SOPHOS

Security made simple.

Sophos Reporting Interface
Benutzeranleitung

Produktversion: 5.2
Stand: Januar 2013

Inhalt

1 Einleitung

Die Anleitung bietet Details zum Sophos Reporting Interface, mit dem Sie mit Hilfe von Software zur Erstellung von Reports von anderen Anbietern Reports zu Threats und Ereignisdaten in Sophos Enterprise Console erstellen. Die Anleitung richtet sich an System- und Datenbankadministratoren.

Es wird davon ausgegangen, dass Sie im Umgang mit Sophos Enterprise Console (SEC) 5.2 oder höher vertraut sind und die Software im Einsatz haben.

Hinweis: Wenn Sie Daten in Protokollüberwachungsanwendungen anderer Anbieter, wie etwa Splunk, exportieren möchten, können Sie hierzu den Sophos Reporting Log Writer verwenden. Weitere Informationen finden Sie in der *Benutzeranleitung zum Reporting Log Writer*.

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

2 Was ist das Sophos Reporting Interface?

Mit dem Sophos Reporting Interface lassen sich detaillierte, benutzerdefinierte Reports zu mit Sophos Enterprise Console verwalteten Endpoints erstellen.

Mit dem Sophos Reporting Interface kann mittels Anwendungen anderer Anbieter, wie etwa Crystal Reports und SQL Reporting Services, auf von Enterprise Console auf dem SQL-Server gespeicherte Daten zugegriffen werden. Die erforderlichen Datenbankobjekte werden im Zuge der Datenbankinstallation von Enterprise Console installiert.

3 Nutzung des Sophos Reporting Interface

Wichtig: Mit dem Sophos Reporting Interface können Daten von Enterprise Console in Anwendungen anderer Anbieter verfügbar gemacht werden. Unter Umständen enthalten die abgerufenen Daten vertrauliche Informationen zu Ihren Benutzern und Computern. Wenn Sie das Sophos Reporting Interface installieren, übernehmen Sie die Verantwortung über die Sicherheit der erfassten Daten und müssen sicherstellen, dass nur berechtigte Benutzer darauf zugreifen können.

Wir empfehlen nicht nur, den Zugang auf die vom Reporting Interface abgerufenen Daten einzuschränken, sondern zudem Verbindungen zwischen Clients und der Datenbank von Enterprise Console zu verschlüsseln. Nähere Informationen entnehmen Sie bitte der Dokumentation zu SQL Server:

- Aktivieren von verschlüsselten Verbindungen zum Datenbankmodul (SQL Server-Konfigurations-Manager), SQL Server 2012
- Verschlüsselung von Verbindungen zu SQL Server 2008 R2
- Anweisungen zur Aktivierung von SSL-Verschlüsselung für eine SQL Server-Instanz mit Microsoft Management Console, SQL Server 2005

Hinweis:

- In manchen Systemumgebungen wirken sich zusätzliche Anfragen an die Enterprise Console-Datenbank beim Zugriff auf das Reporting Interface negativ auf die Leistung anderer Datenbankenvorgänge aus. Bei der Übertragung großer Datenvolumen vom Reporting Interface können merkliche Leistungseinbußen von Enterprise Console auftreten.
- Wenn Sie die vom Reporting Interface abgerufenen Daten 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.

Sie können das Reporting Interface mit Anwendungen anderer Anbieter, wie etwa Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services oder Crystal Reports verwenden.

Ein Beispiel zum Zugriff auf das Reporting Interface mit Crystal Reports entnehmen Sie bitte dem Abschnitt Anhang: Konfigurieren von Crystal Reports mit dem Reporting Interface (Seite 14).

In unserem Diskussionsforum SophosTalk können Sie Informationen zur Nutzung des Sophos Reporting Interface austauschen (in englischer Sprache).

4 Abrufbare Informationen

Sophos Enterprise Console protokolliert Folgendes:

- Computer
- Pakete
- Gruppen
- Ereignisse
- Threats

4.1 Computer

Bei Computern handelt es sich um die einzelnen, von Enterprise Console überwachten Endpoints, die durch eine eindeutige *ComputerID* identifiziert werden. Mit Hilfe der beiden folgenden Datenbankansichten können Sie auf Computerdaten zugreifen:

- **vComputerHostData** liefert Informationen zu allen von Enterprise Console überwachten Computern.
- **vPolicyComplianceData** führt die auf die Computer übertragenen Richtlinien sowie den Status der Richtlinienkonformität auf.

4.2 Gruppen

Bei Gruppen handelt es sich um in Enterprise Console erstellte logische Computergruppierungen, die anhand einer eindeutigen Kennung, der *GroupID*, identifiziert werden. Mit Hilfe der beiden folgenden Datenbankansichten können Sie auf Gruppendaten zugreifen:

- **vGroupPathAndNameData** – Auflistung von Gruppenpfaden.
- **vComputerGroupMapping** – Übersicht über die Gruppenzugehörigkeit von Computern.

4.3 Pakete

Bei Paketen handelt es sich um bestimmte Versionen von Sophos Anti-Virus, die anhand ihrer *PackageID* identifiziert werden. Mit Hilfe der beiden folgenden Datenbankansichten können Sie auf Paketdaten zugreifen:

- **vPackageData** werden die derzeit verfügbaren sowie frühere Versionen von Sophos Anti-Virus aufgeführt.
- Mit **vComputerPackageMapping** werden die jeweils auf den einzelnen Computern installierten Pakete aufgeführt.

4.4 Ereignisse

Bei Ereignissen handelt es sich um Meldungen zu Ereignissen auf Endpoints, die sich anhand ihrer *EventID* sowie ihrer *EventTypeID* identifizieren lassen.

Ereignisse werden je nach Typ in unterschiedliche Kategorien eingeteilt. **vEventsCommonData** bietet Basisinformationen zu sämtlichen Ereignissen und umfasst den Wert **EventTypeName**, der vorgibt, welche der folgenden Ansichten zusätzliche kategoriespezifische Informationen zu dem Ereignis beinhaltet.

- Application Control verwendet **vEventsApplicationControlData**
- Data Control verwendet **vEventsDataControlData**
- Device Control verwendet **vEventsDeviceControlData**
- Firewall verwendet **vEventsFirewallData**
- Manipulationsschutz verwendet **vEventsTamperProtectionData**
- Web Control verwendet **vEventsWebData**
- Threat Actions verwendet **vThreatEventData**

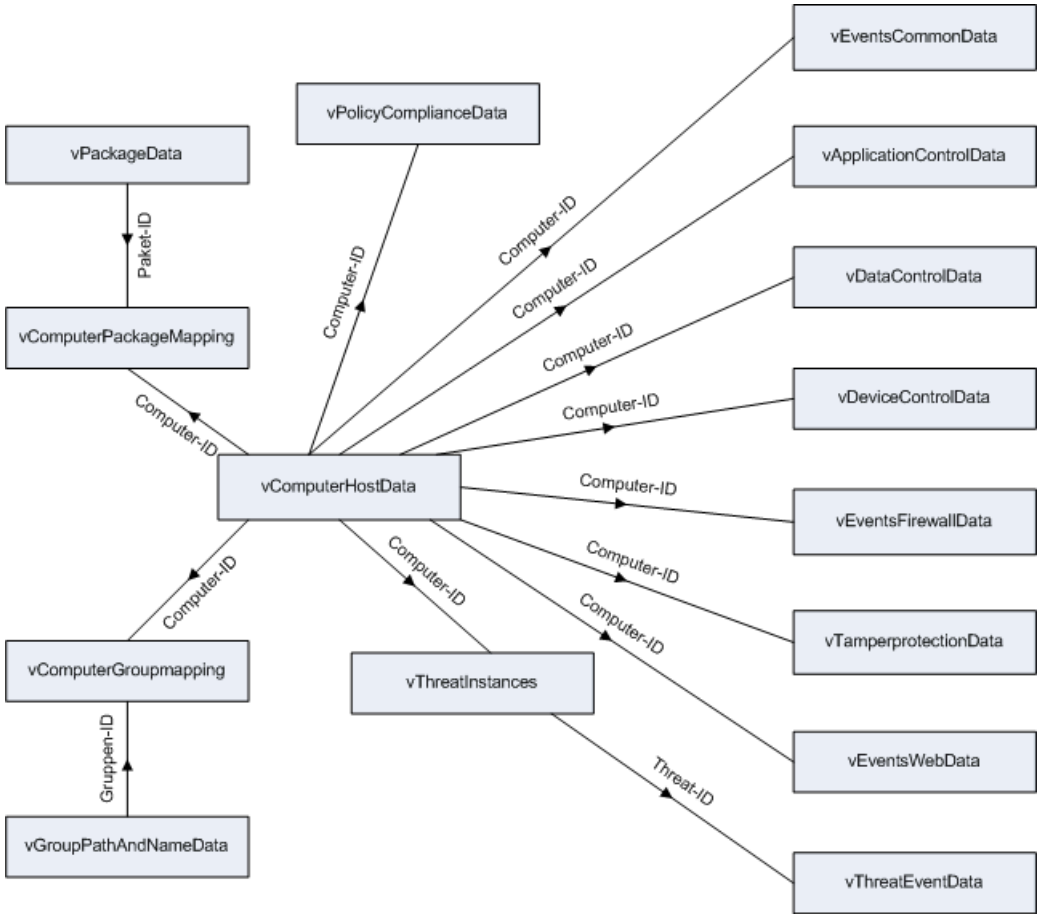
4.5 Threats

Bei Threats handelt es sich um Dateien oder Anwendungen, die in eine der folgenden Alertkategorien fallen: Viren/Spyware, verdächtiges Verhalten/verdächtige Dateien, Adware und PUA. Solche Threats werden durch ihre *ThreatID* eindeutig gekennzeichnet. Mit Hilfe der beiden folgenden Datenbankansichten können Sie auf Threatdaten zugreifen:

- Mit **vThreatInstance** werden die auf allen Computern erkannten Threats aufgelistet.
- Mit **vThreatEventData** lassen sich sämtliche als Reaktion auf im Netzwerk erkannte Threats ergriffene Maßnahmen auflisten.

4.6 Welche Datenquellen sind verbunden?

Bei der Zusammenführung von Daten aus mehreren Ansichten, müssen Zeilen aus allen Ansichten, die sich auf die gleiche Einheit beziehen, verbunden werden. Hierzu müssen die Zeilen, die sich auf die gleichen ID-Nummern beziehen, verbunden werden. Aus dem folgenden Diagramm geht hervor, welche Felder für das Verbinden der verfügbaren Ansichten zuständig sind.


vEventsCommonData
vPolicyComplianceData
vPackageData
vApplicationControlData
Paket-ID
Computer-ID
Computer-ID
vDataControlData
vComputerPackageMapping
Computer-ID
Computer-ID
Computer-ID
vDeviceControlData
Computer-ID
vComputerHostData
Computer-ID
vEventsFirewallData
Computer-ID
Computer-ID
Computer-ID
vTamperprotectionData
vComputerGroupmapping
vThreatInstances
Gruppen-ID
vEventsWebData
Threat-ID
vGroupPathAndNameData
vThreatEventData

5 Datenquellen des Reporting Interface

Die folgenden Datenquellen stehen für das Reporting Interface zur Verfügung.

Hinweis: Der Buchstabe neben einer Datenquelle stellt die Datenquelle der Matrix unten dar.

A. vComputerHostData

B. vThreatInstances

C. vEventsCommonData

D. vEventsApplicationControlData

E. vEventsDataControlData

F. vEventsDeviceControlData

G. vEventsFirewallData

H. vEventsTamperProtectionData

I. vEventsWebData

J. vThreatEventData

K. vComputerGroupMapping

L. vGroupPathAndNameData

M. vComputerPackageMapping

N. vPackageData

O. vPolicyComplianceData

Die folgende Matrix zeigt, welche Datenfelder in welchen Datenquellen vorhanden sind. Zeit- und Datumsangaben liegen im UTC-Format vor: „JJJJ-MM-TT hh:mm:ss“ (24 Stunden).

Datenfeld	Datentyp	Datenquelle														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
EventID	integer			•	•	•	•	•	•	•	•					
ThreatID	integer		•								•					
ComputerID	integer	•	•	•	•	•	•	•	•	•		•		•		•
Name	nvarchar	•		•	•	•	•	•	•	•						
EventTime	datetime			•	•	•	•	•	•	•	•					
EventTypeID	integer			•	•	•	•	•	•	•						
EventTypeName	nvarchar			•	•	•	•	•	•	•						

Datenfeld	Datentyp	Datenquelle														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ReportingName	nvarchar			•	•	•	•	•	•	•						
UserName	nvarchar			•	•	•	•	•	•	•	•					
ActionID	integer			•	•	•	•	•	•	•						
ActionName	nvarchar			•	•	•	•	•	•	•						
ScanTypeID	integer			•	•											
ScanTypeName	nvarchar			•	•											
SubTypeID	integer			•	•		•	•	•	•						
SubTypeName	nvarchar			•	•		•	•	•	•						
InsertedAt	datetime		•	•	•	•	•	•	•	•	•					
Domäne	nvarchar	•														
IPAddress	nvarchar	•														
Beschreibung	nvarchar	•														
LastMessageReceived Time	nvarchar	•														
DNSName	nvarchar	•														
OperatingSystemID	integer	•														
OperatingSystem Name	nvarchar	•														
ServicePack	nvarchar	•														
ThreatTypeID	integer		•													
ThreatTypeName	nvarchar		•													
ThreatSubTypeID	integer		•													
ThreatSubTypeName	nvarchar		•													
Priority	integer		•													
ThreatName	nvarchar		•													

Datenfeld	Datentyp	Datenquelle														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
FullFilePath	nvarchar		•													
FileVersion	nvarchar		•													
CheckSum	nvarchar		•													
FirstDetectedAt	datetime		•													
RuleName	nvarchar					•										
TrueFileType	nvarchar					•										
DestinationPath	nvarchar					•										
DestinationTypeID	integer					•										
DestinationType Name	nvarchar					•										
SourcePath	nvarchar					•										
FileName	nvarchar					•										
DestinationValue	nvarchar					•										
FileSize	long					•										
DeviceTypeID	integer						•									
DeviceTypeName	nvarchar						•									
Modell	nvarchar						•									
DeviceID	integer						•									
Role	nvarchar							•								
FileName	nvarchar							•								
FilePath	nvarchar							•								
FileVersion	nvarchar							•								
FileChecksum	nvarchar							•								
CommandLine	nvarchar							•								

Datenfeld	Datentyp	Datenquelle													
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Session	nvarchar							•								
Desktop	nvarchar							•								
Location	nvarchar							•								
ProtocolID	integer							•								
ProtocolText	nvarchar							•								
DirectionID	integer							•								
DirectionText	nvarchar							•								
LocalAddress	nvarchar							•								
RemoteAddress	nvarchar							•								
LocalPort	integer							•								
RemotePort	integer							•								
TargetTypeID	integer								•							
TargetTypeText	nvarchar								•							
Ziel	nvarchar								•							
RuleID	integer									•						
BlockedSite	nvarchar									•						
ReferringURL	nvarchar									•						
ReasonID	integer									•						
ReasonName	nvarchar									•						
CategoryID	integer									•						
CategoryName	nvarchar									•						
ActionTakenID	integer										•					
ActionTakenName	nvarchar										•					

Datenfeld	Datentyp	Datenquelle														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ScannerTypeID	integer										•					
ScannerTypeName	nvarchar										•					
StatusID	integer										•					
StatusName	nvarchar										•					
GroupID	integer											•	•			
PathAndName	nvarchar												•			
Depth	integer												•			
PackageID	integer													•	•	
Product	nvarchar														•	
SAVVersion	nvarchar														•	
EngineVersion	nvarchar														•	
VirusDataVersion	nvarchar														•	
ExpiryTime	datetime														•	
NotificationTime	datetime														•	
Expired	bit														•	
PolicyTypeID	integer															•
PolicyTypeName	nvarchar															•
ComplianceID	integer															•
ComplianceName	nvarchar															•

6 Anhang: Konfigurieren von Crystal Reports mit dem Reporting Interface

In dem Beispiel wird erklärt, wie Sie mit Crystal Reports 2008 oder höher auf das Reporting Interface zugreifen können.

Der Crystal Reports-Assistent verbindet automatisch Spalten mit identischen Namen in den einzelnen Ansichten, die in den Report aufgenommen wurden. Manche Verbindungen müssen jedoch entfernt werden, da Spalten mit ähnlichen Namen nicht zwangsweise die gleichen Werte mit Bezug auf ein einzelnes Protokollierungsereignis aufweisen.

So ist beispielsweise die Spalte **InsertedAt**, aus der hervorgeht, wann die jeweiligen Einträge hinzugefügt wurden, in allen Ansichten vorhanden. Die einem bestimmten Ereignis entsprechenden Einträge in allen Ansichten können jedoch unterschiedliche Zeitwerte im Bereich **InsertedAt** aufweisen. Wenn der Crystal Reports-Assistent die Spalten automatisch verbindet, müssen die Verbindungen entfernt werden, um die Vollständigkeit der Daten zu gewährleisten. Nähere Informationen zu den verbundenen Datenquellen entnehmen Sie bitte dem Abschnitt Welche Datenquellen sind verbunden? (Seite 7).

So erstellen Sie eine Verbindung zwischen dem Reporting Interface und Crystal Reports her:

1. Öffnen Sie Crystal Reports und erstellen Sie eine neue Verbindung über „**OLE DB (ADO)**“. Wählen Sie „**Microsoft OLE DB Provider for SQL Server**“.
2. Machen Sie die erforderlichen Angaben zur Verbindung und beenden Sie den Assistenten.

   Das Sophos Reporting Interface wird jetzt als Datenquelle aufgeführt. Nähere Informationen zur Report-Erstellung entnehmen Sie bitte der Dokumentation zu Crystal Reports.

Eine Liste der verfügbaren Datenquellen des Reporting Interface finden Sie unter Datenquellen des Reporting Interface (Seite 9).

Nähere Informationen sowie Beispiele zum Zugriff auf die Daten des Sophos Reporting Interface entnehmen Sie bitte dem Support-Artikel 112873 http://www.sophos.com/de-de/support/knowledgebase/112873.aspx.

7 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Besuchen Sie die Sophos Community unter community.sophos.de/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Begleitmaterial zu den Produkten finden Sie hier: 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.

8 Rechtlicher Hinweis