SOPHOS

Security made simple.

Sophos Reporting Interface
guida per utenti

Versione prodotto: 5.2
Data documento: gennaio 2013

Sommario

1 Informazioni sulla guida

Questa guida descrive Sophos Reporting Interface che consente di utilizzare software prodotti da terzi per generare report sui dati relative a minacce ed eventi in Sophos Enterprise Console. È stata scritta per amministratori di sistema e di database.

Si presuppone che si conosca o si abbia già utilizzato Sophos Enterprise Console (SEC) versione 5.2.

Nota: Se si desidera esportare dati in applicazioni per il monitoraggio dei log prodotte da terzi, quali Splunk, sarà possibile farlo tramite Sophos Reporting Log Writer. Per ulteriori informazioni, consultare il *manuale utente di Sophos Reporting Log Writer* .

La documentazione di Sophos è pubblicata alla pagina web http://www.sophos.com/it-it/support/documentation.aspx.

2 Sophos Reporting Interface

Sophos Reporting Interface consente di generare report dettagliati e personalizzati sui computer endpoint gestiti da Sophos Enterprise Console.

Sophos Reporting Interface consente l'utilizzo di applicazioni prodotte da terzi, quali Crystal Report e SQL Reporting Service, per accedere ai dati nel server SQL archiviati da Enterprise Console. Gli oggetti del database richiesti vengono installati durante la procedura di installazione del database di Enterprise Console.

3 Utilizzo di Sophos Reporting Interface

Importante: Sophos Reporting Interface mette a disposizione di applicazioni prodotte da terzi i dati di Enterprise Console. Tali dati potrebbero includere informazioni di tipo confidenziale relative a utenti e computer. Quando si utilizza Sophos Reporting Interface ci si assume la responsabilità della sicurezza dei dati resi accessibili; ciò significa accertarsi che solo utenti autorizzati possano accedere a tali dati.

Oltre a limitare l'accesso ai dati recuperati da Reporting Interface, si consiglia caldamente la cifratura delle connessioni fra i client e database di Enterprise Console. Per ulteriori informazioni, consultare la documentazione relativa a SQL Serve.

- Abilitazione di connessioni cifrate al Motore di database (Gestione configurazione SQL Server), SQL Server 2012
- Connessioni cifrate a SQL Server 2008 R2
- Come abilitare la cifratura SSL per un'istanza di SQL Server utilizzando Microsoft Management Console, SQL Server 2005

Nota:

- In alcuni ambienti di sistema, le query aggiuntive fatte al database di Enterprise Console quando si accede a Reporting Interface potrebbero influenzare le prestazioni di altre operazioni del database. Durante il trasferimento di grandi quantità di dati da Reporting Interface, le prestazioni di Enterprise possono essere notevolmente rallentate.
- Si consiglia l'utilizzo di ID numeriche piuttosto che valori stringa, se si desidera attribuire un ordine logico ai dati rilevati da Reporting Interface. Ciò può evitare problemi di compatibilità nel caso valori stringa vengano modificati nei rilasci futuri di Enterprise Console.

Utilizzare Reporting Interface con applicazioni prodotte da terzi quali Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services o Crystal Reports.

Per informazioni su come utilizzare Crystal Reports per accedere a Reporting Interface, leggere l'Appendice: Configurazione di Crystal Reports tramite Reporting Interface a pagina 14.

Per informazioni condivise su come utilizzare i propri tool di reportistica, leggere la thread realtiva Sophos Reporting Interface sul forum SophosTalk.

4 Informazioni a cui è concesso l'accesso

Sophos Enterprise Console registra informazioni relative a:

- Computer
- Pacchetti
- Gruppi
- Eventi
- Minacce

4.1 Computer

I computer sono ai singoli endpoint attualmente monitorati da Enterprise Console e vengono identificati in modo univoco dai relativi *ComputerID*. È possibile accedere alle informazioni del computer utilizzando le seguenti viste del database:

- **vComputerHostData** fornisce informazioni relative ai computer monitorati da Enterprise Console.
- **vPolicyComplianceData** elenca i criteri applicati a ciascun computer, e dà indicazioni sullo stato di conformità dei criteri.

4.2 Gruppi

I gruppi rappresentano una modalità logica di organizzazione dei computer, vengono creati all'interno di Enterprise Console e identificati in modo univoco dalla relativa *GroupID*. È possibile accedere alle informazioni relative a un gruppo utilizzando le seguenti viste del database:

- **vGroupPathAndNameData** fornisce un elenco di percorsi di gruppo.
- **vComputerGroupMapping** indica quali computer appartengono ai percorsi di gruppo.

4.3 Pacchetti

I pacchetti sono versioni particolari di Sophos Anti-Virus, presenti nella rete e identificati da *PackageID* unico. È possibile accedere alle informazioni relative a un pacchetto utilizzando le seguenti viste del database:

- **vPackageData** elenca le versioni di Sophos Anti-Virus che sono al momento e sono state in passato disponibili.
- **vComputerPackageMapping** indica in quale computer è installato ciascun pacchetto.

4.4 Eventi

Gli eventi rappresentano notifiche di eventi verificatisi negli endpoint e identificati in gruppi dai relativi *EventID* e *EventTypeID*.

Gli eventi vengono classificati in diverse categorie in base al tipo. **vEventsCommonData** fornisce informazioni di base su tutti gli eventi verificatisi, incluso **EventTypeName**, al fine di evidenziare quali delle seguenti viste contengano informazioni inerenti la categoria dell'evento:

- Application Control tramite **vEventsApplicationControlData**
- Data Control tramite **vEventsDataControlData**
- Device Control tramite **vEventsDeviceControlData**
- Firewall tramite **vEventsFirewallData**
- Tamper Protection tramite **vEventsTamperProtectionData**
- Web Control tramite **vEventsWebData**
- Azioni contro le minacce tramite **vThreatEventData**

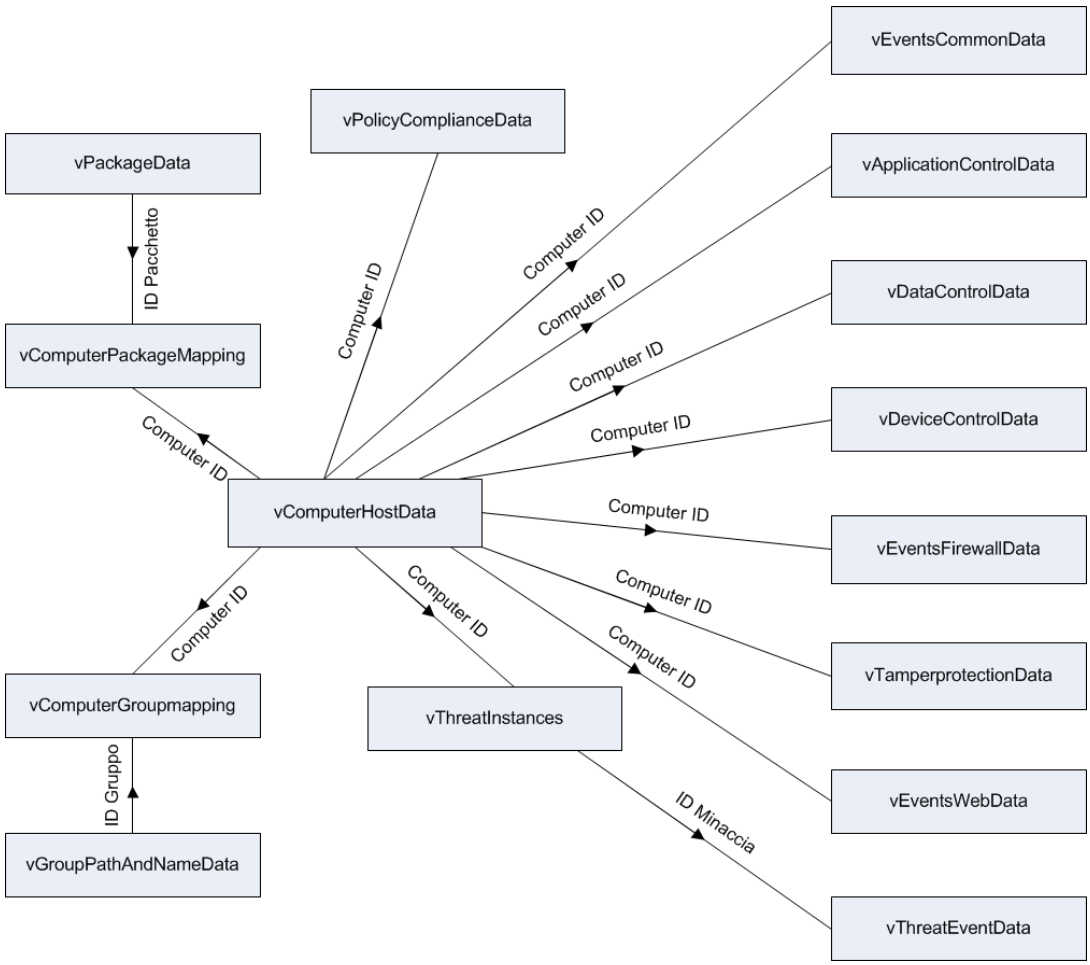
4.5 Minacce

Si identificano come minacce file o applicazioni che appartengono a una delle categorie di allarme (Virus/spyware, Comportamento/file sospetti, Adware e PUA). Vengono identificate da una personale*ThreatID*. È possibile accedere alle informazioni relative a una minaccia utilizzando le seguenti viste del database:

- **vThreatInstances** elenca le minacce rilevate in ciascun computer.
- **vThreatEventData** fornisce un elenco di azioni svolte per fronteggiare le minacce rilevate nella rete.

4.6 Fonti dati di Reporting Interface

Quando si gestiscono i dati da più viste, sarà necessario accorpare le righe di tutte le viste che si riferiscono alla medesima voce. Questa operazione può essere eseguita unendo le righe che si riferiscono agli stessi numeri di ID entità. Il seguente diagramma mostra quali campi utilizzare per unire tutte le viste disponibili.


vEventsCommonData
vPolicyComplianceData
vPackageData
vApplicationControlData
ID Pacchetto
Computer ID
Computer ID
vDataControlData
vComputerPackageMapping
Computer ID
Computer ID
vDeviceControlData
Computer ID
vComputerHostData
Computer ID
vEventsFirewallData
Computer ID
Computer ID
Computer ID
Computer ID
vTamperprotectionData
vComputerGroupmapping
vThreatInstances
ID Gruppo
vEventsWebData
ID Minaccia
vGroupPathAndNameData
vThreatEventData

5 Fonti dati di Reporting Interface

Le seguenti fonti dei dati sono disponibili per Reporting Interface.

Nota: La lettera di fianco alla fonte dei dati viene utilizzata per rappresentare la fonte dei dati nella matrice qui sotto.

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

La seguente matrice mostra quali campi dati siano disponibili in determinate fonti dei dati. Tutte le colonne della data e ora esprimono valori in Tempo universale coordinato (UTC), nel formato "anno-mese-giorno hh:min:ss" (24 ore).

Campo dati	Tipo di dati	Fonte dati														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
EventID	integer			•	•	•	•	•	•	•	•					
ThreatID	integer		•								•					
ComputerID	integer	•	•	•	•	•	•	•	•	•		•		•		•
Nome	nvarchar	•		•	•	•	•	•	•	•						
EventTime	datetime			•	•	•	•	•	•	•	•					
EventTypeID	integer			•	•	•	•	•	•	•						

Campo dati	Tipo di dati	Fonte dati														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
EventTypeName	nvarchar			•	•	•	•	•	•	•						
ReportingName	nvarchar			•	•	•	•	•	•	•						
UserName	nvarchar			•	•	•	•	•	•	•	•					
ActionID	integer			•	•	•	•	•	•	•						
ActionName	nvarchar			•	•	•	•	•	•	•						
ScanTypeID	integer			•	•											
ScanTypeName	nvarchar			•	•											
SubTypeID	integer			•	•		•	•	•	•						
SubTypeName	nvarchar			•	•		•	•	•	•						
InsertedAt	datetime		•	•	•	•	•	•	•	•	•					
Dominio	nvarchar	•														
IPAddress	nvarchar	•														
Descrizione	nvarchar	•														
LastMessageReceived Time	nvarchar	•														
DNSName	nvarchar	•														
OperatingSystemID	integer	•														
OperatingSystem Name	nvarchar	•														
ServicePack	nvarchar	•														
ThreatTypeID	integer		•													
ThreatTypeName	nvarchar		•													
ThreatSubTypeID	integer		•													
ThreatSubTypeName	nvarchar		•													
Priority	integer		•													

Campo dati	Tipo di dati	Fonte dati														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ThreatName	nvarchar		•													
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						•									
Modello	nvarchar						•									
DeviceID	integer						•									
Role	nvarchar							•								
FileName	nvarchar							•								
FilePath	nvarchar							•								
FileVersion	nvarchar							•								
FileChecksum	nvarchar							•								

Campo dati	Tipo di dati	Fonte dati														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
CommandLine	nvarchar							•								
Session	nvarchar							•								
Desktop	nvarchar							•								
Percorso	nvarchar							•								
ProtocolID	integer							•								
ProtocolText	nvarchar							•								
DirectionID	integer							•								
DirectionText	nvarchar							•								
LocalAddress	nvarchar							•								
RemoteAddress	nvarchar							•								
LocalPort	integer							•								
RemotePort	integer							•								
TargetTypeID	integer								•							
TargetTypeText	nvarchar								•							
Obiettivo	nvarchar								•							
RuleID	integer									•						
BlockedSite	nvarchar									•						
ReferringURL	nvarchar									•						
ReasonID	integer									•						
ReasonName	nvarchar									•						
CategoryID	integer									•						
CategoryName	nvarchar									•						
ActionTakenID	integer										•					

Campo dati	Tipo di dati	Fonte dati														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ActionTakenName	nvarchar										•					
ScannerTypeID	integer										•					
ScannerTypeName	nvarchar										•					
StatusID	integer										•					
StatusName	nvarchar										•					
GroupID	integer											•	•			
PathAndName	nvarchar												•			
Depth	integer												•			
PackageID	integer													•	•	
Prodotto	nvarchar														•	
SAVVersion	nvarchar														•	
EngineVersion	nvarchar														•	
VirusDataVersion	nvarchar														•	
ExpiryTime	datetime														•	
NotificationTime	datetime														•	
Expired	bit														•	
PolicyTypeID	integer															•
PolicyTypeName	nvarchar															•
ComplianceID	integer															•
ComplianceName	nvarchar															•

6 Appendice: Configurazione di Crystal Reports tramite Reporting Interface

Questo esempio mostra come utilizzare Crystal Reports versione 2008 o successive per accedere a Reporting Interface.

La procedura guidata di Crystal Report collegherà automaticamente le colonne che hanno lo stesso nome nelle diverse viste incluse nel report selezionato. Potrebbe essere comunque necessario cancellare alcuni di questi collegamenti, in quanto le colonne aventi lo stesso nome non necessariamente riportano dati identici per ogni evento di log.

Per esempio, la colonna **InsertedAt** è presente in ogni vista e indica quando ogni voce del database è stata inserita. Un determinato evento può però avere orari differenti nella colonna **InsertedAt** di ogni vista. Se la procedura guidata di Crystal Reports collega automaticamente queste colonne, sarà necessario cancellare questi collegamenti per evitare la perdita di dati. Per informazioni su quali fonti dei dati vengono collegate, consultare la sezione Fonti dati di Reporting Interface a pagina 7.

Per collegare Reporting Interface con Crystal Report:

1. Aprire Crystal Report e creare un nuovo collegamento tramite **OLE DB (ADO),** quindi scegliere **Microsoft OLE DB Provider for SQL Server**.
2. Inserire le informazioni di connessione e completare la procedura guidata.

   Sophos Reporting Interface verrà inclusa nell'elenco delle fonti dei dati disponibili. Per informazioni su come creare report personalizzati, consultare la documentazione relativa a Crystal Report.

Per consultare un elenco delle fonti dei dati per Reporting Interface, andare alla sezione Fonti dati di Reporting Interface a pagina 9.

Per ulteriori informazioni ed esempi sull'utilizzo di Crystal Report e su come accedere ai dati forniti dalla Sophos Reporting Interface, consultare l'articolo 112873 della knowledge base di Sophos http://www.sophos.com/it-it/support/knowledgebase/112873.aspx.

7 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in uno dei seguenti modi:

- Visitando Sophos Community su community.sophos.com/ e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto su www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket per il nostro supporto tecnico alla pagina https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

8 Note legali