enterprise Console, um Änderungen an der Konfiguration von Enterprise Console und sonstige Benutzer- und Systemaktionen zu überwachen. Die Anleitung richtet sich an System- und Datenbankadministratoren.

Es wird davon ausgegangen, dass Sie im Umgang mit Sophos Enterprise Console (SEC) vertraut sind und die Software im Einsatz haben.

Begleitmaterial zu Sophos Software finden Sie hier:
http://www.sophos.com/de-de/support/documentation.

2 Die Überwachungsfunktion von Sophos

Mit der Sophos Überwachung können Sie Änderungen an der Konfiguration von Enterprise Console und sonstige Benutzer- und Systemaktionen überwachen. Die Daten unterstützen Sie beim Nachweis der Einhaltung gesetzlicher Vorschriften sowie zur Problembehebung. Im Falle krimineller Aktivitäten können sie zudem die Ermittlung unterstützen.

Standardmäßig ist die Überwachung deaktiviert. Nach der Aktivierung der Überwachung in Enterprise Console wird ein Überwachungseintrag in der SQL Server-Datenbank „SophosSecurity“ erstellt, wenn Konfigurationseinstellungen geändert oder bestimmte Aktionen durchgeführt werden.

Der Eintrag zur Überwachung enthält folgende Informationen:

- Durchgeführte Aktion
- Benutzer, der die Aktion durchgeführt hat
- Computer des Benutzers
- Teilverwaltungseinheit des Benutzers
- Datum und Uhrzeit der Aktion

Erfolgreiche und fehlgeschlagene Aktionen werden überwacht. Aus den Einträgen geht also hervor, wer die Aktionen durchgeführt bzw. ohne Erfolg gestartet hat.

Zum Zugriff auf die und zur Analyse der in der Überwachungsdatenbank gespeicherten Daten können Sie Programme anderer Anbieter wie Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services oder Crystal Reports verwenden.

Wichtig: Mit der Überwachung von Sophos können Daten von Enterprise Console in Anwendungen anderer Anbieter verfügbar gemacht werden. Wenn Sie die Funktion nutzen, übernehmen Sie die Verantwortung über die Sicherheit der erfassten Daten und müssen sicherstellen, dass nur berechtigte Benutzer darauf zugreifen können. Hinweise zu Sicherheitsfragen finden Sie unter Gewährleisten der Datenbanksicherheit (Seite 6).

Nähere Informationen zu den von der Überwachung erfassten Aktionen finden Sie hier: Welche Aktionen werden überwacht? (Seite 23).

3 Hauptschritte der Überwachung von Sophos

Die Hauptschritte der Überwachung von Sophos lauten:

- Gewährleisten der Datenbanksicherheit
- Aktivieren der Überwachung
- Gewähren von Zugriff auf die Überwachungsdaten
- Erstellen eines Reports zur Überwachung

4 Gewährleisten der Datenbanksicherheit

4.1 Integrierter Datenbankschutz

Folgende Mechanismen zum Schutz der Überwachungsdaten sind in Enterprise Console und die SophosSecurity-Datenbank integriert:

- Zugriffskontrolle
- Manipulationsschutz

Zugriffskontrolle

Die Zugriffskontrolle findet auf folgenden Ebenen statt:

- Benutzeroberfläche (Front-End)

  Nur Benutzer mit der Berechtigung **Überwachung**, die Mitglieder der Gruppe „Sophos Console Administrators“ sind, können die Überwachung aktivieren/deaktivieren.

- Datenbankebene

  Standardmäßig können nur Mitglieder der Gruppe „Sophos DB Admins“ auf die Datenbankschnittstellen zugreifen. Zudem werden gespeicherte Datenbankvorgänge nur mit einem gültigen Token der Benutzersitzung angezeigt. Das Token wird vom System erstellt, wenn ein Benutzer die Benutzeroberfläche öffnet oder Änderungen an der Teilverwaltungseinheit vornimmt.

Manipulationsschutz

Die Datenbank ist so konzipiert, dass die Ereignisdaten der Überwachung nicht manipuliert werden können. Daten in der Überwachungsdatenbank müssen mit Ausnahme bestimmter Konfigurationseinstellungen nicht aktualisiert werden. Bestimmte Auslöser sorgen dafür, dass Versuche, Daten aus den Tabellen zu aktualisieren bzw. zu löschen, rückgängig gemacht werden.

Die Daten lassen sich nur durch endgültiges Entfernen löschen. Mehr als zwei Jahre alte Daten werden alle 24 Stunden im Rahmen der eingebetteten Standard-Löschaufgabe auf dem Enterprise Console-Server automatisch gelöscht. Zum endgültigen Entfernen der Daten können Sie auch das PurgeDB-Tool verwenden (siehe http://www.sophos.com/de-de/support/knowledgebase/109884.aspx).

4.2 Erhöhen der Datenbanksicherheit

Überwachen der Datenbank

Es empfiehlt sich, weiteren Schutz auf der Ebene der SQL Server-Instanz einzurichten (sofern noch nicht vorhanden), um Benutzeraktivitäten am SQL-Server überwachen zu können.

Wenn Sie beispielsweise eine Enterprise-Edition von SQL Server 2008 nutzen, können Sie die Überwachungsfunktion von SQL Server nutzen. In früheren Versionen von SQL Server sind zudem eine Anmeldungsüberwachung, eine durch bestimmte Ereignisse ausgelöste Überwachung sowie eine Ereignisüberwachung mit integrierter Nachverfolgungsfunktion möglich.

Nähere Informationen zu den Funktionen der Überwachung und Änderungen des SQL Server-Systems entnehmen Sie bitte der Dokumentation zu Ihrer SQL Server-Version. Beispiel:

- SQL Server Audit (Datenbankmodul)
- Überwachung (Datenbankmodul), SQL Server 2008 R2
- Überwachung in SQL Server 2008
- Überwachung (Datenbankmodul), SQL Server 2008

Verschlüsseln von Datenbankverbindungen

Es empfiehlt sich, Verbindungen zwischen Clients und den Enterprise Console-Datenbanken zu verschlüsseln. Nähere Informationen entnehmen Sie bitte der Dokumentation zu SQL Server:

- Aktivieren von verschlüsselten Verbindungen zum Datenbankmodul (SQL Server-Konfigurations-Manager)
- Verschlüsselung von Verbindungen zu SQL Server 2008 R2
- Anweisungen zur Aktivierung von SSL-Verschlüsselung für eine SQL Server-Instanz mit Microsoft Management Console

Steuerung des Zugriffs auf die Datenbank-Backups

Sorgen Sie dafür, dass eine ordnungsgemäße Zugriffskontrolle auf Datenbanksicherungen bzw. -kopien festgelegt wird. So wird verhindert, dass nicht autorisierte Benutzer auf Dateien zugreifen, diese manipulieren oder versehentlich löschen können.

Hinweis: Über die Links in diesem Abschnitt gelangen Sie zu Informationen, die von Drittparteien gepflegt und zu Referenzzwecken bereitgestellt werden. Wir überprüfen die verlinkten Seiten zwar in regelmäßigen Abständen auf ihre Richtigkeit, es ist jedoch nicht auszuschließen, dass ohne unser Wissen Änderungen daran vorgenommen werden.

5 Aktivieren der Überwachungsfunktion von Sophos

Standardmäßig ist die Überwachung deaktiviert. So aktivieren Sie die Überwachung:

1. Klicken Sie in Enterprise Console im Menü **Extras** auf **Überwachung verwalten**.
2. Aktivieren Sie im Dialogfeld **Überwachung verwalten** das Kontrollkästchen **Überwachung aktivieren**.

   Hinweis: Wenn die Option nicht hinterlegt ist, sind Sie nicht zur Nutzung der Überwachung berechtigt. Sie müssen ein Mitglied der Gruppe „Sophos Console Administrators“ sein und in Enterprise Console über die Berechtigung **Überwachung** verfügen, um die Überwachung in Enterprise Console zu aktivieren/deaktivieren. Anweisungen zu Benutzerrechten und der rollenbasierten Verwaltung entnehmen Sie bitte der *Hilfe zu Sophos Enterprise Console*.

6 Gewähren von Zugriff auf die Überwachungsdaten

Standardmäßig können nur Systemadministratoren auf die Daten der Überwachung zugreifen. Anderen Benutzern, die zur Erstellung von Reports auf die Daten zugreifen müssen, muss ausdrücklich das Recht „Select“ am Schema **Reports** in der Datenbank „SophosSecurity“ gewährt werden. Hierzu können Sie das Tool **sqlcmd** oder SQL Server Management Studio verwenden.

6.1 Gewähren von Zugriff auf die Überwachungsdaten mit dem Tool „sqlcmd“

So gewähren Sie Zugriff auf die Überwachungsdaten:

1. Kopieren Sie den folgenden Ausschnitt in ein Dokument, z.B. eine Editordatei.

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* Ersetzen Sie dabei <Domain>\<User> durch den Namen des Kontos,
 dem Zugriff auf die Überwachungsdaten gewährt werden soll. */


SET @Account = N'<Domain>\<User>'

IF NOT EXISTS( SELECT * FROM sys.server_principals WHERE name =
@Account )
BEGIN
     SET @stmt = N'CREATE LOGIN [' + @Account + N'] FROM WINDOWS';

      EXEC sp_executesql @stmt;
END;

IF NOT EXISTS( SELECT * FROM sys.database_principals WHERE name
= @Account )
BEGIN
      SET @stmt = N'CREATE USER [' + @Account + N'] FOR LOGIN ['
 + @Account + N']';
      EXEC sp_executesql @stmt;
END;

SET @stmt = N'GRANT SELECT ON SCHEMA :: [Reports] TO [' + @Account
 + N']';
EXEC sp_executesql @stmt;
GO
```

2. Ersetzen Sie die Platzhalter <Domain> und <User> im Bereich „SET @Account = N'<Domain>\<User>'“ durch die Domäne und den Benutzernamen des Benutzers, dem Zugriff gewährt werden soll.

   Wenn sich die Computer in einer Arbeitsgruppe befinden, ersetzen Sie <Domain> durch den Namen des Computers, auf dem die Datenbank installiert ist. Wenn der Benutzer von einem anderen Computer in der Arbeitsgruppe auf die Daten zugreift, muss das Benutzerkonto mit identischem Benutzernamen und Kennwort auf beiden Computern vorhanden sein.

3. Öffnen Sie die Befehlszeile.
4. Stellen Sie eine Verbindung zur SQL Server-Instanz her. Geben Sie Folgendes ein:

   ```
   sqlcmd -E -S <Server>\<SQL Server instance>
   ```

   SOPHOS ist die Standardinstanz von SQL Server.

5. Kopieren Sie den Skriptausschnitt aus der Datei und fügen Sie ihn in die Befehlszeile ein.
6. Drücken Sie zum Ausführen des Skripts die Eingabetaste.

   Nach dem Ausführen des Skripts verfügt der Benutzer über die Berechtigung „Select“ am Schema **Reports** und kann auf die Daten der Überwachung zugreifen.

7. Wiederholen Sie die Schritte für alle Benutzer, die Zugriff benötigen.

6.2 Gewähren von Zugriff auf die Überwachungsdaten mit SQL Server Management Studio

Sie müssen zunächst sicherstellen, dass der Benutzer sich bei SQL Server anmelden kann und Benutzer der SophosSecurity-Datenbank ist, bevor Sie die Berechtigung „Select“ am Schema **Reports** in der SophosSecurity-Datenbank einem Benutzer in SQL Server Management Studio zuweisen können.

- Wenn der Benutzer bereits über SQL Server-Zugangsdaten verfügt, fügen Sie ihn als Datenbankbenutzer der SophosSecurity-Datenbank hinzu. Erweitern Sie den Server im Objekt-Explorer und erweitern Sie den Ordner **Datenbanken** > **SophosSecurity** und anschließend **Sicherheit**. Rechtsklicken Sie auf **Benutzer** und klicken Sie auf **Neuer Benutzer**. Geben Sie in das Dialogfeld **Datenbankbenutzer** den Benutzernamen ein und wählen Sie den Anmeldenamen aus. Klicken Sie auf **OK**.

  Nähere Informationen zum Erstellen von Datenbankbenutzern finden Sie unter http://msdn.microsoft.com/de-de/library/aa337545.aspx#SSMSProcedure.

- Wenn der Benutzer nicht über Zugangsdaten für SQL Server verfügt, erstellen Sie einen neuen Benutzer, der SophosSecurity-Datenbankbenutzer ist. Erweitern Sie den Server im Objekt-Explorer und erweitern Sie **Security**. Rechtsklicken Sie auf **Anmeldungen** und klicken Sie auf **Neue Anmeldung**. Geben Sie im Dialogfeld **Anmeldung** auf der Seite **Allgemein** den Konto- oder Gruppennamen ein. Rufen Sie die Seite **Benutzerzuordnung** auf und wählen Sie **SophosSecurity** aus. Klicken Sie auf **OK**.

  Nähere Informationen zum Erstellen von SQL Server-Anmeldungen finden Sie unter http://msdn.microsoft.com/en-us/library/aa337562.aspx#SSMSProcedure.

Verwahren Sie zum Gewähren von Zugriff auf die Überwachungsdaten mit SQL Server Management Studio wie folgt:

1. Erweitern Sie den Server im Objekt-Explorer und erweitern Sie den Ordner **Datenbanken** > **SophosSecurity** und anschließend **Sicherheit** > **Schemas**.
2. Rechtsklicken Sie auf **Berichte** und klicken Sie auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Schemaeigenschaften – Berichte** auf der Seite **Berechtigungen** auf **Suchen**. Fügen Sie im Dialogfeld **Benutzer oder Rollen auswählen** einen oder mehrere Benutzer hinzu.
4. Klicken Sie für alle Benutzer unter **Berechtigungen für <Benutzer>** auf die Registerkarte **Ausdrücklich**, wählen Sie unter **Erteilen** die Option **SELECT** aus und klicken Sie anschließend auf **OK**.

7 Erstellen eines Reports zur Überwachung in Microsoft Excel

In diesem Beispiel wird erläutert, wie Sie Daten zur Überwachung von der SQL Server-Datenbank importieren und in Microsoft Excel 2010 analysieren können.

Die folgenden Abschnitte bieten Anweisungen zur Erstellung eines Reports zur Überwachung in Microsoft Excel anhand der folgenden Schritte:

- Herstellen einer Verbindung zur Datenbank (Erstellen einer neuen Datenquelle).
- Erstellen einer Abfrage in Microsoft Query.
- Rückgabe der Daten an Excel.
- Erstellen eines Reports in Excel (als Tabelle oder PivotTable).

Hinweis: Wenn Sie die exportierten Überwachungsdaten mit einer externen Logik kombinieren möchten, sind numerische Kennungen Zeichenketten vorzuziehen. Verwenden Sie also beispielsweise die Werte aus dem Feld **TargetTypeId** und nicht aus dem Feld **TargetType**. So können Sie mögliche Kompatibilitätsprobleme vermeiden, wenn sich Zeichenfolgen in späteren Versionen von Enterprise Console ändern. Eine Tabelle numerischer Kennungen finden Sie unter Anhang: Numerische Kennungen der Datenfeldwerte (Seite 31).

Nähere Informationen zum Import der SQL Server-Daten sowie zur Erstellung von Reports in Excel entnehmen Sie bitte der Microsoft Dokumentation.

7.1 Herstellen einer Verbindung zur Datenbank

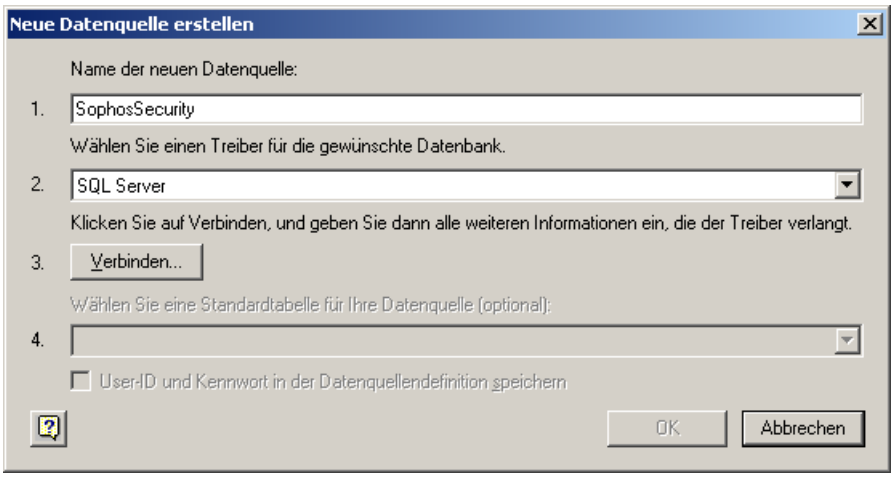
Zunächst müssen Sie eine Verbindung zur Datenbank herstellen.

1. Öffnen Sie Excel. Klicken Sie auf der Registerkarte **Daten** in der Gruppe **Externe Daten** auf **Aus anderen Quellen** und klicken Sie anschließend auf **Von Microsoft Query**.

   Das Dialogfenster **Datenquelle auswählen** wird angezeigt.

2. Auf der Registerkarte **Datenbanken** muss **<Neue Datenbankquelle>** ausgewählt sein. Klicken Sie auf „OK“.
3. Geben Sie im Dialogfeld **Neue Datenquelle erstellen** den gewünschten Namen für Ihre Datenquelle an. Im vorliegenden Beispiel lautet der Name **SophosAuditing**.

4. Wählen Sie im Feld **Treiber für den Datenbanktyp auswählen, auf den Sie zugreifen möchten** die Option **SQL Server**.

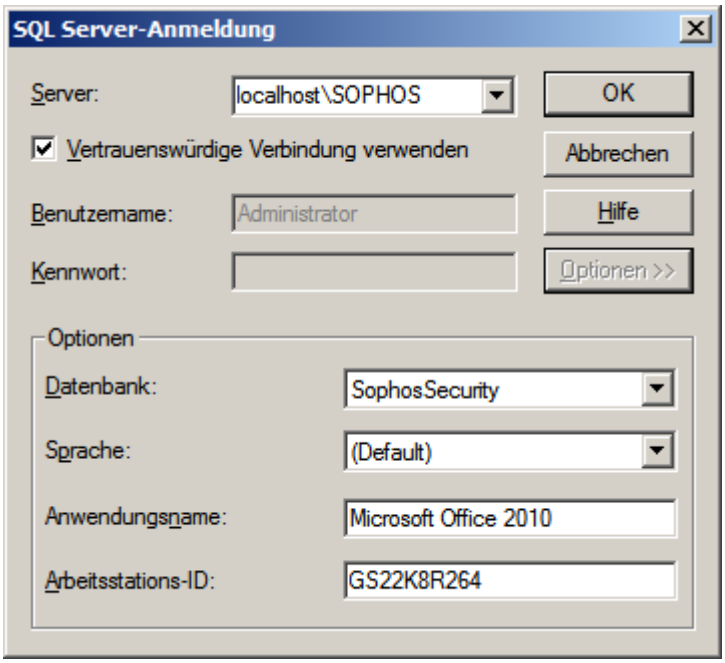


   Klicken Sie auf **Verbinden**.

5. Geben Sie im Dialogfeld **SQL Server-Anmeldung** im Feld **Server** den Namen des SQL-Servers ein, zu dem eine Verbindung hergestellt werden soll.

   Im vorliegenden Beispiel stellen wir eine Verbindung zur SOPHOS-Datenbankinstanz auf dem gleichen Computer (Localhost) her.

6. Klicken Sie auf **Optionen**, um das Feld **Optionen** zu erweitern. Wählen Sie im Feld **Datenbank** die Option **SophosSecurity**.



   Klicken Sie auf **OK**.

7. Wählen Sie im Dialogfeld **Neue Datenquelle erstellen** unter **Standardtabelle für Ihre Datenquelle auswählen (optional)** die Option **vAuditEventsAll**.

   Klicken Sie auf **OK**.

7.2 Erstellen einer Abfrage

In diesem Beispiel wird gezeigt, wie Sie über die soeben erstellte Datenquelle Informationen zu Änderungen an den Data Control-Richtlinien in den letzten drei Monaten abfragen können.

1. Deaktivieren Sie im Dialogfeld **Datenquelle auswählen** die Option **Query-Assistenten zur Erstellung/Bearbeitung von Abfragen verwenden**.
2. Wählen Sie die in den vorangegangen Schritten erstellte Datenquelle (im vorliegenden Beispiel **SophosAuditing**) aus und klicken Sie auf **OK**.

   Im Dialogfeld **Microsoft Query** wird **Abfrage von SophosAuditing** mit der Standardtabelle **vAuditEventsAll** angezeigt, die beim Erstellen der Datenquelle ausgewählt wurde.

3. Führen Sie einen der folgenden Schritte aus:
   - Erstellen Sie eine Abfrage in der Designansicht.
     1. Klicken Sie im Dialogfeld **Microsoft Query** im Menü **Kriterien** auf **Kriterien hinzufügen**.
     2. Wählen Sie im Dialogfeld **Kriterien hinzufügen** neben **Feld** die Option **Zeitstempel** aus. Lassen Sie das Feld **Operator** leer. Geben Sie in das Feld **Wert** Folgendes ein:

        `>=DATEADD(mm,-3,GETUTCDATE())`

        Verwenden Sie das in der Systemsteuerung in den „Region- und Spracheinstellungen“ festgelegte Listentrennzeichen. Wenn es sich bei dem Trennzeichen etwa um einen Strichpunkt handelt, verwenden Sie bei der Anweisung oben Strichpunkte statt Kommas. Bei Verwendung des falschen Listentrennzeichens wird unter Umständen eine Fehlermeldung „Extra“ angezeigt.

        Klicken Sie auf **Hinzufügen**. Das Kriterium wird zur **Abfrage von SophosAuditing** hinzugefügt.

     3. Wählen Sie im Dialogfeld **Kriterien hinzufügen** neben **Feld** die Option **TargetType** aus. Wählen Sie im Feld **Operator** die Option **ist gleich** aus. Wählen Sie im Feld **Wert** die Option **Policy** aus oder geben Sie sie ein.

        Klicken Sie auf **Hinzufügen**. Das Kriterium wird zur **Abfrage von SophosAuditing** hinzugefügt.

     4. Wählen Sie im Dialogfeld **Kriterien hinzufügen** neben **Feld** die Option **TargetSubType** aus. Wählen Sie im Feld **Operator** die Option **ist gleich** aus. Wählen Sie im Feld **Wert** die Option **Data Control** aus oder geben Sie sie ein.

        Klicken Sie auf **Hinzufügen**. Das Kriterium wird zur **Abfrage von SophosAuditing** hinzugefügt.

        Klicken Sie im Dialogfeld **Kriterien hinzufügen** auf **Schließen**.

     5. Fügen Sie im Dialogfeld **Microsoft Query** die Felder von **vAuditEventsAll** per Doppelklick zur Abfrage hinzu. Sie können jedoch auch ein Feld zur Abfrage hinzufügen, indem Sie es von der Tabelle in den Anzeigebereich ziehen.

- Erstellen Sie eine Abfrage in der SQL-Ansicht.
  1. Klicken Sie in **Microsoft Query** auf die Schaltfläche **SQL** und geben Sie Ihre SQL-Anweisung ein. Beispiel:

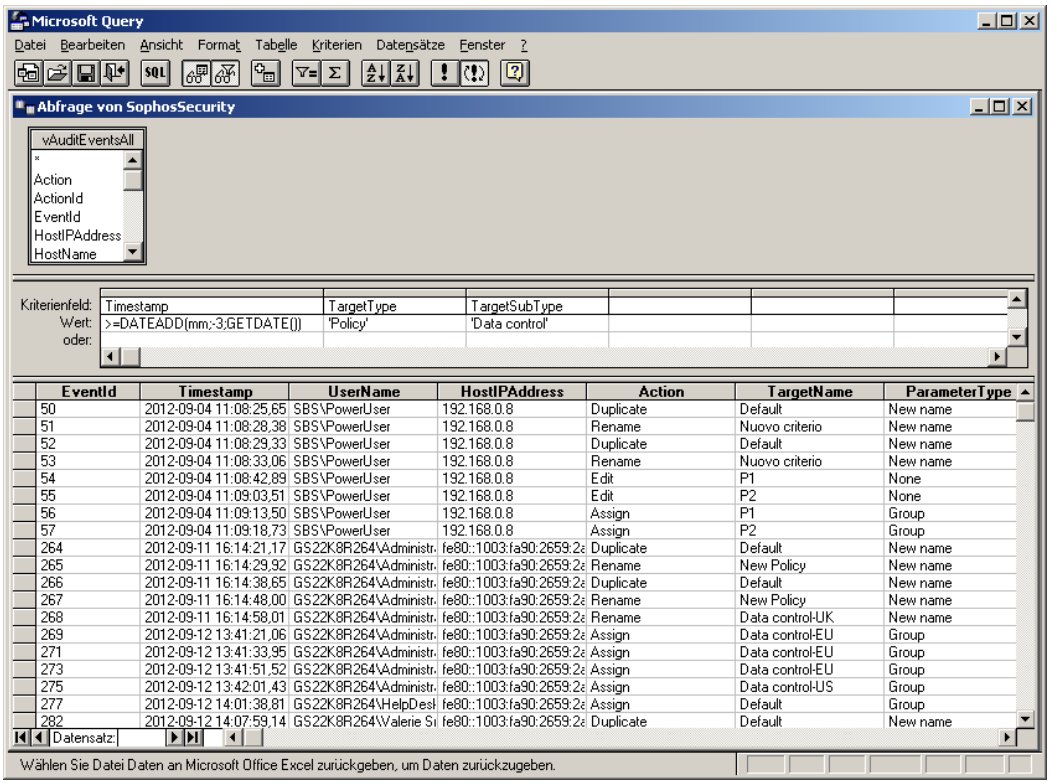
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action,
 TargetName, ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (TargetType='Policy')
AND (TargetSubType='Data control')

ORDER BY EventId ASC
```

     Klicken Sie auf **OK**.



4. Klicken Sie zum Speichern der Abfrage im Menü **Datei** auf **Speichern**.

7.3 Rückgabe der Daten an Excel

1. Um zu Excel zurückzukehren, klicken Sie im Dialogfeld **Microsoft Query** auf die Schaltfläche **Daten zurückgeben**.

   Sie können jedoch auch im Menü **Datei** auf **Daten an Microsoft Excel zurückgeben** klicken.

   In Excel wird das Dialogfeld **Daten importieren** angezeigt. Hier können Sie angeben, welchen Report-Typ Sie erstellen möchten.

   Die folgenden Beispiele bieten Anweisungen zum:

   - Erstellen einer Tabelle (Seite 16)
   - Erstellen eines PivotTable-Reports (Seite 17)

7.4 Erstellen einer Tabelle

1. Wenn Sie die Überwachungsdaten in eine Exceltabelle importieren möchten, muss im Dialogfeld **Daten importieren** die Option **Tabelle** ausgewählt sein.

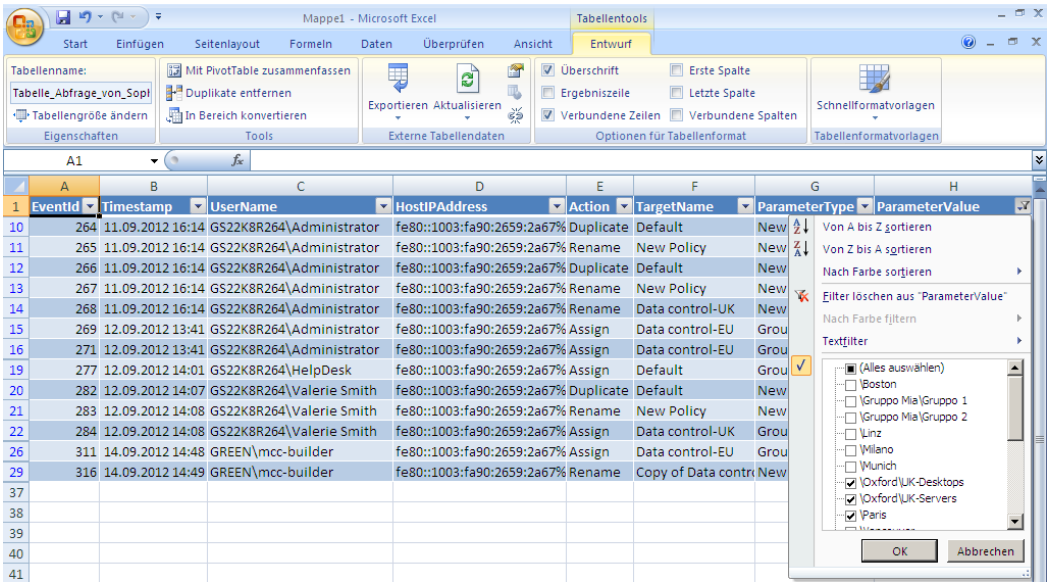
   Wenn Sie die Daten in ein vorhandenes Arbeitsblatt einfügen möchten (angefangen bei Zelle A1), muss die Option **Vorhandenes Arbeitsblatt** ausgewählt sein.

   Klicken Sie auf **OK**.

   Die Daten der Überwachung werden in eine Exceltabelle importiert.

2. Speichern Sie das Arbeitsblatt in Excel.

3. Sie können Ihre Daten mit dem Suchfilter analysieren.



7.5 Erstellen eines PivotTable-Reports

1. Wenn Sie die Überwachungsdaten in eine Excel-Tabelle importieren möchten, muss im Dialogfeld **Daten importieren** die Option **PivotTable-Bericht** ausgewählt sein.

   Wenn Sie die Daten in ein vorhandenes Arbeitsblatt einfügen möchten (angefangen bei Zelle A1), muss die Option **Vorhandenes Arbeitsblatt** ausgewählt sein.

   Klicken Sie auf **OK**.

   Die daraus resultierende leere PivotTable wird im Arbeitsblatt angezeigt.

2. Wählen Sie in der **PivotTable-Feldliste** auf der rechten Seite die anzuzeigenden Felder aus.

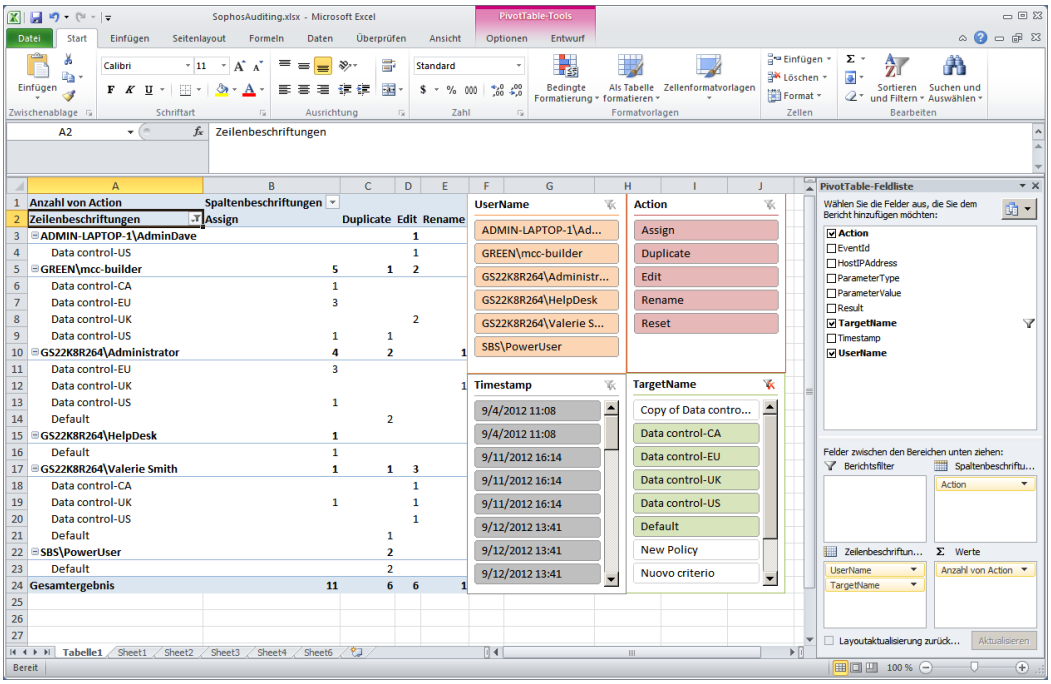
   Tipp: Vor dem Hinzufügen von Feldern können Sie die Daten filtern. Richten Sie den Mauszeiger unter **PivotTable-Feldliste** auf die Option **Wählen Sie die Felder aus, die Sie dem Bericht hinzufügen möchten:** und klicken Sie auf den Dropdown-Pfeil neben dem Feldnamen. Wählen Sie im Menü **Filter** die gewünschten Filteroptionen aus.

3. Je nach gewünschter Anzeige der PivotTable ziehen Sie die Felder zwischen die Bereiche **PivotTable-Feldliste**. So können beispielsweise die Namen der Benutzer sowie der von ihnen aufgerufenen Richtlinien als Zeilenbeschriftung und die von den Benutzern an den Richtlinien durchgeführten Aktionen als Spaltenbeschriftung angezeigt werden.

4. Um die PivotTable filtern zu können, klicken Sie unter **PivotTable-Tools** unter **Optionen** auf **Datenschnitt einfügen**.
5. Wählen Sie im Dialogfeld **Datenschnitt einfügen** den gewünschten Datenschnitt aus, und klicken Sie auf **OK**.

   Sie können die Datenschnitte auf dem Arbeitsblatt anders anordnen, indem Sie einen Datenschnitt auswählen und ihn per Drag & Drop in die gewünschte Position bringen. Sie können die Datenschnitte auch benutzerdefiniert gestalten, indem Sie ihnen etwa unterschiedliche Farben zuweisen. Wählen Sie hierzu einen Datenschnitt aus. Wählen Sie unter **Datenschnitttools** > **Optionen** ein **Datenschnittformat** aus.

   Ihre PivotTable sieht in etwa wie folgt aus:



6. Speichern Sie das Arbeitsblatt.

8 Weitere Beispiele zur Erstellung eines Reports zur Überwachung

In diesem Abschnitt wird erläutert, wie Sie eine neue Abfrage einer vorhandenen Datenquelle in Microsoft Excel durchführen können, und Sie finden weitere beispielhafte Abfragen zur Erstellung von Reports zur Überwachung.

Zudem bietet der Abschnitt Anweisungen zur Erstellung eines Reports mit detaillierten Richtlinienänderungen im XML-Format.

8.1 Erstellen einer Abfrage von einer vorhandenen Datenquelle

Verfahren Sie wie folgt, um einen weiteren Report zur Überwachung aus der unter Herstellen einer Verbindung zur Datenbank (Seite 12) erstellten Datenquelle zu erstellen:

1. Rufen Sie in Excel die Registerkarte **Daten** auf, klicken Sie auf **Aus anderen Quellen** und klicken Sie anschließend auf **Aus Microsoft Query**.
2. Deaktivieren Sie im Dialogfeld **Datenquelle auswählen** die Option **Query-Assistenten zur Erstellung/Bearbeitung von Abfragen verwenden**. Wählen Sie die im Vorfeld erstellte Datenquelle aus (z.B. SophosAuditing) und klicken Sie auf **OK**.
3. Klicken Sie in **Microsoft Query** auf die Schaltfläche **SQL** und geben Sie Ihre SQL-Anweisung ein.

Im folgenden Abschnitt finden Sie einige Beispiele.

8.2 Weitere Beispielabfragen

Beispiel 1: Von einem Benutzer in den letzten 60 Tagen geänderte Richtlinien

```
SELECT EventId, Timestamp, TargetSubType, Action, TargetName,
ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(dd,-60,GETUTCDATE()))
AND (TargetType='Policy')
AND (UserName='GS22K8R264\Administrator')

ORDER BY Timestamp DESC
```

Hinweis: Sie können in einer Anweisung „SELECT *“ angeben, um alle Felder in der Datenbankansicht auszuwählen, anstatt die in den Report einzubeziehenden Felder auszuwählen.

Beispiel 2: In den letzten 6 Monaten einer bestimmten Gruppe zugewiesene Richtlinien

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-6,GETUTCDATE()))
AND (TargetType='Policy')
AND (Action='Assign')
AND (ParameterType='Group')
AND (ParameterValue='\Oxford\UK-Servers')

ORDER BY EventId DESC
```

Hinweis: Wenn es sich bei der Gruppe, zu der der Report erstellt werden soll, um eine Untergruppe einer anderen Gruppe handelt, müssen Sie entweder den vollständigen Pfad der Gruppe angeben oder die Anweisung „ends with“ verwenden (sofern der Name der Gruppe nicht mehrfach vergeben wurde). Wenn Sie beispielsweise einen Report für die Gruppe „\Oxford\UK-Servers“ erstellen möchten, können Sie eine der folgenden Optionen eingeben:

- **`ParameterValue='\Oxford\UK-Servers'`**
- **`ParameterValue Like '%UK-Servers'`**

Beispiel 3: Von einer bestimmten Person in den letzten drei Monaten vorgenommene Gruppenänderungen

Das Ergebnis der folgenden Anweisung ist ein Report, aus dem alle Gruppen hervorgehen, die erstellt, gelöscht, verschoben oder umbenannt wurden. Zudem wird angezeigt, welche Computer der Benutzer in den letzten drei Monaten Gruppen zugewiesen hat.

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (UserName='GS22K8R264\Administrator')
AND ((TargetType='Group') OR ((TargetType='Computer') AND
(Action='Assign')))
```

Beispiel 4: An einer bestimmten Gruppe in den letzten drei Monaten vorgenommene Änderungen

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (ParameterValue='\Oxford\UK-Desktops')
```

8.3 Rückgabe der Daten an Excel

Nach der Erstellung einer Abfrage für den Bericht zur Überwachung können Sie die Daten an Excel zurückgeben (**Datei** > **Daten an Microsoft Excel zurückgeben**) und anhand der Anweisungen in den Abschnitten Erstellen einer Tabelle (Seite 16) bzw. Erstellen eines PivotTable-Reports (Seite 17) entnehmen.

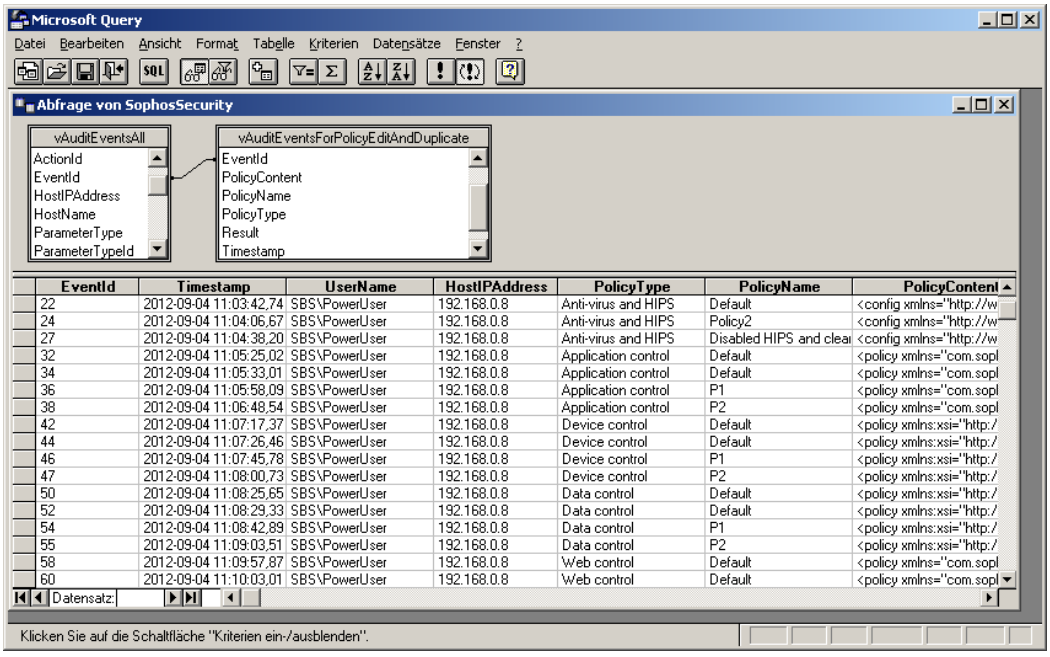
8.4 Erstellen eines Reports mit Richtlinienänderungen im XML-Format

Wenn ein Benutzer eine Richtlinie bearbeitet, werden die Richtlinienänderungen im XML-Format gespeichert und können über die Datenbankansicht **Reports.vAuditEventsForPolicyEditAndDuplicate** abgerufen werden.

Sie können einen Report der zusätzlichen Daten durch Verlinken der beiden Tabellen **Reports.vAuditEventsAll** und **Reports.vAuditEventsForPolicyEditAndDuplicate** erstellen.

1. Erstellen Sie eine neue Abfrage aus einer vorhandenen Datenquelle, wie unter Erstellen einer Abfrage von einer vorhandenen Datenquelle (Seite 19) beschrieben.
2. Klicken Sie in **Microsoft Query** auf **Tabelle** und klicken Sie anschließend auf **Tabellen hinzufügen**. Wählen Sie im Dialogfeld **Tabellen hinzufügen** die Option **vAuditEventsForPolicyEditAndDuplicate** aus und klicken Sie auf **Hinzufügen**. Klicken Sie anschließend auf **Schließen**.
3. Verlinken Sie die Tabellen miteinander, indem Sie Felder verbinden, die beiden Tabellen angehören. Klicken Sie auf das gemeinsame Feld **EventID** in der ersten Tabelle und ziehen Sie die Maus über das Feld **EventID** in der zweiten Tabelle.
4. Fügen Sie Felder zur Abfrage per Doppelklick auf die Felder hinzu. Sie können jedoch auch ein Feld zur Abfrage hinzufügen, indem Sie es von der Tabelle in den Anzeigebereich ziehen.

   Tipp: Über das Dialogfeld **Verknüpfungen** in Microsoft Query (**Tabelle** > **Verknüpfungen**) können Sie eine Abfrage erstellen, bei der die beiden Tabellen zusammengeführt werden.



5. Klicken Sie zum Speichern der Abfrage im Menü **Datei** auf **Speichern**.
6. Kehren Sie zu Excel zurück und klicken Sie auf die Schaltfläche **Daten zurückgeben**.

Sie können jedoch auch im Menü **Datei** auf **Daten an Microsoft Excel zurückgeben** klicken.

In Excel wird das Dialogfeld **Daten importieren** angezeigt. Erstellen Sie eine Tabelle (Erstellen einer Tabelle (Seite 16)). In der Spalte **PolicyContent** finden Sie die Richtlinienkonfigurationsänderungen im XML-Format.

Tipp: Wenn Sie Microsoft SQL Server Management Studio nutzen, können Sie die Ansicht **Reports.vAuditEventsForPolicyEditAndDuplicate** direkt abfragen. Wenn Sie auf einen Link in der Spalte **PolicyContent** in den Abfrageergebnissen klicken, wird der Richtlinieninhalt in einem XML-Editor angezeigt. Daten in diesem Format lassen sich einfacher lesen als in einer Excel-Tabelle.

9 Welche Aktionen werden überwacht?

Unter anderem werden folgende Aktionskategorien überwacht:

- Computeraktionen
- Computergruppenverwaltung
- Richtlinienverwaltung
- Rollenverwaltung
- Management von Sophos Update Manager
- Systemereignisse

9.1 Computeraktionen

Die folgenden Computeraktionen werden überwacht:

- Löschen/Beheben von Alerts und Fehlern
- Schützen eines Computers
- Updaten eines Computers
- Löschen eines Computers
- Durchführen einer vollständigen Systemüberprüfung eines Computers

9.2 Computergruppenverwaltung

Folgende Aktionen werden für die Gruppenverwaltung protokolliert:

- Erstellen einer Gruppe
- Löschen einer Gruppe
- Verschieben einer Gruppe
- Umbenennen einer Gruppe
- Zuweisen eines Computers zu einer Gruppe

9.3 Richtlinienverwaltung

Folgende Aktionen werden für die Richtlinienverwaltung protokolliert:

- Erstellen einer Richtlinie (Seite 24)
- Umbenennen einer Richtlinie
- Duplizieren einer Richtlinie (Seite 24)
- Ändern einer Richtlinie
- Übertragen einer Richtlinie auf einen Computer
- Zurücksetzen der Richtlinie auf Werkseinstellungen

- Löschen einer Richtlinie (Seite 24)

9.3.1 Erstellen einer Richtlinie

Beim Erstellen einer neuen Richtlinie wird die Standardrichtlinie in eine neue Richtlinie mit der Bezeichnung „New Policy“ dupliziert. Sie können die neue Richtlinie unmittelbar nach der Erstellung umbenennen. Wenn beispielsweise eine neue Antivirus- und HIPS-Richtlinie erstellt und in „Servers“ umbenannt wurde, werden folgende Einträge zur Überwachung erstellt:

Tabelle 1: Erstellen einer neuen Richtlinie und Vergabe eines neuen Namens

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Anti-virus and HIPS	Default	New name	New Policy	Success
Rename	Policy	Anti-virus and HIPS	New Policy	New name	Servers	Success

9.3.2 Duplizieren einer Richtlinie

Wenn Sie eine Richtlinie duplizieren, wird ein Ereignis hierzu erstellt. Beispiel:

Tabelle 2: Duplizieren einer Richtlinie

Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
Duplicate	Policy	Web Control	TestPolicy1	New name	Copy of TestPolicy1	Success

9.3.3 Löschen einer Richtlinie

Beim Löschen einer Richtlinie werden alle Gruppen, die die gelöschte Richtlinie verwenden, auf die Standardrichtlinie zurückgesetzt. In diesem Fall wird kein gesondertes Überwachungsereignis erstellt, das anzeigt, dass die Standardrichtlinie wieder zugewiesen wurde.

9.4 Rollenverwaltung

Folgende Aktionen werden für die Rollenverwaltung protokolliert:

- Erstellen einer Rolle
- Löschen einer Rolle
- Umbenennen einer Rolle

- Duplizieren einer Rolle
- Hinzufügen von Benutzern zu einer Rolle
- Entfernen eines Benutzers von einer Rolle
- Hinzufügen eines Rechts zu einer Rolle
- Entfernen eines Rechts von einer Rolle

9.5 Management von Sophos Update Manager

Folgende Maßnahmen zum Management von Sophos Update Manager werden protokolliert:

- Updaten eines Update Managers
- Übernahme der Konfiguration für einen Update Manager
- Löschen von Alerts
- Löschen eines Update Managers
- Konfigurieren eines Update Managers

9.5.1 Aufzeichnung von Änderungen an der Konfiguration des Update Managers

Das Dialogfeld **Update Manager konfigurieren** enthält mehrere Registerkarten und Konfigurationsoptionen, bei denen es sich im Grunde um die Konfigurationsrichtlinien des Update Managers handelt. Beim Bearbeiten der Konfiguration des Update Managers werden zu folgenden Richtlinien Aktionen protokolliert:

- **Update Manager - subscription** – Legt die vom Update Manager auf dem neuesten Stand gehaltenen Abonnements fest.
- **Update Manager - upstream** – Legt die Update-Quelle des Update Managers fest.
- **Update Manager - downstream** – Legt die Freigaben fest, aus denen der Update Manager die Software herunterlädt.
- **Update Manager - schedule** – Legt fest, wie häufig der Update Manager nach Updates zu den Threat-Erkennungsdaten bzw. der Software sucht.
- **Update Manager - general** – Legt die Protokollierungsoptionen des Update Managers fest.
- **Software subscription** – Legt die Konfiguration eines Software-Abonnements fest, z.B. „Recommended“.

Mitunter ziehen Veränderungen an einer Update Manager-Richtlinie Änderungen an anderen Update Manager-Richtlinien nach sich (wie etwa Änderungen der Parameter-ID). In solchen Fällen finden Sie mehrere Einträge in der SophosSecurity-Datenbank zu einer Änderung. Wenn Sie beispielsweise einen Zeitplan auf der Registerkarte **Zeitplan** im Dialogfeld **Update Manager konfigurieren** erstellen und auf „OK“ klicken, werden die folgenden Einträge zur Überwachung erstellt:

Tabelle 3: Erstellen eines Zeitplans für einen Update Manager

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
22	Edit	Policy	Update Manager - schedule	New name	None		Success
21	Edit	Policy	Update Manager - upstream	New Policy	None		Success
20	Edit	Policy	Update Manager - subscription		None		Success

In diesem Fall führt nur die erste, zur Richtlinie **Update Manager - schedule** protokollierte Aktion zu einer Konfigurationsänderung. Bei den übrigen zum Ereignis protokollierten Richtlinienänderungen handelt es sich um interne Parameter-ID-Änderungen. Über die Ansicht **Reports.vAuditEventsForPolicyEditAndDuplicate** der SophosSecurity-Datenbank können Sie sich über die Änderungen informieren. Nähere Informationen hierzu finden Sie unter Erstellen eines Reports mit Richtlinienänderungen im XML-Format (Seite 21).

9.6 Systemereignisse

Die folgenden Systemereignisse werden überwacht:

- Aktivieren der Überwachung
- Deaktivieren der Überwachung

10 Datenfelder der Überwachung von Sophos

Die folgenden Datenbankansichten oder Datenquellen stehen für die Überwachung von Sophos zur Verfügung:

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

Die verfügbaren Datenfelder aller Datenquellen werden unten aufgeführt. Zeit- und Datumsangaben liegen im UTC-Format vor: „JJJJ-MM-TT hh:mm:ss“ (24 Stunden). Die Felder, die beiden Ansichten angehören, werden fett hervorgehoben.

Reports.vAuditEventsAll

Die Datenbankansicht **Reports.vAuditEventsAll** umfasst eine vollständige Liste der Überwachungsereignisse sowie den Großteil der Überwachungsinformationen.

Datenfeld	Datentyp	Beschreibung
EventId	integer	Eine einmalige numerische Kennung des Ereignisses
Timestamp	datetime	Datum und Uhrzeit der Protokollierung des Ereignisses.
Action	nvarchar(128)	Die im Ereignis protokollierte Aktion, wie etwa „Erstellen“, „Bearbeiten“, „Umbenennen“, „Zuweisen“, „Löschen“.
TargetType	nvarchar(128)	Der/die von der Maßnahme geänderte Objekttyp/Konfigurationseinstellung, z.B. Gruppe, Computer, Richtlinie, Rolle.
TargetSubType	nvarchar(128)	Der Subtyp des von der Aktion betroffenen Objekts bzw. der Einstellung (sofern zutreffend). Beispielsweise der Name der modifizierten Richtlinie, wie etwa Antivirus und HIPS oder Data Control.
TargetName	nvarchar(4000)	Der Name des/der von der Aktion geänderten Objekts/Einstellung, z.B. der benutzerdefinierte Name der Richtlinie oder Gruppe.
ParameterType	nvarchar(128)	Der Typ der neuen Einstellung oder des neuen Objekts, der dem Ziel zugewiesen wurde. Beispiel: Maßnahme=„Rename“ und TargetType=„Policy“,

Datenfeld	Datentyp	Beschreibung
		ParameterType=„New name“. Maßnahme=„Assign“ und TargetType=„Computer“, ParameterType=„Group“.
ParameterValue	nvarchar(4000)	Der Wert der neuen Einstellung/des neuen Objekts, z.B. der neue benutzerdefinierte Name der Richtlinie oder die neue Gruppe, der der Computer zugewiesen wurde.
Result	nvarchar(128)	Das Ergebnis der Aktion; der Wert kann „Success“ oder „Failure“ lauten.
UserName	nvarchar(256)	Der Name des Benutzers, der die Aktion durchgeführt hat.
HostName	nvarchar(256)	Der Name des Computers, auf dem der Benutzer die Aktion durchgeführt hat.
HostIPAddress	nvarchar(48)	Die IP-Adresse des Computers, auf dem der Benutzer die Aktion durchgeführt hat. Wenn Netzwerkverbindungen zwischen dem Server und Enterprise Console per IPv6 hergestellt werden, werden IPv6-Adressen protokolliert. Andernfalls werden IPv4-Adressen protokolliert.
ActionId	integer	Eine einmalige numerische Kennung der Aktion
TargetTypeId	integer	Eine einmalige numerische Kennung des Zieltyps
TargetSubTypeId	integer	Eine einmalige numerische Kennung des Zielsubtyps.
ParameterTypeId	integer	Eine einmalige numerische Kennung des Parametertyps.
SubEstateId	integer	Eine einmalige numerische Kennung der Teilverwaltungseinheit des Benutzers.
ResultId	integer	Ein einmalige Kennung des Ergebnisses: 1 (Erfolg) oder 0 (Kein Erfolg).
UserSid	nvarchar(128)	Die Sicherheitskennung des Benutzers

Reports.vAuditEventsForPolicyEditAndDuplicate

Die Datenbankansicht **Reports.vAuditEventsForPolicyEditAndDuplicate** bietet Informationen zu Richtlinienänderungen.

Datenfeld	Datentyp	Beschreibung
EventId	integer	Eine einmalige numerische Kennung des Ereignisses
Timestamp	datetime	Datum und Uhrzeit der Protokollierung des Ereignisses.
Action	nvarchar(128)	Die im Ereignis protokollierte Aktion.
Result	nvarchar(128)	Das Ergebnis der Aktion; der Wert kann „Success“ oder „Failure“ lauten.
PolicyType	nvarchar(128)	Die Art der von der Aktion geänderten Richtlinie, z.B. Antivirus und HIPS oder Web Control.
PolicyName	nvarchar(4000)	Der benutzerdefinierte Name der Richtlinie.
PolicyContent	XML	Der Ausschnitt der Richtlinienkonfigurationsänderungen im XML-Format.
UserName	nvarchar(256)	Der Name des Benutzers, der die Aktion durchgeführt hat.

11 Fehlersuche

Wenn Fehler mit der Überwachung von Sophos auftreten, wird im Ereignisprotokoll der Windows-Anwendung ein Ereignis zur Quelle „Sophos Auditing“ protokolliert. Dies ist in der Regel der Fall, wenn Datenbankverbindungsprobleme auftreten.

12 Anhang: Numerische Kennungen der Datenfeldwerte

Aus den folgenden Tabellen können Sie die numerischen Kennungen einiger Datenfeldwerte der Sophos Überwachung entnehmen.

Wenn Sie die exportierten Überwachungsdaten mit einer externen Logik kombinieren möchten, sind numerische Kennungen Zeichenketten vorzuziehen. So können Sie mögliche Kompatibilitätsprobleme vermeiden, wenn sich Zeichenfolgen in späteren Versionen von Enterprise Console ändern.

Datenfeld	Datenfeldwert	Numerische Kennung
Action	Unknown	0
	Create	1
	Delete	2
	Duplicate	3
	Move	4
	Rename	5
	Add to	6
	Remove from	7
	Edit	8
	Log on	9
	Update	10
	Acknowledge	11
	Reset	12
	Assign	13
	Protect	14
	Scan	15
	Clean up	16

Datenfeld	Datenfeldwert	Numerische Kennung
	Comply	17
TargetType	Unknown	0
	Group	1
	Role	2
	Policy	3
	Computer	4
	Sub-estate	5
	AD synchronization point	6
	Report	7
	Update manager	8
	Configuration	9
TargetSubType for TargetType=Policy	Legacy updating	1
	Anti-virus and HIPS	2
	Firewall	4
	Application Control	7
	NAC	8
	Update Manager - upstream	9
	Update Manager - downstream	10
	Update Manager - general	11
	Update Manager - subscription	12
	Update Manager - schedule	13
	Data Control	15
	Device control	16
	Software subscription	17
	Updating	18

Datenfeld	Datenfeldwert	Numerische Kennung
	Tamper protection	19
	Web Control	22
	Exploit-Abwehr	30
TargetSubType for TargetType=Configuration	Unknown	0
	Dashboard	1
	Email alerts	2
	Purge	3
	Auditing	4
ParameterType	None	0
	New name	1
	New location	2
	Group	3
	User/Group	4
	Right	5
	Computer	6
	Alert	7
	Error	8
	Software update alert	9
	Configuration value	10
Result	Pending	0
	Success	1
	Failure	2

13 Technischer Support

Technischen Support zu Sophos Produkten finden Sie hier:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Besuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation herunter von www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

14 Rechtlicher Hinweis